WebCheckApp

powered by **BudgetPixels**

SECURITY REPORT

66

out of 100

Grade C+

coach.vitalifecenter.nl

DEEP SCAN

Scanned: 26 Apr 2026, 10:11 UTC

Report generated: 26 Apr 2026, 14:19 UTC

Categories: 27 • Checks: 101

Table of Contents

Score Overview

66	11	19	65
SCORE /100	CRITICAL	WARNINGS	PASSED

CHECK RESULTS DISTRIBUTION

Passed (65) Warnings (19) Critical (11)

YOUR SCORE VS. INDUSTRY AVERAGE

Your website scores **4 points above** the industry average.

CATEGORY SCORECARD

CATEGORY	SCORE	PERFORMANCE	STATUS
DNS & Email Security	0/100		Poor
SSL & HTTPS	94/100		Good
TLS / Cipher	100/100		Good
OWASP Top 10	83/100		Good
Robots & Sitemap	13/100		Poor
Content & CMS	100/100		Good
Security Headers	11/100		Poor
Branding & Social	45/100		Poor
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	0/100		Poor
Directory Discovery	97/100		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 **coach.vitalifecenter.nl** across 20 categories. The website received an overall score of **66/100** (grade **C+**), with 11 critical issues, 19 warnings, and 65 passed checks.

Overall assessment: coach.vitalifecenter.nl has a reasonable security foundation but there is room for improvement. Several issues were identified that could expose the website or its users to unnecessary risk. We recommend addressing the critical issues first.

✓	SSL & HTTPS
✓	TLS / Cipher
✓	OWASP Top 10
✓	Content & CMS
✓	Performance & SEO
✗	DNS & Email Security
✗	Email Security
✗	Security Headers
✗	Robots & Sitemap
✗	Branding & Social

Prioritized Action Plan

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

#	ISSUE	CATEGORY	URGENCY	RECOMMENDED ACTION
1	**SPF record configured**	DNS & Email Security	**Immediately**	Add a TXT record to your DNS: v=spf1 include:yourmailprovider.com ~all
2	**DMARC record configured**	DNS & Email Security	**Immediately**	Add a TXT record to _dmarc.coach.vitalifecenter.nl: v=DMARC1; p=quarantine; rua=mailto:dmarc@coach.vitalifecenter.nl
3	**A03:2021 – Injection**	OWASP Top 10	**Immediately**	Implement a strict Content-Security-Policy. Set X-Content-Type-Options: nosniff. Sanitize and encode all user input. Use parameterized queries for database access.
4	**Content-Security-Policy**	Security Headers	**Immediately**	Add a Content-Security-Policy header to restrict which resources the browser may load, preventing XSS attacks.
5	**X-Frame-Options**	Security Headers	**Immediately**	Add X-Frame-Options: DENY or SAMEORIGIN, or use CSP frame-ancestors.
6	**X-Content-Type-Options**	Security Headers	**Immediately**	Add X-Content-Type-Options: nosniff to prevent browsers from MIME-sniffing responses.
7	**Referrer-Policy**	Security Headers	**Immediately**	Add Referrer-Policy: strict-origin-when-cross-origin to control how much referrer info is sent.
8	**Single H1 heading**	Accessibility	**Immediately**	Add a single <h1> tag that describes the main topic of the page.
9	**No SPF record found**	Email Security	**Immediately**	Add an SPF TXT record: "v=spf1 include:your-mail-provider -all".
10	**No DMARC record found**	Email Security	**Immediately**	Add a DMARC TXT record on _dmarc.yourdomain.com: "v=DMARC1; p=reject; rua=mailto:dmarc@yourdomain.com".
11	**Installation wizard found at /install**	Directory Discovery	**Immediately**	Restrict access to /install or remove it from the public web root.
12	**CAA record configured**	DNS & Email Security	**This Week**	Add a CAA DNS record, e.g.: 0 issue "letsencrypt.org" to restrict SSL issuance.
13	**DKIM record configured**	DNS & Email Security	**This Week**	Configure DKIM in your email provider (Google Workspace, Microsoft 365, etc.) and publish the TXT record they provide at {selector}._domainkey.coach.vitalifecenter.nl
14	**MTA-STS (email transport security)**	DNS & Email Security	**This Week**	Implement MTA-STS: add a TXT record at _mta-sts.coach.vitalifecenter.nl with value "v=STSv1; id=YYYYMMDD01" and publish a policy file at https://mta-sts.coach.vitalifecenter.nl/.well-known/mta-sts.txt
15	**HTTP redirects to HTTPS**	SSL & HTTPS	**This Week**	Use 301 permanent redirects at every step from HTTP to HTTPS for better SEO and caching.

