Summary of www.computeon.house [Desktop version] Website Security Test

Provided "as is" without any warranty of any kind.

www.computeon.house was tested 30 times during the last 12 months.

Your final score:

A+

A B C F

Tested on:	Dec 31st, 2025 09:25:00 GMT+0
Server IP:	185.199.38.4
Reverse DNS:	jump12.jump.bg
Location:	Bulgaria
Client:	Desktop version

Web Software Security Test	GDPR Compliance Test	PCI DSS Compliance Test	Content Security Policy Test	HTTP Headers Security Test
NO ISSUES FOUND	1 ISSUE FOUND	COMPLIANT	NO ISSUES FOUND	NO MAJOR ISSUES FOUND

Full Test Results: https://www.immuniweb.com/websec/www.computeon.house/AK5pRnwD/

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com

Copyright © 2025 ImmuniWeb SA

Table of Contents

- Web Server Security Test
- Web Software Security Test
- GDPR Compliance Test
- PCI DSS Compliance Test
- HTTP Headers Security Test
- Content Security Policy (CSP) Test
- Cookies Privacy and Security Test
- External Content Security Test
- Protection from Data Scraping Test
- DNSSEC Configuration Test

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2025 ImmuniWeb SA

Protection from Data Scraping Test

Many companies rely on AI bots to scrape website content, using the collected data to train their machine learning models. To safeguard information, website owners can apply different techniques to detect, limit, or block scraping activities carried out by these bots.

Robots.txt Rules	User-Agent Blocks	Meta Tags	Protection vs. Bots
0	5	0	5

GPTBot by OpenAI

Robots.txt Directives

No robots.txt or applicable rules for GPTBot User-Agent(s) found.	Misconfiguration or weakness

Server-side Blocking

Access blocked based on User-Agent GPTBot. The server responded with a 403 status code.	Good configuration

Gemini by Google

To control whether your website's content can be used to train Google's AI models (such as Gemini), Google follows the special Google-Extended User-Agent directive in your robots.txt file.

Robots.txt Directives

No rule is specified for the Google-Extended User-Agent, so Google imposes no restrictions on AI training and may use any content that its crawlers are allowed to access.	Information

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2025 ImmuniWeb SA

However, Google-Extended does not crawl your site directly. Instead, it respects the access granted to other Google crawlers: Googlebot, Googlebot-Image, Googlebot-Video, Googlebot-News, GoogleOther, GoogleOther-Image, GoogleOther-Video.

No crawling rules are specified for Google, so its crawlers are not subject to any restrictions.	Misconfiguration or weakness

Claude by Anthropic

Robots.txt Directives

No robots.txt or applicable rules for ClaudeBot, Claude-User, Claude-SearchBot User-Agent(s) found.	Misconfiguration or weakness

Server-side Blocking

Access blocked based on User-Agent ClaudeBot. The server responded with a 403 status code.	Good configuration
No server-side User-Agent-based blocking detected for Claude-User, Claude-SearchBot.	Information

Perplexity by Perplexity AI

Robots.txt Directives

No robots.txt or applicable rules for PerplexityBot User-Agent(s) found.	Misconfiguration or weakness

Server-side Blocking

No server-side User-Agent-based blocking detected for PerplexityBot, Perplexity-User.	Information

Copilot by Microsoft

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2025 ImmuniWeb SA

Meta Tag Restrictions

No meta tag restricting usage of website's content found.	Information

Server-side Blocking

No server-side User-Agent-based blocking detected for Bingbot, BingPreview.	Information

DeepSeek by Hangzhou DeepSeek Artificial Intelligence

DeepSeek does not have public policy confirming that it will follow rules as defined in robots.txt. Use server-side blocking based on User-Agent to restrict access.

Server-side Blocking

No server-side User-Agent-based blocking detected for DeepSeekBot.	Information

Meta AI by Meta

Robots.txt Directives

No robots.txt or applicable rules for Meta-ExternalAgent User-Agent(s) found.	Misconfiguration or weakness

Server-side Blocking

No server-side User-Agent-based blocking detected for Meta AI Crawler.	Information

AmazonBot by Amazon

Robots.txt Directives

No robots.txt or applicable rules for AmazonBot User-Agent(s) found.	Misconfiguration or weakness

Full Test Results: https://www.immuniweb.com/websec/www.computeon.house/AK5pRnwD/

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com

Copyright © 2025 ImmuniWeb SA

Meta Tag Restrictions

No meta tag restricting usage of website's content found.	Information

Server-side Blocking

Access blocked based on User-Agent Amazonbot. The server responded with a 403 status code.	Good configuration

Apple Intelligence by Apple

To control whether your website's content can be used to train Apple's AI models (Apple Intelligence), Apple follows the special Applebot-Extended User-Agent directive in your robots.txt file.

