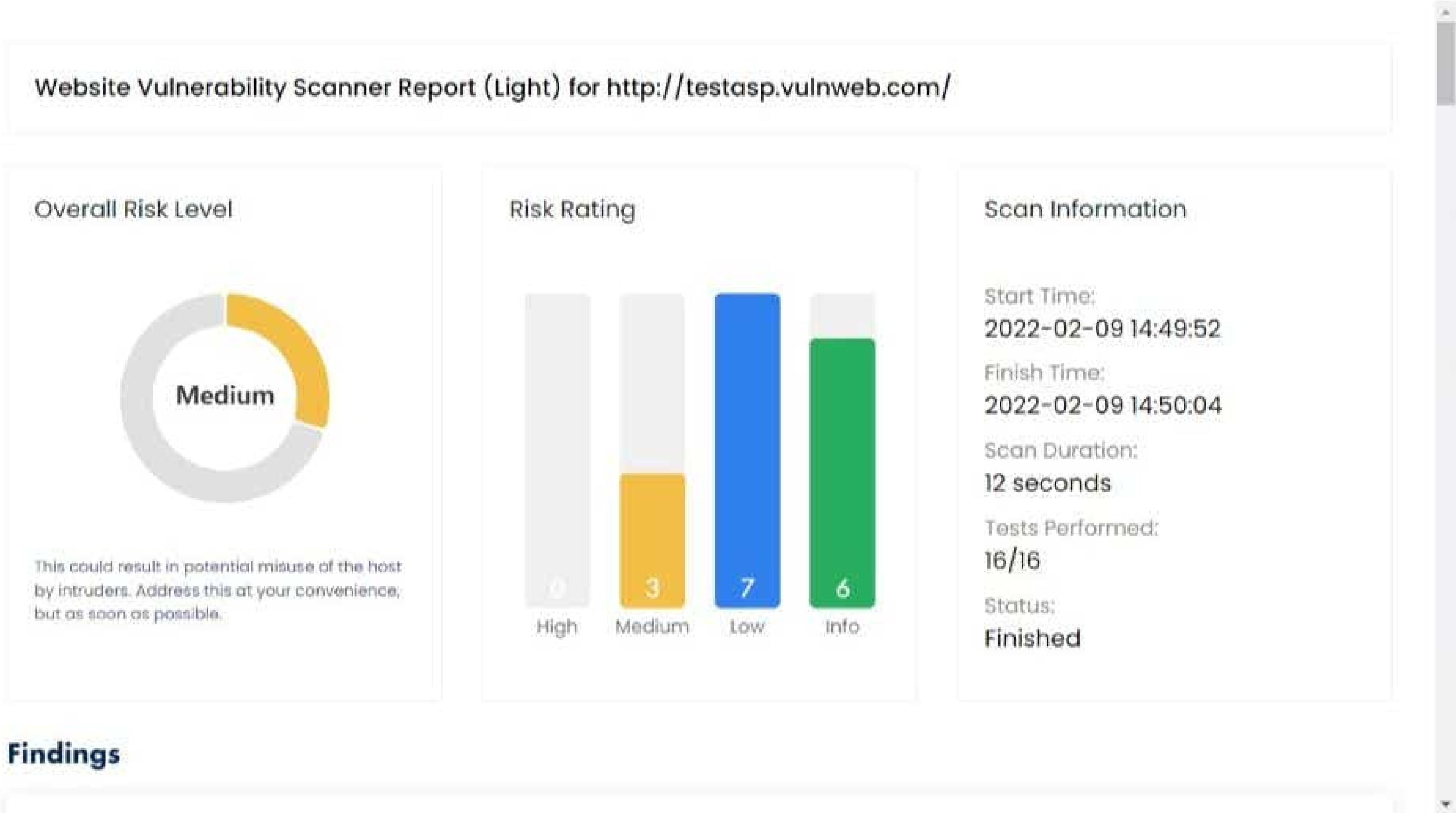


Website Vulnerability Scanner Report (Light) for http://testasp.vulnweb.com/

Overall Risk Level

This could result in potential misuse of the host by intruders. Address this at your convenience, but as soon as possible.

