103 tests running39,822 tests in 24 hours

ImmuniWeb®
AI for Application Security

Customer Login | Partner Login

Community Edition Total Tests: 173,252,747 This Week: 327,916 Today: 102,741

AI Platform Pricing Community Edition Compliance Company Partners Get a Demo

Summary Subdomains Server Security Software Security GDPR PCI DSS HTTP Headers CSP Security Cookies External Content Security

Website Security Test of les-lionceaux.netlify.app

Free online security tool to test your security

✓ GDPR & PCI DSS Test ✓ Website CMS Security Test
✓ CSP & HTTP Headers Check ✓ WordPress & Dr

Free online security tool to test your security

61,538,355 security tests performed

SCAN | API | LATEST TESTS | ABOUT | SCORING | FEEDBACK | NEW MONITORING

https://les-lionceaux.netlify.app/ ▶

□ Hide from Latest Tests

Provided "as is" without any warranty of any kind

Provided "as is" without any warranty of any kind

103 tests running 39,822 tests in 24 hours

Summary of les-lionceaux.netlify.app [Desktop Version] Website Security Test

undefined was tested 6,260 times during the last 12 months.

Your final score

Tested on:	Today, 23:43 CET
Server IP:	52.73.87.228
Reverse DNS:	ec2-52-73-87-228.comp...
Location:	Ashburn
Client:	Desktop Browser

A
B
C ◀
F

C

Refresh test

PDF Download report

Software Security Test	Compliance Test	Compliance Test	Content Security Policy Test	Headers Security Test
1 ISSUE FOUND	2 ISSUES FOUND	3 ISSUES FOUND	MISSING	NO MAJOR ISSUES FOUND

Get instant notifications on website grade or compliance change with ImmuniWeb Discovery. FREE DEMO

Setup free weekly notifications and stay informed about vulnerabilities or misconfigurations of this website. MONITORING

AI Products Ask a Question

Discovered Subdomains

Tested URL	Protocol/Port	Certificate(s)	Tested on	Compliances	Grade
neuyazvimyi.netlify.app	HTTP / 80	?	Not tested yet	?	?
neuyazvimyi.netlify.app	HTTPS / 443	📄	June 9th 2020, 15:27		C
netlify.app	HTTP / 80	?	Not tested yet	?	?
netlify.app	HTTPS / 443	📄	Not tested yet	?	?

VISUAL MAP VIEW SHOW 10 MORE

Discover all your subdomains, APIs and public cloud storage with **ImmuniWeb Discovery**. FREE DEMO

Web Server Security Test

HTTP RESPONSE

AI Products Ask a Question

200

HTTP VERSIONS

HTTP/1.0 HTTP/1.1 HTTP/2

NPN ℹ

N/A

ALPN

H2

CONTENT ENCODING

None

SERVER SIGNATURE

N/A

WAF ℹ

No WAF detected

LOCATION

Amazon.com, Inc.

HTTP METHODS ENABLED

✓ GET ✓ HEAD

Software Security Test

Web Software Found	Web Software Outdated	Web Software Vulnerabilities
1	1	6

FINGERPRINTED CMS & VULNERABILITIES ℹ

No CMS were fingerprinted on the website. Information

FINGERPRINTED CMS COMPONENTS & VULNERABILITIES ℹ

Bootstrap 4.0.0

The fingerprinted component version is outdated and vulnerable to publicly known vulnerabilities. Urgently update to the most recent version **5.0.1**.

CVSSv3.0 Score	Vulnerability CVE-IDCVE	Vulnerability TypeType
5.5 Medium	CVE-2018-14040	CWE-79 — Cross-site scripting
5.5 Medium	CVE-2018-14042	CWE-79 — Cross-site scripting
5.5 Medium	CVE-2018-14041	CWE-79 — Cross-site scripting
5.3 Medium	CVE-2019-8331	CWE-79 — Cross-site scripting
5.3 Medium	CVE-2018-20677	CWE-79 — Cross-site scripting
5.3 Medium	CVE-2018-20676	CWE-79 — Cross-site scripting

GDPR Compliance Test

If the website processes or stores any PII of EU residents, the following requirements of EU GDPR may apply:

PRIVACY POLICY ℹ

Privacy Policy was not found on the website or is not easily accessible. Misconfiguration or weakness

WEBSITE SOFTWARE SECURITY ℹ

Website CMS or its components are outdated and contain known security vulnerabilities. Misconfiguration or weakness

SSL/TLS TRAFFIC ENCRYPTION

SSL/TLS encryption seems to be present.

Good configuration

COOKIE CONFIGURATION

No cookies with potentially sensitive information seem to be sent.

