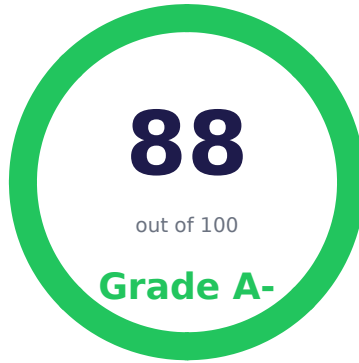


WebCheckApp

powered by **BudgetPixels**

SECURITY REPORT



vboxxcloud.nl

DEEP SCAN

Scanned: 07 Apr 2026, 07:41 UTC

Report generated: 09 Apr 2026, 09:22 UTC

Categories: 27 • Checks: 106

CONFIDENTIAL

Table of Contents

01	Score Overview & Benchmark
02	Executive Summary
03	Prioritized Action Plan
04	Risk Impact Matrix
05	OWASP Top 10 Analysis
06	Critical Issues (1)
07	Warnings (19)
08	Passed Checks (84)
09	Detected Technologies
10	Category Details
11	Next Steps & Recommendations

★ Score Overview

88

SCORE /100

1

CRITICAL

19

WARNINGS

84

PASSED

CHECK RESULTS DISTRIBUTION



YOUR SCORE VS. INDUSTRY AVERAGE



Your website scores **26 points above** the industry average.

CATEGORY SCORECARD

CATEGORY	SCORE	PERFORMANCE	STATUS
DNS & Email Security	75/100	<div><div style="width: 75%;"></div></div>	● Good
SSL & HTTPS	88/100	<div><div style="width: 88%;"></div></div>	● Good
TLS / Cipher	84/100	<div><div style="width: 84%;"></div></div>	● Good
OWASP Top 10	88/100	<div><div style="width: 88%;"></div></div>	● Good
Robots & Sitemap	80/100	<div><div style="width: 80%;"></div></div>	● Good
Content & CMS	88/100	<div><div style="width: 88%;"></div></div>	● Good
Security Headers	82/100	<div><div style="width: 82%;"></div></div>	● Good
Branding & Social	100/100	<div><div style="width: 100%;"></div></div>	● Good
Performance & SEO	100/100	<div><div style="width: 100%;"></div></div>	● Good
API Security	100/100	<div><div style="width: 100%;"></div></div>	● Good
HTTP Methods	100/100	<div><div style="width: 100%;"></div></div>	● Good
Accessibility	85/100	<div><div style="width: 85%;"></div></div>	● Good
Exposed Files	100/100	<div><div style="width: 100%;"></div></div>	● Good
Email Security	88/100	<div><div style="width: 88%;"></div></div>	● Good
Directory Discovery	87/100	<div><div style="width: 87%;"></div></div>	● Good
Error Disclosure	100/100	<div><div style="width: 100%;"></div></div>	● Good
Input Reflection	100/100	<div><div style="width: 100%;"></div></div>	● Good
Session Security	100/100	<div><div style="width: 100%;"></div></div>	● Good
Cookie Compliance	88/100	<div><div style="width: 88%;"></div></div>	● Good
Subdomain Takeover	100/100	<div><div style="width: 100%;"></div></div>	● Good

📄 Executive Summary

We performed a comprehensive security analysis of **vboxxcloud.nl** across 20 categories. The website received an overall score of **88/100** (grade **A-**), with 1 critical issue, 19 warnings, and 84 passed checks.

Overall assessment: vboxxcloud.nl demonstrates a strong security posture. The website follows most security best practices and is well-configured. Minor improvements are possible but no urgent issues were found.

✓ SSL & HTTPS

✓ TLS / Cipher

✓ OWASP Top 10

✓ Robots & Sitemap

✓ Content & CMS

⚠ DNS & Email Security

👉 Prioritized Action Plan

Address these items in order of priority to maximize your security improvement.

