

Website Vulnerability Scanner Report

✓ <https://ebtc-pms.online/>

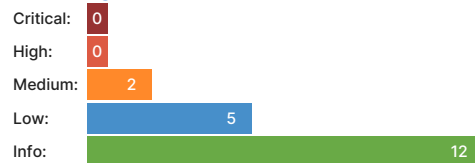
! The Light Website Scanner didn't check for critical issues like SQLi, XSS, Command Injection, XXE, etc. [Upgrade to run Deep scans](#) with 40+ tests and detect more vulnerabilities.

Summary

Overall risk level:

Medium

Risk ratings:



Scan information:

Start time: Mar 23, 2025 / 19:47:45 UTC+08
Finish time: Mar 23, 2025 / 19:48:13 UTC+08
Scan duration: 28 sec
Tests performed: 19/19
Scan status: **Finished**

Findings

🚩 Insecure cookie setting: missing HttpOnly flag

CONFIRMED

URL	Cookie Name	Evidence
https://ebtc-pms.online/	PHPSESSID	The server responded with Set-Cookie header(s) that does not specify the HttpOnly flag: Set-Cookie: PHPSESSID=j2nb1vbqi75rj5hliqskboe5aj 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](#)

🚩 Vulnerabilities found for server-side software

UNCONFIRMED ⓘ

Risk Level	CVSS	CVE	Summary	Affected software
●	6.4	CVE-2024-6484	A vulnerability has been identified in Bootstrap that exposes users to Cross-Site Scripting (XSS) attacks. The issue is present in the carousel component, where the data-slide and data-slide-to attributes can be exploited through the href attribute of an <a> tag due to inadequate sanitization. This vulnerability could potentially enable attackers to execute arbitrary JavaScript within the victim's browser.	bootstrap 3.3.7
●	4.3	CVE-2018-14040	In Bootstrap before 4.1.2, XSS is possible in the collapse data-parent attribute.	bootstrap 3.3.7

●	4.3	CVE-2018-14042	In Bootstrap before 4.1.2, XSS is possible in the data-container property of tooltip.	bootstrap 3.3.7
●	4.3	CVE-2016-10735	In Bootstrap 3.x before 3.4.0 and 4.x-beta before 4.0.0-beta.2, XSS is possible in the data-target attribute, a different vulnerability than CVE-2018-14041.	bootstrap 3.3.7
●	4.3	CVE-2018-20676	In Bootstrap before 3.4.0, XSS is possible in the tooltip data-viewport attribute.	bootstrap 3.3.7

▼ 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:

In order to eliminate the risk of these vulnerabilities, we recommend you check the installed software version and upgrade to the latest version.

Classification:

CWE : [CWE-1026](#)

OWASP Top 10 - 2017 : [A9 - Using Components with Known Vulnerabilities](#)

OWASP Top 10 - 2021 : [A6 - Vulnerable and Outdated Components](#)

🚩 Unsafe security header: Content-Security-Policy

CONFIRMED

URL	Evidence
https://ebtc-pms.online/	<p>Response headers include the HTTP Content-Security-Policy security header with the following security issues:</p> <pre>object-src: Missing object-src allows the injection of plugins which can execute JavaScript. We recommend setting it to 'none'. script-src: script-src directive is missing. 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'. default-src: The default-src directive should be set as a fall-back when other restrictions have not been specified.</pre> <p>Request / Response</p>

▼ 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](#)

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

CONFIRMED

URL	Evidence
https://ebtc-pms.online/	<p>Response headers do not include the X-Content-Type-Options HTTP security header</p> <p>Request / Response</p>

▼ 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 - 2017 : [A6 - Security Misconfiguration](#)

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

Missing security header: Referrer-Policy

CONFIRMED

URL	Evidence
https://ebtc-pms.online/	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](#)

Missing security header: Strict-Transport-Security

CONFIRMED

URL	Evidence
https://ebtc-pms.online/	Response headers do not include the HTTP Strict-Transport-Security header Request / Response

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 - 2017 : [A6 - Security Misconfiguration](#)

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

Server software and technology found

UNCONFIRMED

Software / Version	Category
--------------------	----------

 cdnjs	CDN
 Font Awesome 6.4.0	Font scripts
 Bootstrap 3.3.7	UI frameworks
 Google Analytics UA	Analytics
 Google Font API	Font scripts
 HTTP/3	Miscellaneous
 Google Maps	Maps
 AOS 2.3.1	JavaScript libraries
 PHP	Programming languages
 Unpkg	CDN
 Cloudflare	CDN
 Google Tag Manager	Tag managers
 Hostinger	Hosting
 Hostinger CDN	CDN
 jsDelivr	CDN

▼ 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://ebtc-pms.online/.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 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.

🚩 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 - Content Security Policy.

🚩 Nothing was found for domain too loose set for cookies.

🚩 Nothing was found for Secure flag of cookie.

Scan coverage information

List of tests performed (19/19)

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

Scan parameters

target: https://ebtc-pms.online/
scan_type: Light
authentication: False

Scan stats

Unique Injection Points Detected:	17
URLs spidered:	12
Total number of HTTP requests:	21
Average time until a response was received:	816ms
