WebCheckApp

Website Security Scanner

alturnanetworks.com

Deep Scan Report — 27 categories scanned

Scanned: 03 Apr 2026, 18:59 UTC

Generated: 04 Apr 2026, 00:36 UTC

webcheckapp.com

65
/100

C+

OVERALL GRADE

12 critical | 31 warnings | 65 passed

12 issues require immediate attention.

SSL & HTTPS	73
Security Headers	4
DNS & Email Security	75
Performance & SEO	100
Content & CMS	45
Exposed Files	100

Executive Summary

We performed a comprehensive security analysis of **alturnanetworks.com** across 20 categories. The website received an overall score of **65/100** (grade **C+**), with 12 critical issues, 31 warnings, and 65 passed checks.

Overall assessment: alturnanetworks.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, followed by the warnings.

✓ **Strong areas:** TLS / Cipher, Performance & SEO, API Security, HTTP Methods.

⚠ **Needs improvement:** DNS & Email Security, SSL & HTTPS, OWASP Top 10, Robots & Sitemap.

✗ **Weak areas:** Security Headers, Branding & Social, Content & CMS.

OWASP Top 10 Analysis (Score: 69/100)

The OWASP Top 10 is the globally recognized standard for web application security risks. Below is how alturnanetworks.com scores against each of the ten categories.

✓ 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); X-Content-Type-Options header missing (MIME sniffing risk); 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 Medium Risk

Issues found: Clickjacking protection missing (no X-Frame-Options or frame-ancestors); 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: Server version information is disclosed in headers.

□□ 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 High Risk

Issues found: Cross-Origin-Opener-Policy (COOP) header not set; Cross-Origin-Embedder-Policy (COEP) header not set; 2 external script(s) loaded without Subresource Integrity (SRI).

□□ 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 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 (12)

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

HSTS header configured SSL & HTTPS

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

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

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.

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); 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.

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; 2 external script(s) loaded without Subresource Integrity (SRI).

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

No mixed content detected Content & CMS

Found 2 resource(s) loaded over HTTP on this HTTPS page. Browsers will block or warn about these.

Update all resource URLs (src, action, stylesheet href) to use HTTPS.

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.

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.

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.

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.

Cookie security flags Security Headers

One or more cookies are missing security flags: _icl_current_language (missing: HttpOnly, Secure, SameSite).

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

Image alt attributes Accessibility

5 of 26 images are missing alt attributes.

Add descriptive alt attributes to all <img> tags. Use alt="" for decorative images.

Parameter 'search' reflected in response Input Reflection

The parameter 'search' 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).

Warnings (31)

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.alturnanetworks.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.alturnanetworks.com with value "v=STSv1; id=YYYYMMDD01" and publish a policy file at https://mta-sts.alturnanetworks.com/.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.

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: Clickjacking protection missing (no X-Frame-Options or frame-ancestors); 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: Server version information is disclosed in headers.

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

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.

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.

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.

CMS admin panel not publicly accessible Content & CMS

A CMS admin panel is directly accessible at /wp-login.php. Ensure it requires strong authentication.

□□ Restrict admin access by IP address, or add two-factor authentication.

CMS version not exposed Content & CMS

WordPress detected. Version "6.3.8" is exposed in the page source, which helps attackers target known vulnerabilities.

□□ Remove the generator meta tag and strip ?ver= parameters from script/style URLs.

Subresource Integrity (SRI) Content & CMS

36 of 36 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/

Server version not disclosed Security Headers

Server header reveals version: "Apache/2.4.29 (Ubuntu)".

Configure your web server to suppress the version number from the Server header.

Permissions-Policy Security Headers

No Permissions-Policy header found.

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

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).

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.

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.

Theme color Branding & Social

No theme-color meta tag found.

Add <meta name="theme-color" content="#yourcolor"> to brand the browser address bar on mobile.

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

1 of 1 form inputs may be missing accessible labels.

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

SPF uses soft fail (~all) Email Security

SPF record uses ~all (soft fail) instead of -all (hard fail). Spoofed emails may still be delivered.

Change SPF policy from ~all to -all once you have confirmed all legitimate mail sources are included.

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.

No DANE/TLSA record Email Security

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

Admin panel found at /admin Directory Discovery

Path /admin returned HTTP 302 (redirects). This could expose Admin panel to attackers.

