WebTesting of 192:168:0:103

SSL SECURITY TESTING - WEB APPLICATION of 192.168.0.103

SCAN COMMANDS USED:

ssl_3_0_cipher_suites

session_resumption

tls_1_2_cipher_suites

tls_fallback_scsv

ssl_2_0_cipher_suites

certificate_info

heartbleed

session_renegotiation

tls_compression

robot

tls_1_3_cipher_suites

openssl_ccs_injection

tls_1_0_cipher_suites

tls_1_1_cipher_suites

HEARTBLEED VULN:

False

OPENSSL CCS INJECTION VULN:

False

ROBOT VULN:

NOT_VULNERABLE_NO_ORACLE

SSL 2.0 probing results:

Accepted ciphers:7

Rejected cipher suites:0

SSL 3.0 probing results:

Accepted ciphers:15

Rejected cipher suites:65

TLS1.0 probing results:

Accepted ciphers:15

Rejected cipher suites:65

TLS1.1 probing results:

Accepted ciphers:0

Rejected cipher suites:80

TLS1.2 probing results:

Accepted ciphers:0

Rejected cipher suites:158

TLS1.3 probing results:

Accepted ciphers:0

Rejected cipher suites:5

RESULT:

cipher suite supported:DHE-RSA-AES256-SHA

client auth requirement:DISABLED

highest tls version supported:TLS_1_0

CURRENT STABLE TLS VERSION IN INTERNET IS TLS 1.2 or 1.3 - anything below that is deprecated and prone to attacks

for more details perform a manual scan using: sslyze --regular 192.168.0.103

GOBUSTER SCAN

http://192.168.0.103/.svn/entries : Status: 200

http://192.168.0.103/.svn : Status: 200

http://192.168.0.103/config : Status: 200

http://192.168.0.103/docs : Status: 200

http://192.168.0.103/external : Status: 200

http://192.168.0.103/favicon.ico : Status: 200

http://192.168.0.103/index.php : Status: 200

http://192.168.0.103/php.ini : Status: 200

http://192.168.0.103/phpinfo.php : Status: 200

http://192.168.0.103/phpmyadmin : Status: 200

http://192.168.0.103/robots.txt : Status: 200

http://192.168.0.103/server-status : Status: 200

http://192.168.0.103/server-info : Status: 200

- Nikto v2.1.6/2.1.5

+ Target Host: 192.168.0.103

+ Target Port: 80

+ GET Cookie PHPSESSID created without the httponly flag

+ GET Cookie security created without the httponly flag

+ GET Retrieved x-powered-by header: PHP/5.3.1

+ GET The anti-clickjacking X-Frame-Options header is not present.

+ GET The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ GET The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ GET Server may leak inodes via ETags, header found with file /robots.txt, inode: 2402, size: 26, mtime: Tue Aug 24 19:45:32 2010

+ GET Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698

+ HEAD Apache/2.2.14 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.

+ HEAD Perl/v5.10.1 appears to be outdated (current is at least v5.20.0)

+ HEAD mod_apreq2-20090110/2.7.1 appears to be outdated (current is at least 2.8.0)

+ HEAD PHP/5.3.1 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.

+ HEAD mod_ssl/2.2.14 appears to be outdated (current is at least 2.8.31) (may depend on server version)

+ HEAD OpenSSL/0.9.8l appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.

+ HEAD mod_perl/2.0.4 appears to be outdated (current is at least 2.0.8)

+ OSVDB-877: TRACE HTTP TRACE method is active, suggesting the host is vulnerable to XST

+ GET mod_ssl/2.2.14 OpenSSL/0.9.8l PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1 - mod_ssl 2.8.7 and lower are vulnerable to a remo

+ OSVDB-112004: GET /cgi-bin/printenv: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6271).

+ OSVDB-112004: GET /cgi-bin/printenv: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-3268: GET /config/: Directory indexing found.

+ GET /config/: Configuration information may be available remotely.

+ OSVDB-12184: GET /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that cont

+ OSVDB-12184: GET /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that conta

+ OSVDB-12184: GET /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that conta

+ OSVDB-12184: GET /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that conta

+ OSVDB-561: GET /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources.

+ OSVDB-3092: GET /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

+ OSVDB-3092: GET /phpmyadmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

+ OSVDB-3233: GET /cgi-bin/printenv: Apache 2.0 default script is executable and gives server environment variables. All default scripts should be removed. It

+ OSVDB-3233: GET /cgi-bin/test-cgi: Apache 2.0 default script is executable and reveals system information. All default scripts should be removed.

+ OSVDB-3268: GET /icons/: Directory indexing found.

+ OSVDB-3268: GET /docs/: Directory indexing found.

+ OSVDB-3092: GET /CHANGELOG.txt: A changelog was found.

+ OSVDB-3233: GET /icons/README: Apache default file found.

+ GET /login.php: Admin login page/section found.

+ GET /phpmyadmin/: phpMyAdmin directory found

+ OSVDB-3092: GET /.svn/entries: Subversion Entries file may contain directory listing information.

+ OSVDB-3092: GET /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hos

+ GET /CHANGELOG.txt: Version number implies that there is a SQL Injection in Drupal 7, can be used for authentication bypass (Drupageddon: see https://w

+ OSVDB-3092: GET /phpmyadmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.