

Security_Issues

[ASE > All Other ICs > NCI Webospace > Hosted Outside NIH > https://wolf.cci.emory.edu/qa/ > Security Issues](#)

Exported by (IRT)Chaudhery, Salman - 6/7/2016 5:30 PM
Generated on 6/7/2016 4:58:51 PM

Table of Contents

- Executive Summary** 3
 - Issue Types Discovered** 3
 - Affected URLs/Files** 4
 - Fix Recommendations** 5
 - Security Risks** 6
 - WASC Threat Classification** 7
- Issues Sorted by Severity** 8
 - [Medium] http://wolf.cci.emory.edu/icons/ - 1 issue(s)** 8
 - [Medium] Directory Listing 8
 - [Medium] http://wolf.cci.emory.edu/icons/small/ - 1 issue(s)** 10
 - [Medium] Directory Listing 10
 - [Medium] https://wolf.cci.emory.edu/datascope/ - 1 issue(s)** 12
 - [Medium] Missing Secure Attribute in Encrypted Session (SSL) Cookie 12
 - [Medium] https://wolf.cci.emory.edu/icons/ - 1 issue(s)** 13
 - [Medium] Directory Listing 13
 - [Medium] https://wolf.cci.emory.edu/icons/small/ - 1 issue(s)** 14
 - [Medium] Directory Listing 14
 - [Medium] https://wolf.cci.emory.edu/qa - 1 issue(s)** 15
 - [Medium] Deprecated SSL Version is Supported 15
- Remediation Tasks by Severity** 16
 - [Medium] http://wolf.cci.emory.edu/icons/ - 1 issue(s)** 16
 - [Medium] http://wolf.cci.emory.edu/icons/small/ - 1 issue(s)** 16
 - [Medium] https://wolf.cci.emory.edu/datascope/ - 1 issue(s)** 16
 - [Medium] https://wolf.cci.emory.edu/icons/ - 1 issue(s)** 16
 - [Medium] https://wolf.cci.emory.edu/icons/small/ - 1 issue(s)** 16
 - [Medium] https://wolf.cci.emory.edu/qa - 1 issue(s)** 16
- Advisories and Fix Recommendations** 17
 - Missing Secure Attribute in Encrypted Session (SSL) Cookie** 17
 - Directory Listing** 18
 - Deprecated SSL Version is Supported** 19

Executive Summary

Issue Types Discovered

Issue Type	Number of Issues
 Deprecated SSL Version is Supported	1
 Directory Listing	4
 Missing Secure Attribute in Encrypted Session (SSL) Cookie	1

Affected URLs/Files

URL/File	Number of Issues
 http://wolf.cci.emory.edu/icons/	1
 http://wolf.cci.emory.edu/icons/small/	1
 https://wolf.cci.emory.edu/datascope/	1
 https://wolf.cci.emory.edu/icons/	1
 https://wolf.cci.emory.edu/icons/small/	1
 https://wolf.cci.emory.edu/qa	1

Fix Recommendations

Fix Recommendations	Number of Affected Issues
 Add the 'Secure' attribute to all sensitive cookies	1
 Modify the server configuration to deny directory listing, and install the latest security patches available	4
 Use a different signature algorithm for the certificate	1

Security Risks

Risk	Number of Issues
 It is possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user	1
 It is possible to view and download the contents of certain web application virtual directories, which might contain restricted files	4
 It may be possible to steal user and session information (cookies) that was sent during an encrypted session	1

WASC Threat Classification

WASC Threat Classification	Number of Issues
Information Disclosure: Directory Indexing	4
Information Disclosure: Information Leakage	1
Server Misconfiguration	1

Issues Sorted by Severity

[Medium] <http://wolf.cci.emory.edu/icons/> - 1 issue(s)

Issue 1 of 1

[Medium] Directory Listing

Issue:	97411935
Severity:	Medium
URL:	http://wolf.cci.emory.edu/icons/
Path:	icons/
Risk(s):	It is possible to view and download the contents of certain web application virtual directories, which might contain restricted files
Fix:	Modify the server configuration to deny directory listing, and install the latest security patches available

Variant 1 of 1

The following changes were applied to the original request:

```
Set path to '/icons/'
```

Reasoning:

The response contains the content of a directory (directory listing). This indicates that the server allows the listing of directories, which is not usually recommended.

