Pentest-Tools.com

Website Vulnerability Scanner Report (Light)

Unlock the full capabilities of this scanner

See what the FULL scanner can do

Perform in-depth website scanning and discover high risk vulnerabilities.

Testing areas	Light scan	Full scan
Website fingerprinting	✓	✓
Version-based vulnerability detection	✓	✓
Common configuration issues	✓	✓
SQL injection	✗	✓
Cross-Site Scripting	✗	✓
Local/Remote File Inclusion	✗	✓
Remote command execution	✗	✓
Discovery of sensitive files	✗	✓

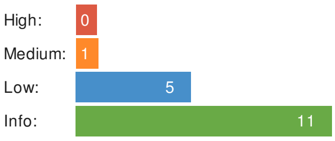
✓ http://demo.owasp-juice.shop

Summary

Overall risk level:

Medium

Risk ratings:



Scan information:

Start time:	2021-05-07 12:32:08 UTC+03
Finish time:	2021-05-07 12:32:26 UTC+03
Scan duration:	18 sec
Tests performed:	17/17
Scan status:	Finished

Findings

Communication is not secure

URL	Evidence
http://demo.owasp-juice.shop	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.

Missing security header: Content-Security-Policy

URL	Evidence
http://demo.owasp-juice.shop	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

Missing security header: X-XSS-Protection

URL	Evidence
http://demo.owasp-juice.shop	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

Missing security header: Referrer-Policy

URL	Evidence
http://demo.owasp-juice.shop	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

Server software and technology found

Software / Version	Category
Cowboy	Web Frameworks, Web Servers

webpack	Build CI Systems
jQuery 2.2.4	JavaScript Frameworks

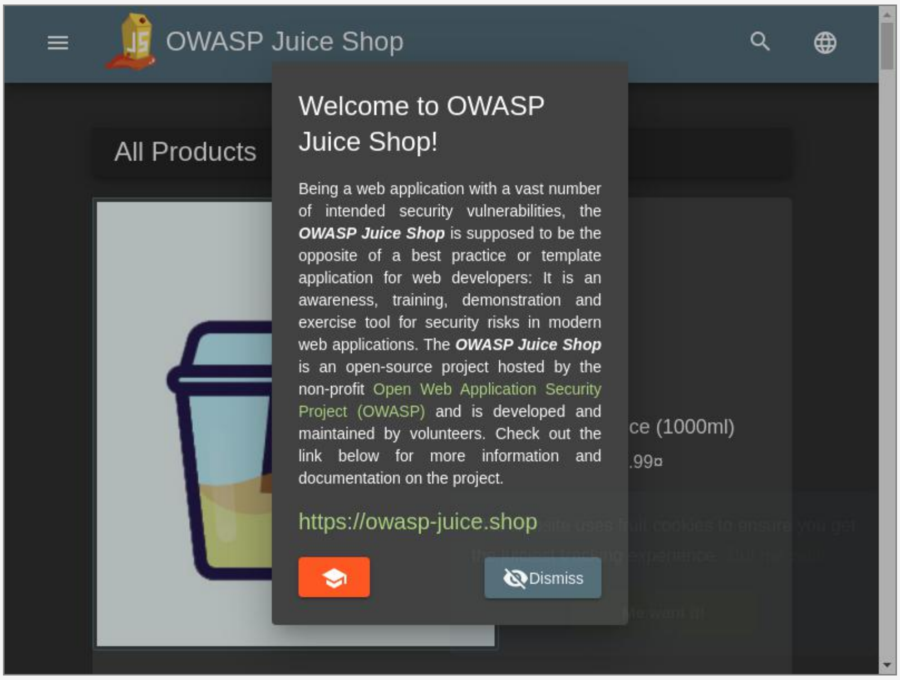
Details

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:



Welcome to OWASP Juice Shop!

Being a web application with a vast number of intended security vulnerabilities, the ***OWASP Juice Shop*** is supposed to be the opposite of a best practice or template application for web developers: It is an awareness, training, demonstration and exercise tool for security risks in modern web applications. The ***OWASP Juice Shop*** is an open-source project hosted by the non-profit Open Web Application Security Project (OWASP) and is developed and maintained by volunteers. Check out the link below for more information and documentation on the project.

https://owasp-juice.shop

Robots.txt file found

http://demo.owasp-juice.shop/robots.txt

Details

Risk description:
There is no particular security risk in having a robots.txt file. However, this file is often misused by website administrators to try to hide some web pages from the users. This should not be considered a security measure because these URLs can be easily read directly from the robots.txt file.

Recommendation:
We recommend you to manually review the entries from robots.txt and remove the ones which lead to sensitive locations in the website (ex. administration panels, configuration files, etc).

More information about this issue:
https://www.theregister.co.uk/2015/05/19/robotstxt/

Website is accessible.

Nothing was found for vulnerabilities of server-side software.

Nothing was found for client access policies.

Nothing was found for use of untrusted certificates.

Nothing was found for domain too loose set for cookies.

Nothing was found for missing HTTP header - X-Frame-Options.

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

Nothing was found for Secure flag of cookie.

Nothing was found for directory listing.

Nothing was found for missing HTTP header - X-Content-Type-Options.

Nothing was found for HttpOnly flag of cookie.

Scan coverage information

List of tests performed (17/17)

- ✓ Checking for website accessibility...
- ✓ Checking for secure communication...
- ✓ Checking for missing HTTP header - Content Security Policy...
- ✓ Checking for missing HTTP header - X-XSS-Protection...
- ✓ Checking for missing HTTP header - Referrer...
- ✓ Checking for website technologies...
- ✓ Checking for vulnerabilities of server-side software...
- ✓ Checking for client access policies...
- ✓ Checking for robots.txt file...
- ✓ Checking for use of untrusted certificates...
- ✓ Checking for domain too loose set for cookies...
- ✓ Checking for missing HTTP header - X-Frame-Options...
- ✓ Checking for missing HTTP header - Strict-Transport-Security...
- ✓ Checking for Secure flag of cookie...
- ✓ Checking for directory listing...
- ✓ Checking for missing HTTP header - X-Content-Type-Options...
- ✓ Checking for HttpOnly flag of cookie...

Scan parameters

Website URL:	http://demo.owasp-juice.shop
Scan type:	Light
Authentication:	False