#	ISSUE	CATEGORY	URGENCY	RECOMMENDED ACTION
1	No weak cipher suites	SSL & HTTPS	Immediately	Restrict your cipher list in your server config: Nginx: ssl_ciphers ECDH+AESGCM:ECDH+AES256:ECDH+AES128:!aNULL:!MD5:!3DES:!RC4; Apache: SSLCipherSuite HIGH:!aNULL:!MD5:!3DES:!RC4 Then reload your server.
2	CAA record configured	DNS & Email Security	This Week	Add a CAA DNS record, e.g.: 0 issue "letsencrypt.org" to restrict SSL issuance.
3	MTA-STS (email transport security)	DNS & Email Security	This Week	Implement MTA-STS: add a TXT record at _mta-sts.vboxxcloud.nl with value "v=STSV1; id=YYYYMMDD01" and publish a policy file at https://mta-sts.vboxxcloud.nl/.well-known/mta-sts.txt
4	DNSSEC	DNS & Email Security	This Week	Enable DNSSEC through your domain registrar to protect against DNS cache poisoning.
5	TLS 1.3 supported	TLS / Cipher	This Week	Enable TLS 1.3 on your web server for better security and performance.
6	A02:2021 - Cryptographic Failures	OWASP Top 10	This Week	Enable HTTPS with strong TLS 1.2+ configuration. Set HSTS header with a long max-age. Remove all mixed content. Use secure cipher suites only.
7	A04:2021 - Insecure Design	OWASP Top 10	This Week	Add X-Frame-Options or CSP frame-ancestors to prevent clickjacking. Disable GraphQL introspection in production. Implement rate limiting on all endpoints.
8	A05:2021 - Security Misconfiguration	OWASP Top 10	This Week	Remove server version headers. Close unnecessary ports. Remove all exposed configuration files. Disable debug mode in production.
9	A08:2021 - Software and Data Integrity Failures	OWASP Top 10	This Week	Add Subresource Integrity (SRI) hashes to all external scripts and stylesheets. Set COOP and COEP headers for cross-origin isolation.
10	Crawlers not fully blocked	Robots & Sitemap	This Week	If this is a production site, remove or restrict the broad Disallow: / rule to allow indexing.
11	Subresource Integrity (SRI)	Content & CMS	This Week	Add integrity= and crossorigin= attributes to external <script> and <link> tags. Generate hashes at https://www.srihash.org/

📊 Risk Impact Matrix

Overview of findings per category, showing the distribution of critical issues, warnings, and passed checks.

CATEGORY	CRITICAL	WARNINGS	PASSED	SCORE
SSL & HTTPS	1	—	5	88
Directory Discovery	—	4	—	87
DNS & Email Security	—	3	3	75
Security Headers	—	2	7	82
TLS / Cipher	—	1	4	84
Robots & Sitemap	—	1	4	80
Content & CMS	—	1	5	88

Performance & SEO	—	1	4	100
Accessibility	—	1	6	85
Email Security	—	1	4	88
Branding & Social	—	—	8	100
API Security	—	—	3	100
HTTP Methods	—	—	3	100
Exposed Files	—	—	10	100
Error Disclosure	—	—	3	100
Input Reflection	—	—	3	100
Session Security	—	—	1	100
Cookie Compliance	—	—	4	88
Subdomain Takeover	—	—	1	100

The OWASP Top 10 is the globally recognized standard for web application security risks.

✓ A01:2021 - Broken Access Control

LOW RISK

No broken access control issues detected. Access restrictions appear properly configured.

⚠ A02:2021 - Cryptographic Failures

MEDIUM RISK

Issues found: SSL/TLS configuration has weaknesses.

☐ Enable HTTPS with strong TLS 1.2+ configuration. Set HSTS header with a long max-age. Remove all mixed content. Use secure cipher suites only.

✓ A03:2021 - Injection

LOW RISK

Injection protections look adequate. CSP and content type headers are in place.

⚠ A04:2021 - Insecure Design

MEDIUM RISK

Issues found: No visible rate limiting headers detected (may still be present server-side).

☐ Add X-Frame-Options or CSP frame-ancestors to prevent clickjacking. Disable GraphQL introspection in production. Implement rate limiting on all endpoints.

⚠ A05:2021 - Security Misconfiguration

MEDIUM RISK

Issues found: Dangerous ports are open and accessible from the internet.

☐ Remove server version headers. Close unnecessary ports. Remove all exposed configuration files. Disable debug mode in production.

✓ A06:2021 - Vulnerable and Outdated Components

LOW RISK

No known vulnerable components detected in the visible technology stack.