Request/Response:

```
GET /icons/ HTTP/1.1
Cookie: ga=GA1.2.1900723985.1464902423
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://wolf.cci.emory.edu/qa/camicroscope/osdCamicroscope.php?tissueId=
Host: wolf.cci.emory.edu
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
```

```
HTTP/1.1 301 Moved Permanently
Date: Tue, 07 Jun 2016 20:23:21 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16
Location: https://wolf.cci.emory.edu/icons/
Content-Length: 241
Content-Type: text/html; charset=iso-8859-1
```

```
...
ke Gecko
```

```
HTTP/1.1 200 OK
Date: Tue, 07 Jun 2016 20:23:21 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16
Transfer-Encoding: chunked
Content-Type: text/html; charset=ISO-8859-1
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"> <html> <head> <title> Index of /
icons</title> </head> <body> <h1> Index of / icons</h1> <table> <tr><th valign="top"></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"></td><td><a href="/"> Parent Directory
</a> </td><td>&nbsp;</td><td align="right"> - </td><td align="right">2004-
11-20 15:16 </td><td align="right">246 </td><td align="right"></td></tr> <tr><td valig
```

```
...
...
ke Gecko
```

```
HTTP/1.1 200 OK
Date: Tue, 07 Jun 2016 20:23:21 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16
Transfer-Encoding: chunked
Content-Type: text/html; charset=ISO-8859-1
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"> <html> <head> <title> Index of /
icons</title> </head> <body> <h1> Index of / icons</h1> <table> <tr><th valign="top"></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"></td><td><a href="/"> Parent Directory
</a> </td><td>&nbsp;</td><td align="right"> - </td><td>&nbsp;</td></tr> <tr><td valign="top"></td><td><a href="a.gif">a.gif</a> </td><td align="right">2004-
11-20 15:16 </td><td align="right">246 </td><td>&nbsp;</td></tr> <tr><td valig
...
```

Issue 1 of 1

[Medium] Directory Listing

Issue:	97411905
Severity:	Medium
URL:	http://wolf.cci.emory.edu/icons/small/
Path:	small/
Risk(s):	It is possible to view and download the contents of certain web application virtual directories, which might contain restricted files
Fix:	Modify the server configuration to deny directory listing, and install the latest security patches available

Variant 1 of 1

The following changes were applied to the original request:

```
Set path to '/icons/small/'
```

Reasoning:

The response contains the content of a directory (directory listing). This indicates that the server allows the listing of directories, which is not usually recommended.

Request/Response:

```
GET /icons/small/ HTTP/1.1
Cookie: ga=GA1.2.1900723985.1464902423
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://wolf.cci.emory.edu/qa/camicroscope/osdCamicroscope.php?tissueId=
Host: wolf.cci.emory.edu
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
```

```
HTTP/1.1 301 Moved Permanently
Date: Tue, 07 Jun 2016 20:23:21 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16
Location: https://wolf.cci.emory.edu/icons/small/
Content-Length: 247
Content-Type: text/html; charset=iso-8859-1
```

```
...
ke Gecko
```

```
HTTP/1.1 200 OK
Date: Tue, 07 Jun 2016 20:23:21 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16
Transfer-Encoding: chunked
Content-Type: text/html; charset=ISO-8859-1
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"> <html> <head> <title> Index of /
icons/small</title> </head> <body> <h1> Index of / icons/small</h1> <table> <tr><th
valign="top"></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"></td><td><a href="/icons/"> Parent Directory </a> </td><td>&nbsp;</td><td
align="right"> - </td><td>&nbsp;</td></tr> <tr><td valign="top"></td><td><a href="back.gif">back.gif</a> </td><td align="right">2004-11-20 15:16
</td><td align="right">129 </td><td>&nbsp;</td></tr> <tr><td va
```

```
...
ke Gecko
```

```
HTTP/1.1 200 OK
Date: Tue, 07 Jun 2016 20:23:21 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16
Transfer-Encoding: chunked
Content-Type: text/html; charset=ISO-8859-1
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"> <html> <head> <title> Index of /
icons/small</title> </head> <body> <h1> Index of / icons/small</h1> <table> <tr><th
valign="top"></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"></td><td><a href="/icons/"> Parent Directory </a> </td><td>&nbsp;</td><td align="right"> - </td><td>&nbsp;</td></tr> <tr><td valign="top"></td><td><a href="back.gif">back.gif</a> </td><td align="right">2004-11-20 15:16 </td><td align="right">129 </td><td>&nbsp;</td></tr> <tr><td va  
...
```