Risk Rating

Scan Information

Start Time:
2022-02-09 14:49:52

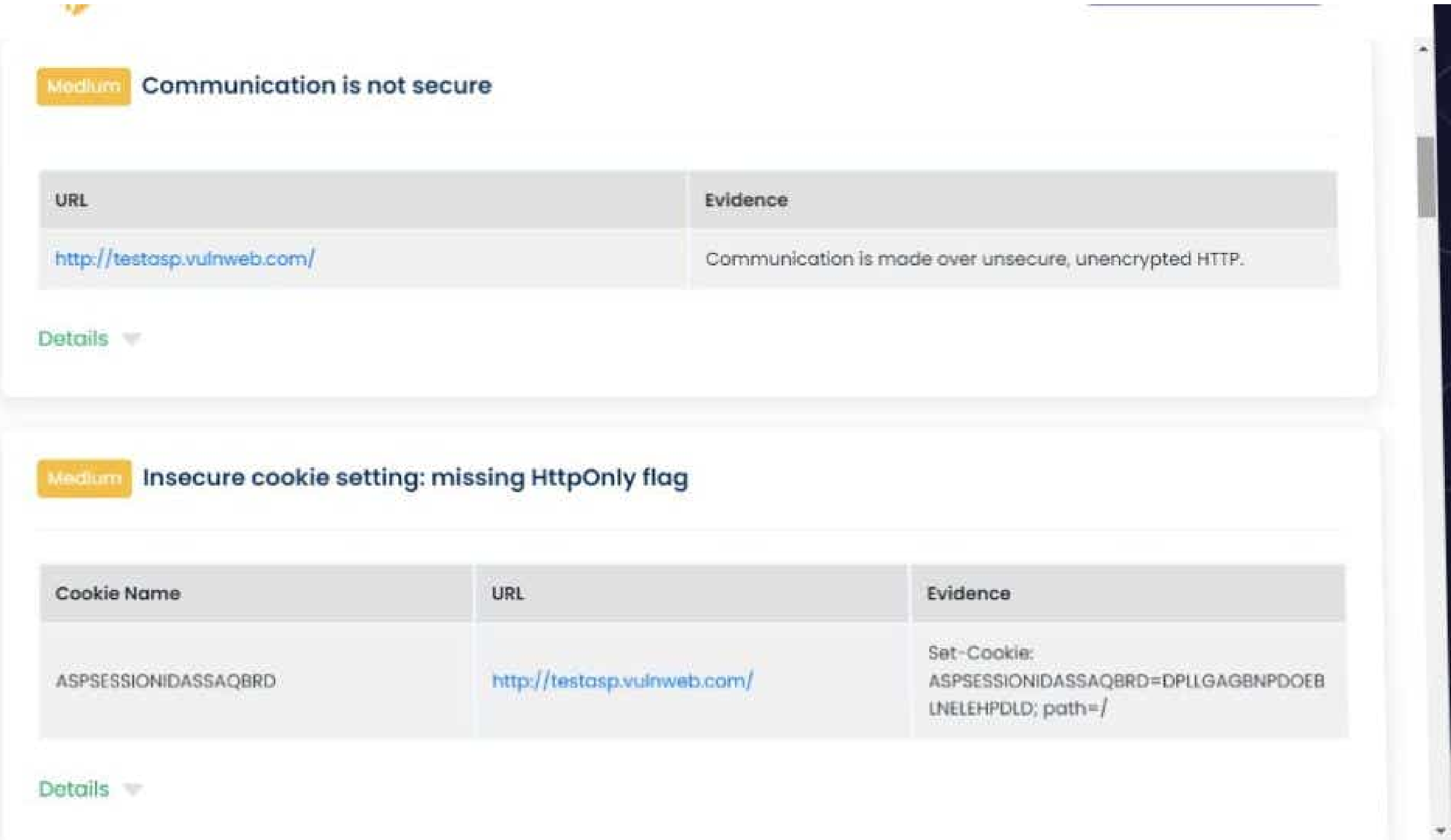
Finish Time:
2022-02-09 14:50:04

Scan Duration:
12 seconds

Tests Performed:
16/16

Status:
Finished

Findings



Medium **Communication is not secure**

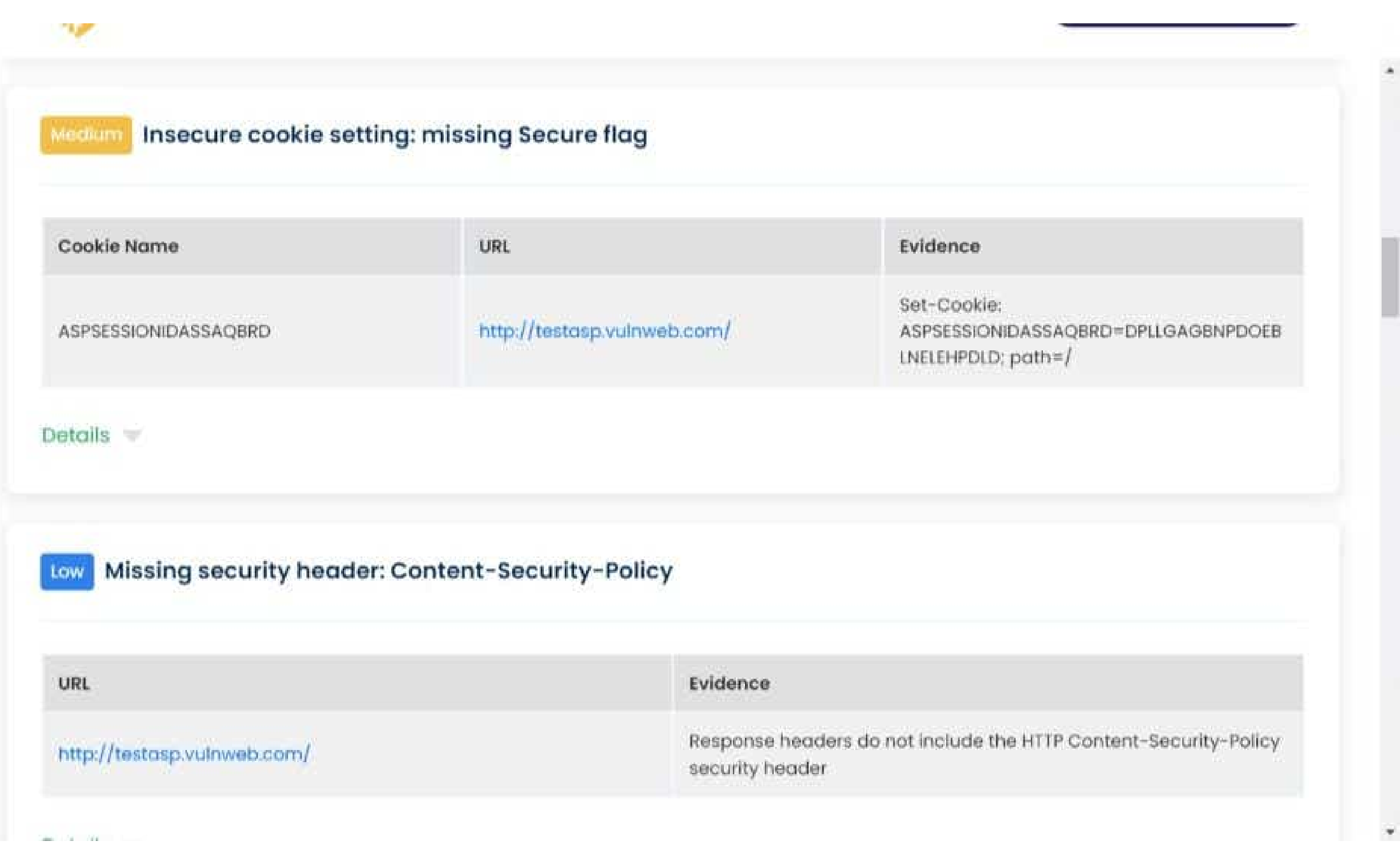
URL	Evidence
http://testasp.vulnweb.com/	Communication is made over unsecure, unencrypted HTTP.

