Brief Summary

…

Some errors cannot be provoked, but attackers can use search engines to locate the errors that disclose information on any site or in a specific site using the search engine filtering tools as described in [[https://www.owasp.org/index.php/Testing:_Search_engine_discovery/reconnaissance_(OWASP-IG-002) “4.2.1 Conduct Search Engine Discovery and Reconnaissance for Information Leakage (OTG-INFO-001)“]

Web Server Errors

…

Other HTTP response codes such as 400 Bad Request, 405 Method Not Allowed, 501 Method Not Implemented, 408 Request Time-out and 505 HTTP Version Not Supported can be forced by an attacker. When sending crafted requests, web servers provide one of these error codes depending on their HTTP implementation.

Disclosed information in the Web Server errors is related to the information disclosed in the HTTP headers as described in the section [https://www.owasp.org/index.php/Fingerprint_Web_Server_(OTG-INFO-002) Fingerprint Web Server (OTG-INFO-002)].

Application Server Errors

Application errors are those that are caused by server application in two different levels: errors generated by the server-side scripting language, such as PHP, ASP or JSP, or errors generated by the application hosted in the server. Applications can be expressly created for the site or packaged applications such as Wordpress, Drupal or PhpBB.

Application server errors usually provide information of server paths, installed libraries and version of the applications.

Database Errors

Database errors are those returned by the Database System when there is a problem with the query or the connection. Each Database system, such as MySQL, Oracle or MSSQL, has their own set of errors. Those errors can provide sensible information such as Database server IPs, tables, columns and login details.

Error Handling in Apache

Apache is a common HTTP server for serving HTML and PHP web pages. By default, Apache shows the server version, products installed and OS system in the HTTP error responses.

Responses to the errors can be configured and customized globally, per site or per directory in the apache2.conf using the ErrorDocument directive [2]

<pre>
ErrorDocument 404 “Customized Not Found error message”
ErrorDocument 403 /myerrorpagefor403.html
ErrorDocument 501 http://www.externaldomain.com/errorpagefor501.html
</pre>

Site administrators are able to manage their own errors using .htaccess file if the global directive AllowOverride is configured properly in apache2.conf [3]

The information shown by Apache in the HTTP errors can also be configured using the directives ServerTokens [4] and ServerSignature [5] at apache2.conf configuration file. “ServerSignature Off” (On by default) removes the server information from the error responses, while ServerTokens [ProductOnly|Major|Minor|Minimal|OS|Full] (Full by default) defines what information has to be shown in the error pages.

Error Handling in Tomcat

Tomcat is a HTTP server to host JSP and Java Servlet applications. By default, Tomcat shows the server version in the HTTP error responses.

Customization of the error responses can be configured in the configuration file web.xml.

<pre>
<error-page>
<error-code>404</error-code>
<location>/myerrorpagefor404.html</location>
</error-page>
</pre>

Black Box Testing and example

'''Test: 404 Not Found'''

<pre>
telnet <host target> 80
GET /<wrong page> HTTP/1.1
host: <host target>
<CRLF><CRLF>
</pre>

'''Result:'''

<pre>

```
        HTTP/1.1 404 Not Found
        Date: Sat, 04 Nov 2006 15:26:48 GMT
        Server: Apache/2.2.3 (Unix) mod_ssl/2.2.3 OpenSSL/0.9.7g
        Content-Length: 310
        Connection: close
        Content-Type: text/html; charset=iso-8859-1
        ...
        <title>404 Not Found</title>
        ...
        <address>Apache/2.2.3 (Unix) mod_ssl/2.2.3 OpenSSL/0.9.7g at <host target> Port
        80</address>
        ...
</pre>
```

