WebCheckApp

powered by **BudgetPixels**

SECURITY REPORT

88

out of 100

Grade A-

vboxxcloud.nl

DEEP SCAN

Scanned: 09 Apr 2026, 07:10 UTC

Report generated: 09 Apr 2026, 11:04 UTC

Categories: 27 • Checks: 106

Table of Contents

Score Overview

88	1	19	84
SCORE /100	CRITICAL	WARNINGS	PASSED

CHECK RESULTS DISTRIBUTION

Passed (84) Warnings (19) Critical (1)

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		Good
SSL & HTTPS	88/100		Good
TLS / Cipher	84/100		Good
OWASP Top 10	88/100		Good
Robots & Sitemap	80/100		Good
Content & CMS	88/100		Good
Security Headers	82/100		Good
Branding & Social	100/100		Good
Performance & SEO	100/100		Good
API Security	100/100		Good
HTTP Methods	100/100		Good
Accessibility	85/100		Good
Exposed Files	100/100		Good
Email Security	88/100		Good
Directory Discovery	87/100		Good
Error Disclosure	100/100		Good
Input Reflection	100/100		Good
Session Security	100/100		Good
Cookie Compliance	88/100		Good
Subdomain Takeover	100/100		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

OWASP Top 10 Analysis

Score: 88/100

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- ✓ A06:2021 – Vulnerable and Outdated Components OWASP Top 10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

✓ No mixed content detected Content & CMS
✓ CMS admin panel not publicly accessible Content & CMS
✓ CMS version not exposed Content & CMS
✓ No open redirect Content & CMS
✓ Directory listing disabled Content & CMS
✓ Server version not disclosed Security Headers
✓ Content-Security-Policy Security Headers
✓ X-Frame-Options Security Headers
✓ X-Content-Type-Options Security Headers
✓ Referrer-Policy Security Headers
✓ Permissions-Policy Security Headers
✓ X-XSS-Protection (deprecated) Security Headers
✓ Favicon Branding & Social
✓ Apple Touch Icon Branding & Social
✓ Web App Manifest Branding & Social
✓ Open Graph title Branding & Social
✓ Open Graph description Branding & Social
✓ Open Graph image Branding & Social
✓ Twitter/X Card Branding & Social
✓ Theme color Branding & Social
✓ web.config not exposed Exposed Files
✓ .git/config not exposed Exposed Files
✓ composer.lock not exposed Exposed Files
✓ Apache server-status not exposed Exposed Files
✓ SPF record is strict (-all) Email Security
✓ DMARC policy is reject Email Security
✓ MX records configured Email Security
✓ SMTP banner not exposing version Email Security
✓ 404 error page is clean Error Disclosure
✓ Server error pages are clean Error Disclosure
✓ No version information in error responses Error Disclosure
✓ No input reflection detected Input Reflection
✓ Error pages do not reflect URL Input Reflection
✓ Forms submit to same origin Input Reflection
✓ No session cookies detected Session Security
✓ No tracking cookies, no consent needed Cookie Compliance
✓ No tracking cookies on initial load Cookie Compliance
✓ Only 0 cookie(s) on initial load Cookie Compliance
✓ No excessively long-lived cookies Cookie Compliance
✓ 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:	**09 Apr 2026, 07:10 UTC**
Report generated:	**09 Apr 2026, 11:04 UTC**
Valid until:	**09 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.