Website Vulnerability Scanner Report

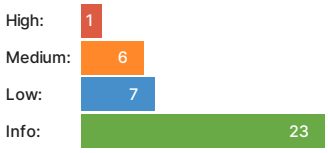
✔ http://demo.pentest-tools.com/webapp/

Summary

Overall risk level:

High

Risk ratings:



Scan information:

Start time:	2021-06-24 14:49:44 UTC+03
Finish time:	2021-06-24 14:55:42 UTC+03
Scan duration:	5 min, 58 sec
Tests performed:	37/37
Scan status:	Finished

Findings

Vulnerabilities found for server-side software

Risk Level	CVSS	CVE	Summary	Exploit	Affected software
●	7.5	CVE-2017-3167	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.	N/A	http_server 2.4.10
●	7.5	CVE-2017-3169	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.	N/A	http_server 2.4.10
●	7.5	CVE-2017-7668	The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.	N/A	http_server 2.4.10
●	7.5	CVE-2017-7679	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.	N/A	http_server 2.4.10
●	7.5	CVE-2021-26691	In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow	N/A	http_server 2.4.10

Details

Risk description:
These vulnerabilities expose the affected applications to the risk of unauthorized access to confidential data and possibly to denial of service attacks. An attacker could search for an appropriate exploit (or create one himself) for any of these vulnerabilities and use it to attack the system.

Recommendation:
We recommend you to upgrade the affected software to the latest version in order to eliminate the risk of these vulnerabilities.

Classification:
CWE : CWE-1026
OWASP Top 10 - 2013 : A9 - Using Components with Known Vulnerabilities
OWASP Top 10 - 2017 : A9 - Using Components with Known Vulnerabilities

Communication is not secure

URL	Evidence
http://demo.pentest-tools.com/webapp/	Communication is made over unsecure, unencrypted HTTP.

Details

Risk description:
The communication between the web browser and the server is done using the HTTP protocol, which transmits data unencrypted over the network. Thus, an attacker who manages to intercept the communication at the network level, is able to read and modify the data transmitted (including passwords, secret tokens, credit card information and other sensitive data).

Recommendation:
We recommend you to reconfigure the web server to use HTTPS - which encrypts the communication between the web browser and the server.

Classification:
CWE : CWE-311
OWASP Top 10 - 2013 : A6 - Sensitive Data Exposure
OWASP Top 10 - 2017 : A3 - Sensitive Data Exposure

Outdated JavaScript libraries

Affected Component	Vulnerability	Risk	CVE	Details	Evidence
Bootstrap 3.0.2	XSS in data-template, data-content and data-title properties of tooltip/popover	Medium	CVE-2019-8331	https://github.com/twbs/bootstrap/issues/28236	http://demo.pentest-tools.com/webapp/assets/js/bootstrap.min.js
Bootstrap 3.0.2	XSS in data-target property of scrollspy	Medium	CVE-2018-14041	https://github.com/twbs/bootstrap/issues/20184	http://demo.pentest-tools.com/webapp/assets/js/bootstrap.min.js
Bootstrap 3.0.2	XSS in collapse data-parent attribute	Medium	CVE-2018-14040	https://github.com/twbs/bootstrap/issues/20184	http://demo.pentest-tools.com/webapp/assets/js/bootstrap.min.js
Bootstrap 3.0.2	XSS in data-container property of tooltip	Medium	CVE-2018-14042	https://github.com/twbs/bootstrap/issues/20184	http://demo.pentest-tools.com/webapp/assets/js/bootstrap.min.js
Jquery 1.10.2	3rd party CORS request may execute	Medium	CVE-2015-9251	https://github.com/jquery/jquery/issues/2432 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ https://nvd.nist.gov/vuln/detail/CVE-2015-9251 http://research.insecurelabs.org/jquery/test/	https://code.jquery.com/jquery-1.10.2.min.js
Jquery 1.10.2	parseHTML() executes scripts in event handlers	Medium	CVE-2015-9251	https://bugs.jquery.com/ticket/11974 https://nvd.nist.gov/vuln/detail/CVE-2015-9251 http://research.insecurelabs.org/jquery/test/	https://code.jquery.com/jquery-1.10.2.min.js
Jquery 1.10.2	jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution	Medium	CVE-2019-11358	https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b	https://code.jquery.com/jquery-1.10.2.min.js
Jquery 1.10.2	Regex in its jQuery.htmlPrefilter sometimes may introduce XSS	Medium	CVE-2020-11022	https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/	https://code.jquery.com/jquery-1.10.2.min.js

