

# Pentest-Tools Web Vulnerability Scanner

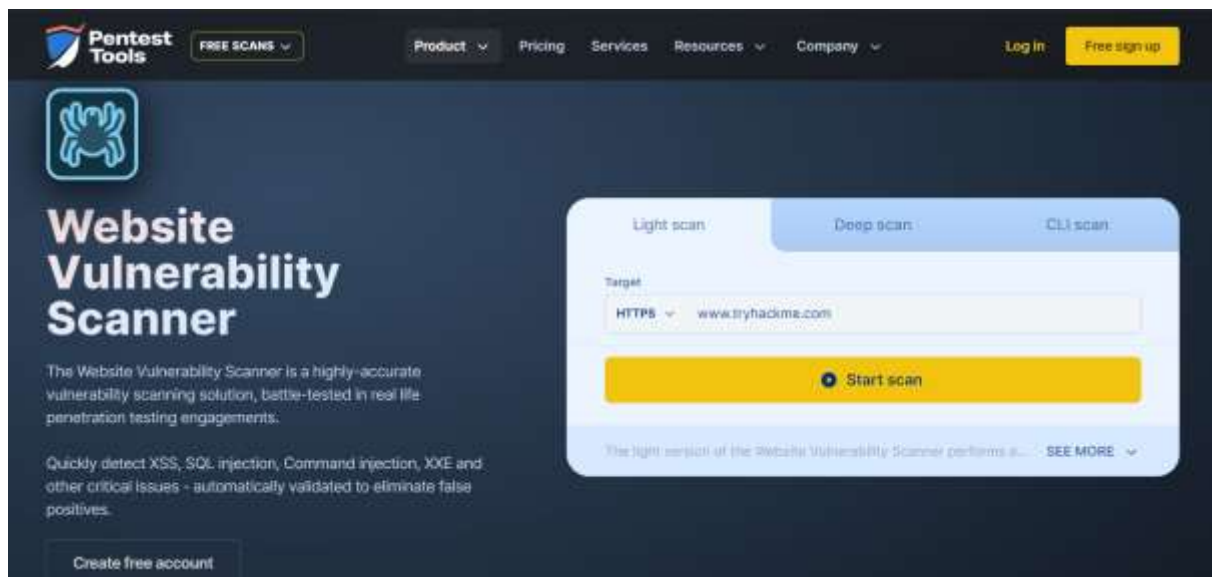
Pentest-tools.com offers a comprehensive suite of online tools designed for penetration testing and vulnerability assessment. One of their key services is the Web Vulnerability Scanner, which is used to identify security weaknesses in web applications.

## Key Functions: -

- **URL Crawling:** The scanner crawls the target URL to discover all linked pages and resources, ensuring comprehensive coverage.
- **Vulnerability Detection:** Utilizes various techniques to detect common web application vulnerabilities, including both known and zero-day threats.
- **Report Generation:** After scanning, it generates a report detailing the findings, which can be used for fixing the identified vulnerabilities.
- **Risk Assessment:** Provides a risk assessment for each detected vulnerability, helping prioritize remediation efforts based on the severity of the issues.
- **Continuous Monitoring:** Some plans offer continuous monitoring to detect new vulnerabilities as they arise.

## Examples: -

1. Go to the website Pentest-tools.com for vulnerability scanning. Here we have three options for scan i.e. Light, Deep and CLI scan. We will have light scan. In order to do so search for your target domain inside the light scan tab.



2. Now we have a summary of the scan. This includes a lot of information in it. Mainly it tells us that it has Medium level of overall risk.

### Scan summary



- Now we have the findings from the scan. Firstly we come to know about the cookie settings vulnerability.

## Findings

FILTER BY RISK LEVEL

All (18) ↕

### Insecure cookie setting: missing Secure flag Confirmed

URL: <https://tryhackme.com/> COOKIE NAME: AWSALB

#### EVIDENCE

Set-Cookie:  
AWSALB=cFcY/2imbmdpb1ca1S/e822UUuw95T+rstUjp1xdQqjbhwtW+CFtYVVALLpHYffwJGIfdLQgI5wyZgmCH9WeffpOSRhJuWFUBY7CyopDn;  
Expires=Mon, 17 Jun 2024 00:04:50 GMT; Path=/;  
AWSALBCORS=cFcY/2imbmdpb1ca1S/e822UUuw95T+rstUjp1xdQqjbhwtW+CFtYVVALLpHYffwJGIfdLQgI5wyZgmCH9WeffpOSRhJuWFUBY7Cy;  
Expires=Mon, 17 Jun 2024 00:04:50 GMT; Path=/; SameSite=None,  
connect.sid=s%3AmZXhX9Zdhgz1ziylrbgKtIJy4xa5vkY9.LM1rY5YO3ZpPn7wSJo85yPJlc%2B5qN7LCMAEKzbBvPEs; Path=/; Expires=Mon, 17 J  
HttpOnly

#### Vulnerability description

We found that a cookie has been set without the Secure flag, which means the browser will send it even on unencrypted channels (http).

- Now here we have the information related the server software and technologies.

### Server software and technology found

SOFTWARE / VERSION	CATEGORY
Express	Web frameworks, Web servers
Google Analytics	Analytics
Node.js	Programming languages
Vimeo	Video players
Cloudflare	CDN
Google Tag Manager	Tag managers
Animate.css 3.7.2	UI frameworks
Amazon Web Services	PaaS
Amazon ALB	Load balancers

5. At the end we have a coverage information of the scan. In which it covers all the part in which vulnerability scan is being done.

### Scan coverage information

#### LIST OF TESTS PERFORMED

- ✓ Starting the scan...
- ✓ Checking for missing HTTP header - X-Content-Type-Options...
- ✓ Checking for HttpOnly flag of cookie...
- ✓ Checking for missing HTTP header - Content Security Policy...
- ✓ Checking for missing HTTP header - Referrer...
- ✓ Checking for missing HTTP header - Strict-Transport-Security...
- ✓ 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...

#### SCAN PARAMETERS

Target:  
**<https://tryhackme.com/>**

Scan type  
**Light**

Authentication  
**False**