# WebCheckApp

Website Security Scanner

## nba.com

Deep Scan Report — 27 categories scanned

Scanned: 04 Apr 2026, 08:51 UTC

Generated: 04 Apr 2026, 15:01 UTC

webcheckapp.com

67
/100

C+

OVERALL GRADE

7 critical | 76 warnings | 61 passed

7 issues require immediate attention.

| | |
|---|---|
| SSL & HTTPS | 64 |
| Security Headers | 36 |
| DNS & Email Security | 75 |
| Performance & SEO | 25 |
| Content & CMS | 100 |
| Exposed Files | 100 |

### Executive Summary

We performed a comprehensive security analysis of **nba.com** across 20 categories. The website received an overall score of **67/100** (grade **C+**), with 7 critical issues, 76 warnings, and 61 passed checks.

**Overall assessment:** nba.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, OWASP Top 10, Content & CMS, HTTP Methods.

⚠ **Needs improvement:** DNS & Email Security, SSL & HTTPS, Accessibility.

✗ **Weak areas:** Robots & Sitemap, Branding & Social, Directory Discovery, Performance & SEO.

### OWASP Top 10 Analysis (Score: 82/100)

The OWASP Top 10 is the globally recognized standard for web application security risks. Below is how nba.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** 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** 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** 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 (7)

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.

**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.

**Response compression enabled** Performance & SEO

No gzip or Brotli compression detected.

Enable gzip or Brotli compression on your web server. This typically reduces HTML/CSS/JS size by 60-80%.

**HTML lang attribute** Accessibility

No lang attribute found on the <html> element.

Add a lang attribute: <html lang="en"> or <html lang="nl">.

**Viewport meta tag** Accessibility

No viewport meta tag found.

Add <meta name="viewport" content="width=device-width, initial-scale=1"> to your <head>.

## Warnings (76)

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

**HSTS header configured** SSL & HTTPS

HSTS header present but max-age is only 86400 seconds (minimum recommended: 31536000).

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

**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.

**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.

**robots.txt present** Robots & Sitemap

No robots.txt file found at /robots.txt.

Create a robots.txt file to guide search engine crawlers. Minimum: User-agent: * Disallow:

**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.

**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).

**Favicon** Branding & Social

No favicon detected.

Add a favicon.ico or <link rel="icon" href="/favicon.ico">. Use a 32×32px PNG or ICO file.

**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.

**robots.txt present** Performance & SEO

No robots.txt file found.

Create a robots.txt file to guide search engine crawlers and prevent indexing of sensitive paths.

**XML sitemap present** Performance & SEO

No sitemap.xml found at common locations (/sitemap.xml, /sitemap_index.xml).

Create and submit an XML sitemap to Google Search Console to improve search indexing.

**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.

**API documentation exposed** API Security

Endpoint accessible at /api/docs (authentication required).

The /api/docs endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**Swagger UI exposed** API Security

Endpoint accessible at /swagger-ui.html (authentication required).

The /swagger-ui.html endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**Swagger UI exposed** API Security

Endpoint accessible at /swagger-ui/ (authentication required).

The /swagger-ui/ endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**Swagger UI exposed** API Security

Endpoint accessible at /api/swagger (authentication required).

The /api/swagger endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**Swagger spec exposed** API Security

Endpoint accessible at /swagger.json (authentication required).

The /swagger.json endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**Swagger spec exposed** API Security

Endpoint accessible at /swagger.yaml (authentication required).

The /swagger.yaml endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**OpenAPI spec exposed** API Security

Endpoint accessible at /openapi.json (authentication required).

The /openapi.json endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**OpenAPI spec exposed** API Security

Endpoint accessible at /openapi.yaml (authentication required).

The /openapi.yaml endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**GraphiQL IDE exposed** API Security

Endpoint accessible at /graphiql (authentication required).

The /graphiql endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**Spring Actuator exposed** API Security

Endpoint accessible at /actuator (authentication required).

The /actuator endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**Spring Actuator health exposed** API Security

Endpoint accessible at /actuator/health (authentication required).