Details ▼

Medium **Insecure cookie setting: missing HttpOnly flag**

Cookie Name	URL	Evidence
ASPSESSIONIDASSAQBRD	http://testasp.vulnweb.com/	Set-Cookie: ASPSESSIONIDASSAQBRD=DPLLGAGBNPDOEBLNELEHPDLD; path=/

Details ▼

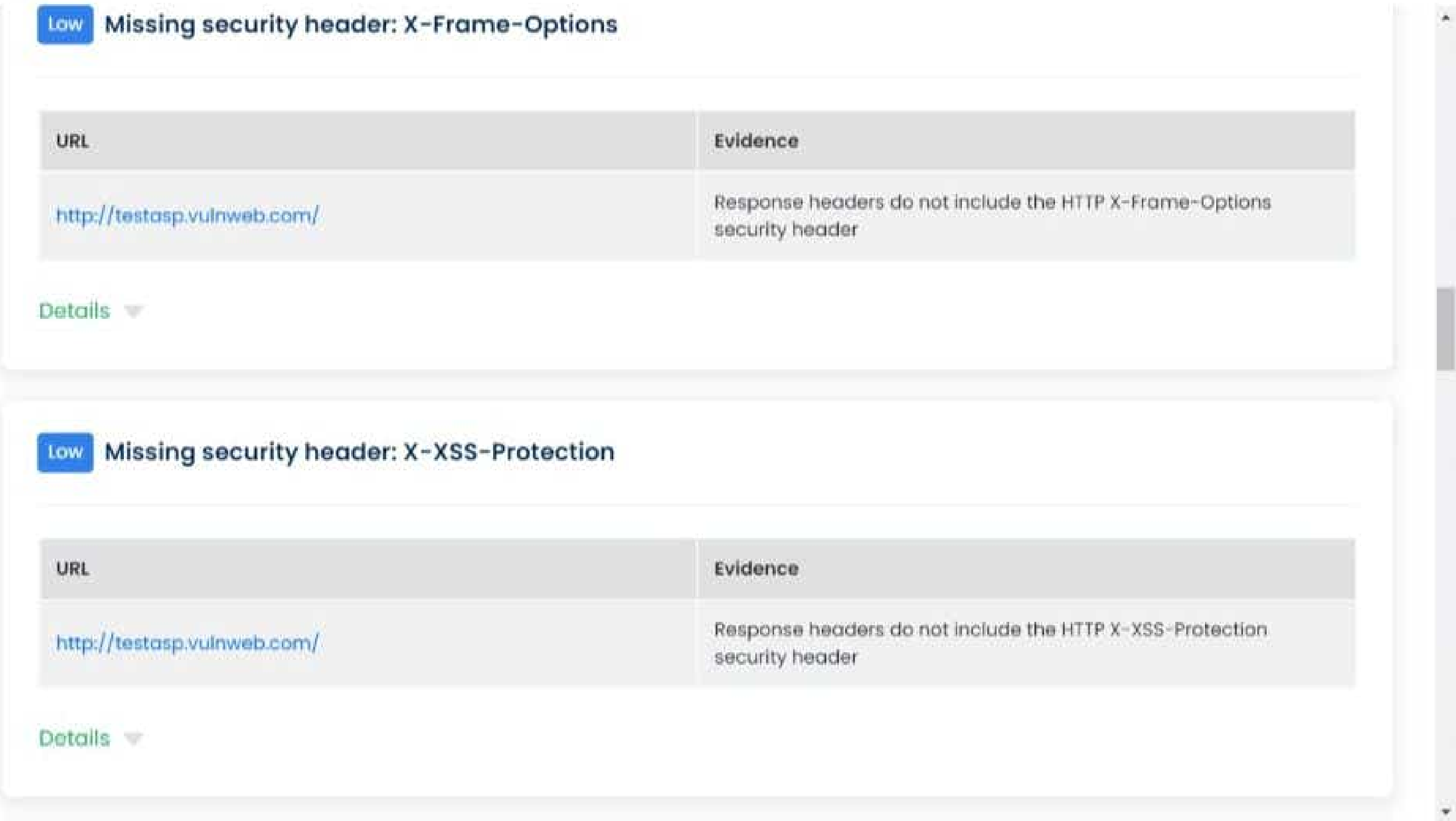


Medium **Insecure cookie setting: missing Secure flag**

Cookie Name	URL	Evidence
ASPSESSIONIDASSAQBRD	http://testasp.vulnweb.com/	Set-Cookie: ASPSESSIONIDASSAQBRD=DPLLGAGBNPDOEBLNELEHPDLD; path=/

Low **Missing security header: Content-Security-Policy**

URL	Evidence
http://testasp.vulnweb.com/	Response headers do not include the HTTP Content-Security-Policy security header



