

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://noc.fire.kerala.gov.in/>

Summary

Overall risk level:

High

Risk ratings:

High:	1
Medium:	2
Low:	7
Info:	5

Scan information:

Start time:	2021-11-01 06:22:30 UTC+02
Finish time:	2021-11-01 06:23:04 UTC+02
Scan duration:	34 sec
Tests performed:	15/15
Scan status:	Finished

Findings

Vulnerabilities found for server-side software

Risk Level	CVSS	CVE	Summary	Exploit	Affected software
●	7.5	CVE-2017-3167	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.	N/A	http_server 2.4.18
●	7.5	CVE-2017-3169	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.	N/A	http_server 2.4.18

●	7.5	CVE-2017-7668	The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.	N/A	http_server 2.4.18
●	7.5	CVE-2017-7679	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.	N/A	http_server 2.4.18
●	7.5	CVE-2021-26691	In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow	N/A	http_server 2.4.18
●	4.3	CVE-2015-9251	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.	N/A	jQuery 2.1.1
●	4.3	CVE-2019-11358	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.	N/A	jQuery 2.1.1
●	4.3	CVE-2020-11022	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.	N/A	jQuery 2.1.1
●	4.3	CVE-2020-11023	In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing	N/A	jQuery 2.1.1

▼ Details

Risk description:

These vulnerabilities expose the affected applications to the risk of unauthorized access to confidential data and possibly to denial of service attacks. 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](#)

🚩 **Insecure cookie setting: missing HttpOnly flag** CONFIRMED

Cookie Name	URL	Evidence
PHPSESSID	https://noc.fire.kerala.gov.in/	Set-Cookie: PHPSESSID=a8ip3a7vomk1up0iq7h7odfmi1; path=/

▼ 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.

<https://owasp.org/www-community/HttpOnly>

Classification:

CWE : [CWE-1004](#)

Insecure cookie setting: missing Secure flag CONFIRMED

Cookie Name	URL	Evidence
PHPSESSID	https://noc.fire.kerala.gov.in/	Set-Cookie: PHPSESSID=a8ip3a7vomk1up0iq7h7odfmi1; path=/

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.

https://owasp.org/www-project-web-security-testing-guide/v41/4-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: Strict-Transport-Security CONFIRMED

URL	Evidence
https://noc.fire.kerala.gov.in/	Response headers do not include the HTTP Strict-Transport-Security header

Details

Risk description:

The HTTP Strict-Transport-Security header instructs the browser to initiate only secure (HTTPS) connections to the web server and deny any unencrypted HTTP connection attempts. 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](#)

Missing security header: Content-Security-Policy CONFIRMED

URL	Evidence
https://noc.fire.kerala.gov.in/	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>

Classification:

CWE : [CWE-693](#)

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

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

🚩 Missing security header: X-Frame-Options CONFIRMED

URL	Evidence
https://noc.fire.kerala.gov.in/	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's 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.

More information about this issue:

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://noc.fire.kerala.gov.in/	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>

Classification:

CWE : [CWE-693](#)

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

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

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

URL	Evidence
https://noc.fire.kerala.gov.in/	Response headers do not include the X-Content-Type-Options HTTP security header

Details

Risk description:

The HTTP header `X-Content-Type-Options` is addressed to the Internet Explorer browser and prevents it from reinterpreting the content of a web page (MIME-sniffing) and thus overriding the value of the Content-Type header). Lack of this header could lead to attacks such as Cross-Site Scripting or phishing.

Recommendation:

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

More information about this issue:

<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](#)

Missing security header: Referrer-Policy CONFIRMED

URL	Evidence
https://noc.fire.kerala.gov.in/	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

Classification:

CWE : [CWE-693](#)

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

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

Server software and technology found CONFIRMED

Software / Version	Category
 Ubuntu	Operating Systems
 Apache 2.4.18	Web Servers
 PHP	Programming Languages
 Twitter Bootstrap	Web Frameworks
 Chart.js	JavaScript Graphics

 Font Awesome	Font Scripts
 Lightbox	JavaScript Frameworks
 MediaElement.js	Video Players
 Modernizr	JavaScript Frameworks
 OWL Carousel	Widgets
 jQuery 2.1.1	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.

Classification:

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

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

🚩 Website is accessible.

🚩 Nothing was found for client access policies.

🚩 Nothing was found for robots.txt file.

🚩 Nothing was found for use of untrusted certificates.

🚩 Nothing was found for enabled HTTP debug methods.

Scan coverage information

List of tests performed (15/15)

- ✓ Checking for website accessibility...
- ✓ 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 - Content Security Policy...
- ✓ 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 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 enabled HTTP debug methods...

Scan parameters

Website URL: https://noc.fire.kerala.gov.in/
Scan type: Light
Authentication: False

Scan stats

URLs spidered: 12
Total number of HTTP request errors: 0
Total number of HTTP requests: 21
Unique Injection Points Detected: 53