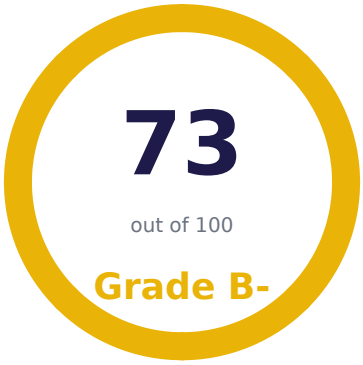
WebCheckApp

powered by **BudgetPixels**

SECURITY REPORT



squadspawn.com

DEEP SCAN

Scanned: 13 Apr 2026, 14:21 UTC

Report generated: 13 Apr 2026, 18:14 UTC

Categories: 27 • Checks: 109

CONFIDENTIAL

Table of Contents

Score Overview

73	9	20	74
SCORE /100	CRITICAL	WARNINGS	PASSED

CHECK RESULTS DISTRIBUTION

Passed (74) Warnings (20) Critical (9)

YOUR SCORE VS. INDUSTRY AVERAGE

Your website scores **11 points above** the industry average.

CATEGORY SCORECARD

CATEGORY	SCORE	PERFORMANCE	STATUS
DNS & Email Security	58/100		Fair
SSL & HTTPS	69/100		Fair
TLS / Cipher	100/100		Good
OWASP Top 10	80/100		Good
Robots & Sitemap	65/100		Fair
Content & CMS	88/100		Good
Security Headers	40/100		Poor
Branding & Social	80/100		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	75/100		Good
Directory Discovery	90/100		Good
Error Disclosure	100/100		Good
Input Reflection	50/100		Fair
Session Security	50/100		Fair
Cookie Compliance	88/100		Good
Subdomain Takeover	100/100		Good

Executive Summary

We performed a comprehensive security analysis of **squadspawn.com** across 20 categories. The website received an overall score of **73/100** (grade **B-**), with 9 critical issues, 20 warnings, and 74 passed checks.

Overall assessment: squadspawn.com 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.

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

Prioritized Action Plan

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

#	ISSUE	CATEGORY	URGENCY	RECOMMENDED ACTION
1	**HTTP redirects to HTTPS**	SSL & HTTPS	**Immediately**	Configure a permanent (301) redirect from HTTP to HTTPS.
2	**HSTS header configured**	SSL & HTTPS	**Immediately**	Add: Strict-Transport-Security: max-age=31536000; includeSubDomains
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	**Referrer-Policy**	Security Headers	**Immediately**	Add Referrer-Policy: strict-origin-when-cross-origin to control how much referrer info is sent.
6	**Cookie security flags**	Security Headers	**Immediately**	Set HttpOnly (prevents JS access), Secure (HTTPS only), and SameSite=Lax or Strict on all cookies.
7	**Single H1 heading**	Accessibility	**Immediately**	Add a single <h1> tag that describes the main topic of the page.
8	**Parameter 'q' reflected in response**	Input Reflection	**Immediately**	Encode all user input before rendering in HTML. Use context-aware output encoding (HTML entities, JavaScript escaping, URL encoding).
9	**Session cookies missing HttpOnly flag**	Session Security	**Immediately**	Set the HttpOnly flag on all session cookies to prevent access from client-side scripts.
10	**CAA record configured**	DNS & Email Security	**This Week**	Add a CAA DNS record, e.g.: 0 issue "letsencrypt.org" to restrict SSL issuance.
11	**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.squadspawn.com
12	**MTA-STS (email transport security)**	DNS & Email Security	**This Week**	Implement MTA-STS: add a TXT record at _mta-sts.squadspawn.com with value "v=STSv1; id=YYYYMMDD01" and publish a policy file at https://mta-sts.squadspawn.com/.well-known/mta-sts.txt
13	**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.
14	**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.
15	**A07:2021 – Identification and Authentication Failures**	OWASP Top 10	**This Week**	Disable WordPress user enumeration. Remove exposed credential files. Set Secure, HttpOnly, and SameSite flags on all session cookies.

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	3	1	4	40
SSL & HTTPS	2	—	4	69
Input Reflection	1	1	1	50

Session Security	1	1	2	50
Accessibility	1	—	6	85
DNS & Email Security	—	3	2	58
Directory Discovery	—	3	—	90
Robots & Sitemap	—	2	3	65
Branding & Social	—	2	6	80
Content & CMS	—	1	5	88
Performance & SEO	—	1	4	100
Email Security	—	1	3	75
TLS / Cipher	—	—	5	100
API Security	—	—	3	100
HTTP Methods	—	—	3	100
Exposed Files	—	—	10	100
Error Disclosure	—	—	3	100
Cookie Compliance	—	—	4	88
Subdomain Takeover	—	—	1	100

OWASP Top 10 Analysis

Score: 80/100

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

CRITICAL RISK

Issues found: Content-Security-Policy is missing or weak (XSS protection reduced); URL parameters are reflected in HTML response (potential XSS).

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

LOW RISK

Application design appears secure. Clickjacking protection and API security are in place.

