SCANALA
AUTOMATED WEBSITE SECURITY ASSESSMENT

Security Assessment Report

Website Vulnerability Assessment

Prepared for
kedai-contoh.test

Report date: 19 November 2026
Assessment type: Full Scan scan (automated, read-only)

CONFIDENTIAL — This report is intended only for the owner of the assessed domain. It documents an automated, outside-in assessment; it is not a substitute for a manual penetration test and cannot determine whether the site has already been compromised.

Document control

VERSION	DATE	DETAIL	AUTHOR
1.0	19 November 2026	Automated assessment generated and released	Scanala

Prepared by	Scanala automated scanner
Assessment method	Automated, read-only (HTTP GET, DNS, TCP connect); CISA KEV cross-reference
Target	kedai-contoh.test

Contents

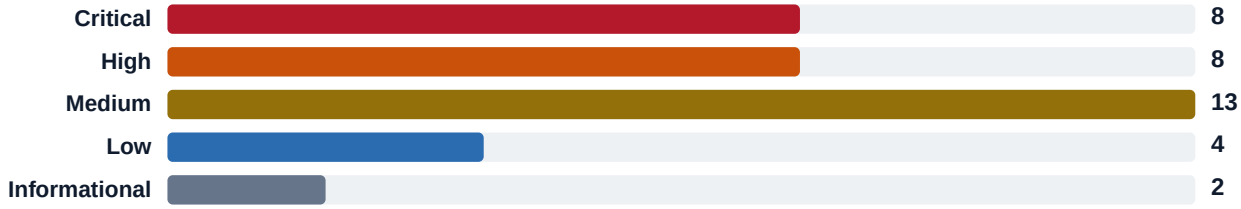
Section I — Executive summary
Section II — Introduction
Section III — Scope & methodology
Section IV — Information gathering
Section V — Findings
Section VI — Checks that passed
Section VII — Appendix: findings by area

Section I — Executive summary

This report documents an automated security assessment of kedai-contoh.test, carried out on 19 November 2026. The site is at high risk of compromise. Address the critical findings today.

A total of 35 issue(s) were identified: 8 critical, 8 high, 13 medium, 4 low and 2 informational. The site scored 0/100 (grade F).

NUMBER OF FINDINGS BY RISK LEVEL



SUMMARY OF FINDINGS

SEVERITY	FINDING	STATUS
Critical	The site does not work over HTTPS	Open
Critical	Environment file is publicly downloadable	Open
Critical	Git repository is exposed	Open
Critical	WordPress config backup is publicly downloadable	Open
Critical	Application settings file with credentials is publicly downloadable	Open
Critical	Site backup archive is publicly downloadable	Open
Critical	Database dump is publicly downloadable	Open
Critical	WordPress 5.8.1 is out of date (latest is 7.1.5)	Open
High	CORS lets any website read logged-in users' data	Open
High	docker-compose file is publicly readable	Open
High	Telerik UI upload handler is exposed	Open
High	Web file manager is reachable without logging in	Open
High	Directory listing is enabled — visitors can browse your files	Open
High	2 outdated WordPress plugin(s)	Open
High	PHP 7.2.34 is end-of-life	Open
High	Apache 2.2.15 is end-of-life	Open
Medium	No Content-Security-Policy	Open
Medium	Site can be embedded in other pages (clickjacking)	Open
Medium	Session cookies are readable by JavaScript	Open
Medium	Full list of installed libraries and versions is public	Open
Medium	Deployment config (fly.toml) is publicly readable	Open
Medium	phpinfo() page is public	Open

Medium	Error log is publicly readable	Open
Medium	WordPress login usernames can be listed by anyone	Open
Medium	WordPress XML-RPC is enabled	Open
Medium	3 vulnerable JavaScript libraries in use	Open
Medium	WordPress has vulnerabilities on CISA's Known Exploited list	Open
Medium	PHP has vulnerabilities on CISA's Known Exploited list	Open
Medium	Apache HTTP Server has vulnerabilities on CISA's Known Exploited list	Open
Low	X-Content-Type-Options is missing	Open
Low	Referrer-Policy is missing	Open
Low	Server software versions are advertised	Open
Low	Cookies have no SameSite attribute	Open
Informational	WordPress version is visible to visitors	Open
Informational	WordPress login page is at the default address	Open

This assessment is a point-in-time snapshot. Security posture changes constantly; monitoring and re-assessment should be an ongoing process.