Robots.txt Directives

No rule is specified for the Apple-Extended User-Agent, so Apple imposes no restrictions on AI training and may use any content that its crawlers are allowed to access.	Information

Applebot-Extended does not crawl your site directly. Instead, it respects the access granted to other Apple crawlers: Applebot. If no Applebot rule is present, Applebot follows the rules defined for Googlebot.

No crawling rules are specified for Apple, so its crawlers are not subject to any restrictions.	Misconfiguration or weakness

Server-side Blocking

Access blocked based on User-Agent Applebot. The server responded with a 403 status code.	Good configuration

Doubao by ByteDance

Doubao is an AI chatbot developed by ByteDance, the company behind TikTok. ByteDance operates the Bytespider web crawler, which may collect website content — potentially for training Doubao and other AI models. ByteDance does not have a public policy confirming that Bytespider will follow robots.txt rules. Use server-side blocking based on User-Agent to restrict access.

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2025 ImmuniWeb SA

Server-side Blocking

Access blocked based on User-Agent Bytespider. The server responded with a 403 status code.	Good configuration

Custom Bot

A custom test crawler User-Agent used to check for simple keyword-based User-Agent blocks. Not associated with any real service and does not actually crawl the content on websites.

Server-side Blocking

Unable to determine server-side User-Agent blocking status for Custom Bot. The server responded with no status code.	Misconfiguration or weakness

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2025 ImmuniWeb SA

DNSSEC Configuration Test

DNSSEC (Domain Name System Security Extensions) is a security protocol that protects against DNS spoofing by ensuring the authenticity and integrity of DNS data.

Domain **www.computeon.house** has 1 unsigned DNS record of CNAME type:

Type	Domain name	Canonical Name
CNAME	www.computeon.house	computeon.house.

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2025 ImmuniWeb SA

Web Server Security Test

HTTP RESPONSE

200

HTTP VERSIONS

HTTP/1.0 HTTP/1.1 HTTP/2

NPN

N/A

ALPN

H2

CONTENT ENCODING

None

SERVER SIGNATURE

LiteSpeed

WAF

Custom

LOCATION

N/A

HTTP METHODS ENABLED

✔ GET ✔ POST ✔ HEAD ✔ OPTIONS ✔ PUT ✔ CUSTOM

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2025 ImmuniWeb SA

Web Software Security Test

Web Software Found	Web Software Outdated	Web Software Vulnerabilities
1	0	0

The following security vulnerabilities are known to be present in the fingerprinted version of web software. To run a comprehensive vulnerability scan of your web application, please use ImmuniWeb® Neuron.

Fingerprinted CMS & Vulnerabilities

Litespeed web server

CMS version is unknown. Make sure the CMS is up2date.

Fingerprinted CMS Components & Vulnerabilities

No components were fingerprinted on the website.	Information

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2025 ImmuniWeb SA

GDPR Compliance Test

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

PRIVACY POLICY

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

WEBSITE SECURITY

No publicly known vulnerabilities were found in the website CMS or its components.	Good configuration

TLS ENCRYPTION

HTTPS encryption is present on the web server.	Good configuration

COOKIE PROTECTION

No cookies with personal or tracking information seem to be sent.	Information

COOKIE DISCLAIMER

No third-party cookies or cookies with tracking information seem to be sent.	Information

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2025 ImmuniWeb SA

PCI DSS Compliance Test

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

REQUIREMENT 6.3

No publicly known vulnerabilities seem to be present in the fingerprinted versions of the website CMS and its components.	Good configuration

REQUIREMENT 6.4

The website seems to be protected by a WAF. Review its logs and configuration on a periodic basis.	Good configuration

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2025 ImmuniWeb SA

HTTP Headers Security Test

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

MISSING OPTIONAL HTTP HEADERS

Access-Control-Allow-Origin

SERVER

Web server does not disclose its version.	Good configuration

Raw HTTP Header

```
Server: LiteSpeed
```

STRICT-TRANSPORT-SECURITY (HSTS)

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

X-FRAME-OPTIONS

The header is properly set.	Good configuration
The header value is not consistent with Content-Security-Policy.	Information

Full Test Results: https://www.immuniweb.com/websec/www.computeon.house/AK5pRnwD/

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com

Copyright © 2025 ImmuniWeb SA

Raw HTTP Header

```
X-Frame-Options: DENY
```

X-CONTENT-TYPE-OPTIONS

The header is properly set.	Good configuration

Raw HTTP Header

```
X-Content-Type-Options: nosniff
```

PERMISSIONS-POLICY

The header is properly set.	Good configuration

Raw HTTP Header

```
Permissions-Policy: camera=(), microphone=(), geolocation=(), usb=(), payment=(),
accelerometer=(), gyroscope=(), magnetometer=(), fullscreen=(self)
```

