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 | – | ✓ |

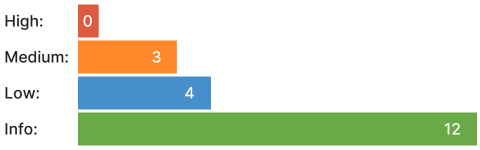
✓ **https://www.investopedia.com**

## Summary

**Overall risk level:**

Medium

**Risk ratings:**



**Scan information:**

| | |
|---|---|
| Start time: | 2023-05-05 18:48:25 UTC+03 |
| Finish time: | 2023-05-05 18:50:42 UTC+03 |
| Scan duration: | 2 min, 17 sec |
| Tests performed: | 19/19 |
| Scan status: | Finished |

## Findings

### Insecure cookie setting: missing HttpOnly flag

CONFIRMED

| URL | Cookie Name | Evidence |
|---|---|---|
| https://www.investopedia.com | Mint, TMog, globalTI_SID | The server responded with Set-Cookie header(s) that does not specify the HttpOnly flag:<br>Set-Cookie: Mint=nd5bd2b779cce41debe78ffc0d09dbce015<br>Set-Cookie: TMog=nd5bd2b779cce41debe78ffc0d09dbce015<br>Set-Cookie: globalTI_SID=a1068a08-06f0-4dfc-a9ca-39e15c859372 |

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.investopedia.com | Mint | Set-Cookie: .investopedia.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

## Insecure cookie setting: missing Secure flag

CONFIRMED

| URL | Cookie Name | Evidence |
|---|---|---|
| https://www.investopedia.com | TMog | Set-Cookie: TMog=nd5bd2b779cce41debe78ffc0d09dbce015; Path=/; Domain=.investopedia.com; Expires=Wed, 23-May-2091 19:02:32 GMT; Max-Age=2147483647, globalTI_SID=a1068a08-06f0-4dfc-a9ca-39e15c859372; Path=/; Domain=.investopedia.com; Expires=Sun, 04-May-2025 15:48:25 GMT; Max-Age=63072000, Mint=nd5bd2b779cce41debe78ffc0d09dbce015; Path=/; Domain=.investopedia.com; Expires=Fri, 05-May-2023 16:18:25 GMT; Max-Age=1800 |

Details

**Risk description:**
Since the `Secure` flag is not set on the cookie, the browser will send it over an unencrypted channel (plain HTTP) if such a request is made. Thus, 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 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

## Missing security header: X-Frame-Options

CONFIRMED

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

**References:**
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

CONFIRMED

| URL | Evidence |
|---|---|
| https://www.investopedia.com | 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` .

**References:**
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

## Robots.txt file found

CONFIRMED

| URL |
|---|
| https://www.investopedia.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 |
|---|---|
| Varnish | Caching |
| OT OneTrust | Cookie compliance |
| Google Tag Manager | Tag managers |
| Google Analytics | Analytics |
| HSTS | Security |

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 - Content Security Policy.

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

Nothing was found for missing HTTP header - Referrer.

## Scan coverage information

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

- ✓ Checking for website accessibility...
- ✓ Checking for HttpOnly flag of cookie...
- ✓ Checking for missing HTTP header - X-Frame-Options...
- ✓ Checking for domain too loose set for cookies...
- ✓ Checking for missing HTTP header - X-XSS-Protection...
- ✓ Checking for Secure flag of cookie...
- ✓ 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 - Content Security Policy...
- ✓ Checking for missing HTTP header - X-Content-Type-Options...
- ✓ Checking for missing HTTP header - Referrer...

### Scan parameters

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

### Scan stats

| | |
|---|---|
| Unique Injection Points Detected: | 532 |
| URLs spidered: | 4 |
| Total number of HTTP requests: | 12 |
| Average time until a response was received: | 117ms |