Jquery 1.10.2	Regex in its jQuery.htmlPrefilter sometimes may introduce XSS	Medium	CVE-2020-11023	https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/	https://code.jquery.com/jquery-1.10.2.min.js
Jquery 2.0.2	3rd party CORS request may execute	Medium	CVE-2015-9251	https://github.com/jquery/jquery/issues/2432 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ https://nvd.nist.gov/vuln/detail/CVE-2015-9251 http://research.insecurelabs.org/jquery/test/	http://demo.pentest-tools.com/webapp/static/smartadmin1.4.1/js/libs/jquery-2.0.2.min.js
Jquery 2.0.2	parseHTML() executes scripts in event handlers	Medium	CVE-2015-9251	https://bugs.jquery.com/ticket/11974 https://nvd.nist.gov/vuln/detail/CVE-2015-9251 http://research.insecurelabs.org/jquery/test/	http://demo.pentest-tools.com/webapp/static/smartadmin1.4.1/js/libs/jquery-2.0.2.min.js
Jquery 2.0.2	jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution	Medium	CVE-2019-11358	https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b	http://demo.pentest-tools.com/webapp/static/smartadmin1.4.1/js/libs/jquery-2.0.2.min.js
Jquery 2.0.2	Regex in its jQuery.htmlPrefilter sometimes may introduce XSS	Medium	CVE-2020-11022	https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/	http://demo.pentest-tools.com/webapp/static/smartadmin1.4.1/js/libs/jquery-2.0.2.min.js
Jquery 2.0.2	Regex in its jQuery.htmlPrefilter sometimes may introduce XSS	Medium	CVE-2020-11023	https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/	http://demo.pentest-tools.com/webapp/static/smartadmin1.4.1/js/libs/jquery-2.0.2.min.js

Details

Risk description:
We found that the target application uses one or more outdated JavaScript libraries. The vulnerabilities which affect these libraries could be exploited in certain circumstances in order affect the confidentiality and integrity of the application data. Please read the details of each CVE in order to understand their specific impact on your application.

Recommendation:
We recommend you to upgrade the affected JavaScript libraries to their latest versions.

Classification:
CWE : CWE-1026
OWASP Top 10 - 2013 : A9 - Using Components with Known Vulnerabilities
OWASP Top 10 - 2017 : A9 - Using Components with Known Vulnerabilities

Sensitive files found

URL
/webapp/backup.tgz

Details

Risk description:
These files can contain confidential information such as: application source code, configuration files, SSL certificates, etc. Manual review is required for the contents of these files.

Recommendation:
We recommend removing these files from the website directory if they are not needed for business purposes.

Classification:

CWE : CWE-200
OWASP Top 10 - 2013 : A6 - Sensitive Data Exposure
OWASP Top 10 - 2017 : A3 - Sensitive Data Exposure

Interesting files found

URL	Summary
/webapp/CHANGELOG.txt	A changelog was found.
/webapp/INSTALL.txt	Default file found.
/webapp/README.TXT	This might be interesting...
/webapp/admin/	This might be interesting...
/webapp/admin/home.php	Admin login page/section found.
/webapp/admin/index.html	Admin login page/section found.
/webapp/debug.php	Possible debug directory/program found.
/webapp/logs/	This might be interesting...
/webapp/test.php	This might be interesting...
/webapp/.git/HEAD	Git HEAD file found. Full repo details may be present.
/webapp/.git/config	Git config file found. Infos about repo details may be present.
/webapp/.git/index	Git Index file may contain directory listing information.
/webapp/setup.sql	Setup SQL file found.
/webapp/static/	Directory indexing found.