⚠ 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

MEDIUM RISK

Issues found: Session cookie 'XSRF-TOKEN' missing HttpOnly flag.

Disable WordPress user enumeration. Remove exposed credential files. Set Secure, HttpOnly, and SameSite flags on all session cookies.

✓ 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 (9)

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

HTTP redirects to HTTPS

SSL & HTTPS

HTTP requests are not being redirected to HTTPS.

Configure a permanent (301) redirect from HTTP to HTTPS.

WHAT THIS MEANS FOR YOUR VISITORS

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

HSTS header configured SSL & HTTPS

No Strict-Transport-Security (HSTS) header found.

Add: Strict-Transport-Security: max-age=31536000; includeSubDomains

WHAT THIS MEANS FOR YOUR VISITORS

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

A03:2021 – Injection OWASP Top 10

Issues found: Content-Security-Policy is missing or weak (XSS protection reduced); URL parameters are reflected in HTML response (potential XSS).

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.

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.

Cookie security flags Security Headers

One or more cookies are missing security flags: XSRF-TOKEN (missing: HttpOnly).

Set HttpOnly (prevents JS access), Secure (HTTPS only), and SameSite=Lax or Strict on all cookies.

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.

Parameter 'q' reflected in response Input Reflection

The parameter 'q' is reflected inside a script block — high XSS risk.

Encode all user input before rendering in HTML. Use context-aware output encoding (HTML entities, JavaScript escaping, URL encoding).

Session cookies missing HttpOnly flag Session Security

One or more session cookies do not have the HttpOnly flag, making them accessible via JavaScript (XSS risk).

Set the HttpOnly flag on all session cookies to prevent access from client-side scripts.

⚠ Warnings (20)

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.squadspawn.com

MTA-STS (email transport security)

DNS & Email Security

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

Implement MTA-STS: add a TXT record at _mta-sts.squadspawn.com with value "v=STSv1; id=YYYYMMDD01" and publish a policy file at https://mta-sts.squadspawn.com/.well-known/mta-sts.txt

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.

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.

A07:2021 – Identification and Authentication Failures

OWASP Top 10

Issues found: Session cookie 'XSRF-TOKEN' missing HttpOnly flag.

Disable WordPress user enumeration. Remove exposed credential files. Set Secure, HttpOnly, and SameSite flags on all session cookies.

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.

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.

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.

Subresource Integrity (SRI)

Content & CMS

4 of 4 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/

Permissions-Policy

Security Headers

No Permissions-Policy header found.

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

Apple Touch Icon

Branding & Social

No Apple Touch Icon found.

Add <link rel="apple-touch-icon" sizes="180x180" href="/apple-touch-icon.png"> for iOS home screen support.

Web App Manifest

Branding & Social

No Web App Manifest found.

Add a manifest.json (or site.webmanifest) with name, icons, and theme_color for PWA support.

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.

DMARC policy is quarantine Email Security

DMARC policy is set to quarantine. For maximum protection, consider upgrading to reject.

After monitoring DMARC reports to confirm no legitimate mail is affected, change policy from p=quarantine to p=reject.

SVN repository found at /.svn Directory Discovery

Path /.svn returned HTTP 403 (forbidden but exists). This could expose SVN repository to attackers.

Verify that /.svn requires proper authentication.

Mercurial repository found at /.hg Directory Discovery

Path /.hg returned HTTP 403 (forbidden but exists). This could expose Mercurial repository to attackers.

Verify that /.hg requires proper authentication.

macOS metadata file found at /.DS_Store Directory Discovery

Path /.DS_Store returned HTTP 403 (forbidden but exists). This could expose macOS metadata file to attackers.

Verify that /.DS_Store requires proper authentication.

URL path reflected in error page Input Reflection

The requested URL path is reflected in the error page response. This could be exploited for XSS if output is not properly encoded.

Ensure error pages use proper HTML encoding for all dynamic content including the requested URL.

No cookie prefix used Session Security

Session cookies do not use the __Host- or __Secure- prefix. These prefixes provide additional protection against cookie overwriting.

Consider using __Host- prefix for session cookies (requires Secure flag, no Domain, Path=/).

Passed Checks (74)

These checks were all successfully validated.

- ✓ SPF record configured DNS & Email Security
- ✓ DMARC record configured DNS & Email Security
- ✓ HTTPS / SSL enabled SSL & HTTPS
- ✓ SSL certificate valid 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
- ✓ A01:2021 – Broken Access Control OWASP Top 10
- ✓ A04:2021 – Insecure Design OWASP Top 10
- ✓ A06:2021 – Vulnerable and Outdated Components OWASP Top 10
- ✓ A08:2021 – Software and Data Integrity Failures OWASP Top 10
- ✓ A10:2021 – Server-Side Request Forgery (SSRF) OWASP Top 10
- ✓ robots.txt present Robots & Sitemap
- ✓ Crawlers not fully blocked Robots & Sitemap
- ✓ Sitemap accessible Robots & Sitemap
- ✓ No mixed content detected Content & CMS
- ✓ CMS admin panel not publicly accessible Content & CMS
- ✓ XML sitemap present Performance & SEO
- ✓ API/docs endpoints API Security
- ✓ GraphQL introspection API Security
- ✓ 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
- ✓ .htpasswd file exposed Exposed Files
- ✓ web.config not exposed Exposed Files
- ✓ .git/config not exposed Exposed Files

