nemasis

Nemasis DA Report

http://php.testsparker.com/process.php

Scan Summary

Vulnerability Rating:

High:	12
Medium:	5
Low:	25
Informational:	12

Scan Info:

Scan Date: Aug 28 2019 12:26 PM

Result Overview:

Insecure Component - Apache 2.2.8

Description:
Based on passive analysis of the response, insecure component Apache 2.2.8 appears to be in use. The highest noted CVSS rating for this product version is 10. In total, 31 vulnerabilities were noted. Some Linux distributions such as Red Hat employ the practice of retaining old version numbers when security fixes are "backported". These cases are noted as "False Positives", but should be manually verified.

Solution:
Upgrade from Apache 2.2.8 to the latest stable version of the product. Use a package manager and package management policies and procedures to manage the installed versions of software packages.

References:
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2010-0425
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2011-3192
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2013-2249
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2009-1890
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2009-1891
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2012-0883
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2009-3555
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2013-1862
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2007-6750
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2008-2364
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2009-2699
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2010-0408
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2010-1452
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2011-3368
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2013-6438
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2014-0098
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2009-1195
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2012-0031
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2011-3607
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2008-2939
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2010-0434
http://www cvedetails com/cve-details php?cve id=CVE-2011-0419

http://www.cvedetails.com/cve-details.php?cve_id=CVE-2011-3348
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2011-3639
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2011-4317
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2012-0053
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2012-3499
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2012-4558
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2013-1896
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2012-2687
http://www.cvedetails.com/cve-details.php?cve_id=CVE-2011-4415

Url	Parameter	Evidence
/		Apache/2.2.8 (Win32) PHP/5.2.6
/?file=Generics/contact.nsp		Apache/2.2.8 (Win32) PHP/5.2.6
/?file=Generics/index.nsp		Apache/2.2.8 (Win32) PHP/5.2.6
/?file=Generics/about.nsp		Apache/2.2.8 (Win32) PHP/5.2.6

X-Frame-Options Header Not Set

Description:
X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.

Solution:
Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).

References:
http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx

Url	Parameter	Evidence
/?file=Generics/contact.nsp	X-Frame-Options	
/?file=Generics/index.nsp	X-Frame-Options	
/?file=Generics/about.nsp	X-Frame-Options	
/	X-Frame-Options	

Application Error Disclosure

Description:
This page contains an error/warning message that may disclose sensitive information like the location of

the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.

Solution:
Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user.

References:

Url	Parameter	Evidence
/?file=Generics/about.nsp		**Warning**: mysql_connect() [function.mysql-connect]: Access denied for user 'root'@'localhost' (using password: YES) in **C:\AppServ\www\Generics\about.nsp** on line **31**

Web Browser XSS Protection Not Enabled

Description:
Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server

Solution:
Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.

References:
https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet
https://www.veracode.com/blog/2014/03/guidelines-for-setting-security-headers/

Url	Parameter	Evidence
/?file=Generics/contact.nsp	X-XSS-Protection	
/?file=Generics/index.nsp	X-XSS-Protection	
/	X-XSS-Protection	
/?file=Generics/about.nsp	X-XSS-Protection	

X-Content-Type-Options Header Missing

Description:
The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

Solution:
Ensure that the application/web server sets the Content-Type header appropriately and that it sets the X-

Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.

References:
http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx
https://www.owasp.org/index.php/List_of_useful_HTTP_headers

Url	Parameter	Evidence
/?file=Generics/contact.nsp	X-Content-Type-Options	
/?file=Generics/about.nsp	X-Content-Type-Options	
/	X-Content-Type-Options	
/?file=Generics/index.nsp	X-Content-Type-Options	

Information Disclosure - Debug Error Messages

Description:
The response appeared to contain common error messages returned by platforms such as ASP.NET, and Web-servers such as IIS and Apache. You can configure the list of common debug messages.

Solution:
Disable debugging messages before pushing to production.

References:

Url	Parameter	Evidence
/?file=Generics/about.nsp		Access denied for user

Server Leaks Version Information via "Server" HTTP Response Header Field

Description:
The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Solution:
Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

References:
http://httpd.apache.org/docs/current/mod/core.html#servertokens
http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

Url	Parameter	Evidence
/?file=Generics/contact.nsp		Apache/2.2.8 (Win32) PHP/5.2.6
/?file=Generics/index.nsp		Apache/2.2.8 (Win32) PHP/5.2.6
/?file=Generics/about.nsp		Apache/2.2.8 (Win32) PHP/5.2.6
/		Apache/2.2.8 (Win32) PHP/5.2.6

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Description:
The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

Solution:
Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.

References:
http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

Url	Parameter	Evidence
/?file=Generics/about.nsp		X-Powered-By: PHP/5.2.6
/		X-Powered-By: PHP/5.2.6
/?file=Generics/contact.nsp		X-Powered-By: PHP/5.2.6
/?file=Generics/index.nsp		X-Powered-By: PHP/5.2.6

Content Security Policy (CSP) Header Not Set

Description:
Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page â€” covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Solution:
Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+.

References:
https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://www.owasp.org/index.php/Content_Security_Policy
http://www.w3.org/TR/CSP/
http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html
http://www.html5rocks.com/en/tutorials/security/content-security-policy/
http://caniuse.com/#feat=contentsecuritypolicy
http://content-security-policy.com/

Url	Parameter	Evidence
/?file=Generics/about.nsp		
/?file=Generics/contact.nsp		
/?file=Generics/index.nsp		
/		

Feature Policy Header Not Set

Description:
Feature Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Feature Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.

Solution:
Ensure that your web server, application server, load balancer, etc. is configured to set the Feature-Policy header.

References:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy
https://developers.google.com/web/updates/2018/06/feature-policy
https://scotthelme.co.uk/a-new-security-header-feature-policy/
https://w3c.github.io/webappsec-feature-policy/
https://www.smashingmagazine.com/2018/12/feature-policy/

Url	Parameter	Evidence
/?file=Generics/contact.nsp		
/		
/?file=Generics/index.nsp		
/?file=Generics/about.nsp		