The /actuator/health endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**Elasticsearch API exposed** API Security

Endpoint accessible at /_cat/indices (authentication required).

The /_cat/indices endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**OpenID Connect metadata exposed** API Security

Endpoint accessible at /.well-known/openid-configuration (authentication required).

The /.well-known/openid-configuration endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**REST API exposed** API Security

Endpoint accessible at /api/v1 (authentication required).

The /api/v1 endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**REST API exposed** API Security

Endpoint accessible at /api/v2 (authentication required).

The /api/v2 endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**JSON Web Key Set (JWKS) exposed** API Security

Endpoint accessible at /.well-known/jwks.json (authentication required).

The /.well-known/jwks.json endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**Meta description** Accessibility

No meta description found.

Add <meta name="description" content="..."> to improve SEO and accessibility.

**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 403 (forbidden but exists). This could expose Admin panel to attackers.

Verify that /admin requires proper authentication.

**Admin panel found at /administrator** Directory Discovery

Path /administrator returned HTTP 403 (forbidden but exists). This could expose Admin panel to attackers.

Verify that /administrator requires proper authentication.

**WordPress admin found at /wp-admin** Directory Discovery

Path /wp-admin returned HTTP 403 (forbidden but exists). This could expose WordPress admin to attackers.

Verify that /wp-admin requires proper authentication.

**phpMyAdmin found at /phpmyadmin** Directory Discovery

Path /phpmyadmin returned HTTP 403 (forbidden but exists). This could expose phpMyAdmin to attackers.

Verify that /phpmyadmin requires proper authentication.

**phpMyAdmin (alias) found at /pma** Directory Discovery

Path /pma returned HTTP 403 (forbidden but exists). This could expose phpMyAdmin (alias) to attackers.

Verify that /pma requires proper authentication.

**Adminer database tool found at /adminer** Directory Discovery

Path /adminer returned HTTP 403 (forbidden but exists). This could expose Adminer database tool to attackers.

Verify that /adminer requires proper authentication.

**cPanel found at /cpanel** Directory Discovery

Path /cpanel returned HTTP 403 (forbidden but exists). This could expose cPanel to attackers.

Verify that /cpanel requires proper authentication.

**Webmail interface found at /webmail** Directory Discovery

Path /webmail returned HTTP 403 (forbidden but exists). This could expose Webmail interface to attackers.

Verify that /webmail requires proper authentication.

**Backup directory found at /backup** Directory Discovery

Path /backup returned HTTP 403 (forbidden but exists). This could expose Backup directory to attackers.

Verify that /backup requires proper authentication.

**Backup directory found at /backups** Directory Discovery

Path /backups returned HTTP 403 (forbidden but exists). This could expose Backup directory to attackers.

Verify that /backups requires proper authentication.

**Test directory found at /test** Directory Discovery

Path /test returned HTTP 403 (forbidden but exists). This could expose Test directory to attackers.

Verify that /test requires proper authentication.

**Staging environment found at /staging** Directory Discovery

Path /staging returned HTTP 403 (forbidden but exists). This could expose Staging environment to attackers.

Verify that /staging requires proper authentication.

**Development directory found at /dev** Directory Discovery

Path /dev returned HTTP 403 (forbidden but exists). This could expose Development directory to attackers.

Verify that /dev requires proper authentication.

**Debug page found at /debug** Directory Discovery

Path /debug returned HTTP 403 (forbidden but exists). This could expose Debug page to attackers.

Verify that /debug requires proper authentication.

**Temporary directory found at /tmp** Directory Discovery

Path /tmp returned HTTP 403 (forbidden but exists). This could expose Temporary directory to attackers.

Verify that /tmp requires proper authentication.

**Temporary directory found at /temp** Directory Discovery

Path /temp returned HTTP 403 (forbidden but exists). This could expose Temporary directory to attackers.

Verify that /temp requires proper authentication.

**Log files found at /log** Directory Discovery

Path /log returned HTTP 403 (forbidden but exists). This could expose Log files to attackers.

Verify that /log requires proper authentication.

