QUALYS FREE SCAN

Vulnerability Scan

02 September 2014 at 20:41

URL : http://qikplay.bectero.com/

Summary: 105 vulnerabilities found

HIGH 0 MED 15 LOW 90 INFO 19

	Name	Vulnerability
	Login Form Is Not Submitted Via HTTPS	
	Directory Listing	
	Path-Based Vulnerability	
	Directory Listing	
	Directory Listing	
	Directory Listing	
	Cookie Does Not Contain The "HTTPOnly" Attribute	
	Cookie Does Not Contain The "secure" Attribute	
	Directory Listing	
	Path-Based Vulnerability	
	Directory Listing	
	Directory Listing	
	Directory Listing	
	Directory Listing	
	Sensitive form field has not disabled autocomplete	
	Directory Listing	
	Directory Listing	
	Directory Listing	

Directory Listing	
Directory Listing	
Cookie Does Not Contain The "secure" Attribute	
Directory Listing	
Directory Listing	
Path-Based Vulnerability	
Directory Listing	
Path-Based Vulnerability	
Directory Listing	
Directory Listing	
Directory Listing	
Directory Listing	
Directory Listing	
Cookie Does Not Contain The "HTTPOnly" Attribute	
Path-Based Vulnerability	
Directory Listing	
Directory Listing	
Directory Listing	
Path-Based Vulnerability	
Directory Listing	
Path-Based Vulnerability	
Cookie Does Not Contain The "secure" Attribute	
Path-Based Vulnerability	
Path-Based Vulnerability	
Directory Listing	

Directory Listing	
Path-Based Vulnerability	
Directory Listing	
Cookie Does Not Contain The "secure" Attribute	
Directory Listing	
Directory Listing	
Directory Listing	
Path-Based Vulnerability	
Cookie Does Not Contain The "HTTPOnly" Attribute	
Path-Based Vulnerability	
Path-Based Vulnerability	
Directory Listing	
Path-Based Vulnerability	
Directory Listing	
Directory Listing	
Directory Listing	
Directory Listing	
Directory Listing	
Directory Listing	
Directory Listing	
Directory Listing	
Directory Listing	
Directory Listing	
Directory Listing	
Path-Based Vulnerability	

Directory Listing	
Directory Listing	
Directory Listing	
Directory Listing	
Directory Listing	
Directory Listing	
Directory Listing	
Directory Listing	
Directory Listing	
Directory Listing	
Directory Listing	
Directory Listing	
Directory Listing	
Directory Listing	
Directory Listing	
Directory Listing	
Directory Listing	
Directory Listing	
Directory Listing	
PHP Session Fixation Vulnerability	
HTTP TRACE / TRACK Methods Enabled	
OpenSSH J-PAKE Session Key Retrieval Vulnerability	
Apache HTTP Server mod_proxy_ajp Denial of Service Vulnerability	
Apache HTTP Server Prior to 2.2.25 Multiple Vulnerabilities	
OpenSSH LoginGraceTime Denial of Service Vulnerability	
Apache HTTP Server Prior to 2.2.23 Multiple Vulnerabilities	

Apache HTTP Server Multiple Denial of Service Vulnerabilities	
Apache HTTP Server mod_cache and mod_dav Undisclosed DoS Vulnerability	
OpenSSH Commands Information Disclosure Vulnerability	
Apache HTTP Server APR "apr_fnmatch()" Denial of Service Vulnerability	
Apache Prior to 2.4.4 and 2.2.24 Multiple Vulnerabilities	
Apache Partial HTTP Request Denial of Service Vulnerability - Zero Day	
PHP Denial of Service Vulnerability	
Web Directories Listable Vulnerability	
Web Server HTTP Trace/Track Method Support Cross-Site Tracing Vulnerability	
Apache HTTP Server APR-util Multiple Denial of Service Vulnerabilities	
OpenSSH "child_set_env()" Security Bypass Issue	
Expose_php Set to On in php.ini	
Remote Access or Management Service Detected	INFO
Operating System Detected	INFO
Host Uptime Based on TCP TimeStamp Option	INFO
PHP Server Detected	INFO
SSH Banner	INFO
Web Server Version	INFO
Open TCP Services List	INFO
Firewall Detected	INFO
Default Web Page	INFO
IP ID Values Randomness	INFO
Degree of Randomness of TCP Initial Sequence Numbers	INFO
Traceroute	INFO

	SSH daemon information retrieving	INFO
	List of Web Directories	INFO
	Host Names Found	INFO
	DNS Host Name	INFO
	Internet Service Provider	INFO
	Host Scan Time	INFO
	HTTP method TRACE and/or TRACK Enabled	INFO

Detailed results

Type: **Web Application**

Login Form Is Not Submitted Via HTTPS

QID: 150053 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The login form's default action contains a link that is not submitted via HTTPS (HTTP over SSL).

Impact:
Sensitive data such as authentication credentials should be encrypted when transmitted over the network. Otherwise they are exposed to sniffing attacks.

Solution:
Change the login form's action to submit via HTTPS.

Results:
```
http://qikplay.bectero.com/index.php?app=member&fnc=login_send_post
-- Login Form Is Not Submitted Via HTTPS
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability.

Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/ -- comment: This directory was
discovered during the crawl phase. <title>Index of
/templates</title> </head> <body> <h1>Index of /templates</h1>
<table><tbody><tr><th><img src="/icons/blank.gif" alt="[ICO]">
</th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last
modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a
href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5">
<hr></th></tr> <tr><td valign="top"><img src="/icons/back.gif"
alt="[DIR]"></td><td><a href="/">Parent Directory</a>
</td><td> </td><td align="right"> - </td><td
```

Path-Based Vulnerability

QID: 150004 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

Impact:
The contents of this file or directory may disclose sensitive information.

Solution:
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

Results:

```
http://qikplay.bectero.com/files/news_event_editor/. -- comment:
This directory was discovered during the crawl phase.
les/news_event_editor</title> </head> <body> <h1>Index of /files
/news_event_editor</h1> <table><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/files/">Parent
Directory</a></td><td> </td><td align="right"> - <
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/js/ -- comment: This directory
```

```
was discovered during the crawl phase. ndex of /templates/js</title>
</head> <body> <h1>Index of /templates/js</h1> <table><tbody>
<tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a
href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last
modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a
href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5">
<hr></th></tr> <tr><td valign="top"><img src="/icons/back.gif"
alt="[DIR]"></td><td><a href="/templates/">Parent Directory</a>
</td><td> </td><td align="right"> - <
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/fonts/ -- comment: This
directory was discovered during the crawl phase. of /templates
/fonts</title> </head> <body> <h1>Index of /templates/fonts</h1>
<table><tbody><tr><th><img src="/icons/blank.gif" alt="[ICO]">
</th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last
modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a
href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5">
<hr></th></tr> <tr><td valign="top"><img src="/icons/back.gif"
alt="[DIR]"></td><td><a href="/templates/">Parent Directory</a>
</td><td> </td><td align="right"> -
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/plugins/layerslider/skins
/minimal/ -- comment: This directory was discovered during the crawl
phase. </head> <body> <h1>Index of /templates/plugins/layerslider
/skins/minimal</h1> <table><tbody><tr><th><img src="/icons
/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a>
```

```
</th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/layerslider/skins/">Parent Directory</a></td><td>
```

Cookie Does Not Contain The "HTTPOnly" Attribute

QID: 150123 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The cookie does not contain the "HTTPOnly" attribute.

Impact:
Cookies without the "HTTPOnly" attribute are permitted to be accessed via JavaScript. Cross-site scripting attacks can steal cookies which could lead to user impersonation or compromise of the application account.

Solution:
If the associated risk of a compromised account is high, apply the "HTTPOnly" attribute to cookies.

Results:

```
http://biz.becasiaticket.com/www/delivery/ajs.php?zoneid=160&
cb=15728858951&charset=UTF-8&loc=http://qikplay.bectero.com/ --
OAID=d36b69f6b1d44325587eeff0ebc4e051; expires=Wed Sep 2 02:22:52
2015; path=/; domain=biz.becasiaticket.com; max-age=31525225
```

Cookie Does Not Contain The "secure" Attribute

QID: 150122 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The cookie does not contain the "secure" attribute.

Impact:
Cookies with the "secure" attribute are only permitted to be sent via HTTPS. Session cookies sent via HTTP expose an unsuspecting user to sniffing attacks that could lead to user impersonation or compromise of the application account.

Solution:
If the associated risk of a compromised account is high, apply the "secure" attribute to cookies and force all sensitive requests to be sent via HTTPS.

Results:

```
http://qikplay.bectero.com/ -- PHPSESSID=8hs9hnni99hp5qp0t31ljoc2m6;
path=/; domain=qikplay.bectero.com
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:

The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/js/freeow/style/freeow/ --
comment: This directory was discovered during the crawl phase.
eow</title> </head> <body> <h1>Index of /templates/js/freeow/style
/freeow</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/js/freeow/style/">Parent Directory</a></td><td> </td><td a
```

Path-Based Vulnerability

QID: 150004 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

Impact:
The contents of this file or directory may disclose sensitive information.

Solution:
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

Results:
```
http://qikplay.bectero.com/index.php/app/artist/fnc/profile
/id/190.test2 -- HTTP/1.1 200 OK
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/royalslider/skins/ --
comment: This directory was discovered during the crawl phase.
```

```
/title> </head> <body> <h1>Index of /templates/plugins/royalslider
/skins</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/royalslider/">Parent Directory</a></td><td> </td><t
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/plugins/nivoslider/ -- comment:
This directory was discovered during the crawl phase.
ivoslider</title> </head> <body> <h1>Index of /templates/plugins
/nivoslider</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/">Parent Directory</a></td><td> </td><td align="
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/plugins/royalslider/skins
/default/ -- comment: This directory was discovered during the crawl
phase. </head> <body> <h1>Index of /templates/plugins/royalslider
/skins/default</h1> <table><tbody><tr><th><img src="/icons
/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a>
</th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
```

```
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/royalslider/skins/">Parent Directory</a></td><td>
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/plugins/layerslider/ --
comment: This directory was discovered during the crawl phase.
erslider</title> </head> <body> <h1>Index of /templates/plugins
/layerslider</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/">Parent Directory</a></td><td> </td><td align="
```

Sensitive form field has not disabled autocomplete

QID: 150112 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
An HTML form that collects sensitive information (such as a password field) does not prevent the browser from prompting the user to save the populated values for late reuse. Stored credentials should not be available to anyone but their owner.

Impact:
If the browser is used in a shared computing environment where more than one person may use the browser, then "autocomplete" values may be submitted by an unauthorized user. For example, if a browser saves the login name and password for a form, then anyone with access to the browser may submit the form and authenticate to the site without having to know the victim's password.

Solution:
Add the following attribute to the form or input element: autocomplete="off" This attribute prevents the browser from prompting the user to save the populated form values for later reuse.