Section II — Introduction

The owner of kedai-contoh.test proved control of the domain and requested an automated security self-test by Scanala. The objective of this assessment is to detect potential vulnerabilities and weaknesses that are visible from outside the application, and to provide practical remediation guidance.

Section III — Scope & methodology

Only kedai-contoh.test (and its www/non-www twin) was assessed, after ownership was verified. All checks are read-only — HTTP GET requests, DNS lookups and TCP connects. No passwords were tried, no forms were submitted, and no vulnerability was exploited. Detected software is cross-referenced against the CISA Known Exploited Vulnerabilities catalogue. Social engineering, denial-of-service and testing of systems outside the named target are out of scope.

RISK LEVEL RATINGS

LEVEL	DESCRIPTION
Critical	Direct, immediate risk of compromise or data loss. Remediate today.
High	Significant impact to confidentiality, integrity or availability. Remediate this week.
Medium	Substantial weakness that should be fixed promptly.
Low	Noticeable weakness; fix as part of normal maintenance.
Informational	For awareness; no direct risk on its own.

OWASP TOP 10 REFERENCE

CATEGORY	DESCRIPTION
A01 Broken Access Control	Users can act outside their intended permissions.
A02 Cryptographic Failures	Sensitive data exposed through weak or missing encryption.
A03 Injection	Untrusted input is run as a command or query (SQLi, XSS).
A05 Security Misconfiguration	Insecure defaults, exposed files, missing hardening.
A06 Vulnerable & Outdated Components	Known-vulnerable software, libraries or plugins in use.
A07 Identification & Authentication Failures	Weaknesses in login, sessions or account handling.

Section IV — Information gathering

Target	kedai-contoh.test
IP address(es)	—
Server / CDN	—
Protocol	HTTPS
Page title	—
Technologies	WordPress 5.8.1, 2 WordPress plugin(s) detected, PHP 7.2.34, Apache 2.2.15, jQuery 1.12.4, Bootstrap 3.3.7, jQuery UI 1.12.1, Lodash 4.17.21

Section V — Findings (35)

CRITICAL

I. The site does not work over HTTPS

HTTPS & certificates · OWASP A02 Cryptographic Failures · Status: Open

DESCRIPTION

Everything visitors send — passwords, contact forms, payment details — travels unencrypted and can be read or changed by anyone on the same network. Browsers also mark the site "Not secure".

IMPLICATION

Information disclosure; traffic interception or tampering.

RECOMMENDATION

Install a TLS certificate. Most hosting providers and cPanel include free Let's Encrypt / AutoSSL certificates — enable it, then redirect all HTTP traffic to HTTPS.

CRITICAL

II. Environment file is publicly downloadable

Exposed files & config · OWASP A05 Security Misconfiguration · A01 Broken Access Control · Status: Open

DESCRIPTION

The .env file holds database passwords, API keys and mail credentials. Anyone on the internet can download it right now, which usually means full takeover of the site and its data.

OBSERVATIONS

Found at: /.env. HTTP 200. Variable names found (values hidden): APP_ENV, DB_HOST, DB_PASSWORD, MAIL_PASSWORD

IMPLICATION

Information disclosure; potential unauthorized access to data or credentials.

RECOMMENDATION

Move the file outside the public web folder or block it in the web server (deny access to dotfiles). Then change every password and key that was in it, because it must be assumed stolen.

CRITICAL

III. Git repository is exposed

Exposed files & config · OWASP A05 Security Misconfiguration · A01 Broken Access Control · Status: Open

DESCRIPTION

The site's .git folder is reachable. An attacker can download the entire source code and its history, including any passwords that were ever committed.

OBSERVATIONS

Found at: /.git/HEAD. HTTP 200

IMPLICATION

Information disclosure; potential unauthorized access to data or credentials.

RECOMMENDATION

Block access to /.git in the web server, or deploy without the .git folder. Rotate any credentials that appear in the repository history.

CRITICAL

IV. WordPress config backup is publicly downloadable

Exposed files & config · OWASP A05 Security Misconfiguration · A01 Broken Access Control · Status: Open

DESCRIPTION

A backup copy of wp-config.php is readable as plain text. It contains the database username and password plus the secret keys that protect logins.