- ✓ CMS version not exposed Content & CMS
- ✓ No open redirect Content & CMS
- ✓ Directory listing disabled Content & CMS
- ✓ Server version not disclosed Security Headers
- ✓ X-Frame-Options Security Headers
- ✓ X-Content-Type-Options Security Headers
- ✓ X-XSS-Protection (deprecated) Security Headers
- ✓ Favicon 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
- ✓ Fast server response time (TTFB) Performance & SEO
- ✓ Response compression enabled Performance & SEO
- ✓ robots.txt present Performance & SEO
- ✓ composer.lock not exposed Exposed Files
- ✓ Apache server-status not exposed Exposed Files
- ✓ SPF record is strict (-all) 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
- ✓ Forms submit to same origin Input Reflection
- ✓ Session cookies have Secure flag Session Security
- ✓ Session cookies have SameSite flag Session Security
- ✓ No tracking cookies, no consent needed Cookie Compliance
- ✓ No tracking cookies on initial load Cookie Compliance
- ✓ Only 2 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 squadspawn.com.

WEB SERVER Nginx

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

Category Details

Security Headers 40/100

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.

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.

Cookie security flags

One or more cookies are missing security flags: XSRF-TOKEN (missing: HttpOnly).

Set HttpOnly (prevents JS access), Secure (HTTPS only), and SameSite=Lax or Strict on all cookies.

Input Reflection 50/100

Parameter 'q' reflected in response

The parameter 'q' is reflected inside a script block — high XSS risk.

Encode all user input before rendering in HTML. Use context-aware output encoding (HTML entities, JavaScript escaping, URL encoding).

URL path reflected in error page

The requested URL path is reflected in the error page response. This could be exploited for XSS if output is not properly encoded.

Ensure error pages use proper HTML encoding for all dynamic content including the requested URL.

Session Security 50/100

Session cookies missing HttpOnly flag

One or more session cookies do not have the HttpOnly flag, making them accessible via JavaScript (XSS risk).

Set the HttpOnly flag on all session cookies to prevent access from client-side scripts.

No cookie prefix used

Session cookies do not use the __Host- or __Secure- prefix. These prefixes provide additional protection against cookie overwriting.

Consider using __Host- prefix for session cookies (requires Secure flag, no Domain, Path=/).

DNS & Email Security 58/100

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.

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.squadspawn.com

MTA-STS (email transport security)

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

□□ Implement MTA-STS: add a TXT record at _mta-sts.squadspawn.com with value "v=STSv1; id=YYYYMMDD01" and publish a policy file at https://mta-sts.squadspawn.com/.well-known/mta-sts.txt

Robots & Sitemap 65/100

Sitemap referenced in robots.txt

robots.txt does not reference a sitemap.

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

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.

SSL & HTTPS 69/100

HTTP redirects to HTTPS

HTTP requests are not being redirected to HTTPS.

□□ Configure a permanent (301) redirect from HTTP to HTTPS.

HSTS header configured

No Strict-Transport-Security (HSTS) header found.

□□ Add: Strict-Transport-Security: max-age=31536000; includeSubDomains

Email Security 75/100

DMARC policy is quarantine

DMARC policy is set to quarantine. For maximum protection, consider upgrading to reject.

□□ After monitoring DMARC reports to confirm no legitimate mail is affected, change policy from p=quarantine to p=reject.

Branding & Social 80/100

Apple Touch Icon

No Apple Touch Icon found.

□□ Add <link rel="apple-touch-icon" sizes="180x180" href="/apple-touch-icon.png"> for iOS home screen support.

Web App Manifest

No Web App Manifest found.

□□ Add a manifest.json (or site.webmanifest) with name, icons, and theme_color for PWA support.

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.

Content & CMS 88/100

Subresource Integrity (SRI)

4 of 4 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/

Cookie Compliance 88/100

✓ All checks passed

Directory Discovery 90/100

SVN repository found at /.svn

Path /.svn returned HTTP 403 (forbidden but exists). This could expose SVN repository to attackers.

Verify that /.svn requires proper authentication.

Mercurial repository found at /.hg

Path /.hg returned HTTP 403 (forbidden but exists). This could expose Mercurial repository to attackers.

Verify that /.hg requires proper authentication.

macOS metadata file found at /.DS_Store

Path /.DS_Store returned HTTP 403 (forbidden but exists). This could expose macOS metadata file to attackers.

Verify that /.DS_Store requires proper authentication.

TLS / Cipher 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

Subdomain Takeover **100/100**

✓ All checks passed

Next Steps & Recommendations

Recommended Next Steps

1. **Address Critical Issues First** — You have 9 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 20 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:	**13 Apr 2026, 14:21 UTC**
Report generated:	**13 Apr 2026, 18:14 UTC**
Valid until:	**13 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

73/100

Grade B-

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