[Medium] <https://wolf.cci.emory.edu/datascope/> - 1 issue(s)

Issue 1 of 1

[Medium] Missing Secure Attribute in Encrypted Session (SSL) Cookie

Issue: 97411936
Severity: Medium
URL: <https://wolf.cci.emory.edu/datascope/>
Cookie: connect.sess
Risk(s): It may be possible to steal user and session information (cookies) that was sent during an encrypted session
Fix: Add the 'Secure' attribute to all sensitive cookies

Variant 1 of 1

Reasoning:

AppScan found that an encrypted session (SSL) is using a cookie without the "secure" attribute.

Request/Response:

```
GET /datascope/?sessionId=09ha45q0gko3131dge2cln2mf2 HTTP/1.1
Cookie: ga=GA1.2.1900723985.1464902423; PHPSESSID=ea4s3kged7adkqcv197btq21s0
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://wolf.cci.emory.edu/qa/select.php
Host: wolf.cci.emory.edu
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

HTTP/1.1 200 OK
Date: Tue, 07 Jun 2016 20:08:54 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 1806
Vary: Accept-Encoding
Set-Cookie: connect.sess=s%3Aj%3A%7B%7D.PBI%2FnBno%2BH1FwsHz86MRxj7P804%2FxfjVktMvNKh3H%2B%2Bc;
Path=/; HttpOnly

<!DOCTYPE html><html><head><title>Demo Visualization</title><link rel="stylesheet"
href="stylesheets/style.css"><link href="stylesheets/jquery.dataTables.css"
rel="stylesheet"><script src="javascripts/lib/dc/d3.js" type="text/javascript"></script><script
src="javascripts/lib/dc/crossfilter.js" type="text/javascript"></script><script
src="javascripts/lib/dc/dc.js" type="text/javascript"></script><script
src="javascripts/lib/dc/colorbrewer.js" type="text/javascript"></script><script
src="javascripts/lib/jquery/jquery-1.9.1.min.js" type="text/javascript"></script><script
src="javascripts/lib/boot
...
```

Issue 1 of 1

[Medium] Directory Listing

Issue:	85756408
Severity:	Medium
URL:	https://wolf.cci.emory.edu/icons/
Path:	icons/
Risk(s):	It is possible to view and download the contents of certain web application virtual directories, which might contain restricted files
Fix:	Modify the server configuration to deny directory listing, and install the latest security patches available

Variant 1 of 1

The following changes were applied to the original request:

```
Set path to '/icons/'
```

Reasoning:

The response contains the content of a directory (directory listing). This indicates that the server allows the listing of directories, which is not usually recommended.