Low Missing security header: X-Frame-Options

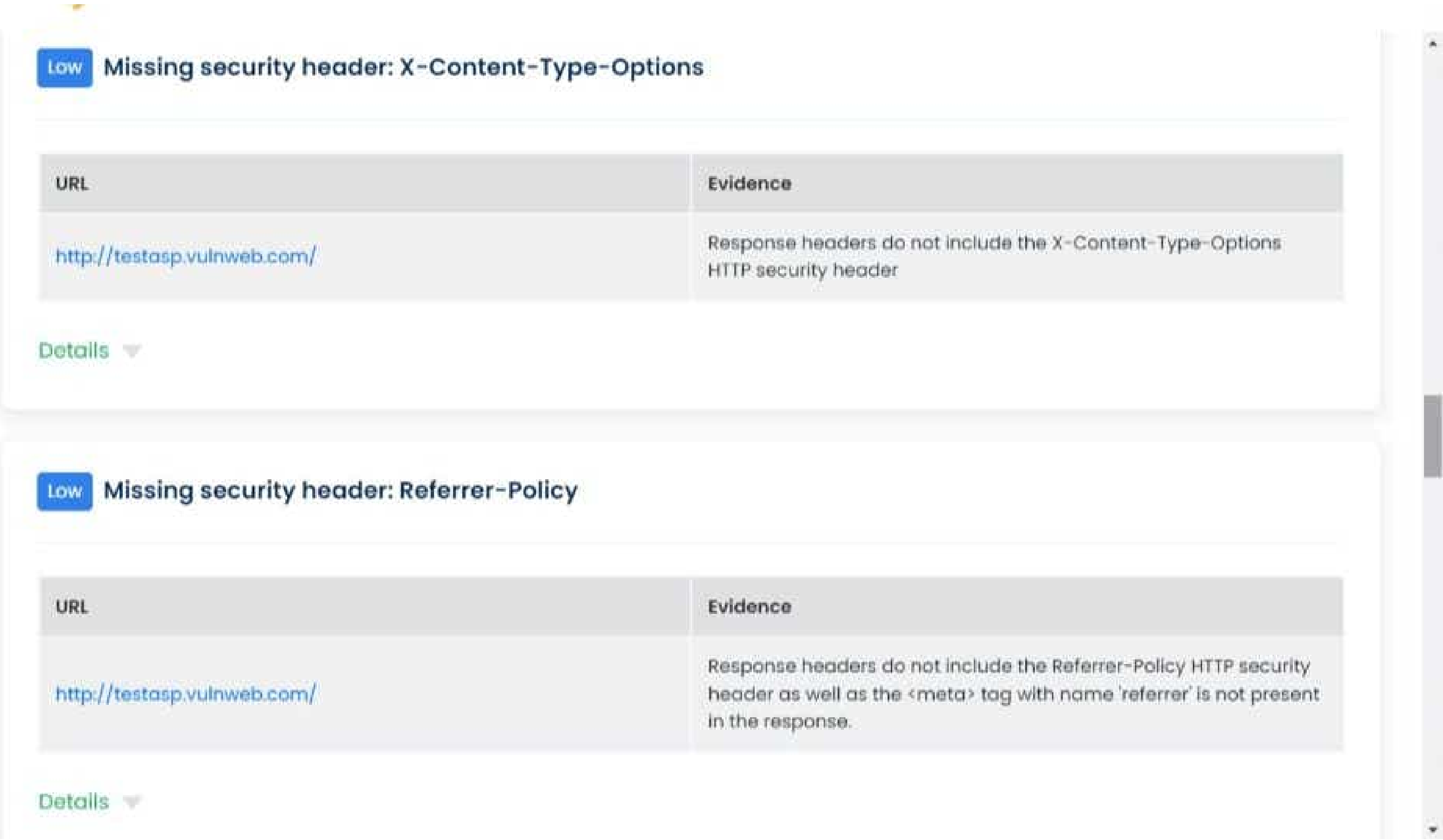
URL	Evidence
http://testasp.vulnweb.com/	Response headers do not include the HTTP X-Frame-Options security header

Details ▼

Low Missing security header: X-XSS-Protection

URL	Evidence
http://testasp.vulnweb.com/	Response headers do not include the HTTP X-XSS-Protection security header

Details ▼



Low **Missing security header: X-Content-Type-Options**

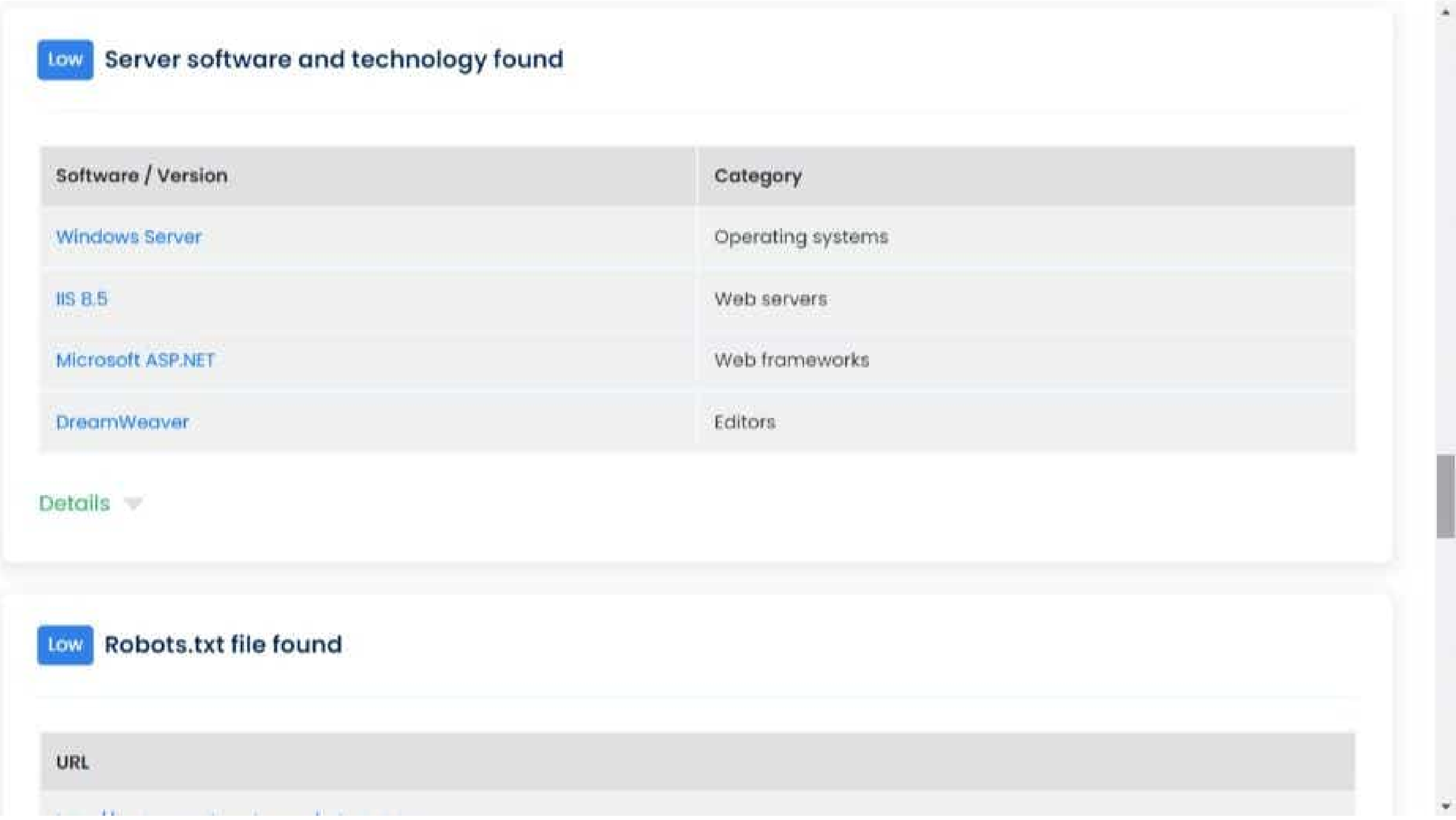
URL	Evidence
http://testasp.vulnweb.com/	Response headers do not include the X-Content-Type-Options HTTP security header

