Fix

Pending

Find

4 issues

Advisories

0 for review

Verify

Domain: Good

Find

4 issues

Application Scan (4)

Scan Date: June 29th, 2016

High (0)

No details found

Medium (0)

No details found

Low (4)

HyperText Transfer Protocol (HTTP) Information
Port: 80 **Service:** proxy

Synopsis: Some information about the remote HTTP configuration can be extracted.

Description: This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution: n/a

Technical Details:

```
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Date: Wed, 29 Jun 2016 11:07:29 GMT
  Server: Apache
  X-Powered-By: PHP/7.0.7
  Location: http://www.eslam.nu/
  Vary: Accept-Encoding
  Content-Length: 0
  Content-Type: text/html; charset=UTF-8
  X-Varnish: 87132252
  Age: 0
  Via: 1.1 varnish-v4
  Connection: keep-alive
```

Web Server robots.txt Information Disclosure
Port: 80 **Service:** proxy

Synopsis: The remote web server contains a 'robots.txt' file.

Description: The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

Solution: Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Technical Details:

```
 Contents of robots.txt :

User-agent: *
```

```
Disallow: /wp-admin/
Allow: /wp-admin/admin-ajax.php
```

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

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 BASELINE-CONTROL 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 PR . . .
. . . SEE DASHBOARD FOR FULL DETAILS . . .
```

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

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-bin, /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: June 29th, 2016

Pages Scanned	Links Checked	Malware Found	Malware Links	Status
501	919	0	0	success

SQL Injection Scan (0)

Scan Date: July 2nd, 2016

XSS Scan (0)

Scan Date: July 2nd, 2016

Fix

Pending

SMART requires configuration to help fix malware on your site

Verify

Domain: Good

Domain Verification

Domain name verified on June 29th, 2016

- end -