✓ A07:2021 - Identification and Authentication Failures

LOW RISK

Authentication-related configurations appear secure. No user enumeration or credential exposure detected.

⚠ A08:2021 - Software and Data Integrity Failures

MEDIUM RISK

Issues found: Cross-Origin-Opener-Policy (COOP) header not set; Cross-Origin-Embedder-Policy (COEP) header not set.

☐ Add Subresource Integrity (SRI) hashes to all external scripts and stylesheets. Set COOP and COEP headers for cross-origin isolation.

✓ A09:2021 - Security Logging and Monitoring Failures

LOW RISK

Security monitoring indicators are in place. A security.txt file is present for vulnerability reporting.

✓ A10:2021 - Server-Side Request Forgery (SSRF)

LOW RISK

No SSRF indicators detected. No open redirects or exposed internal endpoints found.

✗ Critical Issues (1)

These issues pose an immediate security risk and should be addressed as a priority.

No weak cipher suites SSL & HTTPS

Server accepts weak cipher suite(s): RC4, 3DES, EXPORT, NULL. These ciphers have known cryptographic weaknesses.

☐ Restrict your cipher list in your server config: Nginx: ssl_ciphers ECDH+AESGCM:ECDH+AES256:ECDH+AES128:!aNULL:!MD5:!3DES:!RC4; Apache: SSLCipherSuite HIGH:!aNULL:!MD5:!3DES:!RC4 Then reload your server.

WHAT THIS MEANS FOR YOUR VISITORS

Without proper SSL, visitor data (passwords, personal info) can be intercepted by attackers on the same network.

⚠ Warnings (19)

These items are not immediately critical but should be reviewed to strengthen your security posture.

CAA record configured DNS & Email Security

No CAA record found. Any Certificate Authority can issue SSL certs for your domain.

[Add a CAA DNS record, e.g.: 0 issue "letsencrypt.org" to restrict SSL issuance.](#)

MTA-STS (email transport security) DNS & Email Security

No MTA-STS record found at `_mta-sts.vboxxcloud.nl`. Without it, email delivery to your domain could silently fall back to unencrypted connections.

[Implement MTA-STS: add a TXT record at `_mta-sts.vboxxcloud.nl` with value "v=STSV1; id=YYYYMMDD01" and publish a policy file at `https://mta-sts.vboxxcloud.nl/.well-known/mta-sts.txt`](#)

DNSSEC DNS & Email Security

DNSSEC could not be confirmed via this check. Verify with your domain registrar.

[Enable DNSSEC through your domain registrar to protect against DNS cache poisoning.](#)

TLS 1.3 supported TLS / Cipher

TLS 1.3 is not supported.

[Enable TLS 1.3 on your web server for better security and performance.](#)

A02:2021 - Cryptographic Failures OWASP Top 10

Issues found: SSL/TLS configuration has weaknesses.

[Enable HTTPS with strong TLS 1.2+ configuration. Set HSTS header with a long max-age. Remove all mixed content. Use secure cipher suites only.](#)

A04:2021 - Insecure Design OWASP Top 10

Issues found: No visible rate limiting headers detected (may still be present server-side).

[Add X-Frame-Options or CSP frame-ancestors to prevent clickjacking. Disable GraphQL introspection in production. Implement rate limiting on all endpoints.](#)

A05:2021 - Security Misconfiguration OWASP Top 10

Issues found: Dangerous ports are open and accessible from the internet.

[Remove server version headers. Close unnecessary ports. Remove all exposed configuration files. Disable debug mode in production.](#)

A08:2021 - Software and Data Integrity Failures OWASP Top 10

Issues found: Cross-Origin-Opener-Policy (COOP) header not set; Cross-Origin-Embedder-Policy (COEP) header not set.

[Add Subresource Integrity \(SRI\) hashes to all external scripts and stylesheets. Set COOP and COEP headers for cross-origin isolation.](#)

Crawlers not fully blocked Robots & Sitemap

`robots.txt` appears to block all crawlers (`Disallow: /`). This will prevent search engine indexing.

[If this is a production site, remove or restrict the broad `Disallow: /` rule to allow indexing.](#)

Subresource Integrity (SRI) Content & CMS

1 of 1 external script(s)/stylesheet(s) load without an `integrity=` hash. If the CDN is compromised, malicious code could be silently injected into your pages.