Details

Risk description:
These files/folders usually contain sensitive information which may help attackers to mount further attacks against the server. Manual validation is required.

Recommendation:
We recommend you to analyze if the mentioned files/folders contain any sensitive information and restrict their access according to the business purposes of the application.

Classification:
CWE : CWE-200
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Information disclosure

URL	Summary
/webapp/test.php	PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.

Details

Risk description:
An attacker could use these files to find information about the backend application, server software and their specific versions. This information could be further used to mount targeted attacks against the server.

Recommendation:
We recommend you to remove these scripts if they are not needed for business purposes.

More information about this issue:
http://projects.webappsec.org/w/page/13246936/Information%20Leakage

Classification:
CWE : CWE-200

OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Directory listing is enabled

URL
http://demo.pentest-tools.com/webapp/assets/
http://demo.pentest-tools.com/webapp/assets/css/
http://demo.pentest-tools.com/webapp/assets/fonts/
http://demo.pentest-tools.com/webapp/assets/img/
http://demo.pentest-tools.com/webapp/assets/img/clients/
http://demo.pentest-tools.com/webapp/assets/img/portfolio/
http://demo.pentest-tools.com/webapp/assets/img/process/
http://demo.pentest-tools.com/webapp/assets/img/sp/
http://demo.pentest-tools.com/webapp/assets/img/team/
http://demo.pentest-tools.com/webapp/assets/js/
http://demo.pentest-tools.com/webapp/static/
http://demo.pentest-tools.com/webapp/static/smartadmin1.4.1/
http://demo.pentest-tools.com/webapp/static/smartadmin1.4.1/js/
http://demo.pentest-tools.com/webapp/static/smartadmin1.4.1/js/libs/

Details

Risk description:
An attacker can see the entire structure of files and subdirectories from the affected URL. It is often the case that sensitive files are "hidden" among public files in that location and attackers can use this vulnerability to access them.

Recommendation:
We recommend reconfiguring the web server in order to deny directory listing. Furthermore, you should verify that there are no sensitive files at the mentioned URLs.

More information about this issue:
http://projects.webappsec.org/w/page/13246922/Directory%20Indexing.

Classification:
CWE : CWE-548
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Missing security header: Content-Security-Policy

URL	Evidence
http://demo.pentest-tools.com/webapp/	Response headers do not include the HTTP Content-Security-Policy security header

Details

Risk description:
The Content-Security-Policy (CSP) header activates a protection mechanism implemented in web browsers which prevents exploitation of Cross-Site Scripting vulnerabilities (XSS). If the target application is vulnerable to XSS, lack of this header makes it easily exploitable by attackers.

Recommendation:
Configure the Content-Security-Header to be sent with each HTTP response in order to apply the specific policies needed by the application.

Read more about CSP:

https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

Classification:
CWE : CWE-693
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Missing security header: X-Frame-Options

URL	Evidence
http://demo.pentest-tools.com/webapp/	Response headers do not include the HTTP X-Frame-Options security header

Details

Risk description:
Because the X-Frame-Options header is not sent by the server, an attacker could embed this website into an iframe of a third party website. By manipulating the display attributes of the iframe, the attacker could trick the user into performing mouse clicks in the application, thus performing activities without user's consent (ex: delete user, subscribe to newsletter, etc). This is called a Clickjacking attack and it is described in detail here:
https://owasp.org/www-community/attacks/Clickjacking

Recommendation:
We recommend you to add the X-Frame-Options HTTP header with the values DENY or SAMEORIGIN to every page that you want to be protected against Clickjacking attacks.