OBSERVATIONS

Found at: /wp-config.php.bak. HTTP 200

IMPLICATION

Information disclosure; potential unauthorized access to data or credentials.

RECOMMENDATION

Delete the backup file from the server. Change the database password and regenerate the WordPress salts (secret keys).

CRITICAL

V. Application settings file with credentials is publicly downloadable

Exposed files & config · OWASP A05 Security Misconfiguration · A01 Broken Access Control · Status: Open

DESCRIPTION

The application's settings file can be downloaded by anyone. It contains database connection strings or other secrets, which usually gives direct access to the data behind the site.

OBSERVATIONS

Found at: /appsettings.json. HTTP 200. Setting names found (values hidden): ConnectionStrings, Password, JwtSecret

IMPLICATION

Information disclosure; potential unauthorized access to data or credentials.

RECOMMENDATION

Block the file in the web server and keep settings outside the public folder. Then change every password, connection

string and key that was in it — assume they have been copied.

CRITICAL

VI. Site backup archive is publicly downloadable

Exposed files & config · OWASP A05 Security Misconfiguration · A01 Broken Access Control · Status: Open

DESCRIPTION
A backup archive sits in the public web folder. It typically contains the full source code and config files with passwords.

OBSERVATIONS
Found at: /backup.zip. HTTP 200

IMPLICATION
Information disclosure; potential unauthorized access to data or credentials.

RECOMMENDATION
Remove the archive from the web folder and store backups somewhere that is not served to the public.

CRITICAL

VII. Database dump is publicly downloadable

Exposed files & config · OWASP A05 Security Misconfiguration · A01 Broken Access Control · Status: Open

DESCRIPTION
A database export is reachable by anyone. It usually contains customer records, emails and password hashes — a reportable personal-data breach under data-protection law such as the GDPR or PDPA.

OBSERVATIONS
Found at: /database.sql. HTTP 200

IMPLICATION
Information disclosure; potential unauthorized access to data or credentials.

RECOMMENDATION
Remove the file from the web folder immediately. Treat the data as leaked: reset user passwords and assess breach-notification duties.

CRITICAL

VIII. WordPress 5.8.1 is out of date (latest is 7.1.5)

Outdated software · OWASP A06 Vulnerable and Outdated Components · Status: Open

DESCRIPTION
Old WordPress versions have publicly documented vulnerabilities, and automated bots scan the whole internet for them. An outdated core is one of the most common reasons SME websites get hacked.

OBSERVATIONS
Version 5.8.1 detected from generator meta tag

IMPLICATION
Exploitation of publicly known vulnerabilities in outdated components.

RECOMMENDATION
Take a full backup, then update WordPress from Dashboard !' Updates. Enable automatic updates for minor releases at least. If the theme breaks on update, that theme is itself a risk and needs replacing.

HIGH

IX. CORS lets any website read logged-in users' data

Browser security headers · OWASP A05 Security Misconfiguration · Status: Open

DESCRIPTION
The server echoes back whatever origin asks and allows credentials. Any malicious site a logged-in user visits can read their data from your site.

OBSERVATIONS
Access-Control-Allow-Origin: https://scanala-cors-test.example | Access-Control-Allow-Credentials: true

IMPLICATION
Client-side attack exposure (cross-site scripting, clickjacking, session theft).

RECOMMENDATION
Allow only the specific origins that need access, and never combine a reflected origin with credentials.

HIGH

X. docker-compose file is publicly readable

Exposed files & config · OWASP A05 Security Misconfiguration · A01 Broken Access Control · Status: Open

DESCRIPTION
Deployment files show how and where the app is hosted, internal service names and sometimes passwords. They are among the first files attack bots request. Compose files very often contain database passwords in plain text.

OBSERVATIONS
Found at: /docker-compose.yml. HTTP 200

IMPLICATION
Information disclosure; potential unauthorized access to data or credentials.

RECOMMENDATION
Remove the file from the served folder and change any passwords it contains.

HIGH

XI. Telerik UI upload handler is exposed

Exposed files & config · OWASP A05 Security Misconfiguration · A01 Broken Access Control · Status: Open

DESCRIPTION

The Telerik UI for ASP.NET upload handler answers publicly. Versions before 2020 have well-known flaws (CVE-2017-11317, CVE-2019-18935) that let attackers upload files and run code on the server; they have been used in many government website breaches.