Details ▼

Low **Missing security header: Referrer-Policy**

URL	Evidence
http://testasp.vulnweb.com/	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 ▼



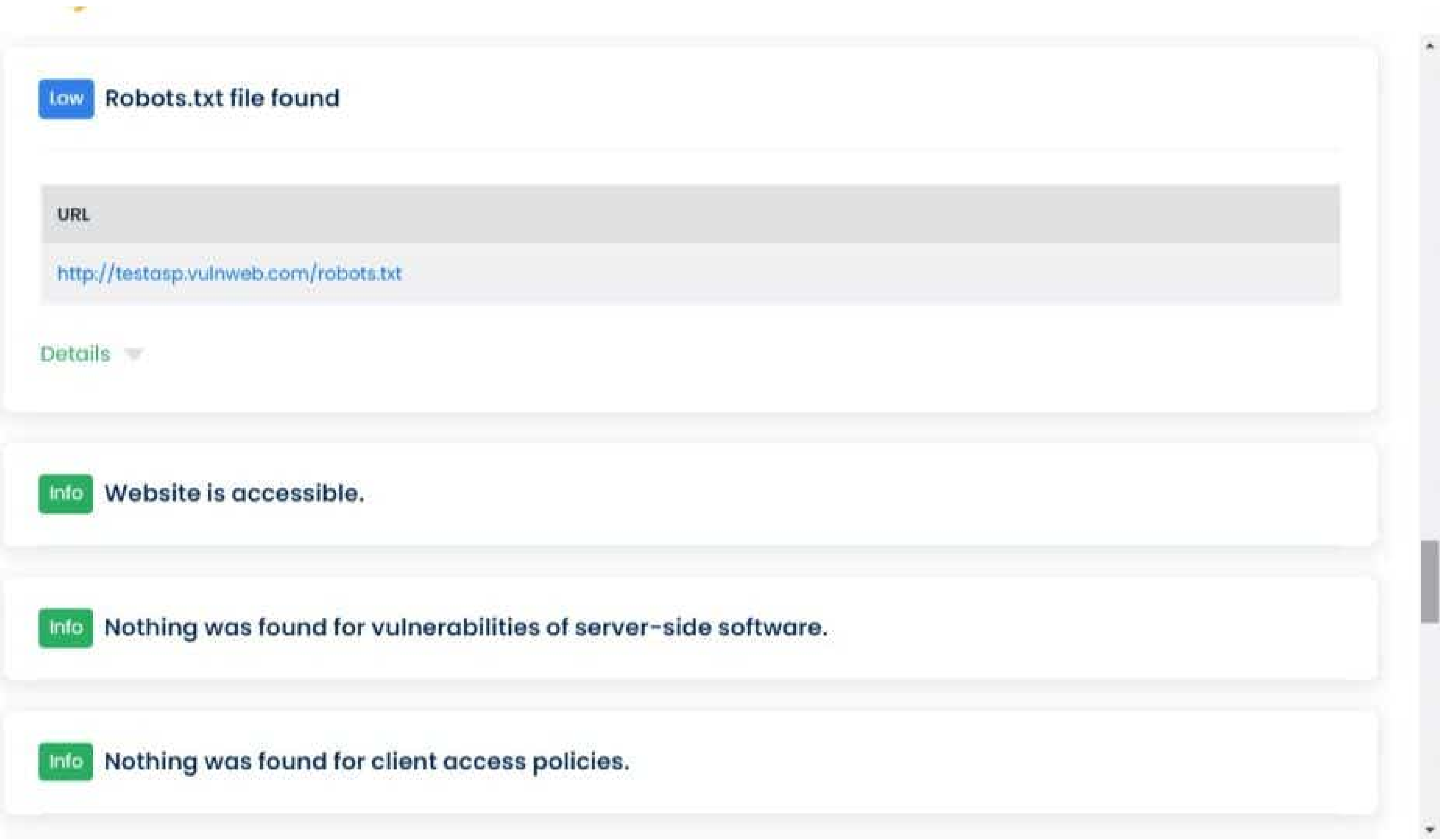
Low **Server software and technology found**

Software / Version	Category
Windows Server	Operating systems
IIS 8.5	Web servers
Microsoft ASP.NET	Web frameworks
DreamWeaver	Editors

Details

Low **Robots.txt file found**

URL



Low Robots.txt file found

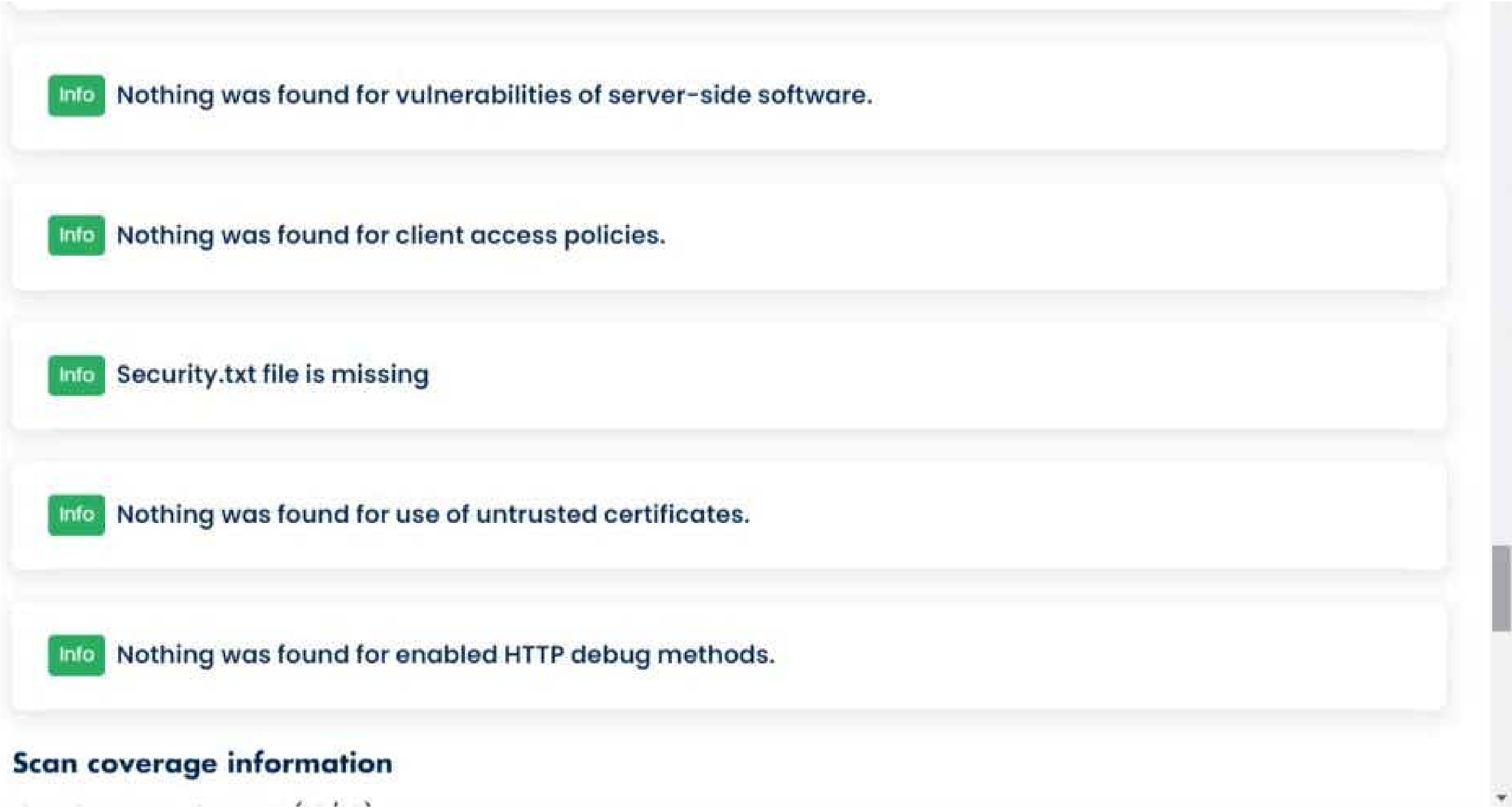
URL
http://testasp.vulnweb.com/robots.txt

