Find

5 issues

Verify

Address: Good, Domain: Good, Phone: Good

Advisories

0 for review

Prevent

0MB saved bandwidth, 0.01MB total bandwidth, 3 saved requests, 2,362 total requests

Find

5 issues

Application Scan (5)

Scan Date: October 31st, 2016

High (0)

No details found

Medium (1)

Web Server HTTP Header Information Disclosure
Port: 80 **Service:** www

Synopsis: The remote web server discloses information via HTTP headers.

Description: The HTTP headers sent by the remote web server disclose information that can aid an attacker, such as the server version and languages used by the web server.

Solution: Modify the HTTP headers of the web server to not disclose detailed information about the

underlying web server.

Technical Details:

```
Server type     : NGINX
Server version  : 1.10.2
Source          : nginx/1.10.2
```

Low (4)

HTTP X-Content-Security-Policy Response Header Usage
Port: 80 **Service:** www

Synopsis: The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description: The remote web server in some responses sets a permissive Content-Security-Policy (CSP) response header or does not set one at all.

The CSP header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

Solution: Set a properly configured Content-Security-Policy header for all requested resources.

Technical Details:

```
The following pages do not set a Content-Security-Policy response header
or set a permissive policy:

  - http://box3112.bluehost.com/
  - http://box3112.bluehost.com//
```

HTTP X-Frame-Options Response Header Usage
Port: 80 **Service:** www

Synopsis: The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description: The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking

attacks and is currently supported by all major browser vendors

Solution: Set a properly configured X-Frame-Options header for all requested resources.

Technical Details:

```
The following pages do not set a X-Frame-Options response header or set a
permissive policy:

  - http://box3112.bluehost.com/
  - http://box3112.bluehost.com//
```

HTTP Methods Allowed (per directory)
Port: 80 **Service:** www

Synopsis: This plugin determines which HTTP methods are allowed on various CGI directories.

Description: By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Solution: n/a

Technical Details:

```
 Based on the response to an OPTIONS request :

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
    //
    /icons


Based on tests of each method :

  - HTTP methods ACL BCOPY BDELETE BMOVE BPROPFIND BPROPPATCH CHECKIN
    CHECKOUT COPY DEBUG DELETE GET HEAD INDEX LABEL LOCK MERGE
    MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS ORDERPATCH PATCH
    POLL POST PROPFIND PROPPA . . .
. . . SEE DASHBOARD FOR FULL DETAILS . . .
```

Web Server Directory Enumeration
Port: 80 **Service:** www

Synopsis: It is possible to enumerate directories on the web server.

Description: This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

Solution: n/a

Technical Details:

```
The following directories were discovered:
/cgi-sys, /CVS, /icons, //

While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
```

Exclusions (0)

No details found

Malware Scan (0)

Scan Date: December 3rd, 2016

Pages Scanned	Links Checked	Malware Found	Malware Links	Status
431	876	0	0	success

SQL Injection Scan (0)

Scan Date: December 6th, 2016

XSS Scan (0)

Scan Date: December 6th, 2016

Verify

Address: Good, Domain: Good, Phone: Good

Address Verification

Address name verified on October 5th, 2016

Phone Verification

Phone name verified on October 5th, 2016

Domain Verification

Domain name verified on February 8th, 2016

- end -
