

# Website Vulnerability Scanner Report

✓ <https://www.dane.gov.co/>

! 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: Jan 18, 2024 / 18:19:02  
Finish time: Jan 18, 2024 / 18:19:53  
Scan duration: 51 sec  
Tests performed: 19/19  
Scan status: **Finished**

## Findings

### Insecure cookie setting: missing Secure flag

CONFIRMED

URL	Cookie Name	Evidence
<a href="https://www.dane.gov.co/">https://www.dane.gov.co/</a>	ec1d9c9ecb5c2f4ef7998e3e52b19fdf	Set-Cookie: ec1d9c9ecb5c2f4ef7998e3e52b19fdf=eu3chiqkj4ni2m1s7fpdbsd13a; path=/; HttpOnly

#### ▼ 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.

#### 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](#)

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

CONFIRMED

URL	Evidence
<a href="https://www.dane.gov.co/">https://www.dane.gov.co/</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](#)

🚩 Unsafe security header: Content-Security-Policy

CONFIRMED

URL	Evidence
<a href="https://www.dane.gov.co/">https://www.dane.gov.co/</a>	Response headers include the HTTP Content-Security-Policy security header with the following vulnerable directive: <code>script-src 'unsafe-inline'</code>

▼ 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 `unsafe-inline` directive is present in the CSP header, it allows the execution of inline scripts and event handlers. This can be exploited by an attacker to execute arbitrary JavaScript code in the context of the vulnerable application.

**Recommendation:**

Remove `unsafe-inline` value from the `script-src` directive in the Content-Security-Policy header.

**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](#)

🚩 Robots.txt file found

CONFIRMED

URL
<a href="https://www.dane.gov.co/robots.txt">https://www.dane.gov.co/robots.txt</a>

▼ 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).

**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	Analytics
 Google Font API	Font scripts
 PHP	Programming languages
 Twitter	Widgets
 AddToAny	Widgets
 Google Tag Manager	Tag managers
 YouTube	Video players
 Twitter Ads	Advertising
 Facebook Login	Authentication
 Font Awesome	Font scripts
 Bootstrap 5	UI frameworks
 GSAP	JavaScript frameworks
 jQuery 3.6.3	JavaScript libraries
 Joomla	CMS
 POWR	Widgets
 RSS	Miscellaneous
 Cart Functionality	Ecommerce

▼ 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.

**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](#)

## Security.txt file is missing

CONFIRMED

URL

Missing: <https://www.dane.gov.co/.well-known/security.txt>

▼ Details

**Risk description:**

We have detected that the server is missing the security.txt file. There is no particular risk in not creating a valid 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](#)

---

 Website is accessible.

---

 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 secure communication.

---

 Nothing was found for directory listing.

---

 Nothing was found for missing HTTP header - Content Security Policy.

---

 Nothing was found for missing HTTP header - X-Frame-Options.

---

 Nothing was found for missing HTTP header - X-Content-Type-Options.

---

 Nothing was found for missing HTTP header - Referrer.

---

 Nothing was found for domain too loose set for cookies.

---

## Scan coverage information

---

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

- ✓ Checking for website accessibility...
- ✓ Checking for missing HTTP header - Strict-Transport-Security...
- ✓ Checking for unsafe HTTP header Content Security Policy...
- ✓ Checking for Secure flag of cookie...
- ✓ 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 secure communication...
- ✓ Checking for directory listing...
- ✓ Checking for missing HTTP header - Content Security Policy...
- ✓ Checking for missing HTTP header - X-Frame-Options...
- ✓ Checking for missing HTTP header - X-Content-Type-Options...
- ✓ Checking for missing HTTP header - Referrer...
- ✓ Checking for domain too loose set for cookies...
- ✓ Checking for HttpOnly flag of cookie...

### Scan parameters

Target: <https://www.dane.gov.co/>  
Scan type: Light  
Authentication: False

### Scan stats

Unique Injection Points Detected:	467
URLs spidered:	4
Total number of HTTP requests:	12
Average time until a response was received:	350ms

---