Details

Info Website is accessible.

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

Info Nothing was found for client access policies.



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

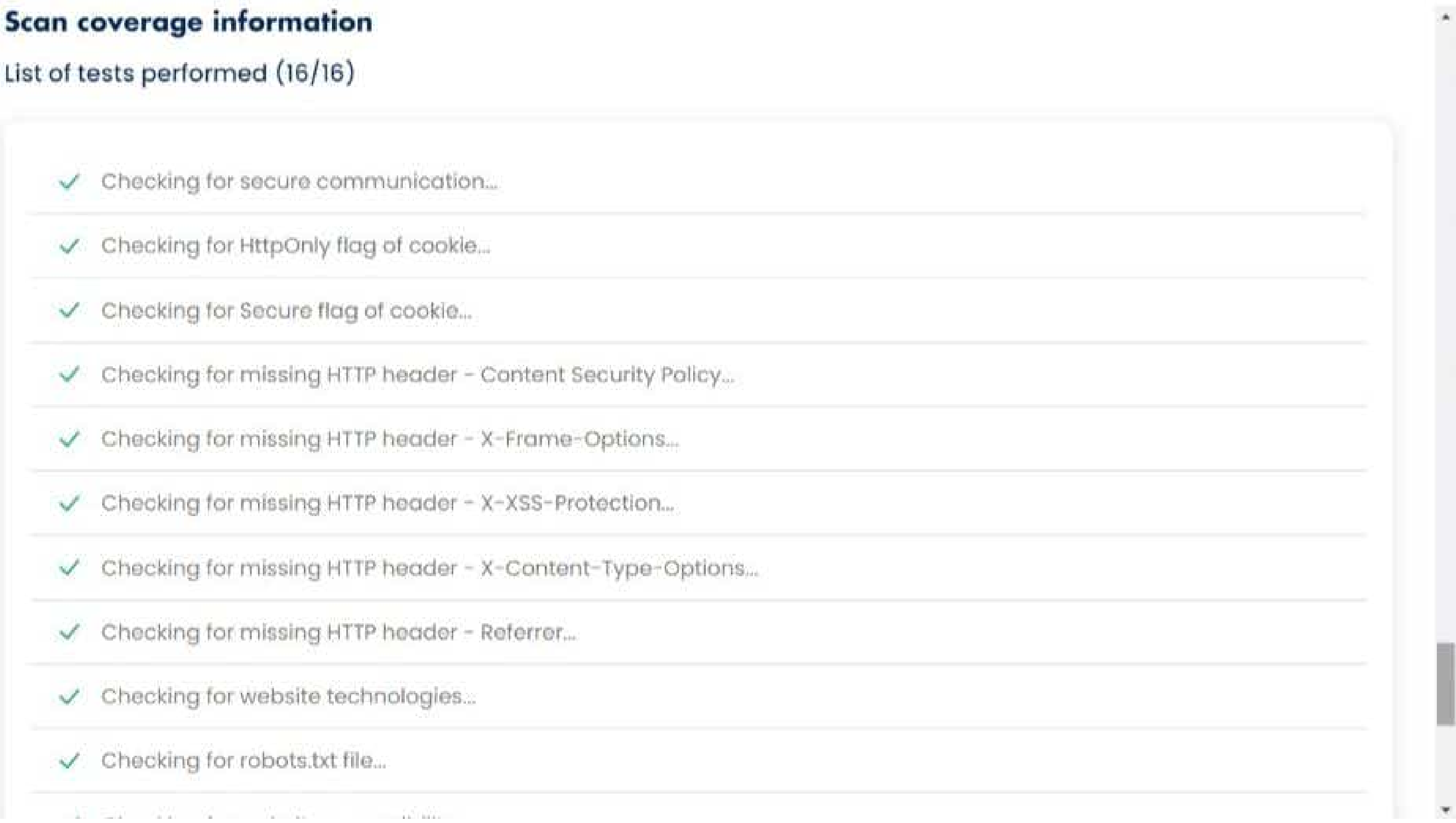
Info Nothing was found for client access policies.

Info Security.txt file is missing

Info Nothing was found for use of untrusted certificates.

Info Nothing was found for enabled HTTP debug methods.