More information about this issue:
https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

Classification:
CWE : CWE-693
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Missing security header: X-XSS-Protection

URL	Evidence
http://demo.pentest-tools.com/webapp/	Response headers do not include the HTTP X-XSS-Protection security header

Details

Risk description:
The X-XSS-Protection HTTP header instructs the browser to stop loading web pages when they detect reflected Cross-Site Scripting (XSS) attacks. Lack of this header exposes application users to XSS attacks in case the web application contains such vulnerability.

Recommendation:
We recommend setting the X-XSS-Protection header to X-XSS-Protection: 1; mode=block .

More information about this issue:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection

Classification:
CWE : CWE-693
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Missing security header: X-Content-Type-Options

URL	Evidence
http://demo.pentest-tools.com/webapp/	Response headers do not include the X-Content-Type-Options HTTP security header

Details

Risk description:
The HTTP header X-Content-Type-Options is addressed to the Internet Explorer browser and prevents it from reinterpreting the content of a

web page (MIME-sniffing) and thus overriding the value of the Content-Type header). Lack of this header could lead to attacks such as Cross-Site Scripting or phishing.

Recommendation:
We recommend setting the X-Content-Type-Options header such as `X-Content-Type-Options: nosniff`.

More information about this issue:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options.

Classification:
CWE : CWE-693
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Missing security header: Referrer-Policy

URL	Evidence
http://demo.pentest-tools.com/webapp/	Response headers do not include the Referrer-Policy HTTP security header

Details

Risk description:
The Referrer-Policy HTTP header controls how much referrer information the browser will send with each request originated from the current web application.
For instance, if a user visits the web page "http://example.com/pricing/" and it clicks on a link from that page going to e.g. "https://www.google.com", the browser will send to Google the full originating URL in the `Referer` header, assuming the Referrer-Policy header is not set. The originating URL could be considered sensitive information and it could be used for user tracking.

Recommendation:
The Referrer-Policy header should be configured on the server side to avoid user tracking and inadvertent information leakage. The value `no-referrer` of this header instructs the browser to omit the Referer header entirely.

Read more:
https://developer.mozilla.org/en-US/docs/Web/Security/Referer_header:_privacy_and_security_concerns

Classification:
CWE : CWE-693
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Exposure of Sensitive Information

Method	URL	Parameters	Evidence
GET	http://demo.pentest-tools.com/webapp/		Email Address: hello@linkagency.com

Details

Risk description:
This application does not properly prevent a person's private, personal information from being accessed by actors who either (1) are not explicitly authorized to access the information or (2) do not have the implicit consent of the person about whom the information is collected.

Recommendation:
Compartmentalize the application to have "safe" areas where trust boundaries can be unambiguously drawn. Do not allow sensitive data to go outside of the trust boundary and always be careful when interfacing with a compartment outside of the safe area.

Server software and technology found

Software / Version	Category
Debian	Operating Systems
Apache 2.4.10	Web Servers
Twitter Bootstrap	Web Frameworks

Font Awesome	Font Scripts
Google Font API	Font Scripts
Modernizr	JavaScript Frameworks
jQuery 1.10.2	JavaScript Frameworks

Details

Risk description:
An attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:
We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

More information about this issue:
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server.html.

Screenshot:

Classification:
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Website is accessible.

Nothing was found for client access policies.

Nothing was found for robots.txt file.

Nothing was found for use of untrusted certificates.

Nothing was found for administration consoles.

Nothing was found for software identification.