REFERRER-POLICY

The header is properly set.	Good configuration

Raw HTTP Header

```
Referrer-Policy: strict-origin-when-cross-origin
```

X-XSS-PROTECTION

This header is deprecated and will not work in modern browsers.	Misconfiguration or weakness

REPORTING-ENDPOINTS

The header is properly set.	Good configuration

Full Test Results: https://www.immuniweb.com/websec/www.computeon.house/AK5pRnwD/

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com

Copyright © 2025 ImmuniWeb SA

Raw HTTP Header

```
Reporting-Endpoints: csp-endpoint="https://computeon.house/reports"
```

CROSS-ORIGIN-RESOURCE-POLICY (CORP)

The header is properly set.	Good configuration

Raw HTTP Header

```
Cross-Origin-Resource-Policy: same-origin
```

CROSS-ORIGIN-OPENER-POLICY (COOP)

The header is properly set.	Good configuration

Raw HTTP Header

```
Cross-Origin-Opener-Policy: same-origin
```

CROSS-ORIGIN-EMBEDDER-POLICY (COEP)

The header is properly set.	Good configuration

Raw HTTP Header

```
Cross-Origin-Embedder-Policy: require-corp
```


This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2025 ImmuniWeb SA

Content Security Policy (CSP) Test

CONTENT-SECURITY-POLICY (CSP)

Content-Security Policy is enforced.	Good configuration

Raw HTTP Header

```
Content-Security-Policy: upgrade-insecure-requests ; default-src 'none'; media-src 'self'; form-action 'none'; base-uri 'none'; object-src 'none'; frame-ancestors 'self'; script-src 'self'; style-src 'self'; img-src 'self' data:; font-src 'self'; connect-src 'self'; report-to csp-endpoint;
```

Directives

Name	Description	Alerts
default-src	The default-src directive serves as a fallback for the other fetch directives. 'none' - Keyword is OK	No problems found
media-src	Restricts the URLs from which video, audio, and associated text track resources may be loaded. 'self' - Keyword is OK	No problems found
form-action	Restricts the URLs which can be used as the target of a form submissions from a given context. 'none' - Keyword is OK	No problems found
base-uri	Restricts the URLs which can be used in a Document's base element.	No problems found

Full Test Results: https://www.immuniweb.com/websec/www.computeon.house/AK5pRnwD/

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com

Copyright © 2025 ImmuniWeb SA

Name	Description	Alerts
	'none' - Keyword is OK	
object-src	Restricts the URLs from which plugin content may be loaded. 'none' - Keyword is OK	No problems found
frame-ancestors	Restricts the URLs which can embed the resource using frame, iframe, object, or embed. 'self' - Keyword is OK	No problems found
script-src	Restricts the locations from which scripts may be executed. 'self' - 'self' can be problematic if you host JSONP, Angular or user uploaded files.	Information
style-src	Restricts the locations from which style may be applied to a Document. 'self' - Keyword is OK	No problems found
img-src	Restricts the URLs from which image resources may be loaded. 'self' - Keyword is OK data: - Scheme is OK	No problems found
font-src	Restricts the URLs from which font resources may be loaded. 'self' - Keyword is OK	No problems found

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2025 ImmuniWeb SA

Name	Description	Alerts
connect-src	Controls requests which transmit or receive data from other origins using script interfaces. 'self' - Keyword is OK	No problems found
report-to	Defines a reporting group to which violation reports ought to be sent. csp-endpoint - Value is OK	No problems found
require-trusted-types-for	MISSING: The HTTP Content-Security-Policy (CSP) require-trusted-types-for Experimental directive instructs user agents to control the data passed to DOM XSS sink functions, like Element.innerHTML setter. Consider requiring Trusted Types for scripts to lock down DOM XSS injection sinks. You can do this by adding "require-trusted-types-for 'script'" to your policy.	Information

CONTENT-SECURITY-POLICY-REPORT-ONLY

The header was not sent by the server.	Information

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2025 ImmuniWeb SA

Cookies Privacy and Security Test

No cookies were sent by the web application.	Good configuration

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2025 ImmuniWeb SA

Need More? Upgrade to ImmuniWeb® AI Platform

Get x10 more findings with 24/7 remediation support and ensure compliance:



ImmuniWeb® Discovery
Continuous Threat
Exposure Management



ImmuniWeb® On-Demand
Compliance-Ready Web
Penetration Testing



ImmuniWeb® Continuous
Continuous Application
Penetration Testing & PTaaS

FREE DEMO

Full Test Results: https://www.immuniweb.com/websec/www.computeon.house/AK5pRnwD/

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com

Copyright © 2025 ImmuniWeb SA

External Content Security Test

No External Content appears to be loaded by the website.	Information

The End of Report

Upgrade from Free Community Edition to ImmuniWeb® AI Platform



This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2025 ImmuniWeb SA