Risk Impact Matrix

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

CATEGORY	CRITICAL	WARNINGS	PASSED	SCORE
Security Headers	4	2	1	11
DNS & Email Security	2	3	—	0

Email Security	2	1	—	0
Accessibility	1	—	6	85
Directory Discovery	1	—	—	97
Robots & Sitemap	—	4	—	13
Branding & Social	—	4	4	45
SSL & HTTPS	—	1	5	94
Performance & SEO	—	1	4	100
TLS / Cipher	—	—	5	100
Content & CMS	—	—	6	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: 83/100

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

⚠ A01:2021 – Broken Access Control

MEDIUM RISK

Issues found: CORS policy allows wildcard origins.

Restrict access to sensitive files and directories. Implement proper authentication on all API endpoints. Disable directory listing. Configure CORS with specific allowed origins.

✓ A02:2021 – Cryptographic Failures

LOW RISK

Cryptographic configuration is strong. SSL/TLS and HSTS are properly configured.

✗ A03:2021 – Injection

CRITICAL RISK

Issues found: Content-Security-Policy is missing or weak (XSS protection reduced); X-Content-Type-Options header missing (MIME sniffing risk).

Implement a strict Content-Security-Policy. Set X-Content-Type-Options: nosniff. Sanitize and encode all user input. Use parameterized queries for database access.

⚠ A04:2021 – Insecure Design

MEDIUM RISK

Issues found: Clickjacking protection missing (no X-Frame-Options or frame-ancestors).

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

LOW RISK

No security misconfigurations detected. Server headers and file access are properly restricted.

✓ 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

LOW RISK

Data integrity protections are in place. External resources are properly secured.

⚠ A09:2021 – Security Logging and Monitoring Failures

MEDIUM RISK

Issues found: No security.txt file found (RFC 9116) — security researchers cannot easily report vulnerabilities.

Add a /.well-known/security.txt file with contact information per RFC 9116. Configure custom error pages that do not expose internal details.

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

LOW RISK

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

✗ Critical Issues (11)

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

SPF record configured

DNS & Email Security

No SPF record found. Anyone can send emails pretending to be from your domain.

Add a TXT record to your DNS: v=spf1 include:yourmailprovider.com ~all

WHAT THIS MEANS FOR YOUR VISITORS

Weak DNS/email security allows attackers to send emails pretending to be your domain (phishing).

DMARC record configured DNS & Email Security

No DMARC record found at _dmarc.coach.vitalifecenter.nl.

Add a TXT record to _dmarc.coach.vitalifecenter.nl: v=DMARC1; p=quarantine; rua=mailto:dmarc@coach.vitalifecenter.nl

WHAT THIS MEANS FOR YOUR VISITORS

Weak DNS/email security allows attackers to send emails pretending to be your domain (phishing).

A03:2021 – Injection OWASP Top 10

Issues found: Content-Security-Policy is missing or weak (XSS protection reduced); X-Content-Type-Options header missing (MIME sniffing risk).

Implement a strict Content-Security-Policy. Set X-Content-Type-Options: nosniff. Sanitize and encode all user input. Use parameterized queries for database access.

WHAT THIS MEANS FOR YOUR VISITORS

These are the most critical web application security risks recognized worldwide.

Content-Security-Policy Security Headers

No Content-Security-Policy header found.

Add a Content-Security-Policy header to restrict which resources the browser may load, preventing XSS attacks.

WHAT THIS MEANS FOR YOUR VISITORS

Missing security headers make your website vulnerable to clickjacking, XSS attacks, and data injection.

X-Frame-Options Security Headers

No X-Frame-Options header found. The site may be vulnerable to clickjacking.

Add X-Frame-Options: DENY or SAMEORIGIN, or use CSP frame-ancestors.