**Log files found at /logs** Directory Discovery

Path /logs returned HTTP 403 (forbidden but exists). This could expose Log files to attackers.

Verify that /logs requires proper authentication.

**Old/archived files found at /old** Directory Discovery

Path /old returned HTTP 403 (forbidden but exists). This could expose Old/archived files to attackers.

Verify that /old requires proper authentication.

**Archive directory found at /archive** Directory Discovery

Path /archive returned HTTP 403 (forbidden but exists). This could expose Archive directory to attackers.

Verify that /archive requires proper authentication.

**Data dump found at /dump** Directory Discovery

Path /dump returned HTTP 403 (forbidden but exists). This could expose Data dump to attackers.

Verify that /dump requires proper authentication.

**SQL files found at /sql** Directory Discovery

Path /sql returned HTTP 403 (forbidden but exists). This could expose SQL files to attackers.

Verify that /sql requires proper authentication.

**Database files found at /db** Directory Discovery

Path /db returned HTTP 403 (forbidden but exists). This could expose Database files to attackers.

Verify that /db requires proper authentication.

**Configuration directory found at /config** Directory Discovery

Path /config returned HTTP 403 (forbidden but exists). This could expose Configuration directory to attackers.

Verify that /config requires proper authentication.

**Installation wizard found at /install** Directory Discovery

Path /install returned HTTP 403 (forbidden but exists). This could expose Installation wizard to attackers.

Verify that /install requires proper authentication.

**Setup wizard found at /setup** Directory Discovery

Path /setup returned HTTP 403 (forbidden but exists). This could expose Setup wizard to attackers.

Verify that /setup 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.

**XML-RPC endpoint found at /xmlrpc.php** Directory Discovery

Path /xmlrpc.php returned HTTP 403 (forbidden but exists). This could expose XML-RPC endpoint to attackers.

Verify that /xmlrpc.php 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.

## ✓ Passed Checks (61)

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 |
| ✓ | 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 |
| ✓ | 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 |
| ✓ | A10:2021 – Server-Side Request Forgery (SSRF) | OWASP Top 10 |
| ✓ | No mixed content detected | Content & CMS |
| ✓ | CMS admin panel not publicly accessible | Content & CMS |
| ✓ | CMS version not exposed | Content & CMS |
| ✓ | Subresource Integrity (SRI) | 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 |
| ✓ | Fast server response time (TTFB) | Performance & SEO |
| ✓ | 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 |
| ✓ | Page title | 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 |
| ✓ | SPF record is strict (-all) | Email Security |
| ✓ | DMARC policy is reject | Email Security |
| ✓ | MX records configured | Email Security |
| ✓ | SMTP banner not exposing version | Email Security |
| ✓ | 404 error page is clean | Error Disclosure |
| ✓ | Server error pages are clean | Error Disclosure |
| ✓ | No version information in error responses | Error Disclosure |
| ✓ | No input reflection detected | Input Reflection |
| ✓ | Forms submit to same origin | Input Reflection |
| ✓ | No session cookies detected | Session Security |
| ✓ | No tracking cookies, no consent needed | Cookie Compliance |
| ✓ | No tracking cookies on initial load | Cookie Compliance |
| ✓ | Only 0 cookie(s) on initial load | Cookie Compliance |
| ✓ | No excessively long-lived cookies | Cookie Compliance |
| ✓ | Subdomain takeover | Subdomain Takeover |

## Category Details

### Robots & Sitemap 0/100

**robots.txt present**

No robots.txt file found at /robots.txt.

Create a robots.txt file to guide search engine crawlers. Minimum: User-agent: * Disallow:

**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 0/100

### Favicon

No favicon detected.

Add a favicon.ico or <link rel="icon" href="/favicon.ico">. Use a 32×32px PNG or ICO file.

### 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.

## Directory Discovery 0/100

**Admin panel found at /admin**

Path /admin returned HTTP 403 (forbidden but exists). This could expose Admin panel to attackers.

Verify that /admin requires proper authentication.