Verify that /admin requires proper authentication.

WordPress admin found at /wp-admin Directory Discovery

Path /wp-admin returned HTTP 301 (redirects). This could expose WordPress admin to attackers.

Verify that /wp-admin requires proper authentication.

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 (65)

These checks were all successfully validated. Keep up the good work.

✓	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
✓	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
✓	A06:2021 – Vulnerable and Outdated Components	OWASP Top 10
✓	A07:2021 – Identification and Authentication 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
✓	WordPress XML-RPC disabled	Content & CMS
✓	WordPress user enumeration blocked	Content & CMS
✓	No open redirect	Content & CMS
✓	Directory listing disabled	Content & CMS
✓	Favicon	Branding & Social
✓	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
✓	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
✓	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
✓	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
✓	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
✓	Error pages do not reflect URL	Input Reflection
✓	Forms submit to same origin	Input Reflection
✓	Session cookies have Secure flag	Session Security
✓	Session cookies have HttpOnly flag	Session Security
✓	Session cookies have SameSite flag	Session Security
✓	No session cookies on homepage	Session Security
✓	Cookie consent mechanism detected	Cookie Compliance
✓	No tracking cookies on initial load	Cookie Compliance
✓	Only 1 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 alturnanetworks.com. Knowing your stack helps identify potential vulnerabilities.

WEB SERVER	Apache
JAVASCRIPT	jQuery
CSS FRAMEWORK	Bootstrap
CMS	WordPress

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

Category Details

Security Headers 4/100

Server version not disclosed

Server header reveals version: "Apache/2.4.29 (Ubuntu)".

Configure your web server to suppress the version number from the Server header.

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.

Cookie security flags

One or more cookies are missing security flags: _icl_current_language (missing: HttpOnly, Secure, SameSite).

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

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).

Branding & Social 15/100

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.

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.

Theme color

No theme-color meta tag found.

Add <meta name="theme-color" content="#yourcolor"> to brand the browser address bar on mobile.

Content & CMS 45/100

No mixed content detected

Found 2 resource(s) loaded over HTTP on this HTTPS page. Browsers will block or warn about these.

Update all resource URLs (src, action, stylesheet href) to use HTTPS.

CMS admin panel not publicly accessible

A CMS admin panel is directly accessible at /wp-login.php. Ensure it requires strong authentication.

Restrict admin access by IP address, or add two-factor authentication.

CMS version not exposed

WordPress detected. Version "6.3.8" is exposed in the page source, which helps attackers target known vulnerabilities.

Remove the generator meta tag and strip ?ver= parameters from script/style URLs.

Subresource Integrity (SRI)

36 of 36 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 63/100

SPF uses soft fail (~all)

SPF record uses ~all (soft fail) instead of -all (hard fail). Spoofed emails may still be delivered.

□□ Change SPF policy from ~all to -all once you have confirmed all legitimate mail sources are included.

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.

No DANE/TLSA record

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

Robots & Sitemap 65/100

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.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.

Input Reflection 67/100

Parameter 'search' reflected in response

The parameter 'search' 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).

SSL & HTTPS 73/100

HSTS header configured

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

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

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.

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.alturnanetworks.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.alturnanetworks.com with value "v=STSv1; id=YYYYMMDD01" and publish a policy file at https://mta-sts.alturnanetworks.com/.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.

Accessibility 81/100

Image alt attributes

5 of 26 images are missing alt attributes.

□□ Add descriptive alt attributes to all <img> tags. Use alt="" for decorative images.

Form labels

1 of 1 form inputs may be missing accessible labels.

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

Directory Discovery 93/100

Admin panel found at /admin

Path /admin returned HTTP 302 (redirects). This could expose Admin panel to attackers.

□□ Verify that /admin requires proper authentication.

WordPress admin found at /wp-admin

Path /wp-admin returned HTTP 301 (redirects). This could expose WordPress admin to attackers.

□□ Verify that /wp-admin 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

Cookie Compliance 100/100

✓ All checks passed

Subdomain Takeover 100/100

✓ All checks passed

Session Security 175/100

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=/).

Scan results are for informational purposes only and do not constitute professional security advice. Results are based on automated checks of publicly accessible information only.

Need a professional security audit? Visit budgetpixels.nl for manual penetration tests, code reviews, and compliance checks.