Website Vulnerability Scanner Report (Light)

Unlock the full capabilities of this scanner

See what the DEEP scanner can do

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

Testing areas	Light scan	Deep 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	–	✓

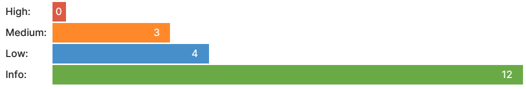
✓ **https://shop.spacex.com/**

The Light Website Scanner didn't check for critical issues like SQLi, XSS, Command Injection, XXE, etc. Upgrade to run Deep scans with 40+ tests and detect more vulnerabilities.

Summary

Overall risk level:
Medium

Risk ratings:



Scan information:

Start time:	Jul 19, 2024 / 02:56:32
Finish time:	Jul 19, 2024 / 02:57:10
Scan duration:	38 sec
Tests performed:	19/19
Scan status:	Finished

Findings

Insecure cookie setting: domain too loose

CONFIRMED

URL	Cookie Name	Evidence
https://shop.spacex.com/	_cmp_a	Set-Cookie: .spacex.com Request / Response

Details

Risk description:
The risk is that a cookie set for example.com may be sent along with the requests sent to dev.example.com, calendar.example.com, hostedsite.example.com. Potentially risky websites under your main domain may access those cookies and use the victim session from the main site.

Recommendation:
The `Domain` attribute should be set to the origin host to limit the scope to that particular server. For example if the application resides on server app.mysite.com, then it should be set to `Domain=app.mysite.com`

Classification:
CWE : CWE-614
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Insecure cookie setting: missing Secure flag

CONFIRMED

URL	Cookie Name	Evidence

https://shop.spacex.com/	_cmp_a	Set-Cookie: secure_customer_sig=; path=/; expires=Fri, 18 Jul 2025 23:56:34 GMT; secure; HttpOnly; SameSite=Lax, localization=US; path=/; expires=Fri, 18 Jul 2025 23:56:34 GMT, cart_currency=USD; p
		_tracking_consent=%7B%22con%22%3A%7B%22CMP%22%3A%7B%22a%22%3A%22%22%2C%22m%22%3A%22%22%2C%22p%22%3A%22%22%2C%22s%22%3A%22%22%7D%7D%2C%22v%22%3A%2
		domain=spacex.com; path=/; expires=Fri, 18 Jul 2025 23:56:34 GMT; SameSite=Lax,
		_cmp_a=%7B%22purposes%22%3A%7B%22p%22%3Afalse%2C%22a%22%3Afalse%2C%22m%22%3Afalse%2C%22t%22%3Atrue%7D%2C%22display_banner%22%3Atrue%2C%22sale_of_data_region%22
		SameSite=Lax, _shopify_y=; Expires=Thu, 01 Jan 1970 00:00:00 GMT; Max-Age=0; Domain=spacex.com; Path=/; SameSite=Lax, _shopify_s=; Expires=Thu, 01 Jan 1970 00:00:00 GMT; Max-Age=0; Domai
		Request / Response

Details

Risk description:
The risk exists that an attacker will intercept the clear-text communication between the browser and the server and he will steal the cookie of the user. If this is a session cookie, the attacker could gain unauthorized access to the victim's web session.

Recommendation:
Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

References:
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html

Classification:
CWE : CWE-614
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Insecure cookie setting: missing HttpOnly flag

CONFIRMED

URL	Cookie Name	Evidence
https://shop.spacex.com/	_cmp_a, _tracking_consent, cart_currency, localization	The server responded with Set-Cookie header(s) that does not specify the HttpOnly flag: Set-Cookie: _cmp_a=%7B%22purposes%22%3A%7B%22p%22%3Afalse%2C%22a%22%3Afalse%2C%22m%22%3Afalse%2C%22t%22%3Atrue%7D%2C%22display_banner%22%3Atrue%2C%22sale_of_data_region%22%3Afalse%7D Set-Cookie: _tracking_consent=%7B%22con%22%3A%7B%22CMP%22%3A%7B%22a%22%3A%22%22%2C%22m%22%3A%22%22%2C%22p%22%3A%22%22%2C%22s%22%3A%22%22%7D%7D%2C%22v%22%3A%222.1%22%2C%22region%22%3A%22GBENG%22%2C%22reg%22%3A%22GDPR%22%7D Set-Cookie: cart_currency=USD Set-Cookie: localization=US Request / Response

Details

Risk description:
The risk is that an attacker who injects malicious JavaScript code on the page (e.g. by using an XSS attack) can access the cookie and can send it to another site. In case of a session cookie, this could lead to session hijacking.