Information

COOKIES DISCLAIMER

No cookies with potentially sensitive or tracking information seem to be sent.

Information

PCI DSS Compliance Test

If the website falls into a CDE (Cardholder Data Environment) scope, the following Requirements of PCI DSS may apply:

REQUIREMENT 6.2

Website CMS or its components seem to be outdated. Check for available updates.

Misconfiguration or weakness

REQUIREMENT 6.5

Fingerprinted website CMS or its components contain publicly known vulnerabilities (Ref. PCI DSS 6.5.1-6.5.10).

Misconfiguration or weakness

REQUIREMENT 6.6

No WAF was detected on the website. Implement a WAF to protect the website against common web attacks.

Misconfiguration or weakness

HTTP Headers Security Test

Some HTTP headers related to security and privacy are missing or misconfigured.

Misconfiguration or weakness

MISSING REQUIRED HTTP HEADERS

X-Frame-Options X-XSS-Protection X-Content-Type-Options

MISSING OPTIONAL HTTP HEADERS

Access-Control-Allow-Origin Public-Key-Pins Public-Key-Pins-Report-Only Expect-CT Permissions-Policy

SERVER

The header was not sent by the server.

Good configuration

STRICT-TRANSPORT-SECURITY

The header is properly set.

Good configuration

Raw HTTP Header

strict-transport-security: max-age=31536000; includeSubDomains; preload

Directives

Name	Description	Alerts
max-age	Sets the time browsers must enforce the use of HTTPS to browse the website.	No problems found

Content Security Policy Test

CONTENT-SECURITY-POLICY

The header was not sent by the server. Misconfiguration or weakness

CONTENT-SECURITY-POLICY-REPORT-ONLY

The header was not sent by the server. Information

Cookies Security Test

No cookies were sent by the web application. Good configuration

External Content Security Test

EXTERNAL CONTENT ON HOMEPAGE

External web content (e.g. images, video, CSS or JavaScript) can improve website loading time. However, the external content can also put privacy of website visitors at risk given that some information about them is transmitted to the third parties operating the external resources, sometimes even without proper HTTPS encryption or user consent.

External Requests	Failed Requests
2	0

maxcdn.bootstrapcdn.com

https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css URL DETAILS

fonts.googleapis.com

https://fonts.googleapis.com/css2?family=Raleway:wght@100;300;500;600&display=swap URL DETAILS

ImmuniWeb®
AI for Application Security

ImmuniWeb® leverages our award-winning AI and Machine Learning technology for acceleration and intelligent automation of Attack Surface Management with Dark Web Monitoring for subsequent threat-aware and risk-based Application Penetration Testing with zero false positives SLA.

ImmuniWeb® AI Platform

ImmuniWeb Discovery
Attack Surface & Dark Web Monitoring
Third-Party & Vendor Risk Management
24/7 AI-Enabled Automated

ImmuniWeb® On-Demand
Web Penetration Test & Remediation
One-Time AI-Enabled Manual

ImmuniWeb® MobileSuite
Mobile Penetration Test & Remediation
One-Time AI-Enabled Manual

ImmuniWeb® Continuous
Web Penetration Testing & Remediation
24/7 AI-Enabled Manual

VISA mastercard AMERICAN EXPRESS PayPal Maestro UnionPay 银联 BANK TRANSFER

Partners

- Integrations
- Partner Program
- Partner Directory
- Become a Partner

Community Edition

- Mobile App Security Test
- Website Security Test
- Dark Web Exposure Test
- SSL Security Test

OWASP Top 10

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Vulnerable Components
- Insufficient Logging & Monitoring

Compliance

- EU & UK GDPR
- Singapore PDPA
- Hong Kong PDPO
- South Africa POPIA
- India IT Act
- Brazil LGPD
- HIPAA / HITECH
- FTCA, GLBA, FCRA / FACTA
- NIST SP 800, FISMA, CMMC
- New York SHIELD, NYDFS
- California CCPA, CPRA
- ISO 27001 / ISO 27002
- Singapore MAS
- PCI DSS

Resources

- Application Penetration Testing
- Automated Penetration Testing
- Attack Surface Management
- Dark Web Monitoring
- Ecommerce Security
- CWE Knowledge Base
- Security Advisories

Security Vulnerabilities

- Path Traversal
- OS Command Injection
- Cross-Site Scripting
- SQL Injection
- LDAP Injection
- XML Injection
- Code Injection
- PHP File Inclusion
- HTTP Response Splitting
- Information Exposure
- Cross-Site Request Forgery
- Open Redirect

AI Products Ask a Question