

Website Vulnerability Scanner Report (Light)

✓ <http://ec2-184-73-185-129.compute-1.amazonaws.com>

10%

Crawling and Scanning...

Findings

🚩 Communication is not secure

URL	Evidence
http://ec2-184-73-185-129.compute-1.amazonaws.com	Communication is made over unsecure, unencrypted HTTP.

▼ Details

Risk description:

The communication between the web browser and the server is done using the HTTP protocol, which transmits data unencrypted over the network. Thus, an attacker who manages to intercept the communication at the network level, is able to read and modify the data transmitted (including passwords, secret tokens, credit card information and other sensitive data).

Recommendation:

We recommend you to reconfigure the web server to use HTTPS - which encrypts the communication between the web browser and the server.

Classification:

CWE : [CWE-311](#)

OWASP Top 10 - 2013 : [A6 - Sensitive Data Exposure](#)

OWASP Top 10 - 2017 : [A3 - Sensitive Data Exposure](#)

🚩 Missing security header: Content-Security-Policy

URL	Evidence
http://ec2-184-73-185-129.compute-1.amazonaws.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.

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

URL	Evidence
http://ec2-184-73-185-129.compute-1.amazonaws.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'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

URL	Evidence
http://ec2-184-73-185-129.compute-1.amazonaws.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**.

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

URL	Evidence
http://ec2-184-73-185-129.compute-1.amazonaws.com	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**

Missing security header: Referrer-Policy

URL	Evidence
http://ec2-184-73-185-129.compute-1.amazonaws.com	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

Nothing was found for website technologies.

Nothing was found for vulnerabilities of server-side software.

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