Recommendation:
Ensure that the HttpOnly flag is set for all cookies.

References:
https://owasp.org/www-community/HttpOnly

Classification:
CWE : CWE-1004
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Missing security header: Referrer-Policy

CONFIRMED

URL	Evidence
https://shop.spacex.com/	Response headers do not include the Referrer-Policy HTTP security header as well as the <meta> tag with name 'referrer' is not present in the response. Request / Response

Details

Risk description:
The risk is that if a user visits a web page (e.g. "http://example.com/pricing/") and 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.

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

Classification:
CWE : CWE-693
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Unsafe security header: Content-Security-Policy

CONFIRMED

URL	Evidence

https://shop.spacex.com/	Response headers include the HTTP Content-Security-Policy security header with the following security issues:
	`default-src:  The default-src directive should be set as a fall-back when other restrictions have not been specified.`
	`script-src:  script-src directive is missing.`
	`object-src:  Missing object-src allows the injection of plugins which can execute JavaScript. We recommend setting it to 'none'.`
	`base-uri:  Missing base-uri allows the injection of base tags. They can be used to set the base URL for all relative (script) URLs to an attacker controlled domain. We recommend setting it to 'none' or 'self'.`
	
	Request / Response

Details

Risk description:
For example, if the unsafe-inline directive is present in the CSP header, the execution of inline scripts and event handlers is allowed. This can be exploited by an attacker to execute arbitrary JavaScript code in the context of the vulnerable application.

Recommendation:
Remove the unsafe values from the directives, adopt nonces or hashes for safer inclusion of inline scripts if they are needed, and explicitly define the sources from which scripts, styles, images or other resources can be loaded.

References:
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 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Robots.txt file found

CONFIRMED

URL
https://shop.spacex.com/robots.txt

Details

Risk description:
There is no particular security risk in having a robots.txt file. However, it's important to note that adding endpoints in it should not be considered a security measure, as this file can be directly accessed and read by anyone.

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).

References:
https://www.theregister.co.uk/2015/05/19/robotstxt/

Classification:
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Server software and technology found

UNCONFIRMED

Software / Version	Category
Shopify	Ecommerce
Cloudflare	CDN
Bold Commerce	Personalisation
Google Hosted Libraries	CDN
Flickity	JavaScript libraries
HTTP/3	Miscellaneous
jQuery	JavaScript libraries
Open Graph	Miscellaneous
Priority Hints	Performance
Apple Pay	Payment processors
Obviyo 1.0.0	Shopify apps, Personalisation
HSTS	Security
Cart Functionality	Ecommerce

Details

Risk description:
The risk is that 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.

References:
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server.html

Classification:
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Security.txt file is missing

CONFIRMED

URL
Missing: https://shop.spacex.com/.well-known/security.txt

Details

Risk description:
There is no particular risk in not having a security.txt file for your server. However, this file is important because it offers a designated channel for reporting vulnerabilities and security issues.

Recommendation:
We recommend you to implement the security.txt file according to the standard, in order to allow researchers or users report any security issues they find, improving the defensive mechanisms of your server.

References:
https://securitytxt.org/

Classification:
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

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 enabled HTTP debug methods.

Nothing was found for enabled HTTP OPTIONS method.

Nothing was found for secure communication.

Nothing was found for directory listing.

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

Nothing was found for missing HTTP header - Content Security Policy.

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

Scan coverage information

List of tests performed (19/19)

- ✓ Starting the scan...
- ✓ Checking for domain too loose set for cookies...
- ✓ Checking for missing HTTP header - Referrer...
- ✓ Checking for Secure flag of cookie...
- ✓ Checking for HttpOnly flag of cookie...
- ✓ Checking for unsafe HTTP header Content Security Policy...
- ✓ Checking for website technologies...
- ✓ Checking for vulnerabilities of server-side software...
- ✓ Checking for client access policies...
- ✓ Checking for robots.txt file...
- ✓ Checking for absence of the security.txt file...
- ✓ Checking for use of untrusted certificates...
- ✓ Checking for enabled HTTP debug methods...
- ✓ Checking for enabled HTTP OPTIONS method...
- ✓ Checking for secure communication...
- ✓ Checking for directory listing...
- ✓ Checking for missing HTTP header - Strict-Transport-Security...
- ✓ Checking for missing HTTP header - Content Security Policy...
- ✓ Checking for missing HTTP header - X-Content-Type-Options...

Scan parameters

Target:	https://shop.spacex.com/
Scan type:	Light
Authentication:	False

Scan stats

Unique Injection Points Detected:	91
URLs spidered:	2
Total number of HTTP requests:	11
Average time until a response was received:	86ms