Pentest Tools

# 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 | – | ✓ |

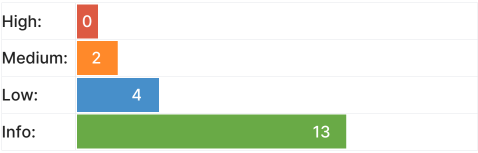
✓ **https://www.shopify.com**

## Summary

**Overall risk level:**

Medium

**Risk ratings:**



**Scan information:**

| | |
|---|---|
| Start time: | 2022-10-17 00:31:18 UTC+03 |
| Finish time: | 2022-10-17 00:31:37 UTC+03 |
| Scan duration: | 19 sec |
| Tests performed: | 19/19 |
| Scan status: | Finished |

## Findings

### Insecure cookie setting: missing HttpOnly flag CONFIRMED

| URL | Cookie Name | Evidence |
|---|---|---|

| | | |
|---|---|---|
| https://www.shopify.com | _shopify_y | Set-Cookie:<br>_shopify_y=77b2a1a6-aa04-478e-9e43-4e74b53783be; domain=.shopify.com; path=/; expires=Mon, 16 Oct 2023 21:31:18 GMT; SameSite=Lax; secure, _shopify_s=ae57c027-e551-4f9e-9ca1-74e7e150ec06; domain=.shopify.com; path=/; expires=Sun, 16 Oct 2022 22:01:18 GMT; SameSite=Lax; secure, _y=77b2a1a6-aa04-478e-9e43-4e74b53783be; domain=.shopify.com; path=/; expires=Mon, 16 Oct 2023 21:31:18 GMT; SameSite=Lax; secure, _s=ae57c027-e551-4f9e-9ca1-74e7e150ec06; domain=.shopify.com; path=/; expires=Sun, 16 Oct 2022 22:01:18 GMT; SameSite=Lax; secure, 0f98ae1fc29391a657457830dda53ca1_assignment=%7B%22group%22%3A%22a6fee7cd8b89ae8f3e5659a4207807e9%22%2C%22created_at%22%3A%222022-10-16T21%3A31%3A18Z%22%7D; path=/; expires=Mon, 17 Apr 2023 12:25:54 GMT; SameSite=Lax; secure, bf07deeb5d94a219a82fc9605f5c1cb4=%7B%22tlt%22%3A%22d41d8cd98f00b204e9800998ecf8427e%22%2C%22er%22%3A%22c34bc8f1eed60edb7d5470200801e334%22%2C%22erd%22%3A%225bbffbec813d46a41d390484d6a870b0%22%2C%22ca%22%3A%222022-10-16T21%3A31%3A18Z%22%7D; path=/; expires=Fri, 16 Dec 2022 21:31:18 GMT; SameSite=Lax; secure |

Details

**Risk description:**
A cookie has been set without the `HttpOnly` flag, which means that it can be accessed by the JavaScript code running inside the web page. If an attacker manages to inject malicious JavaScript code on the page (e.g. by using an XSS attack) then the cookie will be accessible and it can be transmitted 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 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

## Insecure cookie setting: domain too loose CONFIRMED

| URL | Cookie Name | Evidence |
|---|---|---|
| https://www.shopify.com | _s | Set-Cookie:<br>.shopify.com |

Details

**Risk description:**
A cookie may be used in multiple subdomains belonging to the same domain. For instance, 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 on 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 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

## Missing security header: Content-Security-Policy CONFIRMED

| URL | Evidence |
|---|---|
| https://www.shopify.com | 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.

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

## Missing security header: Referrer-Policy CONFIRMED

| URL | Evidence |
|---|---|
| https://www.shopify.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. |

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.

**References:**
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

## Robots.txt file found CONFIRMED

| URL |
|---|
| https://www.shopify.com/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).

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

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

## Server software and technology found UNCONFIRMED

| Software / Version | Category |
|---|---|
| Shopify | Ecommerce |
| Cart Functionality | Ecommerce |
| Cloudflare | CDN |
| webpack | Miscellaneous |
| Tealium | Tag managers, Customer data platform |
| Reddit Ads | Advertising |
| Podsights | Advertising |
| Facebook | Widgets |
| Twitter Ads | Advertising |
| Pinterest Conversion Tag | Analytics |
| Microsoft Clarity | Analytics |
| Linkedin Insight Tag | Analytics |
| LazySizes | JavaScript libraries |
| Google Tag Manager | Tag managers |
| Google Remarketing Tag | Retargeting |
| Google Analytics | Analytics |
| Google Ads Conversion Tracking | Analytics |
| Facebook Pixel 2.9.85 | Analytics |
| Dreamdata | Marketing automation, Analytics |
| Datadog | RUM, Analytics |
| core-js 3.25.0 | JavaScript libraries |
| BugSnag | Analytics |
| Microsoft Advertising | Advertising |
| Pinterest Ads | Advertising |

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.

**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 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - 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 absence of the security.txt file.

### Nothing was found for use of untrusted certificates.

### Nothing was found for enabled HTTP debug methods.

### 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 - X-Frame-Options.

### Nothing was found for missing HTTP header - X-XSS-Protection.

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

### Nothing was found for Secure flag of cookie.

## Scan coverage information

**List of tests performed (19/19)**

- ✓ Checking for website accessibility...
- ✓ Checking for missing HTTP header - Content Security Policy...
- ✓ Checking for HttpOnly flag of cookie...
- ✓ Checking for domain too loose set for cookies...
- ✓ 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 absence of the security.txt file...
- ✓ Checking for use of untrusted certificates...
- ✓ Checking for enabled HTTP debug methods...
- ✓ Checking for secure communication...
- ✓ Checking for directory listing...
- ✓ Checking for missing HTTP header - Strict-Transport-Security...
- ✓ 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 Secure flag of cookie...

### Scan parameters

| | |
|---|---|
| Website URL: | https://www.shopify.com |
| Scan type: | Light |
| Authentication: | False |

### Scan stats

| | |
|---|---|
| Unique Injection Points Detected: | 1732 |
| URLs spidered: | 7 |
| Total number of HTTP requests: | 17 |