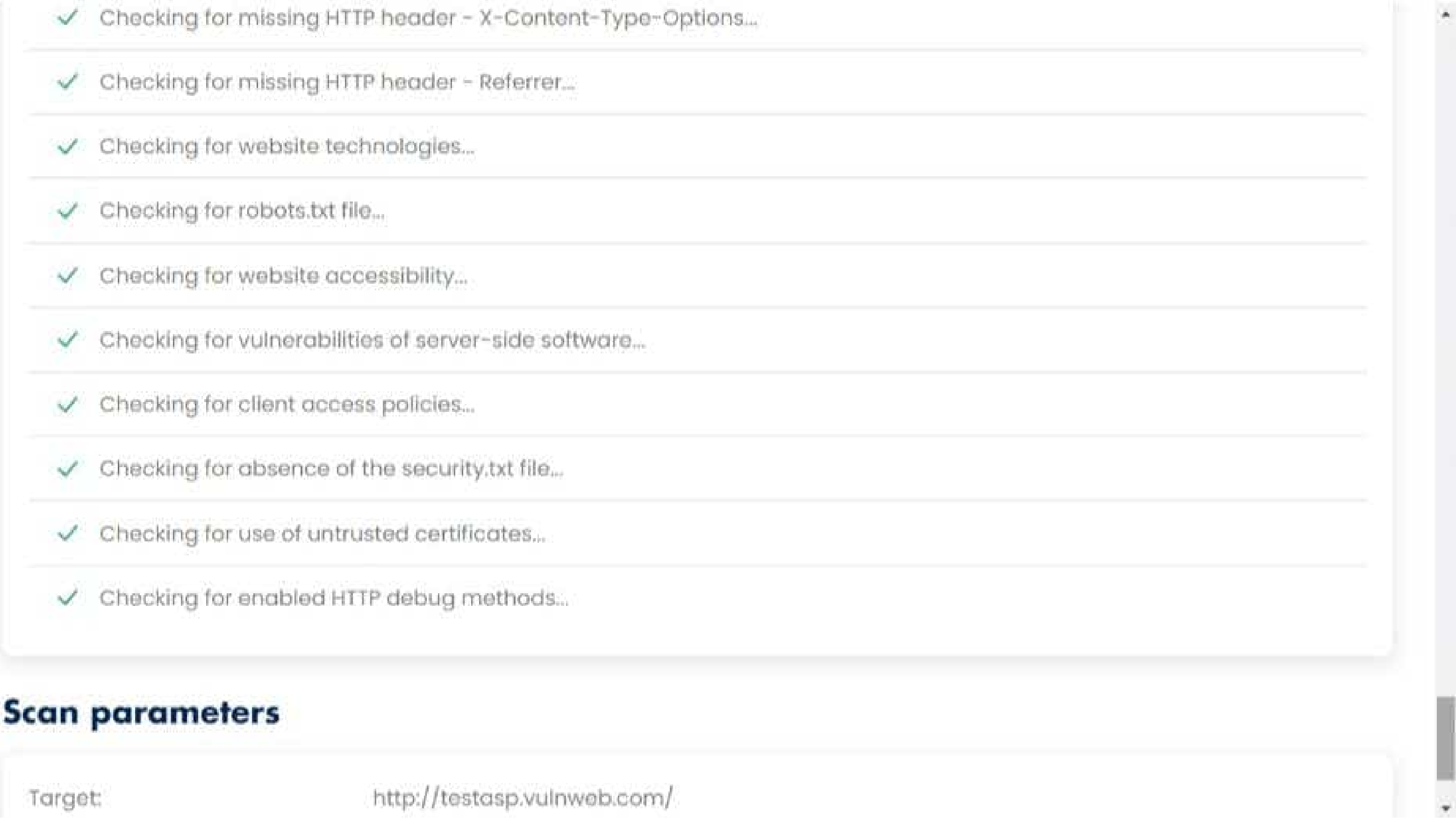
Scan coverage information



Scan coverage information

List of tests performed (16/16)

- ✓ Checking for secure communication...
- ✓ Checking for HttpOnly flag of cookie...
- ✓ Checking for Secure flag of cookie...
- ✓ 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 website technologies...
- ✓ Checking for robots.txt file...



✓ Checking for missing HTTP header - X-Content-Type-Options...

✓ Checking for missing HTTP header - Referrer...

✓ Checking for website technologies...

✓ Checking for robots.txt file...

✓ Checking for website accessibility...

✓ Checking for vulnerabilities of server-side software...

✓ Checking for client access policies...

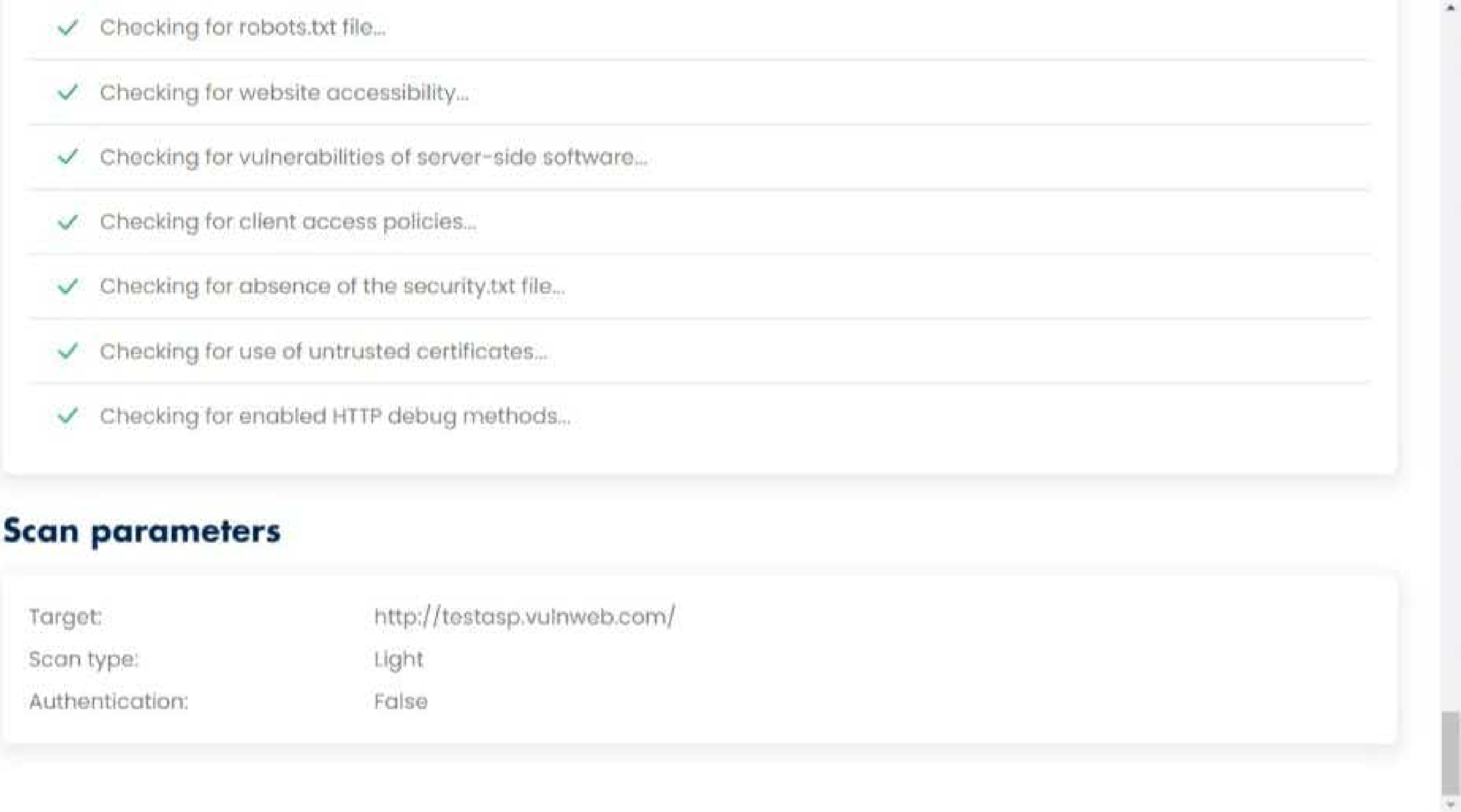
✓ Checking for absence of the security.txt file...

