Apache and ModSecurity: Supplement

# Notes & References

Table 14-1. Default included version of Apache and OpenSSL, by Linux distribution.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Distribution | Apache | OpenSSL |  | Distribution | Apache | OpenSSL |
| CentOS |  |  |  | 15 | 2.2.22 | 1.0.1c |
| 7.4.1708 | 2.4.6-67 | 1.0.2k-8 |  | 14 | 2.2.22 | 1.0.1c |
| 7.3.1611 | 2.4.6-45 | 1.0.1e-60 |  | 13 | 2.2.22 | 1.0.1 |
| 7.2.1511 | 2.4.6-40 | 1.0.1e-42 |  | 12 | 2.2.20 | 1.0.0e |
| 7.1.1503 | 2.4.6-31 | 1.0.1e-42 |  | 11 | 2.2.17 | 0.9.8o |
| 7.0.1406 | 2.4.6-17 | 1.0.1e-34 |  | OpenSuSE |  |  |
| 6.8 | 2.2.15-53 | 1.0.1e-48 |  | 42.3 | 2.4.23 | 1.0.2j |
| 6.7 | 2.2.15-45 | 1.0.1e-42 |  | 42.2 | 2.4.23 | 1.0.2j |
| 6.6 | 2.2.15-39 | 1.0.1e-30 |  | 42.1 | 2.4.16 | 1.0.1i |
| 6.5 | 2.2.15-29 | 1.0.1e |  | 13.2 | 2.4.10 | 1.0.1i |
| 6.4 | 2.2.15-26 | 1.0.0-27 |  | 13.1 | 2.4.6 | 1.0.1e |
| 6.3 | 2.2.15-15 | 1.0.0-20 |  | 12.3 | 2.2.22 | 1.0.1e |
| 6.2 | 2.2.15-15 | 1.0.0-20 |  | 12.2 | 2.2.22 | 1.0.1c |
| 6.1 | 2.2.15-9 | 1.0.0-10 |  | 12.1 | 2.2.21 | 1.0.0e |
| 6.0 | 2.2.15-5 | 1.0.0-4 |  | 11.4 | 2.2.17 | 1.0.0c |
| 5.11 | 2.2.3-91 | 0.9.8e-27 |  | Ubuntu |  |  |
| 5.10 | 2.2.3-82 | 0.9.8e-26 |  | 17.10 | 2.4.27 | 1.0.2g |
| 5.9 | 2.2.3-74 | 0.9.8e-22 |  | 17.04 | 2.4.25 | 1.0.2g |
| 5.8 | 2.2.3-63 | 0.9.8e-22 |  | 16.10 | 2.4.18 | 1.0.2g |
| 5.7 | 2.2.3-53 | 0.9.8e-20 |  | 16.04 | 2.4.18 | 1.0.2g |
| 5.6 | 2.2.3-45 | 0.9.8e-12 |  | 15.10 | 2.4.12 | 1.0.2d |
| Mint |  |  |  | 15.04 | 2.4.10 | 1.0.1f |
| 18.3 | 2.4.18 | 1.0.2g |  | 14.10 | 2.4.10 | 1.0.1f |
| 18.2 | 2.4.18 | 1.0.2g |  | 14.04 | 2.4.7 | 1.0.1f |
| 18.1 | 2.4.18 | 1.0.2g |  | 13.10 | 2.4.6 | 1.0.1e |
| 18 | 2.4.18 | 1.0.2g |  | 13.04 | 2.2.22 | 1.0.1c |
| 17.2 | 2.4.7 | 1.0.1f |  | 12.10 | 2.2.22 | 1.0.1c |
| 17.2 | 2.4.7 | 1.0.1f |  | 12.04 | 2.2.22 | 1.0.1 |
| 17.1 | 2.4.7 | 1.0.1f |  | 11.10 | 2.2.20 | 1.0.0e |
| 17 | 2.4.7 | 1.0.1f |  | 11.04 | 2.2.17 | 0.9.8o |
| 16 | 2.4.6 | 1.0.1e |  |  |  |  |

The HTTP status code registry at <http://www.iana.org/assignments/http-status-codes/http-status-codes.xhtml> lists the various HTTP status codes, including providing references to the defining RFC.

Table 14-2. HTTP Status Codes.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 100 | Continue | 307 | Temporary Redirect | 421 | Misdirected Request |
| 101 | Switching Protocols | 308 | Permanent Redirect | 422 | Unprocessable Entity |
| 102 | Processing | 400 | Bad Request | 423 | Locked |
| 103 | Early Hints | 401 | Unauthorized | 424 | Failed Dependency |
| 200 | OK | 402 | Payment Required | 426 | Upgrade Required |
| 201 | Created | 403 | Forbidden | 428 | Precondition Required |
| 202 | Accepted | 404 | Not Found | 429 | Too Many Requests |
| 203 | Non-Authoritative Information | 405 | Method Not Allowed | 431 | Request Header Fields Too Large |
| 204 | No Content | 406 | Not Acceptable | 500 | Internal Server Error |
| 205 | Reset Content | 407 | Proxy Authentication Required | 501 | Not Implemented |
| 206 | Partial Content | 408 | Request Timeout | 502 | Bad Gateway |
| 207 | Multi-Status | 409 | Conflict | 503 | Service Unavailable |
| 208 | Already Reported | 410 | Gone | 504 | Gateway Timeout |
| 226 | IM Used | 411 | Length Required | 505 | HTTP Version Not Supported |
| 300 | Multiple Choices | 412 | Precondition Failed | 506 | Variant Also Negotiates |
| 301 | Moved Permanently | 413 | Payload Too Large | 507 | Insufficient Storage |
| 302 | Found | 414 | URI Too Long | 508 | Loop Detected |
| 303 | See Other | 415 | Unsupported Media Type | 510 | Not Extended |
| 304 | Not Modified | 416 | Range Not Satisfiable | 511 | Network Authentication Required |
| 305 | Use Proxy | 417 | Expectation Failed | |  |