Results:

```
http://qikplay.bectero.com/index.php?app=member&fnc=login_send_post
-- Form field does not set autocomplete="off".
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/bootstrap-select/js/ --
comment: This directory was discovered during the crawl phase. tle>
</head> <body> <h1>Index of /templates/plugins/bootstrap-select
/js</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/bootstrap-select/">Parent Directory</a></td><td> </t
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/royalslider/ --
comment: This directory was discovered during the crawl phase.
alslider</title> </head> <body> <h1>Index of /templates/plugins
/royalslider</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/">Parent Directory</a></td><td> </td><td align="
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/royalslider/css/ --
comment: This directory was discovered during the crawl phase.
</title> </head> <body> <h1>Index of /templates/plugins/royalslider
/css</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/royalslider/">Parent Directory</a></td><td> </td><td
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/layerslider/skins
/fullwidthdark/ -- comment: This directory was discovered during the
crawl phase. /head> <body> <h1>Index of /templates/plugins
/layerslider/skins/fullwidthdark</h1> <table><tbody><tr><th><img
src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;
O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a>
</th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;
O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]">
</td><td><a href="/templates/plugins/layerslider/skins/">Parent
Directory</a></td><td>&nb
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/js/freeow/style/ -- comment:
This directory was discovered during the crawl phase.
eow/style</title> </head> <body> <h1>Index of /templates/js/freeow
/style</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/js/freeow/">Parent Directory</a></td><td> </td><td align="r
```

Cookie Does Not Contain The "secure" Attribute

QID: 150122 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The cookie does not contain the "secure" attribute.

Impact:
Cookies with the "secure" attribute are only permitted to be sent via HTTPS. Session cookies sent via HTTP expose an unsuspecting user to sniffing attacks that could lead to user impersonation or compromise of the application account.

Solution:
If the associated risk of a compromised account is high, apply the "secure" attribute to cookies and force all sensitive requests to be sent via HTTPS.

Results:
```
https://apis.google.com/js/plusone.js --
NID=67=XFH_DLfr3XR0dU54tpGdgRZidw7JZ54EzLXYxXfSzrcE5RGb_dxXn1S9RZweM
_GGhdERsKREx3r_sF6TR-j7K3G1k4_ryeJWRekLB1K3GAOxh6AqFgxZUlIlM-QfwdhN;
expires=Wed Mar 4 01:22:51 2015; path=/; domain=.google.com;
max-age=15800424; httponly
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability.

Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/plugins/mask/ -- comment: This
directory was discovered during the crawl phase.
plugins/mask</title> </head> <body> <h1>Index of /templates/plugins
/mask</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/">Parent Directory</a></td><td> </td><td align="rig
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/js/ie/ -- comment: This
directory was discovered during the crawl phase. f /templates
/js/ie</title> </head> <body> <h1>Index of /templates/js/ie</h1>
<table><tbody><tr><th><img src="/icons/blank.gif" alt="[ICO]">
</th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last
modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a
href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5">
<hr></th></tr> <tr><td valign="top"><img src="/icons/back.gif"
alt="[DIR]"></td><td><a href="/templates/js/">Parent Directory</a>
</td><td> </td><td align="right">
```

Path-Based Vulnerability

QID: 150004 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

Impact:
The contents of this file or directory may disclose sensitive information.

Solution:
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

Results:

```
http://qikplay.bectero.com/templates/. -- comment: This directory
```

```
was discovered during the crawl phase. d> <title>Index of
/templates</title> </head> <body> <h1>Index of /templates</h1>
<table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a
href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last
modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a
href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5">
<hr></th></tr> <tr><td valign="top"><img src="/icons/back.gif"
alt="[DIR]"></td><td><a href="/">Parent Directory</a>
</td><td> </td><td align="right"> - </td><td>&n
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/images/loading/ -- comment:
This directory was discovered during the crawl phase.
ges/loading</title> </head> <body> <h1>Index of /templates/images
/loading</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/images/">Parent Directory</a></td><td> </td><td align="rig
```

Path-Based Vulnerability

QID: 150004 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

Impact:
The contents of this file or directory may disclose sensitive information.

Solution:
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

Results:

```
http://qikplay.bectero.com/files/person_thumb/. -- comment: This
directory was discovered during the crawl phase. of /files
/person_thumb</title> </head> <body> <h1>Index of /files
/person_thumb</h1> <table><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
```

```
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/files/">Parent
Directory</a></td><td> </td><td align="right"> - </td
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/plugins/layerslider/skins
/glass/ -- comment: This directory was discovered during the crawl
phase. > </head> <body> <h1>Index of /templates/plugins/layerslider
/skins/glass</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/layerslider/skins/">Parent Directory</a></td><td> <
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/plugins/layerslider/skins/ --
comment: This directory was discovered during the crawl phase.
/title> </head> <body> <h1>Index of /templates/plugins/layerslider
/skins</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/layerslider/">Parent Directory</a></td><td> </td><t
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/music/ -- comment: This
directory was discovered during the crawl phase. of /templates
/music</title> </head> <body> <h1>Index of /templates/music</h1>
<table><tbody><tr><th><img src="/icons/blank.gif" alt="[ICO]">
</th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last
modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a
href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5">
<hr></th></tr> <tr><td valign="top"><img src="/icons/back.gif"
alt="[DIR]"></td><td><a href="/templates/">Parent Directory</a>
</td><td> </td><td align="right"> -
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/layerslider/skins
/borderlessdark/ -- comment: This directory was discovered during
the crawl phase. /head> <body> <h1>Index of /templates/plugins
/layerslider/skins/borderlessdark</h1> <table><tbody><tr><th><img
src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;
O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a>
</th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;
O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]">
</td><td><a href="/templates/plugins/layerslider/skins/">Parent
Directory</a></td><td>&n
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/jPlayer/ -- comment:
This directory was discovered during the crawl phase.
ns/jPlayer</title> </head> <body> <h1>Index of /templates/plugins
/jPlayer</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/">Parent Directory</a></td><td> </td><td align="ri
```

Cookie Does Not Contain The "HTTPOnly" Attribute

QID: 150123 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The cookie does not contain the "HTTPOnly" attribute.

Impact:
Cookies without the "HTTPOnly" attribute are permitted to be accessed via JavaScript. Cross-site scripting attacks can steal cookies which could lead to user impersonation or compromise of the application account.

Solution:
If the associated risk of a compromised account is high, apply the "HTTPOnly" attribute to cookies.

Results:
```
http://www.youtube.com/embed/uCZJummFrtE -- GPS=1; expires=Tue Sep 2
02:58:10 2014; path=/; domain=.youtube.com
```

Path-Based Vulnerability

QID: 150004 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

Impact:
The contents of this file or directory may disclose sensitive information.

Solution:
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

Results:
```
http://qikplay.bectero.com/templates/music/. -- comment: This
directory was discovered during the crawl phase. dex of /templates
/music</title> </head> <body> <h1>Index of /templates/music</h1>
<table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a
href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last
modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a
href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5">
<hr></th></tr> <tr><td valign="top"><img src="/icons/back.gif"
alt="[DIR]"></td><td><a href="/templates/">Parent Directory</a>
</td><td> </td><td align="right"> - </t
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/bootstrap-select/ --
comment: This directory was discovered during the crawl phase.
select</title> </head> <body> <h1>Index of /templates/plugins
/bootstrap-select</h1> <table><tbody><tr><th><img src="/icons
/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a>
</th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/">Parent Directory</a></td><td> </td><td alig
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/soundmanager/ --
comment: This directory was discovered during the crawl phase.
dmanager</title> </head> <body> <h1>Index of /templates/plugins
/soundmanager</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/">Parent Directory</a></td><td> </td><td align=
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/layerslider/skins
/borderlesslight3d/ -- comment: This directory was discovered during
the crawl phase. ead> <body> <h1>Index of /templates/plugins
/layerslider/skins/borderlesslight3d</h1> <table><tbody><tr><th><img
src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;
O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a>
</th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;
O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]">
</td><td><a href="/templates/plugins/layerslider/skins/">Parent
Directory</a></td><td>&
```

Path-Based Vulnerability

QID: 150004 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

Impact:
The contents of this file or directory may disclose sensitive information.

Solution:
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

Results:
```
null -- HTTP/1.1 200 OK
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/layerslider/skins
/lightskin/ -- comment: This directory was discovered during the
crawl phase. </head> <body> <h1>Index of /templates/plugins
/layerslider/skins/lightskin</h1> <table><tbody><tr><th><img
src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;
O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a>
</th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;
O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]">
</td><td><a href="/templates/plugins/layerslider/skins/">Parent
Directory</a></td><td>
```

Path-Based Vulnerability

QID: 150004 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

Impact:
The contents of this file or directory may disclose sensitive information.

Solution:
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

Results:
```
http://qikplay.bectero.com/icons/. -- comment: This directory was
discovered during the crawl phase. <head> <title>Index of
/icons</title> </head> <body> <h1>Index of /icons</h1> <table>
<tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a
href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last
modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a
href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5">
<hr></th></tr> <tr><td valign="top"><img src="/icons/back.gif"
alt="[DIR]"></td><td><a href="/">Parent Directory</a>
</td><td> </td><td align="right">  - </td><td>&nbs
```

Cookie Does Not Contain The "secure" Attribute

QID: 150122 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The cookie does not contain the "secure" attribute.

Impact:
Cookies with the "secure" attribute are only permitted to be sent via HTTPS. Session cookies sent via HTTP expose an unsuspecting user to sniffing attacks that could lead to user impersonation or compromise of the application account.

Solution:
If the associated risk of a compromised account is high, apply the "secure" attribute to cookies and force all sensitive requests to be sent via HTTPS.

Results:
```
http://biz.becasiaticket.com/www/delivery/ajs.php?zoneid=160&
cb=15728858951&charset=UTF-8&loc=http://qikplay.bectero.com/ --
OAID=d36b69f6b1d44325587eeff0ebc4e051; expires=Wed Sep 2 02:22:52
2015; path=/; domain=biz.becasiaticket.com; max-age=31525225
```

Path-Based Vulnerability

QID: 150004 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

Impact:
The contents of this file or directory may disclose sensitive information.

Solution:
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

Results:
```
http://qikplay.bectero.com/files/member/. -- comment: This directory
was discovered during the crawl phase. tle>Index of /files
/member</title> </head> <body> <h1>Index of /files/member</h1>
<table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a
href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last
modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a
href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5">
<hr></th></tr> <tr><td valign="top"><img src="/icons/back.gif"
alt="[DIR]"></td><td><a href="/files/">Parent Directory</a>
</td><td> </td><td align="right">  - </td><t
```

Path-Based Vulnerability

QID: 150004 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

Impact:
The contents of this file or directory may disclose sensitive information.

Solution:
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

Results:
```
http://qikplay.bectero.com/templates/plugins/jPlayer/skin/qikplay
/images/. -- comment: This directory was discovered during the crawl
phase. > </head> <body> <h1>Index of /templates/plugins/jPlayer
/skin/qikplay/images</h1> <table><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/jPlayer/skin/qikplay/">Parent Directory</a></td><td> <
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/datepicker/ -- comment:
This directory was discovered during the crawl phase.
atepicker</title> </head> <body> <h1>Index of /templates/plugins
/datepicker</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/">Parent Directory</a></td><td> </td><td align="
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/bootstrap-select/css/
-- comment: This directory was discovered during the crawl phase.
le> </head> <body> <h1>Index of /templates/plugins/bootstrap-select
/css</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/bootstrap-select/">Parent Directory</a></td><td> </t
```

Path-Based Vulnerability

QID: 150004 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

Impact:
The contents of this file or directory may disclose sensitive information.