✓ Checking for use of untrusted certificates...

✓ Checking for enabled HTTP debug methods...

Scan parameters

Target:	http://testasp.vulnweb.com/



- ✓ Checking for robots.txt file...
- ✓ Checking for website accessibility...
- ✓ Checking for vulnerabilities of server-side software...
- ✓ Checking for client access policies...
- ✓ Checking for absence of the security.txt file...
- ✓ Checking for use of untrusted certificates...
- ✓ Checking for enabled HTTP debug methods...

Scan parameters

Target:	http://testasp.vulnweb.com/
Scan type:	Light
Authentication:	False

Report:-

Website Vulnerability Scanner Report (Light) For Http://Testasp.vulnweb.com/

Medium: Communication Is Not Secure

URL	Evidence
http://testasp.vulnweb.com/	Communication is made over unsecure, unencrypted HTTP.

Recommendation

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

and the server.

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).

Medium : **Insecure Cookie Setting: Missing Httponly Flag**

Cookie Name	URL	Evidence
ASPSESSIONIDASSAQBRD	http://testasp.vulnweb.com/	SetCookie: ASPSESSIONIDASSAQBRD=DPLLGAGBNPDOEBLNELEHPDLD; path=/

Recommendation

Ensure that the HttpOnly flag is set for all cookies.

https://owasp.org/www-community/HttpOnly

Risk Description

A cookie has been set without the HttpOnly flag, which means that it can be accessed by the JavaScript code running inside the web page. If an

attacker manages to inject malicious JavaScript code on the page (e.g. by using an XSS attack) then the cookie will be accessible and it can be

transmitted to another site. In case of a session cookie, this could lead to session hijacking.

Medium: Insecure Cookie Setting: Missing Secure Flag

Cookie Name	URL	Evidence
ASPSESSIONIDASSAQBRD	http://testasp.vulnweb.com/	Set-Cookie: ASPSESSIONIDASSAQBRD=DPLLGAGBNPDOEBLNELEHPDLD; path=/

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.

https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html

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.

Low:- Missing Security Header: Content-Security-Policy

URL	**Evidence**
http://testasp.vulnweb.com/	Response headers do not include the HTTP Content-Security-Policy security header

Recommendation

Configure the Content-Security-Header to be sent with each HTTP response in order to apply the specific policies needed by the

application.

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.

Low:- Missing Security Header: X-Frame-Options

URL	**Evidence,**
http://testasp.vulnweb.com/	**Response headers do not include the HTTP X-Frame-Options security header**

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.

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

Low : Missing Security Header: X-Xss-Protection

URL	**Evidence**
http://testasp.vulnweb.com/	**Response headers do not include the HTTP X-XSS-Protection security header**

Recommendation

We recommend setting the X-XSS-Protection header to X-XSS-Protection: 1; mode=block.

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.

Low : Missing Security Header: X-Content-Type-Options

URL	**Evidence**
http://testasp.vulnweb.com/	Response headers do not include the X-Content-Type-Options HTTP security header

Recommendation

We recommend setting the X-Content-Type-Options header such as X-Content-Type-Options: nosniff.

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.

Low :- Missing Security Header: Referrer-Policy

URL	Evidence
http://testasp.vulnweb.com/	**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.

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.

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.

Low : Server Software And Technology Found

Software / Version	Category
Windows Server	Operating systems

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.

Risk Description

An attacker could use this information to mount specific attacks against the identified software type and version.

Low:. Robots.txt File Found

URL

http://testasp.vulnweb.com/robots.txt

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).

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.

- Info Website Is Accessible.
- Info Nothing Was Found For Vulnerabilities Of Server-Side Software.
- Info Nothing Was Found For Client Access Policies.
- Info Security.txt File Is Missing
- URL
- URL
- Missing: http://testasp.vulnweb.com/.well-known/security.txt
- Info Nothing Was Found For Use Of Untrusted Certificates.
- Info Nothing Was Found For Enabled Http Debug Methods.

Scan Coverage Information

List Of Tests Performed (16/16)

Checking for secure communication...

Checking for HttpOnly flag of cookie...

Checking for Secure flag of cookie...

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 website technologies...

Checking for robots.txt file...

Checking for website accessibility...

Checking for vulnerabilities of server-side software...

Checking for client access policies...

Checking for absence of the security.txt file...

Checking for use of untrusted certificates...

Checking for enabled HTTP debug methods...

Scan Parameters

Target : http://testasp.vulnweb.com/

Scan type : Light

Authentication : False