'''Test: 400 Bad Request'''

```
<pre>
        telnet <host target> 80
        GET / HTTP/1.1
        <CRLF><CRLF>
</pre>
'''Result:'''
<pre>
        HTTP/1.1 400 Bad Request
        Date: Fri, 06 Dec 2013 23:57:53 GMT
        Server: Apache/2.2.22 (Ubuntu) PHP/5.3.10-1ubuntu3.9 with Suhosin-Patch
        Vary: Accept-Encoding
        Content-Length: 301
        Connection: close
        Content-Type: text/html; charset=iso-8859-1
        ...
        <title>400 Bad Request</title>
        ...
        <address>Apache/2.2.22 (Ubuntu) PHP/5.3.10-1ubuntu3.9 with Suhosin-Patch at 127.0.1.1 Port
        80</address>
        ...
</pre>
```

'''Test: 405 Method Not Allowed'''

```
<pre>
        telnet <host target> 80
        PUT /index.html HTTP/1.1
        Host: <host target>
```

<CRLF><CRLF>
</pre>
'''Result:'''
<pre>
HTTP/1.1 405 Method Not Allowed
Date: Fri, 07 Dec 2013 00:48:57 GMT
Server: Apache/2.2.22 (Ubuntu) PHP/5.3.10-1ubuntu3.9 with Suhosin-Patch
Allow: GET, HEAD, POST, OPTIONS
Vary: Accept-Encoding
Content-Length: 315
Connection: close
Content-Type: text/html; charset=iso-8859-1
...
<title>405 Method Not Allowed</title>
...
<address>Apache/2.2.22 (Ubuntu) PHP/5.3.10-1ubuntu3.9 with Suhosin-Patch at <host target>
Port 80</address>
...
</pre>

'''Test: 408 Request Time-out'''
<pre>
telnet <host target> 80
GET / HTTP/1.1
- Wait X seconds – (Depending on the target server, 21 seconds for Apache by default)
</pre>
'''Result:'''
<pre>
HTTP/1.1 408 Request Time-out
Date: Fri, 07 Dec 2013 00:58:33 GMT
Server: Apache/2.2.22 (Ubuntu) PHP/5.3.10-1ubuntu3.9 with Suhosin-Patch
Vary: Accept-Encoding
Content-Length: 298
Connection: close
Content-Type: text/html; charset=iso-8859-1
...
<title>408 Request Time-out</title>
...
<address>Apache/2.2.22 (Ubuntu) PHP/5.3.10-1ubuntu3.9 with Suhosin-Patch at <host target>
Port 80</address>
...
</pre>

'''Test: 501 Method Not Implemented'''

<pre>
telnet <host target> 80
RENAME /index.html HTTP/1.1
Host: <host target>
<CRLF><CRLF>
</pre>

'''Result:'''

<pre>
HTTP/1.1 501 Method Not Implemented
Date: Fri, 08 Dec 2013 09:59:32 GMT
Server: Apache/2.2.22 (Ubuntu) PHP/5.3.10-1ubuntu3.9 with Suhosin-Patch
Allow: GET, HEAD, POST, OPTIONS
Vary: Accept-Encoding
Content-Length: 299
Connection: close
Content-Type: text/html; charset=iso-8859-1
...
<title>501 Method Not Implemented</title>
...
<address>Apache/2.2.22 (Ubuntu) PHP/5.3.10-1ubuntu3.9 with Suhosin-Patch at <host target>
Port 80</address>
...
</pre>

Tools

Error

* [1] ErrorMint - http://sourceforge.net/projects/errormint/

References

* [2] [[http://httpd.apache.org/docs/2.2/mod/core.html#errordocument ErrorDocument]] Apache ErrorDocument Directive

* [3] [[http://httpd.apache.org/docs/2.2/mod/core.html#allowoverride AllowOverride]] Apache AllowOverride Directive

* [4] [[http://httpd.apache.org/docs/2.2/mod/core.html#servertokens ServerTokens]] Apache ServerTokens Directive

* [5] [[http://httpd.apache.org/docs/2.2/mod/core.html#serversignature ServerSignature]] Apache ServerSignature Directive