Solution:
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

Results:
```
http://qikplay.bectero.com/templates/images/. -- comment: This
directory was discovered during the crawl phase. x of /templates
/images</title> </head> <body> <h1>Index of /templates/images</h1>
<table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a
href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last
modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a
href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5">
<hr></th></tr> <tr><td valign="top"><img src="/icons/back.gif"
alt="[DIR]"></td><td><a href="/templates/">Parent Directory</a>
</td><td> </td><td align="right"> - </t
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/layerslider/skins
/defaultskin/ -- comment: This directory was discovered during the
crawl phase. </head> <body> <h1>Index of /templates/plugins
/layerslider/skins/defaultskin</h1> <table><tbody><tr><th><img
```

```
src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;
O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a>
</th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;
O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]">
</td><td><a href="/templates/plugins/layerslider/skins/">Parent
Directory</a></td><td>&nbs
```

Cookie Does Not Contain The "secure" Attribute

QID: 150122 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The cookie does not contain the "secure" attribute.

Impact:
Cookies with the "secure" attribute are only permitted to be sent via HTTPS. Session cookies sent via HTTP expose an unsuspecting user to sniffing attacks that could lead to user impersonation or compromise of the application account.

Solution:
If the associated risk of a compromised account is high, apply the "secure" attribute to cookies and force all sensitive requests to be sent via HTTPS.

Results:

```
http://www.youtube.com/embed/uCZJummFrtE -- VISITOR_INFO1_LIVE=AgAK-
kYaCoc; expires=Sun May 3 14:21:10 2015; path=/;
domain=.youtube.com; max-age=21027523
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/images/ -- comment: This
directory was discovered during the crawl phase. f /templates
/images</title> </head> <body> <h1>Index of /templates/images</h1>
<table><tbody><tr><th><img src="/icons/blank.gif" alt="[ICO]">
</th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last
modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a
href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5">
<hr></th></tr> <tr><td valign="top"><img src="/icons/back.gif"
alt="[DIR]"></td><td><a href="/templates/">Parent Directory</a>
</td><td> </td><td align="right"> -
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/nivoslider/themes/ --
comment: This directory was discovered during the crawl phase.
</title> </head> <body> <h1>Index of /templates/plugins/nivoslider
/themes</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/nivoslider/">Parent Directory</a></td><td> </td><t
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/royalslider/images/ --
comment: This directory was discovered during the crawl phase.
/title> </head> <body> <h1>Index of /templates/plugins/royalslider
/images</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/royalslider/">Parent Directory</a></td><td> </td><
```

Path-Based Vulnerability

QID: 150004 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

Impact:
The contents of this file or directory may disclose sensitive information.

Solution:
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

Results:
```
http://qikplay.bectero.com/files/product_thumb/. -- comment: This
directory was discovered during the crawl phase. of /files
/product_thumb</title> </head> <body> <h1>Index of /files
/product_thumb</h1> <table><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/files/">Parent
Directory</a></td><td> </td><td align="right"> - </t
```

Cookie Does Not Contain The "HTTPOnly" Attribute

QID: 150123 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The cookie does not contain the "HTTPOnly" attribute.

Impact:
Cookies without the "HTTPOnly" attribute are permitted to be accessed via JavaScript. Cross-site scripting attacks can steal cookies which could lead to user impersonation or compromise of the application account.

Solution:
If the associated risk of a compromised account is high, apply the "HTTPOnly" attribute to cookies.

Results:
```
http://qikplay.bectero.com/ -- PHPSESSID=8hs9hnni99hp5qp0t31ljoc2m6;
path=/; domain=qikplay.bectero.com
```

Path-Based Vulnerability

QID: 150004 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

Impact:
The contents of this file or directory may disclose sensitive information.

Solution:

Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

Results:

```
http://qikplay.bectero.com/templates/images/msgBox/. -- comment:
This directory was discovered during the crawl phase. s/images
/msgBox</title> </head> <body> <h1>Index of /templates/images
/msgBox</h1> <table><tr><th><img src="/icons/blank.gif" alt="[ICO]">
</th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last
modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a
href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5">
<hr></th></tr> <tr><td valign="top"><img src="/icons/back.gif"
alt="[DIR]"></td><td><a href="/templates/images/">Parent
Directory</a></td><td> </td><td align="right">
```

Path-Based Vulnerability

QID: 150004 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

Impact:
The contents of this file or directory may disclose sensitive information.

Solution:
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

Results:

```
http://qikplay.bectero.com/templates/plugins/. -- comment: This
directory was discovered during the crawl phase. of /templates
/plugins</title> </head> <body> <h1>Index of /templates/plugins</h1>
<table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a
href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last
modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a
href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5">
<hr></th></tr> <tr><td valign="top"><img src="/icons/back.gif"
alt="[DIR]"></td><td><a href="/templates/">Parent Directory</a>
</td><td> </td><td align="right"> - </
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/plugins/jPlayer
```

```
/skin/blue.monday/ -- comment: This directory was discovered during
the crawl phase. le> </head> <body> <h1>Index of /templates/plugins
/jPlayer/skin/blue.monday</h1> <table><tbody><tr><th><img
src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;
O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a>
</th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;
O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]">
</td><td><a href="/templates/plugins/jPlayer/skin/">Parent
Directory</a></td><td> </t
```

Path-Based Vulnerability

QID: 150004 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

Impact:
The contents of this file or directory may disclose sensitive information.

Solution:
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

Results:

```
http://qikplay.bectero.com/icons/small/. -- comment: This directory
was discovered during the crawl phase. title>Index of /icons
/small</title> </head> <body> <h1>Index of /icons/small</h1> <table>
<tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a
href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last
modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a
href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5">
<hr></th></tr> <tr><td valign="top"><img src="/icons/back.gif"
alt="[DIR]"></td><td><a href="/icons/">Parent Directory</a>
</td><td> </td><td align="right"> - </td><t
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/uploads/ -- comment: This
directory was discovered during the crawl phase. /templates
/uploads</title> </head> <body> <h1>Index of /templates/uploads</h1>
<table><tbody><tr><th><img src="/icons/blank.gif" alt="[ICO]">
</th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last
modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a
```

```
href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5">
<hr></th></tr> <tr><td valign="top"><img src="/icons/back.gif"
alt="[DIR]"></td><td><a href="/templates/">Parent Directory</a>
</td><td> </td><td align="right"> -
```

Directory Listing

QID: 150023
Category: Web Application
CVEID: -
CVSS Base: null
Port: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/plugins/ImageZoom/ -- comment:
This directory was discovered during the crawl phase.
ImageZoom</title> </head> <body> <h1>Index of /templates/plugins
/ImageZoom</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/">Parent Directory</a></td><td> </td><td align="r
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/prettyCheckboxes/ --
comment: This directory was discovered during the crawl phase.
kboxes</title> </head> <body> <h1>Index of /templates/plugins
/prettyCheckboxes</h1> <table><tbody><tr><th><img src="/icons
/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a>
</th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/">Parent Directory</a></td><td> </td><td alig
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/layerslider/skins
/noskin/ -- comment: This directory was discovered during the crawl
phase. > </head> <body> <h1>Index of /templates/plugins/layerslider
/skins/noskin</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/layerslider/skins/">Parent Directory</a></td><td>
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/datepicker/css/ --
comment: This directory was discovered during the crawl phase.
s</title> </head> <body> <h1>Index of /templates/plugins/datepicker
/css</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/datepicker/">Parent Directory</a></td><td> </td><td
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/layerslider/skins/v5/
-- comment: This directory was discovered during the crawl phase.
le> </head> <body> <h1>Index of /templates/plugins/layerslider/skins
/v5</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/layerslider/skins/">Parent Directory</a></td><td> </
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/jPlayer/skin/qikplay/
-- comment: This directory was discovered during the crawl phase.
itle> </head> <body> <h1>Index of /templates/plugins/jPlayer
/skin/qikplay</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/jPlayer/skin/">Parent Directory</a></td><td> </td>
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/layerslider/skins
/borderlessdark3d/ -- comment: This directory was discovered during
the crawl phase. head> <body> <h1>Index of /templates/plugins
/layerslider/skins/borderlessdark3d</h1> <table><tbody><tr><th><img
src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;
O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a>
</th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;
O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]">
</td><td><a href="/templates/plugins/layerslider/skins/">Parent
Directory</a></td><td>&
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/layerslider/js/ --
comment: This directory was discovered during the crawl phase.
s</title> </head> <body> <h1>Index of /templates/plugins/layerslider
/js</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/layerslider/">Parent Directory</a></td><td> </td><td
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/js/freeow/style/freeow/images/
-- comment: This directory was discovered during the crawl phase.
tle> </head> <body> <h1>Index of /templates/js/freeow/style/freeow
/images</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/js/freeow/style/freeow/">Parent Directory</a></td><td> </t
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:

The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/plugins/jPlayer/skin/qikplay
/images/ -- comment: This directory was discovered during the crawl
phase. </head> <body> <h1>Index of /templates/plugins/jPlayer
/skin/qikplay/images</h1> <table><tbody><tr><th><img src="/icons
/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a>
</th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/jPlayer/skin/qikplay/">Parent Directory</a></td><td>&nb
```

Path-Based Vulnerability

QID: 150004 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

Impact:
The contents of this file or directory may disclose sensitive information.

Solution:
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

Results:

```
http://qikplay.bectero.com/templates/uploads/. -- comment: This
directory was discovered during the crawl phase. of /templates
/uploads</title> </head> <body> <h1>Index of /templates/uploads</h1>
<table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a
href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last
modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a
href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5">
<hr></th></tr> <tr><td valign="top"><img src="/icons/back.gif"
alt="[DIR]"></td><td><a href="/templates/">Parent Directory</a>
</td><td> </td><td align="right"> - </
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/plugins/jPlayer
/skin/qikplay/css/ -- comment: This directory was discovered during
the crawl phase. </head> <body> <h1>Index of /templates/plugins
/jPlayer/skin/qikplay/css</h1> <table><tbody><tr><th><img
src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;
O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a>
</th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;
O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]">
</td><td><a href="/templates/plugins/jPlayer/skin/qikplay/">Parent
Directory</a></td><td>
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/plugins/royalslider/skins
/preloaders/ -- comment: This directory was discovered during the
crawl phase. </head> <body> <h1>Index of /templates/plugins
/royalslider/skins/preloaders</h1> <table><tbody><tr><th><img
src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;
O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a>
</th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;
O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]">
</td><td><a href="/templates/plugins/royalslider/skins/">Parent
Directory</a></td><td>&nbs
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/plugins/layerslider/skins
/fullwidth/ -- comment: This directory was discovered during the
```

```
crawl phase. </head> <body> <h1>Index of /templates/plugins
/layerslider/skins/fullwidth</h1> <table><tbody><tr><th><img
src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;
O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a>
</th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;
O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]">
</td><td><a href="/templates/plugins/layerslider/skins/">Parent
Directory</a></td><td>
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/plugins/layerslider/css/ --
comment: This directory was discovered during the crawl phase.
</title> </head> <body> <h1>Index of /templates/plugins/layerslider
/css</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/layerslider/">Parent Directory</a></td><td> </td><td
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/images/msgBox/ -- comment: This
directory was discovered during the crawl phase.
mages/msgBox</title> </head> <body> <h1>Index of /templates/images
/msgBox</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
```