Request/Response:

```
GET /icons/ HTTP/1.1
Cookie: ga=GA1.2.1900723985.1464902423
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: wolf.cci.emory.edu
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
```

```
HTTP/1.1 200 OK
Date: Tue, 07 Jun 2016 20:20:09 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16
Transfer-Encoding: chunked
Content-Type: text/html; charset=ISO-8859-1
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"> <html> <head> <title> Index of /
icons</title> </head> <body> <h1> Index of / icons</h1> <table> <tr><th valign="top"></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"></td><td><a href="/"> Parent Directory
</a> </td><td>&nbsp;</td><td align="right"> - </td><td>&nbsp;</td></tr> <tr><td valign="top"></td><td><a href="a.gif">a.gif</a> </td><td align="right">2004-
11-20 15:16 </td><td align="right">246 </td><td>&nbsp;</td></tr> <tr><td valig
...
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"> <html> <head> <title> Index of /
icons</title> </head> <body> <h1> Index of / icons</h1> <table> <tr><th valign="top"></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"></td><td><a href="/"> Parent Directory
</a> </td><td>&nbsp;</td><td align="right"> - </td><td>&nbsp;</td></tr> <tr><td valign="top"></td><td><a href="a.gif">a.gif</a> </td><td align="right">2004-
11-20 15:16 </td><td align="right">246 </td><td>&nbsp;</td></tr> <tr><td valig
...
```

Issue 1 of 1

[Medium] Directory Listing

Issue:	85756360
Severity:	Medium
URL:	https://wolf.cci.emory.edu/icons/small/
Path:	small/
Risk(s):	It is possible to view and download the contents of certain web application virtual directories, which might contain restricted files
Fix:	Modify the server configuration to deny directory listing, and install the latest security patches available

Variant 1 of 1

The following changes were applied to the original request:

```
Set path to '/icons/small/'
```

Reasoning:

The response contains the content of a directory (directory listing). This indicates that the server allows the listing of directories, which is not usually recommended.

Request/Response:

```
GET /icons/small/ HTTP/1.1
Cookie: ga=GA1.2.1900723985.1464902423
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: wolf.cci.emory.edu
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
```

```
HTTP/1.1 200 OK
Date: Tue, 07 Jun 2016 20:20:09 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16
Transfer-Encoding: chunked
Content-Type: text/html; charset=ISO-8859-1
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"> <html> <head> <title> Index of /
icons/small</title> </head> <body> <h1> Index of / icons/small</h1> <table> <tr><th
valign="top"></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"></td><td><a href="/icons/"> Parent Directory </a> </td><td>&nbsp;</td><td
align="right"> - </td><td>&nbsp;</td></tr> <tr><td valign="top"></td><td><a href="back.gif">back.gif</a> </td><td align="right">2004-11-20 15:16
</td><td align="right">129 </td><td>&nbsp;</td></tr> <tr><td va
```

```
...
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"> <html> <head> <title> Index of /
icons/small</title> </head> <body> <h1> Index of / icons/small</h1> <table> <tr><th
valign="top"></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"></td><td><a href="/icons/"> Parent Directory </a> </td><td>&nbsp;</td><td
align="right"> - </td><td>&nbsp;</td></tr> <tr><td valign="top"></td><td><a href="back.gif">back.gif</a> </td><td align="right">2004-11-20 15:16
</td><td align="right">129 </td><td>&nbsp;</td></tr> <tr><td va
```

```
...
```

[Medium] <https://wolf.cci.emory.edu/qa> - 1 issue(s)

Issue 1 of 1

[Medium] Deprecated SSL Version is Supported

Issue:	97411900
Severity:	Medium
URL:	https://wolf.cci.emory.edu/qa
Path:	wolf.cci.emory.edu
Risk(s):	It is possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Fix:	Use a different signature algorithm for the certificate

Variant 1 of 1

Reasoning:

AppScan discovered that the server supports a deprecated SSL version (either SSLv2 or SSLv3)

Request/Response:

```
GET /qa HTTP/1.1
Cookie: ga=GA1.2.1900723985.1464902423
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: wolf.cci.emory.edu
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
```

```
HTTP/1.1 301 Moved Permanently
Date: Tue, 07 Jun 2016 20:08:50 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16
Location: https://wolf.cci.emory.edu/qa/
Content-Length: 238
Content-Type: text/html; charset=iso-8859-1
```