Spider results

Method	URL	Parameters
GET	http://demo.pentest-tools.com/webapp/	
GET	http://demo.pentest-tools.com/webapp/about.html	
GET	http://demo.pentest-tools.com/webapp/assets	
GET	http://demo.pentest-tools.com/webapp/assets/css	
GET	http://demo.pentest-tools.com/webapp/assets/fonts	
GET	http://demo.pentest-tools.com/webapp/assets/ico/	
GET	http://demo.pentest-tools.com/webapp/assets/img/	
GET	http://demo.pentest-tools.com/webapp/assets/img/clients	
GET	http://demo.pentest-tools.com/webapp/assets/img/portfolio	
GET	http://demo.pentest-tools.com/webapp/assets/js	
GET	http://demo.pentest-tools.com/webapp/portfolio.html	
GET	http://demo.pentest-tools.com/webapp/services.html	
GET	http://demo.pentest-tools.com/webapp/singleproject.html	
GET	http://demo.pentest-tools.com/webapp/static	

Nothing was found for SQL Injection.

Nothing was found for Cross-Site Scripting.

Nothing was found for OS Command Injection.

Nothing was found for File Inclusion.

Nothing was found for domain too loose set for cookies.

Nothing was found for code comments.

Nothing was found for debug messages.

Nothing was found for missing HTTP header - Strict-Transport-Security.

Nothing was found for login interfaces.

Nothing was found for Secure flag of cookie.

Nothing was found for secure password submission.

Nothing was found for mixed content between HTTP and HTTPS.

Nothing was found for cross domain file inclusion.

Nothing was found for passwords submitted unencrypted.

Nothing was found for error messages.

Nothing was found for HttpOnly flag of cookie.

Scan coverage information

List of tests performed (37/37)

- Checking for website accessibility...
- Checking for secure communication...
- Checking for missing HTTP header - Content Security Policy...
- Checking for missing HTTP header - X-Frame-Options...
- Checking for missing HTTP header - X-XSS-Protection...
- Checking for missing HTTP header - X-Content-Type-Options...
- Checking for missing HTTP header - Referrer...
- Checking for sensitive data...
- Checking for website technologies...
- Checking for vulnerabilities of server-side software...
- Checking for client access policies...
- Checking for robots.txt file...
- Checking for outdated JavaScript libraries...
- Checking for use of untrusted certificates...
- Checking for sensitive files...
- Checking for interesting files... (this might take a few hours)
- Checking for information disclosure... (this might take a few hours)
- Checking for administration consoles...
- Checking for software identification...
- Spidering target...
- Checking for directory listing...
- Checking for SQL Injection...
- Checking for Cross-Site Scripting...
- Checking for OS Command Injection...
- Checking for File Inclusion...
- Checking for domain too loose set for cookies...
- Checking for code comments...
- Checking for debug messages...
- Checking for missing HTTP header - Strict-Transport-Security...
- Checking for login interfaces...
- Checking for Secure flag of cookie...
- Checking for secure password submission...
- Checking for mixed content between HTTP and HTTPS...
- Checking for cross domain file inclusion...
- Checking for passwords submitted unencrypted...
- Checking for error messages...
- Checking for HttpOnly flag of cookie...

Scan parameters

Website URL:	http://demo.pentest-tools.com/webapp/
Scan type:	Ptt_engine
Authentication:	False
Fingerprint Website:	True
Server Software Vulnerabilities:	True
Robots.txt:	True
JavaScript libraries:	True
SSL/TLS Certificates:	True
Client access policies:	True
Resource Discovery:	True
Approach:	Classic
Depth:	10
XSS:	True

SQL Injection:	True
Local File Inclusion:	True
OS Command Injection:	True
Security Headers:	True
Cookie Security:	True
Directory Listing:	True
Secure Communication:	True
Weak Password Submission Method:	True
Commented code/Error codes:	True
Clear Text Submission of Credentials:	True
Verify Domain Sources:	True
Mixed Encryptions Content:	True
Sensitive Data Crawl:	True
Find Login Interfaces:	True

Scan stats

URLs spidered:	42
Total number of HTTP request errors:	0
Total number of HTTP requests:	1340
Unique Injection Points Detected:	14