

# 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://www.citysite.co.in>

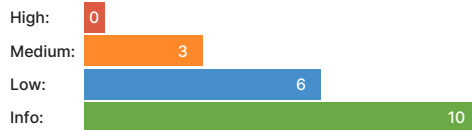
! The Light Website Scanner didn't check for critical issues like SQLi, XSS, Command Injection, XXE, etc. [Upgrade to run Deep scans](#) with 40+ tests and detect more vulnerabilities.

## Summary

### Overall risk level:

Medium

### Risk ratings:



### Scan information:

Start time: Jul 06, 2024 / 10:39:50  
 Finish time: Jul 06, 2024 / 10:41:03  
 Scan duration: 1 min, 13 sec  
 Tests performed: 19/19  
 Scan status: Finished

## Findings

### 🚩 Insecure cookie setting: missing HttpOnly flag

CONFIRMED

URL	Cookie Name	Evidence
<a href="https://www.citysite.co.in">https://www.citysite.co.in</a>	PHPSESSID	The server responded with Set-Cookie header(s) that does not specify the HttpOnly flag: Set-Cookie: PHPSESSID=da80612e6a09c6df8a5edcd8cfd32535 <a href="#">Request / Response</a>

▼ 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 - 2013 : [A5 - Security Misconfiguration](#)  
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
<a href="https://www.citysite.co.in">https://www.citysite.co.in</a>	PHPSESSID	Set-Cookie: PHPSESSID=da80612e6a09c6df8a5edcd8cfd32535; path=/  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](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](#)  
OWASP Top 10 - 2021 : [A5 - Security Misconfiguration](#)

## Vulnerabilities found for server-side software

UNCONFIRMED ⓘ

Risk Level	CVSS	CVE	Summary	Affected software
	4.3	<a href="#">CVE-2015-9251</a>	jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.	jquery 2.2.4
	4.3	<a href="#">CVE-2019-11358</a>	jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.	jquery 2.2.4
	4.3	<a href="#">CVE-2020-11023</a>	In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.	jquery 2.2.4
	4.3	<a href="#">CVE-2020-11022</a>	In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.	jquery 2.2.4

▼ Details

**Risk description:**

The risk is that 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](#)

OWASP Top 10 - 2021 : [A6 - Vulnerable and Outdated Components](#)

## Missing security header: Strict-Transport-Security

CONFIRMED

URL	Evidence
<a href="https://www.citysite.co.in">https://www.citysite.co.in</a>	Response headers do not include the HTTP Strict-Transport-Security header <a href="#">Request / Response</a>

▼ Details

**Risk description:**

The risk is that lack of this header permits an attacker to force a victim user to initiate a clear-text HTTP connection to the server, thus opening the possibility to eavesdrop on the network traffic and extract sensitive information (e.g. session cookies).

**Recommendation:**

The Strict-Transport-Security HTTP header should be sent with each HTTPS response. The syntax is as follows:

```
Strict-Transport-Security: max-age=<seconds>[; includeSubDomains]
```

The parameter `max-age` gives the time frame for requirement of HTTPS in seconds and should be chosen quite high, e.g. several months. A value below 7776000 is considered as too low by this scanner check.

The flag `includeSubDomains` defines that the policy applies also for sub domains of the sender of the response.

**Classification:**

CWE : [CWE-693](#)

OWASP Top 10 - 2013 : [A5 - Security Misconfiguration](#)

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

OWASP Top 10 - 2021 : [A5 - Security Misconfiguration](#)

## Missing security header: Referrer-Policy

CONFIRMED

URL	Evidence
<a href="https://www.citysite.co.in">https://www.citysite.co.in</a>	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. <a href="#">Request / Response</a>

▼ 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](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](#)

OWASP Top 10 - 2021 : [A5 - Security Misconfiguration](#)

## Missing security header: Content-Security-Policy

CONFIRMED

URL	Evidence
-----	----------

<a href="https://www.citysite.co.in">https://www.citysite.co.in</a>	Response does not include the HTTP Content-Security-Policy security header or meta tag <a href="#">Request / Response</a>
---	--

▼ Details

**Risk description:**

The risk is that 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://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](#)
- OWASP Top 10 - 2021 : [A5 - Security Misconfiguration](#)

🚩 Missing security header: X-Content-Type-Options

CONFIRMED

URL	Evidence
<a href="https://www.citysite.co.in">https://www.citysite.co.in</a>	Response headers do not include the X-Content-Type-Options HTTP security header <a href="#">Request / Response</a>

▼ Details

**Risk description:**

The risk is that lack of this header could make possible attacks such as Cross-Site Scripting or phishing in Internet Explorer browsers.

**Recommendation:**

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

**References:**

- <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](#)
- OWASP Top 10 - 2021 : [A5 - Security Misconfiguration](#)

🚩 Robots.txt file found

CONFIRMED

URL
<a href="https://www.citysite.co.in/robots.txt">https://www.citysite.co.in/robots.txt</a>

▼ 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 - 2013 : [A5 - Security Misconfiguration](#)
- OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

## Server software and technology found

UNCONFIRMED ⓘ

Software / Version	Category
 Google Analytics GA4	Analytics
 Google Font API	Font scripts
 Google Maps	Maps
 Nginx	Web servers, Reverse proxies
 PHP	Programming languages
 Cloudflare	CDN
 Google Tag Manager	Tag managers
 cdnjs	CDN
Microsoft Clarity 0.7.34	Analytics
 Google Hosted Libraries	CDN
 Bootstrap 4.4.1	UI frameworks
 jQuery 2.2.4	JavaScript libraries
Slick 1.6.0	JavaScript libraries
 lit-element 4.0.2	JavaScript libraries
 lit-html 3.1.0	JavaScript libraries
 OWL Carousel	JavaScript libraries
 Popper	Miscellaneous
 WhatsApp Business Chat	Live chat

### ▼ 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](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](#)  
 OWASP Top 10 - 2021 : [A5 - Security Misconfiguration](#)

## Security.txt file is missing

CONFIRMED

URL
Missing: <a href="https://www.citysite.co.in/.well-known/security.txt">https://www.citysite.co.in/.well-known/security.txt</a>

### ▼ 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 - 2013 : [A5 - Security Misconfiguration](#)

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

OWASP Top 10 - 2021 : [A5 - Security Misconfiguration](#)

---

 Website is accessible.

---

 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 domain too loose set for cookies.

---

 Nothing was found for unsafe HTTP header Content Security Policy.

---

## Scan coverage information

---

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

- ✓ Starting the scan...
- ✓ Checking for HttpOnly flag of cookie...
- ✓ Checking for Secure flag of cookie...
- ✓ Checking for missing HTTP header - Strict-Transport-Security...
- ✓ Checking for missing HTTP header - Referrer...
- ✓ Checking for missing HTTP header - Content Security Policy...
- ✓ Checking for missing HTTP header - X-Content-Type-Options...
- ✓ 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 domain too loose set for cookies...

✓ Checking for unsafe HTTP header Content Security Policy...

### Scan parameters

Target: https://www.citysite.co.in  
Scan type: Light  
Authentication: False

### Scan stats

Unique Injection Points Detected:	98
URLs spidered:	3
Total number of HTTP requests:	12
Average time until a response was received:	86ms