WHAT THIS MEANS FOR YOUR VISITORS

Missing security headers make your website vulnerable to clickjacking, XSS attacks, and data injection.

X-Content-Type-Options Security Headers

X-Content-Type-Options header is missing.

Add X-Content-Type-Options: nosniff to prevent browsers from MIME-sniffing responses.

WHAT THIS MEANS FOR YOUR VISITORS

Missing security headers make your website vulnerable to clickjacking, XSS attacks, and data injection.

Referrer-Policy Security Headers

No Referrer-Policy header found.

Add Referrer-Policy: strict-origin-when-cross-origin to control how much referrer info is sent.

WHAT THIS MEANS FOR YOUR VISITORS

Missing security headers make your website vulnerable to clickjacking, XSS attacks, and data injection.

Single H1 heading Accessibility

No H1 heading found on the page.

Add a single <h1> tag that describes the main topic of the page.

No SPF record found Email Security

No SPF record is configured for this domain, allowing anyone to send email as this domain.

Add an SPF TXT record: "v=spf1 include:your-mail-provider -all".

No DMARC record found Email Security

No DMARC record found. Without DMARC, receiving servers cannot verify your email authentication policies.

Add a DMARC TXT record on _dmarc.yourdomain.com: "v=DMARC1; p=reject; rua=mailto:dmarc@yourdomain.com".

Installation wizard found at /install Directory Discovery

Path /install returned HTTP 200 (accessible). This could expose Installation wizard to attackers.

Restrict access to /install or remove it from the public web root.

⚠ 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.

DKIM record configured DNS & Email Security

No DKIM record found for common selectors. DKIM cryptographically signs outgoing emails, making them verifiable and preventing tampering in transit.

Configure DKIM in your email provider (Google Workspace, Microsoft 365, etc.) and publish the TXT record they provide at {selector}._domainkey.coach.vitalifecenter.nl

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

No MTA-STS record found at _mta-sts.coach.vitalifecenter.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.coach.vitalifecenter.nl with value "v=STSv1; id=YYYYMMDD01" and publish a policy file at https://mta-sts.coach.vitalifecenter.nl/.well-known/mta-sts.txt

HTTP redirects to HTTPS SSL & HTTPS

HTTP redirects to HTTPS, but not via a fully permanent redirect chain.

Use 301 permanent redirects at every step from HTTP to HTTPS for better SEO and caching.

A01:2021 – Broken Access Control OWASP Top 10

Issues found: CORS policy allows wildcard origins.

Restrict access to sensitive files and directories. Implement proper authentication on all API endpoints. Disable directory listing. Configure CORS with specific allowed origins.

A04:2021 – Insecure Design OWASP Top 10

Issues found: Clickjacking protection missing (no X-Frame-Options or frame-ancestors).

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

A09:2021 – Security Logging and Monitoring Failures OWASP Top 10

Issues found: No security.txt file found (RFC 9116) — security researchers cannot easily report vulnerabilities.

Add a /.well-known/security.txt file with contact information per RFC 9116. Configure custom error pages that do not expose internal details.

robots.txt present Robots & Sitemap

A robots.txt file exists but does not appear to be valid (no User-agent directive found).

Ensure robots.txt starts with User-agent: directives.

Sitemap referenced in robots.txt Robots & Sitemap

robots.txt does not reference a sitemap.

Add a Sitemap: https://yourdomain.com/sitemap.xml line to robots.txt.

Sitemap accessible Robots & Sitemap

No accessible XML sitemap found at /sitemap.xml or /sitemap_index.xml.

Create an XML sitemap and submit it to Google Search Console and Bing Webmaster Tools.

security.txt present Robots & Sitemap

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

Create a security.txt file (RFC 9116) with Contact: and Expires: fields to enable responsible vulnerability disclosure.

Permissions-Policy Security Headers

No Permissions-Policy header found.

Add a Permissions-Policy header to restrict browser features like camera, microphone, and geolocation.

CORS policy Security Headers

Access-Control-Allow-Origin: * is set. Any website can make cross-origin requests to this server and read the response.

Replace the wildcard with specific trusted origins: Access-Control-Allow-Origin: https://yourtrustedapp.com Only use * for fully public APIs that serve no authenticated or user-specific data.

Open Graph title Branding & Social

No og:title meta tag found.