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"> <html><head> <title>301 Moved Permanently</title> </head><body> <h1>Moved Permanently</h1> <p>The document has moved <a href="https://wolf.cci.emory.edu/qa/">here</a>.</p> </body></html>
```

```
GET /qa/ HTTP/1.1
Cookie: ga=GA1.2.1900723985.1464902423
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://wolf.cci.emory.edu/qa
Host: wolf.cci.emory.edu
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
```

```
HTTP/1.1 200 OK
Date: Tue, 07 Jun 2016 20:08:50
...
```

Remediation Tasks by Severity

[Medium] <http://wolf.cci.emory.edu/icons/> - 1 issue(s)

Remediation Tasks	Addressed Security Issues
Modify the server configuration to deny directory listing, and install the latest security patches available (Medium) Path: icons/	Directory Listing

[Medium] <http://wolf.cci.emory.edu/icons/small/> - 1 issue(s)

Remediation Tasks	Addressed Security Issues
Modify the server configuration to deny directory listing, and install the latest security patches available (Medium) Path: small/	Directory Listing

[Medium] <https://wolf.cci.emory.edu/datascope/> - 1 issue(s)

Remediation Tasks	Addressed Security Issues
Add the 'Secure' attribute to all sensitive cookies (Medium) Cookie: connect.sess	Missing Secure Attribute in Encrypted Session (SSL) Cookie

[Medium] <https://wolf.cci.emory.edu/icons/> - 1 issue(s)

Remediation Tasks	Addressed Security Issues
Modify the server configuration to deny directory listing, and install the latest security patches available (Medium) Path: icons/	Directory Listing

[Medium] <https://wolf.cci.emory.edu/icons/small/> - 1 issue(s)

Remediation Tasks	Addressed Security Issues
Modify the server configuration to deny directory listing, and install the latest security patches available (Medium) Path: small/	Directory Listing

[Medium] <https://wolf.cci.emory.edu/qa> - 1 issue(s)

Remediation Tasks	Addressed Security Issues
Use a different signature algorithm for the certificate (Medium) Path: wolf.cci.emory.edu	Deprecated SSL Version is Supported

Advisories and Fix Recommendations

Missing Secure Attribute in Encrypted Session (SSL) Cookie

Application

WASC Threat Classification

Information Leakage
<http://projects.webappsec.org/Information-Leakage>

Security Risks

It may be possible to steal user and session information (cookies) that was sent during an encrypted session

Possible Causes

The web application sends non-secure cookies over SSL

Technical Description

During the application test, it was detected that the tested web application set a cookie without the "secure" attribute, during an encrypted session. Since this cookie does not contain the "secure" attribute, it might also be sent to the site during an unencrypted session. Any information such as cookies, session tokens or user credentials that are sent to the server as clear text, may be stolen and used later for identity theft or user impersonation.

In addition, several privacy regulations state that sensitive information such as user credentials will always be sent encrypted to the web site

Fix Recommendation - General

Basically the only required attribute for the cookie is the "name" field. Common optional attributes are: "comment", "domain", "path", etc.

The "secure" attribute must be set accordingly in order to prevent to cookie from being sent unencrypted.

RFC 2965 states:

"The Secure attribute (with no value) directs the user agent to use only (unspecified) secure means to contact the origin server whenever it sends back this cookie, to protect the confidentiality and authenticity of the information in the cookie."

For further reference please see the HTTP State Management Mechanism RFC 2965 at:

<http://www.ietf.org/rfc/rfc2965.txt>

and for "Best current practice" for use of HTTP State Management please see

<http://tools.ietf.org/html/rfc2964>

References and Relevant Links

[Financial Privacy: The Gramm-Leach Bliley Act](#)
[Health Insurance Portability and Accountability Act \(HIPAA\)](#)
[Sarbanes-Oxley Act](#)
[California SB1386](#)

Directory Listing

Infrastructure

WASC Threat Classification

Directory Indexing
<http://projects.webappsec.org/Directory-Indexing>

Security Risks

It is possible to view and download the contents of certain web application virtual directories, which might contain restricted files

Possible Causes

Directory browsing is enabled

Technical Description