```
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/images/">Parent Directory</a></td><td> </td><td align="rig
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/plugins/raty/ -- comment: This
directory was discovered during the crawl phase.
plugins/raty</title> </head> <body> <h1>Index of /templates/plugins
/raty</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/">Parent Directory</a></td><td> </td><td align="rig
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/js/freeow/ -- comment: This
directory was discovered during the crawl phase. plates/js
/freeow</title> </head> <body> <h1>Index of /templates
/js/freeow</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
```

```
/js/">Parent Directory</a></td><td> </td><td align="right">
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/plugins/royalslider/js/ --
comment: This directory was discovered during the crawl phase.
s</title> </head> <body> <h1>Index of /templates/plugins/royalslider
/js</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/royalslider/">Parent Directory</a></td><td> </td><td
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/icons/small/ -- comment: This directory
was discovered during the crawl phase. e>Index of /icons
/small</title> </head> <body> <h1>Index of /icons/small</h1> <table>
<tbody><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a
href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last
modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a
href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5">
<hr></th></tr> <tr><td valign="top"><img src="/icons/back.gif"
alt="[DIR]"></td><td><a href="/icons/">Parent Directory</a>
</td><td> </td><td align="right"> - </td
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/jPlayer/skin/ --
comment: This directory was discovered during the crawl phase.
skin</title> </head> <body> <h1>Index of /templates/plugins/jPlayer
/skin</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/jPlayer/">Parent Directory</a></td><td> </td><td al
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/layerslider/skins
/darkskin/ -- comment: This directory was discovered during the
crawl phase. </head> <body> <h1>Index of /templates/plugins
/layerslider/skins/darkskin</h1> <table><tbody><tr><th><img
src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;
O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a>
</th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;
O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]">
</td><td><a href="/templates/plugins/layerslider/skins/">Parent
Directory</a></td><td>
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/layerslider/skins
/borderlesslight/ -- comment: This directory was discovered during
the crawl phase. head> <body> <h1>Index of /templates/plugins
/layerslider/skins/borderlesslight</h1> <table><tbody><tr><th><img
src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;
O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a>
</th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;
O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]">
</td><td><a href="/templates/plugins/layerslider/skins/">Parent
Directory</a></td><td>&n
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/layerslider/skins
/carousel/ -- comment: This directory was discovered during the
crawl phase. </head> <body> <h1>Index of /templates/plugins
/layerslider/skins/carousel</h1> <table><tbody><tr><th><img
src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;
O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a>
</th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;
O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]">
</td><td><a href="/templates/plugins/layerslider/skins/">Parent
Directory</a></td><td>
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**

CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/js/freeow/style/freeow
/images/osx/ -- comment: This directory was discovered during the
crawl phase. </head> <body> <h1>Index of /templates/js/freeow/style
/freeow/images/osx</h1> <table><tbody><tr><th><img src="/icons
/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a>
</th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/js/freeow/style/freeow/images/">Parent Directory</a></td><td>&nbs
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:

```
http://qikplay.bectero.com/templates/plugins/ -- comment: This
directory was discovered during the crawl phase. /templates
/plugins</title> </head> <body> <h1>Index of /templates/plugins</h1>
<table><tbody><tr><th><img src="/icons/blank.gif" alt="[ICO]">
</th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last
modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a
href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5">
<hr></th></tr> <tr><td valign="top"><img src="/icons/back.gif"
alt="[DIR]"></td><td><a href="/templates/">Parent Directory</a>
</td><td> </td><td align="right"> -
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/jPlayer
/skin/circleplayer/ -- comment: This directory was discovered during
the crawl phase. le> </head> <body> <h1>Index of /templates/plugins
/jPlayer/skin/circleplayer</h1> <table><tbody><tr><th><img
src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;
O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a>
</th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;
O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]">
</td><td><a href="/templates/plugins/jPlayer/skin/">Parent
Directory</a></td><td> </
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/css/ -- comment: This directory
was discovered during the crawl phase. ex of /templates/css</title>
</head> <body> <h1>Index of /templates/css</h1> <table><tbody>
<tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a
href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last
modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a
href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5">
<hr></th></tr> <tr><td valign="top"><img src="/icons/back.gif"
alt="[DIR]"></td><td><a href="/templates/">Parent Directory</a>
</td><td> </td><td align="right"> - <
```

Directory Listing

QID: 150023 **CVSS Base: null**
Category: Web Application **Port: -**
CVEID: -

Threat:
The Web server presents a directory listing.

Impact:
All file names in this directory are exposed.

Solution:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

Results:
```
http://qikplay.bectero.com/templates/plugins/datepicker/js/ --
comment: This directory was discovered during the crawl phase.
js</title> </head> <body> <h1>Index of /templates/plugins/datepicker
/js</h1> <table><tbody><tr><th><img src="/icons/blank.gif"
alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;
O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr> <tr><td valign="top"><img
src="/icons/back.gif" alt="[DIR]"></td><td><a href="/templates
/plugins/datepicker/">Parent Directory</a></td><td> </td><td
```

Type: **Vulnerability**

PHP Session Fixation Vulnerability

QID: 12722
Category: CGI
CVEID: CVE-2011-4718
CVSS Base: null
Port: 80

Threat:
PHP is a general purpose scripting language that is suited for web development and can be embedded in HTML.
The detected PHP version is exposed to a session fixation vulnerability in the sessions subsystem. This issue allows remote attackers to hijack web sessions by specifying a session ID.
Affected Versions:
Versions prior to PHP 5.5.2

Impact:
Successful exploitation of this vulnerability allows remote attackers to hijack and gain unauthorized access to user session.

Solution:
Upgrade to PHP version 5.5.2 or above. For more details about PHP releases and patches please visit PHP Homepage . Additionally, customers may want to follow the following guidelines that would prevent such session fixation vulnerabilities:
- Implement the session.use_strict_mod php.ini directive which when enabled, discards uninitialized session IDs.
- Implement the session.safe_session_cookie directive that deletes possible malicious cookies, effectively preventing crafted session IDs.
- Implement the session.use_trans_sid directive that prevents PHP applications from exposing the session identifier in a URL.
- Implement the session.use_only_cookies php.ini directive that directs PHP to never use URLs with session identifiers.
However, customers are advised to test their applications after applying these guidelines as they may affect application behaviour in certain cases.

Results:
```
Date: Tue, 02 Sep 2014 09:23:51 GMT Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.4.30 Location: http://biz2.becasiaticket.com
/www/admin/index.php Content-Length: 0 Connection: close
Content-Type: text/html; charset=UTF-8
```

HTTP TRACE / TRACK Methods Enabled

QID: 12680 **CVSS Base: null**
Category: CGI **Port: 80**
CVEID: CVE-2004-2320, CVE-2010-0386, CVE-2003-1567

Threat:
The remote Web server supports the TRACE and/or TRACK HTTP methods, which makes it easier for remote attackers to steal cookies and authentication credentials or bypass the HttpOnly protection mechanism.
Track / Trace are required to be disabled to be PCI compliance.

Impact:
If this vulnerability is successfully exploited, attackers can potentially steal cookies and authentication credentials, or bypass the HttpOnly protection mechanism.

Solution:
Disable these methods in your web server's configuration file.

Results:
```
TRACE /QUALYS12680.html HTTP/1.1 Host:
ppp-111.223.39.140.revip.proen.co.th HTTP/1.1 200 OK Date: Tue, 02
Sep 2014 09:31:34 GMT Server: Apache/2.2.15 (CentOS) Connection:
close Transfer-Encoding: chunked Content-Type: message/http TRACE
/QUALYS12680.html HTTP/1.1 Host:
ppp-111.223.39.140.revip.proen.co.th Connection: Keep-Alive -CR-
```

OpenSSH J-PAKE Session Key Retrieval Vulnerability

QID: 42384 **CVSS Base: null**
Category: General remote services **Port: 0**
CVEID: CVE-2010-4478

Threat:
OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
OpenSSH, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol. This allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol.
Affected Software:
OpenSSH versions 5.6 and prior.

Impact:
Successful exploitation allows attacker to get access to the remote system.

Solution:
Upgrade to OpenSSH 5.7 or later, available from the OpenSSH Web site .

Results:
```
SSH-2.0-OpenSSH_5.3
```

Apache HTTP Server mod_proxy_ajp Denial of Service Vulnerability

QID: 12529 **CVSS Base: null**
Category: CGI **Port: 0**
CVEID: CVE-2011-3348

Threat:
A vulnerability exists in Apache HTTP Server due to an error within the processing of malformed HTTP requests in mod_proxy_ajp when being used in combination with mod_proxy_balancer.

Affected Versions:-
Apache versions 2.2.12, 2.2.13, 2.2.14, 2.2.15, 2.2.16, 2.2.17, 2.2.18, 2.2.19, and 2.2.20.

Impact:
The vulnerability can be exploited to put a backend server into an error state by sending specially crafted HTTP requests, resulting in a temporary DoS until the retry timeout expires.

Solution:
This issue has been resolved in Apache 2.2.21 and later. Refer to Apache 2.2 Release Notes for further information.

Results:
```
QID: 12529 detected on port 80 over TCP - Apache/2.2.15 (CentOS)
```

Apache HTTP Server Prior to 2.2.25 Multiple Vulnerabilities

QID: 87233 **CVSS Base: null**
Category: Web server **Port: 80**
CVEID: CVE-2013-1896, CVE-2013-1862

Threat:
Apache HTTP Server is an HTTP web server application.
Apache HTTP Server versons before to 2.2.25 are exposed to following vulnerabilities:
mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator (CVE-2013-1862).
mod_dav.c in the Apache HTTP Server versions before 2.2.25 do not properly determine whether DAV is enabled for a URI, which allows remote attackers to cause a denial of service (segmentation fault) via a MERGE request in which the URI is configured for handling by the mod_dav_svn module, but a certain href attribute in XML data refers to a non-DAV URI (CVE-2013-1896).

Impact:
Successfully exploiting these vulnerabilities might allow a remote attacker to execute code or cause denial of service.

Solution:
These vulnerabilities have been patched in Apache 2.2.25. Refer to Apache httpd 2.2.25 Changelog .

Results:
```
QID 87233 detected on port 80 - Apache/2.2.15 (CentOS)
```

OpenSSH LoginGraceTime Denial of Service Vulnerability

QID: 42413 **CVSS Base: null**
Category: General remote services **Port: 0**
CVEID: CVE-2010-5107

Threat:
OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
Default OpenSSH installations have an overly long LoginGraceTime and a lack of early connection release for MaxStartups settings. Remote unauthenticated attackers could bypass the LoginGraceTime and MaxStartups thresholds by intermittently transmitting a large number of new TCP connections to the targeted server. This could lead to connection slot exhaustion.
Affected Software:
OpenSSH 6.1 and prior.

Impact:
Successful exploitation could allow an unauthenticated remote attacker to cause the targeted server to stop responding to legitimate user queries, leading to a denial of service on the targeted server.

Solution:
Customers are advised to upgrade to OpenSSH 6.2 and apply the associated server configuration settings to remediate this vulnerability.