Add <meta property="og:title" content="..."> for proper social media previews on Facebook, LinkedIn, and WhatsApp.

Open Graph description Branding & Social

No og:description meta tag found.

Add <meta property="og:description" content="..."> for social media link previews.

Open Graph image Branding & Social

No og:image meta tag found.

Add <meta property="og:image" content="..."> with a 1200×630px image for social sharing previews.

Twitter/X Card Branding & Social

No twitter:card meta tag found.

Add <meta name="twitter:card" content="summary_large_image"> for rich link previews on X/Twitter.

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.

No MX records found Email Security

No MX records found. This domain cannot receive email. If email is not needed, consider adding a null MX record (RFC 7505).

✓ Passed Checks (65)

These checks were all successfully validated.

- ✓ HTTPS / SSL enabled SSL & HTTPS
- ✓ SSL certificate valid SSL & HTTPS
- ✓ HSTS header configured SSL & HTTPS
- ✓ No weak cipher suites SSL & HTTPS
- ✓ TLS 1.0 and 1.1 disabled SSL & HTTPS
- ✓ TLS 1.3 supported TLS / Cipher
- ✓ TLS 1.2 supported TLS / Cipher
- ✓ TLS 1.1 disabled TLS / Cipher
- ✓ TLS 1.0 disabled TLS / Cipher
- ✓ Perfect Forward Secrecy (PFS) TLS / Cipher
- ✓ A02:2021 – Cryptographic Failures OWASP Top 10
- ✓ A05:2021 – Security Misconfiguration OWASP Top 10
- ✓ A06:2021 – Vulnerable and Outdated Components OWASP Top 10
- ✓ A07:2021 – Identification and Authentication Failures OWASP Top 10
- ✓ A08:2021 – Software and Data Integrity Failures OWASP Top 10
- ✓ WordPress user enumeration API Security
- ✓ OPTIONS method does not expose allowed methods 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
- ✓ Form labels 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

✓ A10:2021 – Server-Side Request Forgery (SSRF) OWASP Top 10	✓ .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
✓ Subresource Integrity (SRI) Content & CMS	✓ Apache server-status not exposed Exposed Files
✓ No open redirect Content & CMS	✓ 404 error page is clean Error Disclosure
✓ Directory listing disabled Content & CMS	✓ Server error pages are clean Error Disclosure
✓ Server version not disclosed Security Headers	✓ No version information in error responses Error Disclosure
✓ Favicon Branding & Social	✓ No input reflection detected Input Reflection
✓ Apple Touch Icon Branding & Social	✓ Error pages do not reflect URL Input Reflection
✓ Web App Manifest Branding & Social	✓ Forms submit to same origin Input Reflection
✓ Theme color Branding & Social	✓ No session cookies detected Session Security
✓ Fast server response time (TTFB) Performance & SEO	✓ No tracking cookies, no consent needed Cookie Compliance
✓ Response compression enabled Performance & SEO	✓ No tracking cookies on initial load Cookie Compliance
✓ robots.txt present Performance & SEO	✓ Only 0 cookie(s) on initial load Cookie Compliance
✓ XML sitemap present Performance & SEO	✓ No excessively long-lived cookies Cookie Compliance
✓ API/docs endpoints API Security	✓ Subdomain takeover Subdomain Takeover
✓ GraphQL introspection disabled API Security	

Detected Technologies

The following technologies were detected on coach.vitalifecenter.nl.

JAVASCRIPT Next.js

⚠ **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 0/100

SPF record configured

No SPF record found. Anyone can send emails pretending to be from your domain.

Add a TXT record to your DNS: v=spf1 include:yourmailprovider.com ~all

DMARC record configured

No DMARC record found at _dmarc.coach.vitalifecenter.nl.

Add a TXT record to _dmarc.coach.vitalifecenter.nl: v=DMARC1; p=quarantine; rua=mailto:dmarc@coach.vitalifecenter.nl

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.

DKIM record configured

No DKIM record found for common selectors. DKIM cryptographically signs outgoing emails, making them verifiable and preventing tampering in transit.