OBSERVATIONS

Found at: /Telerik.Web.UI.WebResource.axd?type=rau. HTTP 200

IMPLICATION

Information disclosure; potential unauthorized access to data or credentials.

RECOMMENDATION

Check the Telerik.Web.UI.dll version. Upgrade to R1 2020 or later, set unique encryption keys in web.config, and disable the handler if file upload is not used.

HIGH

XII. Web file manager is reachable without logging in

Exposed files & config · OWASP A05 Security Misconfiguration · A01 Broken Access Control · Status: Open

DESCRIPTION

A bundled file-manager library (elFinder, CKFinder, KCFinder, Responsive FileManager or similar) is exposed. These components have a long record of flaws that let attackers browse and download server files — including settings files — or upload a backdoor.

OBSERVATIONS

Found at: /elfinder/elfinder.html. HTTP 200

IMPLICATION

Information disclosure; potential unauthorized access to data or credentials.

RECOMMENDATION

Remove the file manager if it is not needed. Otherwise update it, require an admin login before it loads, and restrict it to the uploads folder.

HIGH

XIII. Directory listing is enabled — visitors can browse your files

Exposed files & config · OWASP A05 Security Misconfiguration · A01 Broken Access Control · Status: Open

DESCRIPTION

The web server shows the full list of files in these folders to anyone. Attackers use this to find backups, uploaded documents, invoices and forgotten scripts that were never meant to be public.

OBSERVATIONS

Browsable folders: /backup/, /wp-content/uploads/

IMPLICATION

Information disclosure; potential unauthorized access to data or credentials.

RECOMMENDATION

Turn off directory listing. On Apache/cPanel add "Options -Indexes" to .htaccess (or use cPanel !’ Indexes !’ No Indexing). On nginx set "autoindex off;".

HIGH

XIV. 2 outdated WordPress plugin(s)

Outdated software · OWASP A06 Vulnerable and Outdated Components · Status: Open

DESCRIPTION

Vulnerable plugins are the number one way WordPress sites are hacked. Once a plugin flaw is published, bots start attacking every site that still runs the old version, usually within days.

OBSERVATIONS

contact-form-7 5.4 !’ 6.2.5 | elementor 3.1.0 !’ 4.4.1

IMPLICATION

Exploitation of publicly known vulnerabilities in outdated components.

RECOMMENDATION

Update these plugins from Dashboard !’ Plugins and switch on auto-updates. Delete plugins you do not use — deactivated plugins can still be exploited. Replace any plugin that has been abandoned by its author.

HIGH

XV. PHP 7.2.34 is end-of-life

Outdated software · OWASP A06 Vulnerable and Outdated Components · Status: Open

DESCRIPTION

This PHP version no longer receives security fixes. Vulnerabilities in PHP itself affect every site on it, whatever CMS is used.

OBSERVATIONS

X-Powered-By: PHP/7.2.34

IMPLICATION

Exploitation of publicly known vulnerabilities in outdated components.

RECOMMENDATION
Switch to a supported PHP version (8.3 or newer) in your hosting panel — in cPanel: Select PHP Version / MultiPHP Manager. Test the site afterwards; very old themes or extensions may need updating first.

HIGH

XVI. Apache 2.2.15 is end-of-life

Outdated software · OWASP A06 Vulnerable and Outdated Components · Status: Open

DESCRIPTION
Apache 2.2 and older have not received security fixes since 2017.

OBSERVATIONS
Server: Apache/2.2.15 (CentOS)

IMPLICATION
Exploitation of publicly known vulnerabilities in outdated components.

RECOMMENDATION
Ask your hosting provider to move the site to a server running a current Apache 2.4 release, or change host.

MEDIUM

XVII. No Content-Security-Policy

Browser security headers · OWASP A05 Security Misconfiguration · Status: Open

DESCRIPTION
A Content-Security-Policy limits which scripts the browser will run. Without one, any injected script (for example card-skimming code added after a hack) runs with no restriction.

IMPLICATION
Client-side attack exposure (cross-site scripting, clickjacking, session theft).

RECOMMENDATION
Start with a report-only policy to see what would break, then enforce it. A reasonable start: default-src 'self'; plus the specific script/CDN hosts the site uses.

MEDIUM

XVIII. Site can be embedded in other pages (clickjacking)

Browser security headers · OWASP A05 Security Misconfiguration · Status: Open

DESCRIPTION
Another website can load your pages in an invisible frame and trick logged-in users into clicking buttons they cannot see.

IMPLICATION
Client-side attack exposure (cross-site scripting, clickjacking, session theft).

RECOMMENDATION
Send X-Frame-Options: SAMEORIGIN (or CSP frame-ancestors 'self').

MEDIUM

XIX. Session cookies are readable by JavaScript

Browser security headers · OWASP A05 Security Misconfiguration · Status: Open

DESCRIPTION
Without the HttpOnly flag, any injected script can read the session cookie and take over the logged-in account.

OBSERVATIONS
Cookies: PHPSESSID

IMPLICATION
Client-side attack exposure (cross-site scripting, clickjacking, session theft).

RECOMMENDATION
Set the HttpOnly flag on session cookies. For PHP sessions: session.cookie_httponly = 1.

MEDIUM

XX. Full list of installed libraries and versions is public

Exposed files & config · OWASP A05 Security Misconfiguration · A01 Broken Access Control · Status: Open

DESCRIPTION
Composer's installed.json lists every PHP library on the site with its exact version. Attackers match that list against known vulnerabilities to pick a working exploit. It also shows the /vendor folder is web-accessible, which several library exploits depend on.

OBSERVATIONS
Found at: /vendor/composer/installed.json. HTTP 200

IMPLICATION
Information disclosure; potential unauthorized access to data or credentials.

RECOMMENDATION
Block the /vendor folder in the web server, or point the web root at the /public folder only.

MEDIUM

XXI. Deployment config (fly.toml) is publicly readable

Exposed files & config · OWASP A05 Security Misconfiguration · A01 Broken Access Control · Status: Open

DESCRIPTION

Deployment files show how and where the app is hosted, internal service names and sometimes passwords. They are among the first files attack bots request.

OBSERVATIONS

Found at: /fly.toml. HTTP 200

IMPLICATION

Information disclosure; potential unauthorized access to data or credentials.

RECOMMENDATION

Do not copy fly.toml into the folder that is served. Check its [env] section for secrets and move any into "fly secrets".

MEDIUM

XXII. phpinfo() page is public

Exposed files & config · OWASP A05 Security Misconfiguration · A01 Broken Access Control · Status: Open

DESCRIPTION

A phpinfo page reveals the exact PHP version, loaded modules, file paths and environment variables — a map for an attacker choosing which exploit to use.

OBSERVATIONS

Found at: /phpinfo.php. HTTP 200

IMPLICATION

Information disclosure; potential unauthorized access to data or credentials.

RECOMMENDATION

Delete the file from the server.

MEDIUM

XXIII. Error log is publicly readable

Exposed files & config · OWASP A05 Security Misconfiguration · A01 Broken Access Control · Status: Open

DESCRIPTION

Error logs leak server file paths, plugin names, database queries and sometimes user data, all of which help an attacker.

OBSERVATIONS

Found at: /wp-content/debug.log. HTTP 200

IMPLICATION

Information disclosure; potential unauthorized access to data or credentials.

RECOMMENDATION

Delete or block the log file, and turn off on-site debug logging (WP_DEBUG_LOG) on the live site.

MEDIUM

XXIV. WordPress login usernames can be listed by anyone

WordPress / Joomla · OWASP A07 Identification and Authentication Failures · Status: Open

DESCRIPTION

The site hands out its usernames, including administrators. Attackers then only have to guess the password, and they do so with automated tools.

OBSERVATIONS

2 username(s) exposed, e.g. ad***, si***

IMPLICATION

Account compromise; unauthorized administrative access.

RECOMMENDATION

Block the /wp-json/wp/v2/users endpoint and ?author= scans for logged-out visitors (Wordfence, iThemes/Solid Security and similar plugins have a one-click setting). Enforce strong passwords and two-factor authentication for all admins.

MEDIUM

XXV. WordPress XML-RPC is enabled

WordPress / Joomla · OWASP A07 Identification and Authentication Failures · Status: Open

DESCRIPTION

xmlrpc.php lets attackers try hundreds of passwords in a single request and is abused to launch DDoS attacks. Almost no modern site needs it.

IMPLICATION

Account compromise; unauthorized administrative access.

RECOMMENDATION

Disable XML-RPC with a security plugin, or block xmlrpc.php in .htaccess. Keep it only if you use the Jetpack plugin or the WordPress mobile app.

MEDIUM

XXVI. 3 vulnerable JavaScript libraries in use

Outdated software · OWASP A06 Vulnerable and Outdated Components · Status: Open

DESCRIPTION

The pages load front-end libraries with publicly documented vulnerabilities. Depending on how the site uses them, an attacker can run their own script in a visitor's browser — to steal sessions, alter pages or redirect visitors.

OBSERVATIONS

jQuery 1.12.4: cross-site scripting (CVE-2020-11022, CVE-2020-11023); fixed in 3.5.0 | Bootstrap 3.3.7: cross-site scripting (CVE-2019-8331); fixed in 3.4.1 | jQuery UI 1.12.1: cross-site scripting (CVE-2021-41182 to 41184, CVE-2022-31160); fixed in 1.13.2

IMPLICATION

Exploitation of publicly known vulnerabilities in outdated components.

RECOMMENDATION

Upgrade each library to its current release. If it comes bundled with a theme, plugin or template, update that instead. Remove libraries the site no longer uses.

MEDIUM

XXVII. WordPress has vulnerabilities on CISA's Known Exploited list

Outdated software · OWASP A06 Vulnerable and Outdated Components · Status: Open

DESCRIPTION

Your site runs WordPress. This product has 8 vulnerabilities that CISA records as actively exploited in the wild, some used in ransomware campaigns. This flag is based on the product, not your exact version — confirm you are on the latest patched release.

OBSERVATIONS

Detected WordPress 5.8.1. Most recent known-exploited entry: CVE-2026-119977 (WordPress WordPress Core Time-of-check Time-of-use (TOCTOU) Race Condition Vulnerability), added 2026-11-03.

IMPLICATION

Exploitation of publicly known vulnerabilities in outdated components.

RECOMMENDATION

Update WordPress to the current patched version and enable automatic security updates. Review CISA KEV for WordPress to confirm none of the listed CVEs affect your version.

MEDIUM

XXVIII. PHP has vulnerabilities on CISA's Known Exploited list

Outdated software · OWASP A06 Vulnerable and Outdated Components · Status: Open

DESCRIPTION

Your site runs PHP. This product has 10 vulnerabilities that CISA records as actively exploited in the wild, some used in ransomware campaigns. This flag is based on the product, not your exact version — confirm you are on the latest patched release.

OBSERVATIONS

Detected PHP 7.2.34. Most recent known-exploited entry: CVE-2026-109619 (PHP Stale Internal Request-State Vulnerability), added 2026-10-26.

IMPLICATION

Exploitation of publicly known vulnerabilities in outdated components.

RECOMMENDATION

Update PHP to the current patched version and enable automatic security updates. Review CISA KEV for PHP to confirm none of the listed CVEs affect your version.

MEDIUM

XXIX. Apache HTTP Server has vulnerabilities on CISA's Known Exploited list

Outdated software · OWASP A06 Vulnerable and Outdated Components · Status: Open

DESCRIPTION

Your site runs Apache HTTP Server. This product has 5 vulnerabilities that CISA records as actively exploited in the wild, some used in ransomware campaigns. This flag is based on the product, not your exact version — confirm you are on the latest patched release.

OBSERVATIONS

Detected Apache 2.2.15. Most recent known-exploited entry: CVE-2026-21962 (Oracle HTTP Server and Oracle Weblogic Server Proxy Plug-in Improper Access Control Vulnerability), added 2026-08-24.

IMPLICATION

Exploitation of publicly known vulnerabilities in outdated components.

RECOMMENDATION

Update Apache HTTP Server to the current patched version and enable automatic security updates. Review CISA KEV for Apache HTTP Server to confirm none of the listed CVEs affect your version.

LOW

XXX. X-Content-Type-Options is missing

Browser security headers · OWASP A05 Security Misconfiguration · Status: Open

DESCRIPTION
Browsers may guess file types, which lets an uploaded file be treated as a script.