Results:
```
QID: 42413 detected on port 22 over TCP - SSH-2.0-OpenSSH_5.3
```

Apache HTTP Server Prior to 2.2.23 Multiple Vulnerabilities

QID: 87133 **CVSS Base: 6.9**
Category: Web server **Port: 0**
CVEID: CVE-2012-2687, CVE-2012-0883

Threat:
Apache HTTP Server is an HTTP web server application.
Apache server prior to version 2.2.23 is affected by multiple issues:
Insecure LD_LIBRARY_PATH handling
Cross-site scripting in mod_negotiation when untrusted uploads are supported Affected Versions:
Apache HTTP Server prior to version 2.2.23

Impact:
Successful exploitation may lead to execution of arbitrary code on the system within the context of the affected applications.

Solution:
These vulnerabilities have been patched in Apache 2.2.23. Refer to Apache httpd 2.2 Security Vulnerabilities .

Results:
```
QID 87133 detected on port 80 - Apache/2.2.15 (CentOS)
```

Apache HTTP Server Multiple Denial of Service Vulnerabilities

QID: 87242 **CVSS Base: null**
Category: Web server **Port: 80**
CVEID: CVE-2012-4557, CVE-2012-0021

Threat:
Apache HTTP Server is an HTTP web server application.
Apache HTTP Server versions before to 2.2.22 are exposed to following vulnerabilities:
- mod_proxy_ajp module is affected by remote denial of service vulnerability (CVE-2012-4557).
- mod_log_config is affected by denial of service vulnerability by sending crafted cookie value if the '%{cookiename}C' log format string is in use (CVE-2012-0021).
Affected Products:
Apache HTTP Server prior to 2.2.22

Impact:
Successful exploitation of these issues allows an attacker to gain sensitive information or cause denial of service conditions.

Solution:
Upgrade to Apache HTTP Server version 2.2.22 or above. For more details please refer to vendor advisory : Apache 2.2.22

Results:
```
Date: Tue, 02 Sep 2014 09:23:51 GMT Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.4.30 Location: http://biz2.becasiaticket.com
/www/admin/index.php Content-Length: 0 Connection: close
Content-Type: text/html; charset=UTF-8
```

Apache HTTP Server mod_cache and mod_dav Undisclosed DoS Vulnerability

QID: 86908 **CVSS Base: null**
Category: Web server **Port: 0**
CVEID: CVE-2010-1452

Threat:
The Apache HTTP Server is a freely available Web server.
An undisclosed vulnerability exists in Apache mod_cache and mod_dav, which could allow an attacker to cause a denial of service.
To exploit this issue, an attacker would need to locate an Apache Web server running mod_cache and mod_dav.
Affected Versions:
Apache HTTP Server 2.2.x before 2.2.16.

Impact:
By exploiting this vulnerability, an attacker can cause a denial of service.

Solution:
Update to Version 2.2.16 to resolve this issue. The latest version is available for download from Apache Web site

Results:
```
QID: 86908 detected on port 80 over TCP - Apache/2.2.15 (CentOS)
```

OpenSSH Commands Information Disclosure Vulnerability

QID: 42382 **CVSS Base: null**
Category: General remote services **Port: 0**
CVEID: CVE-2012-0814

Threat:
OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
Openssh-server could allow a remote attacker to obtain sensitive information because of the improper handling of forced commands.

Impact:
Only authenticated users can exploit this vulnerability to obtain usernames and other sensitive information.

Solution:
Upgrade to OpenSSH 5.7 or later, available from the OpenSSH Web site .

Results:
```
SSH-2.0-OpenSSH_5.3
```

Apache HTTP Server APR "apr_fnmatch()" Denial of Service Vulnerability

QID: 12500 **CVSS Base: null**
Category: CGI **Port: 0**
CVEID: CVE-2011-0419

Threat:
The Apache HTTP Server is a freely available Web server.
The vulnerability is caused by an infinite recursion error within the "apr_fnmatch()" function when processing certain patterns. This can be exploited to cause a stack overflow via a specially crafted request containing wildcard characters (e.g. "*").

Impact:
This vulnerability can be exploited by malicious people to cause a denial of service.

Solution:
The vendor has released Apache HTTP Server version 2.2.19 Apache 2.2.19 to resolve these issues.
The vendor also released Apache HTTP Server version 2.0.65-DEV. The latest version is available for download from Apache Web site

Results:
```
QID: 12500 detected on port 80 over TCP - Apache/2.2.15 (CentOS)
```

Apache Prior to 2.4.4 and 2.2.24 Multiple Vulnerabilities

QID: 87156 **CVSS Base: null**
Category: Web server **Port: 80**
CVEID: CVE-2012-3499, CVE-2012-4558

Threat:
Apache HTTP Server is an HTTP web server application.
Apache HTTP Server is prone to multiple cross-site scripting vulnerabilities because it fails to properly sanitize user-supplied input.
- Various XSS flaws exist due to unescaped hostnames and URIs HTML output in mod_info, mod_status, mod_imagemap, mod_ldap, and mod_proxy_ftp.
- A XSS flaw affects the mod_proxy_balancer manager interface.
Affected Versions:
Apache HTTP Server prior to 2.4.4
Apache HTTP Server prior to 2.2.24

Impact:
An attacker may leverage these issues to execute arbitrary HTML and script code in the browser of an unsuspecting user in the context of the affected site. This may let the attacker launch additional attacks.

Solution:
These vulnerabilities have been patched in Apache 2.2.24 and 2.4.4. Refer to Apache httpd 2.4.4 Changelog and Apache httpd 2.2.24 Changelog .
Ubuntu users refer to Ubuntu advisory USN-1765-1 for affected packages and patching details, or update with your package manager.

Results:
```
QID 87156 detected on port 80 - Apache/2.2.15 (CentOS)
```

Apache Partial HTTP Request Denial of Service Vulnerability - Zero Day

QID: 86847 **CVSS Base: null**
Category: Web server **Port: 0**
CVEID: CVE-2007-6750

Threat:
The Apache HTTP Server, commonly referred to as Apache is a freely available Web server.
Apache is vulnerable to a denial of service due to holding a connection open for partial HTTP requests.
Apache Versions 1.x and 2.x are vulnerable.

Impact:
A remote attacker can cause a denial of service against the Web server which would prevent legitimate users from accessing the site.
Denial of service tools and scripts such as Slowloris takes advantage of this vulnerability.

Solution:
Patch -
There are no vendor-supplied patches available at this time.
Workaround:
- Server-specific recommendations can be found here.
- Countermeasures for Apache are described here.
- Reverse proxies, load balancers and iptables can help to prevent this attack from occurring.
- Adjusting the TimeOut Directive can also prevent this attack from occurring.
- A new module mod_reqtimeout has been introduced since Apache 2.2.15 to provide tools for mitigation against these forms of attack.
Also refer to Cert Blog and Slowloris and Mitigations for Apache document for further information.

Results:
```
QID: 86847 detected on port 80 over TCP - Apache/2.2.15 (CentOS)
```

PHP Denial of Service Vulnerability

QID: 12808 **CVSS Base: null**
Category: CGI **Port: 80**
CVEID: CVE-2013-6712

Threat:
PHP is a general purpose scripting language that is suited for web development and can be embedded in HTML.
PHP is exposed to a denial of service vulnerability as it fails to properly restrict creation DateInterval objects used in scan function in ext/date/lib/parse_iso_intervals.c which can allow remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted interval specification.
Affected Versions:
Versions prior to PHP 5.5.6

Impact:
Successful exploitation of this vulnerability will allow a remote attacker to cause a denial of service.

Solution:
Users are advised to upgrade to the latest version of PHP available. For more details about PHP releases and patches please visit PHP Homepage .

Results:
```
Date: Tue, 02 Sep 2014 09:23:51 GMT Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.4.30 Location: http://biz2.becasiaticket.com
/www/admin/index.php Content-Length: 0 Connection: close
Content-Type: text/html; charset=UTF-8
```

Web Directories Listable Vulnerability

QID: 86445 **CVSS Base: null**
Category: Web server **Port: 80**
CVEID: -

Threat:
The Web server has some listable directories. Very sensitive information can be obtained

from directory listings.

Impact:
A remote user may exploit this vulnerability to obtain very sensitive information on the host. The information obtained may assist in further attacks against the host.

Solution:
Disable directory browsing or listing for all directories.

Results:
```
#table cols="1" Listable_Directories /manual/images/
```

Web Server HTTP Trace/Track Method Support Cross-Site Tracing Vulnerability

QID: 86473 **CVSS Base: null**
Category: Web server **Port: 80**
CVEID: CVE-2004-2320, CVE-2007-3008

Threat:
A Web server was detected that supports the HTTP TRACE method. This method allows debugging and connection trace analysis for connections from the client to the Web server. Per the HTTP specification, when this method is used, the Web server echoes back the information sent to it by the client unmodified and unfiltered. Microsoft IIS web server uses an alias TRACK for this method, and is functionally the same.
A vulnerability related to this method was discovered. A malicious, active component in a Web page can send Trace requests to a Web server that supports this Trace method. Usually, browser security disallows access to Web sites outside of the present site's domain. Although unlikely and difficult to achieve, it's possible, in the presence of other browser vulnerabilities, for the active HTML content to make external requests to arbitrary Web servers beyond the hosting Web server. Since the chosen Web server then echoes back the client request unfiltered, the response also includes cookie-based or Web-based (if logged on) authentication credentials that the browser automatically sent to the specified Web application on the specified Web server.
The significance of the Trace capability in this vulnerability is that the active component in the page visited by the victim user has no direct access to this authentication information, but gets it after the target Web server echoes it back as its Trace response.
Since this vulnerability exists as a support for a method required by the HTTP protocol specification, most common Web servers are vulnerable.
The exact method(s) supported, Trace and/or Track, and their responses are in the Results section below.
Track / Trace are required to be disabled to be PCI compliance.

Impact:
If this vulnerability is successfully exploited, users of the Web server may lose their authentication credentials for the server and/or for the Web applications hosted by the server to an attacker. This may be the case even if the Web applications are not vulnerable to cross site scripting attacks due to input validation errors.

Solution:
Solutions for some of the common Web servers are supplied below. For other Web servers, please check your vendor's documentation.
Apache: Recent Apache versions have a Rewrite module that allows HTTP requests to be rewritten or handled in a specific way. Compile the Apache server with the mod_rewrite module. You might need to uncomment the 'AddModule' and 'LoadModule' directives in the httpd.conf configuration file. Add the following lines for each virtualhost in your configuration file (Please note that, by default, Rewrite configurations are not inherited. This means that you need to have Rewrite directives for each virtual host in which you wish to use it):
```
<IfModule mod_rewrite.c> RewriteEngine on RewriteCond
%{REQUEST_METHOD} ^TRACE RewriteRule .* - [F] </IfModule>
```
With this configuration, Apache catches all TRACE requests, and replies with a page reporting the request as forbidden. None of the original request's contents are echoed back.
A slightly tighter fix is to use:

```
<IfModule mod_rewrite.c> RewriteEngine on RewriteCond
%{REQUEST_METHOD} !^(GET|POST|HEAD)$ RewriteRule .* - [F]
</IfModule>
```

Please note that RewriteEngine can be processor intensive and may impact the web server performance. The trace method can also be controlled by use of the TraceEnable directive. In the httpd.conf add or modify:
TraceEnable Off
Microsoft IIS: Microsoft released URLScan, which can be used to screen all incoming requests based on customized rulesets. URLScan can be used to sanitize or disable the TRACE requests from the clients. Note that IIS aliases 'TRACK' to 'TRACE'. Therefore, if URLScan is used to specfically block the TRACE method, the TRACK method should also be added to the filter.
URLScan uses the 'urlscan.ini' configuration file, usually in \System32\InetSrv\URLScan directory. In that, we have two sections - AllowVerbs and DenyVerbs. The former is used if the UseAllowVerbs variable is set to 1, else (if its set to 0), the DenyVerbs are used. Clearly, either can be used, depending on whether we want a Default-Deny-Explicit-Allow or a Default-Allow-Explicit-Deny policy. To disallow TRACE and TRACK methods through URLScan, first remove 'TRACK', 'TRACE' methods from the 'AllowVerbs' section and add them to the 'DenyVerbs' section. With this, URLScan will disallow all 'TRACE' and 'TRACK' methods, and generate an error page for all requests using that method. To enable the changes, restart the 'World Wide Web Publishing Service' from the 'Services' Control Panel item.
For more details about other web servers : Cert Advisory.