**Admin panel found at /administrator**

Path /administrator returned HTTP 403 (forbidden but exists). This could expose Admin panel to attackers.

Verify that /administrator requires proper authentication.

**WordPress admin found at /wp-admin**

Path /wp-admin returned HTTP 403 (forbidden but exists). This could expose WordPress admin to attackers.

Verify that /wp-admin requires proper authentication.

**phpMyAdmin found at /phpmyadmin**

Path /phpmyadmin returned HTTP 403 (forbidden but exists). This could expose phpMyAdmin to attackers.

Verify that /phpmyadmin requires proper authentication.

**phpMyAdmin (alias) found at /pma**

Path /pma returned HTTP 403 (forbidden but exists). This could expose phpMyAdmin (alias) to attackers.

Verify that /pma requires proper authentication.

**Adminer database tool found at /adminer**

Path /adminer returned HTTP 403 (forbidden but exists). This could expose Adminer database tool to attackers.

Verify that /adminer requires proper authentication.

**cPanel found at /cpanel**

Path /cpanel returned HTTP 403 (forbidden but exists). This could expose cPanel to attackers.

Verify that /cpanel requires proper authentication.

**Webmail interface found at /webmail**

Path /webmail returned HTTP 403 (forbidden but exists). This could expose Webmail interface to attackers.

Verify that /webmail requires proper authentication.

**Backup directory found at /backup**

Path /backup returned HTTP 403 (forbidden but exists). This could expose Backup directory to attackers.

Verify that /backup requires proper authentication.

**Backup directory found at /backups**

Path /backups returned HTTP 403 (forbidden but exists). This could expose Backup directory to attackers.

Verify that /backups requires proper authentication.

**Test directory found at /test**

Path /test returned HTTP 403 (forbidden but exists). This could expose Test directory to attackers.

Verify that /test requires proper authentication.

**Staging environment found at /staging**

Path /staging returned HTTP 403 (forbidden but exists). This could expose Staging environment to attackers.

Verify that /staging requires proper authentication.

**Development directory found at /dev**

Path /dev returned HTTP 403 (forbidden but exists). This could expose Development directory to attackers.

Verify that /dev requires proper authentication.

**Debug page found at /debug**

Path /debug returned HTTP 403 (forbidden but exists). This could expose Debug page to attackers.

Verify that /debug requires proper authentication.

**Temporary directory found at /tmp**

Path /tmp returned HTTP 403 (forbidden but exists). This could expose Temporary directory to attackers.

Verify that /tmp requires proper authentication.

**Temporary directory found at /temp**

Path /temp returned HTTP 403 (forbidden but exists). This could expose Temporary directory to attackers.

Verify that /temp requires proper authentication.

**Log files found at /log**

Path /log returned HTTP 403 (forbidden but exists). This could expose Log files to attackers.

Verify that /log requires proper authentication.

**Log files found at /logs**

Path /logs returned HTTP 403 (forbidden but exists). This could expose Log files to attackers.

Verify that /logs requires proper authentication.

**Old/archived files found at /old**

Path /old returned HTTP 403 (forbidden but exists). This could expose Old/archived files to attackers.

Verify that /old requires proper authentication.

**Archive directory found at /archive**

Path /archive returned HTTP 403 (forbidden but exists). This could expose Archive directory to attackers.

Verify that /archive requires proper authentication.

**Data dump found at /dump**

Path /dump returned HTTP 403 (forbidden but exists). This could expose Data dump to attackers.

Verify that /dump requires proper authentication.

**SQL files found at /sql**

Path /sql returned HTTP 403 (forbidden but exists). This could expose SQL files to attackers.

Verify that /sql requires proper authentication.

**Database files found at /db**

Path /db returned HTTP 403 (forbidden but exists). This could expose Database files to attackers.

Verify that /db requires proper authentication.

**Configuration directory found at /config**

Path /config returned HTTP 403 (forbidden but exists). This could expose Configuration directory to attackers.

Verify that /config requires proper authentication.

**Installation wizard found at /install**

Path /install returned HTTP 403 (forbidden but exists). This could expose Installation wizard to attackers.