Configure DKIM in your email provider (Google Workspace, Microsoft 365, etc.) and publish the TXT record they provide at {selector}._domainkey.coach.vitalifecenter.nl

MTA-STS (email transport security)

No MTA-STS record found at _mta-sts.coach.vitalifecenter.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.coach.vitalifecenter.nl with value "v=STSv1; id=YYYYMMDD01" and publish a policy file at https://mta-sts.coach.vitalifecenter.nl/.well-known/mta-sts.txt

Email Security 0/100

No SPF record found

No SPF record is configured for this domain, allowing anyone to send email as this domain.

Add an SPF TXT record: "v=spf1 include:your-mail-provider -all".

No DMARC record found

No DMARC record found. Without DMARC, receiving servers cannot verify your email authentication policies.

Add a DMARC TXT record on _dmarc.yourdomain.com: "v=DMARC1; p=reject; rua=mailto:dmarc@yourdomain.com".

No MX records found

No MX records found. This domain cannot receive email. If email is not needed, consider adding a null MX record (RFC 7505).

Security Headers 11/100

Content-Security-Policy

No Content-Security-Policy header found.

□□ Add a Content-Security-Policy header to restrict which resources the browser may load, preventing XSS attacks.

X-Frame-Options

No X-Frame-Options header found. The site may be vulnerable to clickjacking.

□□ Add X-Frame-Options: DENY or SAMEORIGIN, or use CSP frame-ancestors.

X-Content-Type-Options

X-Content-Type-Options header is missing.

□□ Add X-Content-Type-Options: nosniff to prevent browsers from MIME-sniffing responses.

Referrer-Policy

No Referrer-Policy header found.

□□ Add Referrer-Policy: strict-origin-when-cross-origin to control how much referrer info is sent.

Permissions-Policy

No Permissions-Policy header found.

□□ Add a Permissions-Policy header to restrict browser features like camera, microphone, and geolocation.

CORS policy

Access-Control-Allow-Origin: * is set. Any website can make cross-origin requests to this server and read the response.

□□ Replace the wildcard with specific trusted origins: Access-Control-Allow-Origin: https://yourtrustedapp.com Only use * for fully public APIs that serve no authenticated or user-specific data.

Robots & Sitemap 13/100

robots.txt present

A robots.txt file exists but does not appear to be valid (no User-agent directive found).

□□ Ensure robots.txt starts with User-agent: directives.

Sitemap referenced in robots.txt

robots.txt does not reference a sitemap.

□□ Add a Sitemap: https://yourdomain.com/sitemap.xml line to robots.txt.

Sitemap accessible

No accessible XML sitemap found at /sitemap.xml or /sitemap_index.xml.

□□ Create an XML sitemap and submit it to Google Search Console and Bing Webmaster Tools.

security.txt present

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

□□ Create a security.txt file (RFC 9116) with Contact: and Expires: fields to enable responsible vulnerability disclosure.

Branding & Social — 45/100

Open Graph title

No og:title meta tag found.

Add <meta property="og:title" content="..."> for proper social media previews on Facebook, LinkedIn, and WhatsApp.

Open Graph description

No og:description meta tag found.

Add <meta property="og:description" content="..."> for social media link previews.

Open Graph image

No og:image meta tag found.

Add <meta property="og:image" content="..."> with a 1200×630px image for social sharing previews.

Twitter/X Card

No twitter:card meta tag found.

Add <meta name="twitter:card" content="summary_large_image"> for rich link previews on X/Twitter.

Accessibility — 85/100

Single H1 heading

No H1 heading found on the page.

Add a single <h1> tag that describes the main topic of the page.

Cookie Compliance — 88/100

✓ All checks passed

SSL & HTTPS — 94/100

HTTP redirects to HTTPS

HTTP redirects to HTTPS, but not via a fully permanent redirect chain.

Use 301 permanent redirects at every step from HTTP to HTTPS for better SEO and caching.

Directory Discovery — 97/100

Installation wizard found at /install

Path /install returned HTTP 200 (accessible). This could expose Installation wizard to attackers.

Restrict access to /install or remove it from the public web root.

TLS / Cipher — 100/100

✓ All checks passed

Content & CMS — 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 11 critical issues that require 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:	**26 Apr 2026, 10:11 UTC**
Report generated:	**26 Apr 2026, 14:19 UTC**
Valid until:	**26 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

66/100

Grade C+

Good foundation. Address the identified issues to reach an A-grade.