[Add `integrity=` and `crossorigin=` attributes to external `<script>` and `<link>` tags. Generate hashes at <https://www.srihash.org/>](#)

Cross-Origin-Opener-Policy Security Headers

No Cross-Origin-Opener-Policy (COOP) header found.

[Add Cross-Origin-Opener-Policy: `same-origin` to isolate your browsing context and protect against cross-origin attacks and Spectre-like vulnerabilities.](#)

Cross-Origin-Embedder-Policy Security Headers

No Cross-Origin-Embedder-Policy (COEP) header found.

[Add Cross-Origin-Embedder-Policy: `require-corp` to enable advanced browser isolation features \(required for SharedArrayBuffer and high-resolution timers\).](#)

security.txt present Performance & SEO

No `security.txt` file found at `/.well-known/security.txt` or `/security.txt`.

[Create a `security.txt` file \(RFC 9116\) at `/.well-known/security.txt` to provide security researchers with a responsible disclosure contact.](#)

Form labels Accessibility

2 of 2 form inputs may be missing accessible labels.

☐ Associate each `<input>` with a `<label for="...">` or use `aria-label/aria-labelledby`.

No DANE/TLSA record Email Security

No DANE TLSA record found. DANE provides additional verification for TLS certificates on mail servers.

phpMyAdmin found at /phpmyadmin Directory Discovery

Path /phpmyadmin returned HTTP 302 (redirects). This could expose phpMyAdmin to attackers.

☐ Verify that /phpmyadmin requires proper authentication.

phpMyAdmin (alias) found at /pma Directory Discovery

Path /pma returned HTTP 302 (redirects). This could expose phpMyAdmin (alias) to attackers.

☐ Verify that /pma requires proper authentication.

Webmail interface found at /webmail Directory Discovery

Path /webmail returned HTTP 302 (redirects). This could expose Webmail interface to attackers.

☐ Verify that /webmail requires proper authentication.

Configuration directory found at /config Directory Discovery

Path /config returned HTTP 302 (redirects). This could expose Configuration directory to attackers.

☐ Verify that /config requires proper authentication.

✓ Passed Checks (84)

These checks were all successfully validated.

✓ SPF record configured DNS & Email Security	✓ Fast server response time (TTFB) Performance & SEO
✓ DMARC record configured DNS & Email Security	✓ Response compression enabled Performance & SEO
✓ DKIM record configured DNS & Email Security	✓ robots.txt present Performance & SEO
✓ HTTPS / SSL enabled SSL & HTTPS	✓ XML sitemap present Performance & SEO
✓ SSL certificate valid SSL & HTTPS	✓ API/docs endpoints API Security
✓ HTTP redirects to HTTPS SSL & HTTPS	✓ GraphQL introspection API Security
✓ HSTS header configured SSL & HTTPS	✓ WordPress user enumeration API Security
✓ TLS 1.0 and 1.1 disabled SSL & HTTPS	✓ Only safe HTTP methods allowed HTTP Methods
✓ TLS 1.2 supported TLS / Cipher	✓ TRACE method is disabled HTTP Methods
✓ TLS 1.1 disabled TLS / Cipher	✓ PUT method rejects arbitrary uploads HTTP Methods
✓ TLS 1.0 disabled TLS / Cipher	✓ HTML lang attribute Accessibility
✓ Perfect Forward Secrecy (PFS) TLS / Cipher	✓ Viewport meta tag Accessibility
✓ A01:2021 - Broken Access Control OWASP Top 10	✓ Page title Accessibility
✓ A03:2021 - Injection OWASP Top 10	✓ Meta description Accessibility
✓ A06:2021 - Vulnerable and Outdated Components OWASP Top 10	✓ Image alt attributes Accessibility
✓ A07:2021 - Identification and Authentication Failures OWASP Top 10	✓ Single H1 heading Accessibility
✓ A09:2021 - Security Logging and Monitoring Failures OWASP Top 10	✓ .env file exposed Exposed Files
✓ A10:2021 - Server-Side Request Forgery (SSRF) OWASP Top 10	✓ .git directory exposed Exposed Files
✓ robots.txt present Robots & Sitemap	✓ phpinfo() page exposed Exposed Files
✓ Sitemap referenced in robots.txt Robots & Sitemap	✓ Database backup file exposed Exposed Files
✓ Sitemap accessible Robots & Sitemap	✓ WordPress config backup exposed Exposed Files
✓ security.txt present Robots & Sitemap	✓ .htpasswd file exposed Exposed Files