Verify that /install requires proper authentication.

**Setup wizard found at /setup**

Path /setup returned HTTP 403 (forbidden but exists). This could expose Setup wizard to attackers.

Verify that /setup 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.

**XML-RPC endpoint found at /xmlrpc.php**

Path /xmlrpc.php returned HTTP 403 (forbidden but exists). This could expose XML-RPC endpoint to attackers.

Verify that /xmlrpc.php requires proper authentication.

## Performance & SEO 25/100

**Response compression enabled**

No gzip or Brotli compression detected.

Enable gzip or Brotli compression on your web server. This typically reduces HTML/CSS/JS size by 60-80%.

**robots.txt present**

No robots.txt file found.

Create a robots.txt file to guide search engine crawlers and prevent indexing of sensitive paths.

**XML sitemap present**

No sitemap.xml found at common locations (/sitemap.xml, /sitemap_index.xml).

Create and submit an XML sitemap to Google Search Console to improve search indexing.

**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.

## Security Headers 36/100

### 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.

### 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).

## API Security 50/100

**API documentation exposed**

Endpoint accessible at /api/docs (authentication required).

The /api/docs endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**Swagger UI exposed**

Endpoint accessible at /swagger-ui.html (authentication required).

The /swagger-ui.html endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**Swagger UI exposed**

Endpoint accessible at /swagger-ui/ (authentication required).

The /swagger-ui/ endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**Swagger UI exposed**

Endpoint accessible at /api/swagger (authentication required).

The /api/swagger endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**Swagger spec exposed**

Endpoint accessible at /swagger.json (authentication required).

The /swagger.json endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**Swagger spec exposed**

Endpoint accessible at /swagger.yaml (authentication required).

The /swagger.yaml endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**OpenAPI spec exposed**

Endpoint accessible at /openapi.json (authentication required).

The /openapi.json endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**OpenAPI spec exposed**

Endpoint accessible at /openapi.yaml (authentication required).

The /openapi.yaml endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**GraphiQL IDE exposed**

Endpoint accessible at /graphiql (authentication required).

The /graphiql endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**Spring Actuator exposed**

Endpoint accessible at /actuator (authentication required).

The /actuator endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**Spring Actuator health exposed**

Endpoint accessible at /actuator/health (authentication required).

The /actuator/health endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**Elasticsearch API exposed**

Endpoint accessible at /_cat/indices (authentication required).

The /_cat/indices endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**OpenID Connect metadata exposed**

Endpoint accessible at /.well-known/openid-configuration (authentication required).

The /.well-known/openid-configuration endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**REST API exposed**

Endpoint accessible at /api/v1 (authentication required).

The /api/v1 endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**REST API exposed**

Endpoint accessible at /api/v2 (authentication required).

The /api/v2 endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

**JSON Web Key Set (JWKS) exposed**

Endpoint accessible at /.well-known/jwks.json (authentication required).

The /.well-known/jwks.json endpoint is accessible but requires authentication. Review whether it should be publicly reachable.

## SSL & HTTPS 64/100

**HTTP redirects to HTTPS**

HTTP requests are not being redirected to HTTPS.

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

**HSTS header configured**

HSTS header present but max-age is only 86400 seconds (minimum recommended: 31536000).

Set 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.

## Accessibility 65/100

**HTML lang attribute**

No lang attribute found on the <html> element.

Add a lang attribute: <html lang="en"> or <html lang="nl">.

**Viewport meta tag**

No viewport meta tag found.

Add <meta name="viewport" content="width=device-width, initial-scale=1"> to your <head>.

**Meta description**

No meta description found.

Add <meta name="description" content="..."> to improve SEO and accessibility.

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

## Input Reflection 83/100

**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.

## Email Security 88/100

**No DANE/TLSA record**

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

## Cookie Compliance 88/100

✓ All checks passed

## TLS / Cipher 100/100

✓ All checks passed

## Content & CMS 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

### Session Security 100/100

✓ All checks passed

### Subdomain Takeover 100/100

✓ All checks passed