HTTP Methods Allowed (per directory)

Description

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

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticated Users' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

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

Reference

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Output

Based on tests of each method:

- HTTP methods ACL CHECKOUT COPY DELETE GET HEAD LOCK MERGE

  MKACTIVITY MKCOL MOVE NOTIFY OPTIONS PATCH POST PROPFIND

  PROPPATCH PUT REPORT SEARCH SUBSCRIBE UNLOCK UNSUBSCRIBE

  Are allowed on:

  /

Hosts

80 / tcp / www

beta4.digitallocker.gov.in

Based on tests of each method:

- HTTP method ACL is allowed on:

  /signin

- HTTP methods ACL CHECKOUT COPY DELETE GET HEAD LOCK MERGE

  MKACTIVITY MKCOL MOVE NOTIFY OPTIONS PATCH POST PROPFIND

  PROPPATCH PUT REPORT SEARCH SUBSCRIBE are allowed on :

  /signup

  /system

- HTTP methods ACL CHECKOUT COPY DELETE GET HEAD LOCK MERGE

  MKACTIVITY MKCOL MOVE NOTIFY OPTIONS PATCH POST PROPFIND

  PROPPATCH PUT REPORT SEARCH SUBSCRIBE UNLOCK UNSUBSCRIBE

  Are allowed on:

  /

- HTTP methods ACL CHECKOUT DELETE GET HEAD LOCK MERGE MKACTIVITY

  MKCOL NOTIFY OPTIONS PATCH POST PROPFIND PROPPATCH PUT REPORT

  Are allowed on:

  /application

Hosts

443 / tcp / www

beta4.digitallocker.gov.in

Hypertext Transfer Protocol (HTTP) Redirect Information

Description

The remote web server issues an HTTP redirect when requesting the root directory of the web server.

Solution

Analyse the redirect(s) to verify that this is valid operation for your web server and/or application.

Output

Request : http://beta4.digitallocker.gov.in/

HTTP response : HTTP/1.1 301 Moved Permanently

Redirect to : https://beta4.digitallocker.gov.in/

Redirect type : 30x redirect

Hosts

80 / tcp / www

beta4.digitallocker.gov.in