✓ No mixed content detected	Content & CMS	✓ web.config not exposed	Exposed Files
✓ CMS admin panel not publicly accessible	Content & CMS	✓ .git/config not exposed	Exposed Files
✓ CMS version not exposed	Content & CMS	✓ composer.lock not exposed	Exposed Files
✓ No open redirect	Content & CMS	✓ Apache server-status not exposed	Exposed Files
✓ Directory listing disabled	Content & CMS	✓ SPF record is strict (-all)	Email Security
✓ Server version not disclosed	Security Headers	✓ DMARC policy is reject	Email Security
✓ Content-Security-Policy	Security Headers	✓ MX records configured	Email Security
✓ X-Frame-Options	Security Headers	✓ SMTP banner not exposing version	Email Security
✓ X-Content-Type-Options	Security Headers	✓ 404 error page is clean	Error Disclosure
✓ Referrer-Policy	Security Headers	✓ Server error pages are clean	Error Disclosure
✓ Permissions-Policy	Security Headers	✓ No version information in error responses	Error Disclosure
✓ X-XSS-Protection (deprecated)	Security Headers	✓ No input reflection detected	Input Reflection
✓ Favicon	Branding & Social	✓ Error pages do not reflect URL	Input Reflection
✓ Apple Touch Icon	Branding & Social	✓ Forms submit to same origin	Input Reflection
✓ Web App Manifest	Branding & Social	✓ No session cookies detected	Session Security
✓ Open Graph title	Branding & Social	✓ No tracking cookies, no consent needed	Cookie Compliance
✓ Open Graph description	Branding & Social	✓ No tracking cookies on initial load	Cookie Compliance
✓ Open Graph image	Branding & Social	✓ Only 0 cookie(s) on initial load	Cookie Compliance
✓ Twitter/X Card	Branding & Social	✓ No excessively long-lived cookies	Cookie Compliance
✓ Theme color	Branding & Social	✓ Subdomain takeover	Subdomain Takeover

Detected Technologies

The following technologies were detected on vboxxcloud.nl.

WEB SERVER

Apache

⚠️ **HTTP/2 not enabled** — The server is using HTTP/1.1. Enabling HTTP/2 can noticeably improve page load speed.

Category Details

DNS & Email Security

75/100

CAA record configured

No CAA record found. Any Certificate Authority can issue SSL certs for your domain.

🔗 [Add a CAA DNS record, e.g.: 0 issue "letsencrypt.org" to restrict SSL issuance.](#)

MTA-STS (email transport security)

No MTA-STS record found at `_mta-sts.vboxxcloud.nl`. Without it, email delivery to your domain could silently fall back to unencrypted connections.

🔗 [Implement MTA-STS: add a TXT record at `_mta-sts.vboxxcloud.nl` with value `"v=STSV1; id=YYYYMMDD01"` and publish a policy file at `https://mta-sts.vboxxcloud.nl/.well-known/mta-sts.txt`](#)

DNSSEC

DNSSEC could not be confirmed via this check. Verify with your domain registrar.

🔗 [Enable DNSSEC through your domain registrar to protect against DNS cache poisoning.](#)

Robots & Sitemap

80/100

Crawlers not fully blocked

`robots.txt` appears to block all crawlers (`Disallow: /`). This will prevent search engine indexing.

🔗 [If this is a production site, remove or restrict the broad `Disallow: /` rule to allow indexing.](#)

Security Headers

82/100

Cross-Origin-Opener-Policy

No Cross-Origin-Opener-Policy (COOP) header found.

🔗 [Add Cross-Origin-Opener-Policy: `same-origin` to isolate your browsing context and protect against cross-origin attacks and Spectre-like vulnerabilities.](#)

Cross-Origin-Embedder-Policy

No Cross-Origin-Embedder-Policy (COEP) header found.

