

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://admin.worksphere.com.br>

Summary

Overall risk level:

Low

Risk ratings:

High:	0
Medium:	0
Low:	5
Info:	14

Scan information:

Start time:	2022-07-04 15:48:19 UTC+03
Finish time:	2022-07-04 15:48:34 UTC+03
Scan duration:	15 sec
Tests performed:	19/19
Scan status:	Finished

Findings



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

URL	Evidence
https://admin.worksphere.com.br	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`.

References:

<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://admin.worksphere.com.br	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.

▼ 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.

References:

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](#)

🚩 Robots.txt file found CONFIRMED

URL
https://admin.worksphere.com.br/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).

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](#)

Missing security header: X-XSS-Protection CONFIRMED

URL	Evidence
https://admin.worksphere.com.br	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**.

References:

<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](#)

Server software and technology found UNCONFIRMED

Software / Version	Category
 PHP	Programming languages
 Bootstrap	UI frameworks
 Nginx 1.20.0	Web servers, Reverse proxies
 jQuery 3.6.0	JavaScript libraries

▼ 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

Classification:

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

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

Website is accessible.

Nothing was found for missing HTTP header - Strict-Transport-Security.

Nothing was found for HttpOnly flag of cookie.

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

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

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

🚩 Nothing was found for use of untrusted certificates.

🚩 Nothing was found for directory listing.

🚩 Nothing was found for secure communication.

🚩 Nothing was found for enabled HTTP debug methods.

🚩 Nothing was found for absence of the security.txt file.

🚩 Nothing was found for client access policies.

🚩 Nothing was found for vulnerabilities of server-side software.

🚩 Nothing was found for Secure flag of cookie.

Scan coverage information

List of tests performed (19/19)

- ✓ Checking for website accessibility...
- ✓ 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 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 - Strict-Transport-Security...
- ✓ Checking for missing HTTP header - Content Security Policy...
- ✓ Checking for missing HTTP header - X-Frame-Options...
- ✓ Checking for domain too loose set for cookies...
- ✓ Checking for HttpOnly flag of cookie...

✔ Checking for Secure flag of cookie...

Scan parameters

Website URL: https://admin.worksphere.com.br
Scan type: Light
Authentication: False

Scan stats

Unique Injection Points Detected: 4
URLs spidered: 13
Total number of HTTP requests: 23
