WebCheckApp

Website Security Scanner

bcnsports.nl

Deep Scan Report — 27 categories scanned

Scanned: 03 Apr 2026, 15:57 UTC

Generated: 04 Apr 2026, 00:29 UTC

webcheckapp.com

C+

OVERALL GRADE

6 critical | 29 warnings | 73 passed

6 issues require immediate attention.

SSL & HTTPS	73
Security Headers	33
DNS & Email Security	38
Performance & SEO	100
Content & CMS	88
Exposed Files	100

Executive Summary

We performed a comprehensive security analysis of **bcnsports.nl** across 20 categories. The website received an overall score of **69/100** (grade **C+**), with 6 critical issues, 29 warnings, and 73 passed checks.

Overall assessment: bcnsports.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, followed by the warnings.

✓ **Strong areas:** TLS / Cipher, Content & CMS, Branding & Social, Performance & SEO.

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

✗ **Weak areas:** Security Headers, DNS & Email Security, Email Security, Session Security.

OWASP Top 10 Analysis (Score: 77/100)

The OWASP Top 10 is the globally recognized standard for web application security risks. Below is how bcnsports.nl 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 Medium Risk

Issues found: Content-Security-Policy is missing or weak (XSS protection reduced).

□□ 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: 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 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 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 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 (6)

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.

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.

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: XSRF-TOKEN (missing: HttpOnly).

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

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 (29)

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

DMARC record configured DNS & Email Security

DMARC found but policy is "none" — emails are monitored but not rejected. Value: "v=DMARC1; p=none; rua=mailto:postmaster@bcnsports.nl; ruf=mailto:postmaster@bcnsports.nl; fo=1; adkim=r; aspf=r".

□□ Upgrade your DMARC policy from p=none to p=quarantine or p=reject to actively block spoofed emails.

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.bcnsports.nl

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

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

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.

A03:2021 – Injection OWASP Top 10

Issues found: Content-Security-Policy is missing or weak (XSS protection reduced).

□□ 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 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.

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.

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.

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.

Subresource Integrity (SRI) Content & CMS

3 of 3 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.

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).

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.

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.

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 none (monitoring only) Email Security

DMARC policy is set to none, meaning failed emails are still delivered. This only monitors, it does not protect.

Progress DMARC policy from p=none to p=quarantine, then to p=reject after monitoring reports.

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.

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.

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 (73)

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

✓	SPF 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
✓	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
✓	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
✓	X-Frame-Options	Security Headers
✓	X-Content-Type-Options	Security Headers
✓	X-XSS-Protection (deprecated)	Security Headers
✓	Favicon	Branding & Social
✓	Apple Touch Icon	Branding & Social
✓	Open Graph title	Branding & Social
✓	Open Graph description	Branding & Social
✓	Open Graph image	Branding & Social
✓	Twitter/X Card	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
✓	Image alt attributes	Accessibility
✓	Single H1 heading	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
✓	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
✓	No input reflection detected	Input Reflection
✓	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 SameSite flag	Session Security
✓	Cookie consent mechanism detected	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 bcnsports.nl. Knowing your stack helps identify potential vulnerabilities.

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 33/100

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.

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).

DNS & Email Security 38/100

DMARC record configured

DMARC found but policy is "none" — emails are monitored but not rejected. Value: "v=DMARC1; p=none; rua=mailto:postmaster@bcnsports.nl; ruf=mailto:postmaster@bcnsports.nl; fo=1; adkim=r; aspf=r".

□□ Upgrade your DMARC policy from p=none to p=quarantine or p=reject to actively block spoofed emails.

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.bcnsports.nl

MTA-STS (email transport security)

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

Email Security 45/100

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 none (monitoring only)

DMARC policy is set to none, meaning failed emails are still delivered. This only monitors, it does not protect.

□□ Progress DMARC policy from p=none to p=quarantine, then to p=reject after monitoring reports.

No DANE/TLSA record

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

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=/).

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.

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.

Branding & Social 80/100

Web App Manifest

No Web App Manifest found.

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

Theme color

No theme-color meta tag found.

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

Directory Discovery 87/100

Admin panel found at /admin

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

Verify that /admin requires proper authentication.

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.

Content & CMS 88/100

Subresource Integrity (SRI)

3 of 3 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/

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

Accessibility 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

Cookie Compliance 100/100

✓ All checks passed

Subdomain Takeover 100/100

✓ All checks passed

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.