🔗 [Add Cross-Origin-Embedder-Policy: `require-corp` to enable advanced browser isolation features \(required for `SharedArrayBuffer` and high-resolution timers\).](#)

TLS / Cipher

84/100

TLS 1.3 supported

TLS 1.3 is not supported.

🔗 [Enable TLS 1.3 on your web server for better security and performance.](#)

Accessibility

85/100

Form labels

2 of 2 form inputs may be missing accessible labels.

[☐ Associate each <input> with a <label for="..."> or use aria-label/aria-labelledby.](#)

Directory Discovery

87/100

phpMyAdmin found at /phpmyadmin

Path /phpmyadmin returned HTTP 302 (redirects). This could expose phpMyAdmin to attackers.

[☐ Verify that /phpmyadmin requires proper authentication.](#)

phpMyAdmin (alias) found at /pma

Path /pma returned HTTP 302 (redirects). This could expose phpMyAdmin (alias) to attackers.

[☐ Verify that /pma requires proper authentication.](#)

Webmail interface found at /webmail

Path /webmail returned HTTP 302 (redirects). This could expose Webmail interface to attackers.

[☐ Verify that /webmail requires proper authentication.](#)

Configuration directory found at /config

Path /config returned HTTP 302 (redirects). This could expose Configuration directory to attackers.

[☐ Verify that /config requires proper authentication.](#)

SSL & HTTPS

88/100

No weak cipher suites

Server accepts weak cipher suite(s): RC4, 3DES, EXPORT, NULL. These ciphers have known cryptographic weaknesses.

[☐ Restrict your cipher list in your server config: Nginx: ssl_ciphers ECDH+AESGCM:ECDH+AES256:ECDH+AES128:!aNULL:!MD5:!3DES:!RC4; Apache: SSLCipherSuite HIGH:!aNULL:!MD5:!3DES:!RC4 Then reload your server.](#)

Content & CMS

88/100

Subresource Integrity (SRI)

1 of 1 external script(s)/stylesheet(s) load without an integrity= hash. If the CDN is compromised, malicious code could be silently injected into your pages.

[☐ Add integrity= and crossorigin= attributes to external <script> and <link> tags. Generate hashes at <https://www.srihash.org/>](#)

Email Security

88/100

No DANE/TLSA record

No DANE TLSA record found. DANE provides additional verification for TLS certificates on mail servers.

Cookie Compliance

88/100

✓ All checks passed

Branding & Social

100/100

✓ All checks passed

Performance & SEO

100/100

security.txt present

No security.txt file found at /.well-known/security.txt or /security.txt.

[🔗 Create a security.txt file \(RFC 9116\) at /.well-known/security.txt to provide security researchers with a responsible disclosure contact.](#)

API Security

100/100

✓ All checks passed

HTTP Methods

100/100

✓ All checks passed

Exposed Files

100/100

✓ All checks passed

Error Disclosure

100/100

✓ All checks passed

Input Reflection

100/100

✓ All checks passed

Session Security

100/100

✓ All checks passed

Subdomain Takeover

100/100

✓ All checks passed

Next Steps & Recommendations

Recommended Next Steps

- 1 Address Critical Issues First** — You have 1 critical issue that requires immediate attention. Start with the items marked "Immediately" in the Action Plan.
- 2 Review Warnings** — After resolving critical issues, address the 19 warnings to strengthen your overall security posture.
- 3 Re-scan Your Website** — After implementing fixes, run a new scan to verify improvements and ensure no new issues were introduced.
- 4 Schedule Regular Scans** — Security is not a one-time effort. We recommend scanning your website at least once per month to catch new vulnerabilities.

Report Validity

Scan performed: **07 Apr 2026, 07:41 UTC**

Report generated: **09 Apr 2026, 09:22 UTC**

Valid until: **07 May 2026**

Scan type: **Deep Scan**

This report reflects the state of the website at the time of scanning. Security configurations may change over time. We recommend re-scanning after 30 days or after significant changes to your website.

YOUR SECURITY SCORE

88/100

Grade A-

Excellent! Your website meets high security standards.

Need Professional Help?

Our security experts can help you fix every issue in this report.
Manual penetration testing • Code reviews • Compliance audits

budgetpixels.nl

This report was generated by WebCheckApp (webcheckapp.com). All information is for informational purposes only and does not constitute professional security advice. Results are based on automated checks of publicly accessible information.