Web servers are usually configured to disallow listings of directories containing scripts and textual contents. However, if the web server was configured improperly, it is possible to retrieve a directory listing by sending a request for a specific directory, rather than for a file. Example request for a directory listing of the directory named "some_dir" :
`http://TARGET/some_dir/`

Another possible way to acquire directory listing is by exploiting specific issues in web servers and web applications, such as URL Trickery attacks, or malformed HTTP requests, which force the web server to return a directory listing. These security breaches should be solved by downloading a patch from your application or server vendor.

In some web servers running on Win32 operating systems, the access control may be bypassed by using short filenames (8.3 DOS format).
For example, the directory `/longdirname/` is denied browsing by the web-server, but its DOS 8.3 equivalent name `/LONGDI~1/` may be open to browsing.

Note: The directory listing is used by an attacker to locate files in the web directories that are not normally exposed through links on the web site. Configuration files and other components of web applications that potentially contain sensitive information can be viewed this way.

Fix Recommendation - General

- [1] Configure the web server to deny listing of directories.
- [2] Download a specific security patch according to the issue existing on your web server or web application. Some of the known directory listing issues are listed in the "References" field of this advisory.
- [3] A Workaround from the "CERT" advisory found in the "References" field of this advisory, to fix the short filenames (8.3 DOS format) problem:
 - a. Use only 8.3-compliant short file names for the files that you want to have protected solely by the web server. On FAT file systems (16-bit) this can be enforced by enabling (setting to 1) the "Win31FileSystem" registry key (registry path: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem`).
 - b. On NTFS (32-bit), you can disable the creation of the 8.3-compliant short file name for files with long file names by enabling (setting to 1) the "NtfsDisable8dot3NameCreation" registry key (registry path: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem`). However, this step may cause compatibility problems with 16-bit applications.
 - c. Use NTFS-based ACLs (directory or file level access control lists) to augment or replace web server-based security.

References and Relevant Links

[Apache directory listing \(CAN-2001-0729\)](#)
[Microsoft IIS 5.0+WebDav support - directory listing](#)
[Jrun directory listing](#)
[CERT Advisory CA-98.04](#)

Deprecated SSL Version is Supported

Infrastructure

WASC Threat Classification

Server Misconfiguration

<http://projects.webappsec.org/Server-Misconfiguration>

Security Risks

It is possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Possible Causes

The web server or application server are configured in an insecure way

Technical Description

The server supports SSL cipher suites that either do not offer encryption or use weak encryption algorithms. An attacker may therefore be able to decrypt the secure communication between the client and the server, or successfully execute a "man-in-the-middle" attack on the client, enabling him to view sensitive information and perform actions on behalf of the client.

Fix Recommendation - General

Reconfigure the server to avoid the use of weak cipher suites. The configuration changes are server-specific.

For Microsoft Windows XP and Microsoft Windows Server 2003, follow these instructions:

<http://support.microsoft.com/kb/245030>

For Microsoft Windows Vista, Microsoft Windows 7, and Microsoft Windows Server 2008, remove the cipher suites that were identified as weak from the Supported Cipher Suite list by following these instructions:

[http://msdn.microsoft.com/en-us/library/windows/desktop/bb870930\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/bb870930(v=vs.85).aspx)

For Apache TomCat server, follow these instructions:

https://www.owasp.org/index.php/Talk:Securing_tomcat#Disabling_weak_ciphers_in_Tomcat

For Apache server, modify (or add) the SSLCipherSuite directive in the httpd.conf or ssl.conf file:

" SSLCipherSuite HIGH:MEDIUM:!MD5!EXP:!NULL:!LOW:!ADH " (without quotation marks). For more information please visit:

http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslciphersuite

References and Relevant Links

IBM customers are responsible for ensuring their own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws.