

## 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://app.bluealert.pl/formfactory/wizard/formularz-testowy>

### Summary

#### Overall risk level:

Low

#### Risk ratings:

High:	0
Medium:	0
Low:	7
Info:	11

#### Scan information:

Start time:	2021-07-31 10:25:09 UTC+03
Finish time:	2021-07-31 10:25:20 UTC+03
Scan duration:	11 sec
Tests performed:	18/18
Scan status:	Finished

### Findings

#### Missing security header: Strict-Transport-Security

URL	Evidence
<a href="https://app.bluealert.pl/robots.txt">https://app.bluealert.pl/robots.txt</a>	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

URL	Evidence
<a href="https://app.bluealert.pl/robots.txt">https://app.bluealert.pl/robots.txt</a>	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://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
<a href="https://app.bluealert.pl/robots.txt">https://app.bluealert.pl/robots.txt</a>	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](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
-----	----------

<a href="https://app.bluealert.pl/robots.txt">https://app.bluealert.pl/robots.txt</a>	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
<a href="https://app.bluealert.pl/robots.txt">https://app.bluealert.pl/robots.txt</a>	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

URL	Evidence
<a href="https://app.bluealert.pl/robots.txt">https://app.bluealert.pl/robots.txt</a>	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](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**

## 🚩 Robots.txt file found

<https://app.bluealert.pl/static/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).

More information about this issue:

<https://www.theregister.co.uk/2015/05/19/robotstxt/>

**Classification:**

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

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

🚩 Website is accessible.

🚩 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 use of untrusted certificates.

🚩 Nothing was found for enabled HTTP debug methods

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

🚩 Nothing was found for Secure flag of cookie.

🚩 Nothing was found for directory listing.

🚩 Nothing was found for secure communication.

🚩 Nothing was found for HttpOnly flag of cookie.

## Scan coverage information

### List of tests performed (18/18)

- ✓ Checking for website accessibility...
- ✓ Checking for website technologies...
- ✓ Checking for vulnerabilities of server-side software...
- ✓ Checking for client access policies...
- ✓ 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 robots.txt file...
- ✓ Checking for use of untrusted certificates...
- ✓ Checking for enabled HTTP debug methods
- ✓ Checking for domain too loose set for cookies...
- ✓ Checking for Secure flag of cookie...
- ✓ Checking for directory listing...
- ✓ Checking for secure communication...
- ✓ Checking for HttpOnly flag of cookie...

### Scan parameters

Website URL:      <https://app.bluealert.pl/formfactory/wizard/formularz-testowy>  
Scan type:        Light  
Authentication:   False

### Scan stats

URLs spidered:                      1  
Total number of HTTP request errors: 0  
Total number of HTTP requests:    11  
Unique Injection Points Detected:   1

---