## Checklist: Building an SSL/TLS Site

To help the reader, here is a checklist of the key steps described in the text to build an SSL/TLS web site.

* Ensure that mod\_ssl is installed

CentOS: Use yum to install mod\_ssl

OpenSuSE: Check APACHE\_SERVER\_FLAGS in /etc/sysconfig/apache2

Mint/Ubuntu: Run the command sudo a2enmod ssl

* Verify that the SSL module is loaded in Apache with a LoadModule directive.

CentOS 5/6: /etc/httpd/conf.d/ssl.conf

CentOS 7: /etc/httpd/conf.modules.d/00-ssl.conf

OpenSuSE: /etc/apache2/ssl-global.conf

Mint/Ubuntu: /etc/apache2/mods-enabled/ssl.load

* Choose the SSL protocol and cipher suite using <https://mozilla.github.io/server-side-tls/ssl-config-generator/> or manually.
* Ensure that SSLProtocol and SSLCipherSuite have the chosen values. This may occur inside a VirtualHost directive (CentOS) or outside (OpenSuSE, Mint, Ubuntu). Set the SSLHonorCipherOrder directive if desired.

CentOS: /etc/httpd/conf.d/ssl.conf

OpenSuSE: /etc/apache2/ssl-global.conf

Mint/Ubuntu: /etc/apache2/mods-enabled/ssl.conf

* Verify that the Listen directive is configured so that Apache is listening on TCP/443. Be sure that proper port in the firewall is opened.

CentOS: /etc/httpd/conf.d/ssl.conf

OpenSuSE: /etc/apache2/listen.conf

Mint/Ubuntu: /etc/apache2/ports.conf

* Verify that there is a virtual host for the SSL/TLS protected site.

CentOS: /etc/httpd/conf.d/ssl.conf

OpenSuSE: Copy /etc/apache2/vhosts.d/vhost-ssl.template to /etc/apache2/vhosts.d/vhost-ssl.conf. Not necessary on OpenSuSE 12.2, 12.3, 13.1, and 13.2.

Mint/Ubuntu: Run sudo a2ensite default-ssl, and check either /etc/apache2/sites-available/default-ssl.conf (Ubuntu ≥ 13.10; Mint ≥ 16) or /etc/apache2/sites-available/default-ssl (Ubuntu ≤ 13.04; Mint ≤ 15)

* Configure the virtual host used for SSL/TLS. This can include ServerAdmin, ServerName, DocumentRoot, CGI scripting directory, and logging for this virtual host. The directive SSLEngine on must be present. If a custom DocumentRoot is used, provide an appropriate Directory directive that allows Apache access to the directory.

CentOS: /etc/httpd/conf.d/ssl.conf

OpenSuSE: /etc/apache2/vhosts.d/vhost-ssl.conf, though this file may need to be copied from a template first.

Mint/Ubuntu: Either /etc/apache2/sites-available/default-ssl.conf (Ubuntu ≥ 13.10; Mint ≥ 16) or /etc/apache2/sites-available/default (Ubuntu ≤ 13.04; Mint ≤ 15)

* Create a private key for the server using openssl. Store the result

CentOS: /etc/pki/tls/private

Ubuntu, Mint: /etc/ssl/private

OpenSuSE: /etc/apache2/ssl.key

* Either create a self-signed certificate, or create a certificate signing request and have the certificate signed. Store the resulting certificate.

CentOS: /etc/pki/tls/certs

Ubuntu, Mint: /etc/ssl/certs

OpenSuSE: /etc/apache2/ssl.crt

* Provide the location of the SSLCertificateKeyFile and the SSLCertificateFile to Apache.

CentOS: /etc/httpd/conf.d/ssl.conf

OpenSuSE: /etc/apache2/vhosts.d/vhost-ssl.conf, though this file may need to be copied from a template first.

Mint/Ubuntu: Either /etc/apache2/sites-available/default-ssl.conf (Ubuntu ≥ 13.10; Mint ≥ 16) or /etc/apache2/sites-available/default (Ubuntu ≤ 13.04; Mint ≤ 15)

When these steps are completed, the administrator can restart the Apache service and begin running a TLS/SSL protected site.

Exercises

1. What is wget? Use it to download a web page.
2. What is curl? Use it to download a web page.
3. Is the program web.cgi (Listing 14-7) vulnerable to a cross site scripting attack? If so, how?
4. Change the values of the Apache directives ServerTokens and ServerSignature. What are the security implications?
5. Use the ErrorDocument directive to change the page returned by the server for a 404 error.
6. What happens when a client makes a request of a server by IP address rather than name if the server is running ModSecurity with the OWASP CRS?