Results:

```
TRACE / HTTP/1.1 Host: ppp-111.223.39.140.revip.proen.co.th Via:
<script>alert('QualysXSS');</script> HTTP/1.1 200 OK Date: Tue, 02
Sep 2014 09:29:18 GMT Server: Apache/2.2.15 (CentOS) Connection:
close Transfer-Encoding: chunked Content-Type: message/http TRACE /
HTTP/1.1 Host: ppp-111.223.39.140.revip.proen.co.th Via:
<script>alert('QualysXSS');</script> -CR-TRACE / HTTP/1.0 Via:
<script>alert('QualysXSS');</script> HTTP/1.1 200 OK Date: Tue, 02
Sep 2014 09:29:19 GMT Server: Apache/2.2.15 (CentOS) Connection:
close Content-Type: message/http TRACE / HTTP/1.0 Via:
<script>alert('QualysXSS');</script>
```

Apache HTTP Server APR-util Multiple Denial of Service Vulnerabilities

QID: 86920 **CVSS Base: null**
Category: Web server **Port: 0**
CVEID: CVE-2009-3560, CVE-2009-3720, CVE-2010-1623

Threat:
The Apache HTTP Server is a freely available Web server.
Apache Server is prone to the following vulnerabilities:
- Two XML parsing vulnerabilities exist in the Apache HTTP Server.
- An error within the "apr_brigade_split_line()" function in buckets/apr_brigade.c can be exploited to cause high memory consumption.
Apache HTTP Server versions prior to 2.2.17 are affected.
Apache HTTP Server versions prior to 2.0.64 are also affected.

Impact:
Successful exploitation allows malicious users to cause a denial of service.

Solution:
The vendor has released Apache HTTP Server Version 2.2.17 and version 2.0.64 to resolve these issues.
The latest version is available for download from Apache Web site

Results:

```
QID: 86920 detected on port 80 over TCP - Apache/2.2.15 (CentOS)
```

OpenSSH "child_set_env()" Security Bypass Issue

QID: 42428 **CVSS Base: null**
Category: General remote services **Port: 0**
CVEID: CVE-2014-2532

Threat:
OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
The security issue is caused by an error within the "child_set_env()" function (usr.bin/ssh /session.c) and can be exploited to bypass intended environment restrictions by using a substring before a wildcard character.
Affected Versions:
OpenSSH Versions prior to 6.6 are affected

Impact:
This issue can be exploited by malicious local users to bypass certain security restrictions.

Solution:
Upgrade to OpenSSH 6.6 or later to resolve this issue. Refer to OpenSSH 6.6 Release Notes for further information.

Results:
```
SSH-2.0-OpenSSH_5.3 detected on port 22 over TCP.
```

Expose_php Set to On in php.ini

QID: 12087 **CVSS Base: 1.9**
Category: CGI **Port: 80**
CVEID: -

Threat:
The scanner found PHP version information in the headers returned by the PHP-enabled target Web server. This likely means that the "expose_php" variable is set to "On" in the "php.ini" configuration file for the Web server.

Impact:
This allows remote users to easily know that PHP is installed on the Web server. It also provides version information of the PHP installation. This could aid an attacker in launching more targeted attacks in the future.

Solution:
Locate the "php.ini" configuration file on the target host and add this setting to it: "expose_php=Off". Restart the Web server.

Results:
```
GET /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000 HTTP/1.1 Host:
ppp-111.223.39.140.revip.proen.co.th Connection: Keep-Alive
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"DTD/xhtml1-transitional.dtd"> <html xmlns="http://www.w3.org
/1999/xhtml"><head> <style type="text/css"> body {background-color:
#ffffff; color: #000000;} body, td, th, h1, h2 {font-family:
sans-serif;} pre {margin: 0px; font-family: monospace;} a:link
{color: #000099; text-decoration: none; background-color: #ffffff;}
a:hover {text-decoration: underline;} table {border-collapse:
collapse;} .center {text-align: center;} .center table {
margin-left: auto; margin-right: auto; text-align: left;} .center th
{ text-align: center !important; } td, th { border: 1px solid
#000000; font-size: 75%; vertical-align: baseline;} h1 {font-size:
150%;} h2 {font-size: 125%;} .p {text-align: left;} .e {background-
color: #ccccff; font-weight: bold; color: #000000;} .h {background-
color: #9999cc; font-weight: bold; color: #000000;} .v {background-
```

color: #cccccc; color: #000000;} .vr {background-color: #cccccc;
text-align: right; color: #000000;} img {float: right; border: 0px;}
hr {width: 600px; background-color: #cccccc; border: 0px; height:
1px; color: #000000;} </style> <title>phpinfo()</title><meta
name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE" /></head>
<body> <h1>PHP Credits</h1> <table border="0"
cellpadding="3" width="600"> <tr class="h"><th>PHP Group</th></tr>
<tr><td class="e">Thies C. Arntzen, Stig Bakken, Shane Caraveo, Andi
Gutmans, Rasmus Lerdorf, Sam Ruby, Sascha Schumann, Zeev Suraski,
Jim Winstead, Andrei Zmievski </td></tr> </table>
 <table
border="0" cellpadding="3" width="600"> <tr class="h"><th>Language
Design & Concept</th></tr> <tr><td class="e">Andi Gutmans, Rasmus
Lerdorf, Zeev Suraski, Marcus Boerger </td></tr> </table>
<table border="0" cellpadding="3" width="600"> <tr class="h"><th
colspan="2">PHP Authors</th></tr> <tr class="h">
<th>Contribution</th><th>Authors</th></tr> <tr><td class="e">Zend
Scripting Language Engine </td><td class="v">Andi Gutmans, Zeev
Suraski, Stanislav Malyshev, Marcus Boerger, Dmitry Stogov
</td></tr> <tr><td class="e">Extension Module API </td><td
class="v">Andi Gutmans, Zeev Suraski, Andrei Zmievski </td></tr>
<tr><td class="e">UNIX Build and Modularization </td><td
class="v">Stig Bakken, Sascha Schumann, Jani Taskinen </td></tr>
<tr><td class="e">Windows Port </td><td class="v">Shane Caraveo,
Zeev Suraski, Wez Furlong, Pierre-Alain Joye </td></tr> <tr><td
class="e">Server API (SAPI) Abstraction Layer </td><td
class="v">Andi Gutmans, Shane Caraveo, Zeev Suraski </td></tr>
<tr><td class="e">Streams Abstraction Layer </td><td class="v">Wez
Furlong, Sara Golemon </td></tr> <tr><td class="e">PHP Data Objects
Layer </td><td class="v">Wez Furlong, Marcus Boerger, Sterling
Hughes, George Schlossnagle, Ilia Alshanetsky </td></tr> <tr><td
class="e">Output Handler </td><td class="v">Zeev Suraski, Thies C.
Arntzen, Marcus Boerger, Michael Wallner </td></tr> </table>
<table border="0" cellpadding="3" width="600"> <tr class="h"><th
colspan="2">SAPI Modules</th></tr> <tr class="h">
<th>Contribution</th><th>Authors</th></tr> <tr><td
class="e">AOLserver </td><td class="v">Sascha Schumann </td></tr>
<tr><td class="e">Apache 1.3 (apache_hooks) </td><td
class="v">Rasmus Lerdorf, Zeev Suraski, Stig Bakken, David Sklar,
George Schlossnagle, Lukas Schroeder </td></tr> <tr><td
class="e">Apache 1.3 </td><td class="v">Rasmus Lerdorf, Zeev
Suraski, Stig Bakken, David Sklar </td></tr> <tr><td
class="e">Apache 2.0 Filter </td><td class="v">Sascha Schumann,
Aaron Bannert </td></tr> <tr><td class="e">Apache 2.0 Handler
</td><td class="v">Ian Holsman, Justin Erenkrantz (based on Apache
2.0 Filter code) </td></tr> <tr><td class="e">Caudium / Roxen
</td><td class="v">David Hedbor </td></tr> <tr><td class="e">CGI /
FastCGI </td><td class="v">Rasmus Lerdorf, Stig Bakken, Shane
Caraveo, Dmitry Stogov </td></tr> <tr><td class="e">CLI </td><td
class="v">Edin Kadribasic, Marcus Boerger, Johannes Schlueter,
Moriyoshi Koizumi, Xinchen Hui </td></tr> <tr><td
class="e">Continuity </td><td class="v">Alex Leigh (based on nsapi
code) </td></tr> <tr><td class="e">Embed </td><td class="v">Edin
Kadribasic </td></tr> <tr><td class="e">FastCGI Process Manager
</td><td class="v">Andrei Nigmatulin, dreamcat4, Antony Dovgal,
Jerome Loyet </td></tr> <tr><td class="e">ISAPI </td><td
class="v">Andi Gutmans, Zeev Suraski </td></tr> <tr><td
class="e">litespeed </td><td class="v">George Wang </td></tr>
<tr><td class="e">NSAPI </td><td class="v">Jayakumar
Muthukumarasamy, Uwe Schindler </td></tr> <tr><td class="e">phttpd
</td><td class="v">Thies C. Arntzen </td></tr> <tr><td
class="e">pi3web </td><td class="v">Holger Zimmermann </td></tr>
<tr><td class="e">Sendmail Milter </td><td class="v">Harald Radi
</td></tr> <tr><td class="e">thttpd </td><td class="v">Sascha
Schumann </td></tr> <tr><td class="e">tux </td><td class="v">Sascha
Schumann </td></tr> <tr><td class="e">WebJames </td><td
class="v">Alex Waugh </td></tr> </table>
 <table border="0"
cellpadding="3" width="600"> <tr class="h"><th colspan="2">Module
Authors</th></tr> <tr class="h"><th>Module</th><th>Authors</th></tr>
<tr><td class="e">BC Math </td><td class="v">Andi Gutmans </td></tr>
<tr><td class="e">Bzip2 </td><td class="v">Sterling Hughes
</td></tr> <tr><td class="e">Calendar </td><td class="v">Shane

Caraveo, Colin Viebrock, Hartmut Holzgraefe, Wez Furlong </td></tr>
<tr><td class="e">COM and .Net </td><td class="v">Wez Furlong
</td></tr> <tr><td class="e">ctype </td><td class="v">Hartmut
Holzgraefe </td></tr> <tr><td class="e">cURL </td><td
class="v">Sterling Hughes </td></tr> <tr><td class="e">Date/Time
Support </td><td class="v">Derick Rethans </td></tr> <tr><td
class="e">DB-LIB (MS SQL, Sybase) </td><td class="v">Wez Furlong,
Frank M. Kromann </td></tr> <tr><td class="e">DBA </td><td
class="v">Sascha Schumann, Marcus Boerger </td></tr> <tr><td
class="e">DOM </td><td class="v">Christian Stocker, Rob Richards,
Marcus Boerger </td></tr> <tr><td class="e">enchant </td><td
class="v">Pierre-Alain Joye, Ilia Alshanetsky </td></tr> <tr><td
class="e">ereg </td><td class="v">Rasmus Lerdorf, Jim Winstead,
Jaakko Hyvtti </td></tr> <tr><td class="e">EXIF </td><td
class="v">Rasmus Lerdorf, Marcus Boerger </td></tr> <tr><td
class="e">fileinfo </td><td class="v">Ilia Alshanetsky, Pierre Alain
Joye, Scott MacVicar, Derick Rethans </td></tr> <tr><td
class="e">Firebird/InterBase driver for PDO </td><td class="v">Ard
Biesheuvel </td></tr> <tr><td class="e">FTP </td><td
class="v">Stefan Esser, Andrew Skalski </td></tr> <tr><td
class="e">GD imaging </td><td class="v">Rasmus Lerdorf, Stig Bakken,
Jim Winstead, Jouni Ahto, Ilia Alshanetsky, Pierre-Alain Joye,
Marcus Boerger </td></tr> <tr><td class="e">GetText </td><td
class="v">Alex Plotnick </td></tr> <tr><td class="e">GNU GMP support
</td><td class="v">Stanislav Malyshev </td></tr> <tr><td
class="e">Iconv </td><td class="v">Rui Hirokawa, Stig Bakken,
Moriyoshi Koizumi </td></tr> <tr><td class="e">IMAP </td><td
class="v">Rex Logan, Mark Musone, Brian Wang, Kaj-Michael Lang,
Antoni Pamies Olive, Rasmus Lerdorf, Andrew Skalski, Chuck
Hagenbuch, Daniel R Kalowsky </td></tr> <tr><td class="e">Input
Filter </td><td class="v">Rasmus Lerdorf, Derick Rethans,
Pierre-Alain Joye, Ilia Alshanetsky </td></tr> <tr><td
class="e">InterBase </td><td class="v">Jouni Ahto, Andrew Avdeev,
Ard Biesheuvel </td></tr> <tr><td class="e">Internationalization
</td><td class="v">Ed Batutis, Vladimir Iordanov, Dmitry Lakhtyuk,
Stanislav Malyshev, Vadim Savchuk, Kirti Velankar </td></tr> <tr><td
class="e">JSON </td><td class="v">Omar Kilani, Scott MacVicar
</td></tr> <tr><td class="e">LDAP </td><td class="v">Amitay Isaacs,
Eric Warnke, Rasmus Lerdorf, Gerrit Thomson, Stig Venaas </td></tr>
<tr><td class="e">LIBXML </td><td class="v">Christian Stocker, Rob
Richards, Marcus Boerger, Wez Furlong, Shane Caraveo </td></tr>
<tr><td class="e">mcrypt </td><td class="v">Sascha Schumann, Derick
Rethans </td></tr> <tr><td class="e">MS SQL </td><td class="v">Frank
M. Kromann </td></tr> <tr><td class="e">Multibyte String Functions
</td><td class="v">Tsukada Takuya, Rui Hirokawa </td></tr> <tr><td
class="e">MySQL driver for PDO </td><td class="v">George
Schlossnagle, Wez Furlong, Ilia Alshanetsky, Johannes Schlueter
</td></tr> <tr><td class="e">MySQL </td><td class="v">Zeev Suraski,
Zak Greant, Georg Richter </td></tr> <tr><td class="e">MySQLi
</td><td class="v">Zak Greant, Georg Richter, Andrey Hristov, Ulf
Wendel </td></tr> <tr><td class="e">MySQLnd </td><td
class="v">Andrey Hristov, Ulf Wendel, Georg Richter </td></tr>
<tr><td class="e">OCI8 </td><td class="v">Stig Bakken, Thies C.
Arntzen, Andy Sautins, David Benson, Maxim Maletsky, Harald Radi,
Antony Dovgal, Andi Gutmans, Wez Furlong, Christopher Jones, Oracle
Corporation </td></tr> <tr><td class="e">ODBC driver for PDO
</td><td class="v">Wez Furlong </td></tr> <tr><td class="e">ODBC
</td><td class="v">Stig Bakken, Andreas Karajannis, Frank M.
Kromann, Daniel R. Kalowsky </td></tr> <tr><td class="e">OpenSSL
</td><td class="v">Stig Venaas, Wez Furlong, Sascha Kettler
</td></tr> <tr><td class="e">Oracle (OCI) driver for PDO </td><td
class="v">Wez Furlong </td></tr> <tr><td class="e">pcntl </td><td
class="v">Jason Greene, Arnaud Le Blanc </td></tr> <tr><td
class="e">Perl Compatible Regexps </td><td class="v">Andrei Zmievski
</td></tr> <tr><td class="e">PHP Archive </td><td class="v">Gregory
Beaver, Marcus Boerger </td></tr> <tr><td class="e">PHP Data Objects
</td><td class="v">Wez Furlong, Marcus Boerger, Sterling Hughes,
George Schlossnagle, Ilia Alshanetsky </td></tr> <tr><td
class="e">PHP hash </td><td class="v">Sara Golemon, Rasmus Lerdorf,
Stefan Esser, Michael Wallner, Scott MacVicar </td></tr> <tr><td
class="e">Posix </td><td class="v">Kristian Koehntopp </td></tr>

<tr><td class="e">PostgreSQL driver for PDO </td><td class="v">Edin Kadribasic, Ilia Alshanetsky </td></tr> <tr><td class="e">PostgreSQL </td><td class="v">Jouni Ahto, Zeev Suraski, Yasuo Ohgaki, Chris Kings-Lynne </td></tr> <tr><td class="e">Pspell </td><td class="v">Vlad Krupin </td></tr> <tr><td class="e">Readline </td><td class="v">Thies C. Arntzen </td></tr> <tr><td class="e">Recode </td><td class="v">Kristian Koehntopp </td></tr> <tr><td class="e">Reflection </td><td class="v">Marcus Boerger, Timm Friebe, George Schlossnagle, Andrei Zmievski, Johannes Schlueter </td></tr> <tr><td class="e">Sessions </td><td class="v">Sascha Schumann, Andrei Zmievski </td></tr> <tr><td class="e">Shared Memory Operations </td><td class="v">Slava Poliakov, Ilia Alshanetsky </td></tr> <tr><td class="e">SimpleXML </td><td class="v">Sterling Hughes, Marcus Boerger, Rob Richards </td></tr> <tr><td class="e">SNMP </td><td class="v">Rasmus Lerdorf, Harrie Hazewinkel, Mike Jackson, Steven Lawrance, Johann Hanne, Boris Lytochkin </td></tr> <tr><td class="e">SOAP </td><td class="v">Brad Lafountain, Shane Caraveo, Dmitry Stogov </td></tr> <tr><td class="e">Sockets </td><td class="v">Chris Vandomelen, Sterling Hughes, Daniel Beulshausen, Jason Greene </td></tr> <tr><td class="e">SPL </td><td class="v">Marcus Boerger, Etienne Kneuss </td></tr> <tr><td class="e">SQLite 3.x driver for PDO </td><td class="v">Wez Furlong </td></tr> <tr><td class="e">SQLite3 </td><td class="v">Scott MacVicar, Ilia Alshanetsky, Brad Dewar </td></tr> <tr><td class="e">Sybase-CT </td><td class="v">Zeev Suraski, Tom May, Timm Friebe </td></tr> <tr><td class="e">System V Message based IPC </td><td class="v">Wez Furlong </td></tr> <tr><td class="e">System V Semaphores </td><td class="v">Tom May </td></tr> <tr><td class="e">System V Shared Memory </td><td class="v">Christian Cartus </td></tr> <tr><td class="e">tidy </td><td class="v">John Coggeshall, Ilia Alshanetsky </td></tr> <tr><td class="e">tokenizer </td><td class="v">Andrei Zmievski, Johannes Schlueter </td></tr> <tr><td class="e">WDDX </td><td class="v">Andrei Zmievski </td></tr> <tr><td class="e">XML </td><td class="v">Stig Bakken, Thies C. Arntzen, Sterling Hughes </td></tr> <tr><td class="e">XMLReader </td><td class="v">Rob Richards </td></tr> <tr><td class="e">xmlrpc </td><td class="v">Dan Libby </td></tr> <tr><td class="e">XMLWriter </td><td class="v">Rob Richards, Pierre-Alain Joye </td></tr> <tr><td class="e">XSL </td><td class="v">Christian Stocker, Rob Richards </td></tr> <tr><td class="e">Zip </td><td class="v">Pierre-Alain Joye </td></tr> <tr><td class="e">Zlib </td><td class="v">Rasmus Lerdorf, Stefan Roehrich, Zeev Suraski, Jade Nicoletti, Michael Wallner </td></tr> </table>
 <table border="0" cellpadding="3" width="600"> <tr class="h"><th colspan="2">PHP Documentation</th></tr> <tr><td class="e">Authors </td><td class="v">Mehdi Achour, Friedhelm Betz, Antony Dovgal, Nuno Lopes, Hannes Magnusson, Georg Richter, Damien Seguy, Jakub Vrana </td></tr> <tr><td class="e">Editor </td><td class="v">Philip Olson </td></tr> <tr><td class="e">User Note Maintainers </td><td class="v">Daniel P. Brown, Thiago Henrique Pojda </td></tr> <tr><td class="e">Other Contributors </td><td class="v">Previously active authors, editors and other contributors are listed in the manual. </td></tr> </table>
 <table border="0" cellpadding="3" width="600"> <tr class="h"><th>PHP Quality Assurance Team</th></tr> <tr><td class="e">Ilia Alshanetsky, Joerg Behrens, Antony Dovgal, Stefan Esser, Moriyoshi Koizumi, Magnus Maatta, Sebastian Nohn, Derick Rethans, Melvyn Sopacua, Jani Taskinen, Pierre-Alain Joye, Dmitry Stogov, Felipe Pena </td></tr> </table>
 <table border="0" cellpadding="3" width="600"> <tr class="h"><th colspan="2">Websites and Infrastructure team</th></tr> <tr><td class="e">PHP Websites Team </td><td class="v">Rasmus Lerdorf, Hannes Magnusson, Philip Olson, Lukas Kahwe Smith, Pierre-Alain Joye, Kalle Sommer Nielsen </td></tr> <tr><td class="e">Event Maintainers </td><td class="v">Damien Seguy, Daniel P. Brown </td></tr> <tr><td class="e">Network Infrastructure </td><td class="v">Daniel P. Brown </td></tr> <tr><td class="e">Windows Infrastructure </td><td class="v">Alex Schoenmaker </td></tr> </table>
 </body></html> -CR-

INFO

Remote Access or Management Service Detected

QID: 42017 **CVSS Base: null**
Category: General remote services **Port: 0**
CVEID: -

Threat:
A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.
The Results section includes information on the remote access service that was found on the target.
Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

Impact:
Consequences vary by the type of attack.

Solution:
Expose the remote access or remote management services only to the system administrators or intended users of the system.

Results:
```
Service name: SSH on TCP port 22.
```

INFO

Operating System Detected

QID: 45017 **CVSS Base: null**
Category: Information gathering **Port: 0**
CVEID: -

Threat:
Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) **TCP/IP Fingerprint**: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that for the firewall instead of for the host being scanned.
2) **NetBIOS**: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) **PHP Info**: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) **SNMP**: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include

"MIB_II.system.sysDescr" for the operating system.

Impact:
Not applicable.

Solution:
Not applicable.

Results:
```
#table cols="3" Operating_System Technique ID Ubuntu_/_Linux_2.6.x_
/_Linux_2.6 TCP/IP_Fingerprint M4856:5927::22
```

INFO

Host Uptime Based on TCP TimeStamp Option

QID: 82063 **CVSS Base: null**
Category: TCP/IP **Port: 0**
CVEID: -

Threat:
The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

Impact:
N/A

Solution:
N/A

Results:
```
Based on TCP timestamps obtained via port 22, the host's uptime is 4
days, 21 hours, and 58 minutes. The TCP timestamps from the host are
in units of 1 milliseconds.
```

INFO

PHP Server Detected

QID: 45110 **CVSS Base: null**
Category: Information gathering **Port: 0**
CVEID: -

Threat:
PHP is a general purpose scripting language that is especially suited for Web development and can be embedded in HTML.

Impact:
N/A

Solution:
N/A

Results:
```
Date: Tue, 02 Sep 2014 09:23:51 GMT Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.4.30 Location: http://biz2.becasiaticket.com
/www/admin/index.php Content-Length: 0 Connection: close
Content-Type: text/html; charset=UTF-8
```

INFO

SSH Banner

QID: 38050 **CVSS Base: null**
Category: General remote services **Port: 22**
CVEID: -

Threat:

Impact:

Solution:

Results:
```
SSH-2.0-OpenSSH_5.3
```

INFO

Web Server Version

QID: 86000 **CVSS Base: null**
Category: Web server **Port: 80**
CVEID: -

Threat:
N/A

Impact:
N/A

Solution:
N/A

Results:
```
#table cols="2" Server_Version Server_Banner Apache/2.2.15_(CentOS)
Apache/2.2.15_(CentOS)
```

INFO

Open TCP Services List

QID: 82023 **CVSS Base: null**
Category: TCP/IP **Port: 0**
CVEID: -

Threat:
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

Impact:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

Solution:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site .

Results:

```
#table cols="5" Port IANA_Assigned_Ports/Services Description
Service_Detected OS_On_Redirected_Port 22 ssh
SSH_Remote_Login_Protocol ssh_ _ 80 www World_Wide_Web_HTTP http_ _
```

INFO

Firewall Detected

QID: 34011 **CVSS Base: null**
Category: Firewall **Port: 0**
CVEID: -

Threat:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

Impact:

Solution:

Results:

```
Some of the ports filtered by the firewall are: 20, 21, 23, 25, 53,
111, 135, 445, 1, 7. Listed below are the ports filtered by the
firewall. No response has been received when any of these ports is
probed.
1-3,5,7,9,11,13,15,17-21,23-25,27,29,31,33,35,37-39,41-79,81-112,114
-223,
242-246,256-265,280-282,309,311,318,322-325,344-351,363,369-442,444-
581,
587,592-593,598,600,606-620,624,627,631,633-637,666-674,700,704-705,
707,
709-711,729-731,740-742,744,747-754,758-765,767,769-777,780-783,786,
799-801,
860,873,886-888,900-901,911,950,954-955,990-993,995-1001,1008,1010-1
011,
1015,1023-1100,1109-1112,1114,1123,1155,1167,1170,1207,1212,1214,122
0-1222,
1234-1236,1241,1243,1245,1248,1269,1313-1314,1337,1344-1625,1636-177
4,
1776-1815,1818-1824,1900-1909,1911-1920,1944-1951,1973,1981,1985-202
8, 2030,2032-2036,2038,2040-2049,2053,2065,2067,2080,2097,2100,2102,
and more. We have omitted from this list 706 higher ports to keep
the report size manageable.
```

INFO

Default Web Page

QID: 12230 **CVSS Base: null**
Category: CGI **Port: 80**
CVEID: -

Threat:
The Result section displays the default Web page for the Web server.

Impact:
N/A

Solution:
N/A

Results:

```
HTTP/1.1 302 Found Date: Tue, 02 Sep 2014 09:27:44 GMT Server:
Apache/2.2.15 (CentOS) X-Powered-By: PHP/5.4.30 Location:
http://biz2.becasiaticket.com/www/admin/index.php Content-Length: 0
Connection: close Content-Type: text/html; charset=UTF-8
```

INFO

IP ID Values Randomness

QID: 82046 **CVSS Base: null**
Category: TCP/IP **Port: 0**
CVEID: -

Threat:
The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

Impact:
N/A

Solution:
N/A

Results:
```
IP ID changes observed (network order) for port 22: 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 Duration: 321 milli
seconds
```

INFO

Degree of Randomness of TCP Initial Sequence Numbers

QID: 82045 **CVSS Base: null**
Category: TCP/IP **Port: 0**
CVEID: -

Threat:
TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

Impact:
N/A

Solution:
N/A

Results:
```
Average change between subsequent TCP initial sequence numbers is
1031794778 with a standard deviation of 848816107. These TCP initial
sequence numbers were triggered by TCP SYN probes sent to the host
at an average rate of 1/(10525 microseconds). The degree of
difficulty to exploit the TCP initial sequence number generation
scheme is: hard.
```

INFO

Traceroute

QID: 45006 **CVSS Base: null**
Category: Information gathering **Port: 0**

CVEID: -

Threat:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

Impact:

Solution:

Results:
```
#table cols="4" Hops IP Round_Trip_Time Probe 1 64.39.111.2 16.25ms
ICMP 2 64.95.143.161 1.79ms ICMP 3 66.151.144.21 2.96ms ICMP 4
107.6.73.237 1.58ms ICMP 5 107.6.91.241 10.41ms ICMP 6 *.*.*.*
0.00ms Other 7 61.19.9.213 216.41ms ICMP 8 61.19.7.77 216.93ms ICMP
9 61.19.7.134 211.94ms ICMP 10 122.155.226.74 229.74ms ICMP 11
202.170.119.201 213.40ms ICMP 12 111.223.39.140 223.45ms TCP
```

INFO

SSH daemon information retrieving

QID: 38047 **CVSS Base: 4.9**
Category: General remote services **Port: 22**
CVEID: CVE-1999-0634

Threat:
SSH is a secure protocol, provided it is fully patched, properly configured, and uses FIPS approved algorithms.
```
For Red Hat ES 4:- SSH1 supported yes Supported authentification
methods for SSH1 RSA,password Supported ciphers for SSH1
3des,blowfish SSH2 supported yes Supported keys exchange algorithm
for SSH2 diffie-hellman-group-exchange-sha1,diffie-hellman-group14-
sha1,diffie-hellman-group1-sha1 Supported decryption ciphers for
SSH2 aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-
cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-
ctr,aes256-ctr Supported encryption ciphers for SSH2 aes128-
cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-
cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
Supported decryption mac for SSH2 hmac-md5,hmac-sha1,hmac-
ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
Supported encryption mac for SSH2 hmac-md5,hmac-sha1,hmac-
ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
Supported authentification methods for SSH2 publickey,gssapi-
with-mic,password
```

Impact:
Successful exploitation allows an attacker to execute arbitrary commands on the SSH server or otherwise subvert an encrypted SSH channel with arbitrary data.

Solution:
SSH version 2 is preferred over SSH version 1.

Results:
```
#table cols="2" SSH1_supported no SSH2_supported yes
Supported_keys_exchange_algorithm_for_SSH2 diffie-hellman-group-
exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-
group14-sha1,diffie-hellman-group1-sha1
Supported_decryption_ciphers_for_SSH2 aes128-ctr,aes192-ctr,aes256-
ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,cast128-
cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se
Supported_encryption_ciphers_for_SSH2 aes128-ctr,aes192-ctr,aes256-
ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,cast128-
cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se
Supported_decryption_mac_for_SSH2 hmac-md5,hmac-sha1,umac-
64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-
sha1-96,hmac-md5-96 Supported_encryption_mac_for_SSH2 hmac-md5,hmac-
sha1,umac-64@openssh.com,hmac-ripemd160,hmac-
```

```
ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
Supported_authentication_methods_for_SSH2 password,publickey
```

INFO

List of Web Directories

QID: 86672 **CVSS Base: null**
Category: Web server **Port: 80**
CVEID: -

Threat:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

Impact:

Solution:

Results:
```
#table cols="2" Directory Source /cgi-bin/ brute_force /scripts/
brute_force /manual/ brute_force /error/ brute_force /www/
brute_force /pma/ brute_force /plugins/ brute_force /manual/images/
brute_force /pma/ web_page /pma/doc/ web_page /pma/doc/html/
web_page /pma/__static/ web_page /manual/ web_page /manual/style/
web_page /manual/style/css/ web_page /manual/images/ web_page
/manual/mod/ web_page /manual/misc/ web_page /manual/howto/ web_page
/manual/platform/ web_page /pma/doc/html/__static/ web_page /icons/
web_page /icons/small/ web_page
```

INFO

Host Names Found

QID: 45039 **CVSS Base: null**
Category: Information gathering **Port: 0**
CVEID: -

Threat:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

Impact:
N/A

Solution:
N/A

Results:
```
#table cols="2" Host_Name Source qikplay.bectero.com
User-provided_DNS ppp-111.223.39.140.revip.proen.co.th FQDN
```

INFO

DNS Host Name

QID: 6 **CVSS Base: 0**
Category: Information gathering **Port: 0**
CVEID: -

Threat:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

Impact:

Solution:

Results:
```
#table IP_address Host_name 111.223.39.140 qikplay.bectero.com
111.223.39.140 ppp-111.223.39.140.revip.proen.co.th
```

INFO

Internet Service Provider

QID: 45005 **CVSS Base: null**
Category: Information gathering **Port: 0**
CVEID: -

Threat:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

Impact:
This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

Solution:
N/A

Results:
```
The ISP network handle is: PROENNET ISP Network description: Proen
Internet, Internet Service Provider, Bangkok, Thailand
```

INFO

Host Scan Time

QID: 45038 **CVSS Base: null**
Category: Information gathering **Port: 0**
CVEID: -

Threat:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

Impact:
N/A

Solution:
N/A

Results:
```
Scan duration: 1068 seconds Start time: Tue, Sep 02 2014, 09:22:03
GMT End time: Tue, Sep 02 2014, 09:39:51 GMT
```

INFO

HTTP method TRACE and/or TRACK Enabled

QID: 45033 **CVSS Base: null**
Category: Information gathering **Port: 80**
CVEID: -

Threat:
The target Web server supports the TRACE and/or TRACK HTTP methods. These methods allow debugging and connection trace analysis for connections from the client to the Web server. Per the HTTP specification, when this method is used, the Web server echoes back the information sent to it by the client unmodified and unfiltered. Microsoft IIS Web server uses an alias TRACK for the TRACE method, and is functionally the same.
The exact method(s) used are shown in the Results section.

Impact:
N/A

Solution:
N/A

Results:
```
TRACE method enabled on / directory
```