IMPLICATION
Client-side attack exposure (cross-site scripting, clickjacking, session theft).

RECOMMENDATION
Send X-Content-Type-Options: nosniff

LOW

XXXI. Referrer-Policy is missing

Browser security headers · OWASP A05 Security Misconfiguration · Status: Open

DESCRIPTION
Full page addresses (which can include order numbers or reset tokens) may be sent to other sites when visitors click links.

IMPLICATION
Client-side attack exposure (cross-site scripting, clickjacking, session theft).

RECOMMENDATION
Send Referrer-Policy: strict-origin-when-cross-origin

LOW

XXXII. Server software versions are advertised

Browser security headers · OWASP A05 Security Misconfiguration · Status: Open

DESCRIPTION
Response headers tell attackers exactly which software versions to look up exploits for.

OBSERVATIONS
Server: Apache/2.2.15 (CentOS) | X-Powered-By: PHP/7.2.34

IMPLICATION
Client-side attack exposure (cross-site scripting, clickjacking, session theft).

RECOMMENDATION
Hide version details: "ServerTokens Prod" and "ServerSignature Off" (Apache), "server_tokens off;" (nginx), "expose_php = Off" (php.ini).

LOW

XXXIII. Cookies have no SameSite attribute

Browser security headers · OWASP A05 Security Misconfiguration · Status: Open

DESCRIPTION
SameSite stops other websites from making requests that carry your visitors' cookies (CSRF).

OBSERVATIONS
Cookies: PHPSESSID, lang

IMPLICATION
Client-side attack exposure (cross-site scripting, clickjacking, session theft).

RECOMMENDATION
Set SameSite=Lax (or Strict) on cookies.

INFORMATIONAL

XXXIV. WordPress version is visible to visitors

WordPress / Joomla · OWASP A07 Identification and Authentication Failures · Status: Open

DESCRIPTION
Advertising the exact version helps bots pick the right exploit.

OBSERVATIONS
5.8.1 via generator meta tag

IMPLICATION
Account compromise; unauthorized administrative access.

RECOMMENDATION
Remove the generator tag (remove_action('wp_head', 'wp_generator')) or use a security plugin that hides it.

INFORMATIONAL

XXXV. WordPress login page is at the default address

WordPress / Joomla · OWASP A07 Identification and Authentication Failures · Status: Open

DESCRIPTION
Bots try passwords against /wp-login.php all day. That is only a problem if a password is weak or reused.

IMPLICATION
Account compromise; unauthorized administrative access.

RECOMMENDATION
Turn on two-factor authentication for every admin account and install a plugin that limits login attempts. Do not use "admin" as a username.

Section VII — Appendix: findings by area

HTTPS & certificates

- Critical — The site does not work over HTTPS

Exposed files & config

- Critical — Environment file is publicly downloadable
- Critical — Git repository is exposed
- Critical — WordPress config backup is publicly downloadable
- Critical — Application settings file with credentials is publicly downloadable
- Critical — Site backup archive is publicly downloadable
- Critical — Database dump is publicly downloadable
- High — docker-compose file is publicly readable
- High — Telerik UI upload handler is exposed
- High — Web file manager is reachable without logging in
- High — Directory listing is enabled — visitors can browse your files
- Medium — Full list of installed libraries and versions is public
- Medium — Deployment config (fly.toml) is publicly readable
- Medium — phpinfo() page is public
- Medium — Error log is publicly readable

Outdated software

- Critical — WordPress 5.8.1 is out of date (latest is 7.1.5)
- High — 2 outdated WordPress plugin(s)
- High — PHP 7.2.34 is end-of-life
- High — Apache 2.2.15 is end-of-life
- Medium — 3 vulnerable JavaScript libraries in use
- Medium — WordPress has vulnerabilities on CISA's Known Exploited list
- Medium — PHP has vulnerabilities on CISA's Known Exploited list
- Medium — Apache HTTP Server has vulnerabilities on CISA's Known Exploited list

Browser security headers

- High — CORS lets any website read logged-in users' data
- Medium — No Content-Security-Policy
- Medium — Site can be embedded in other pages (clickjacking)
- Medium — Session cookies are readable by JavaScript
- Low — X-Content-Type-Options is missing
- Low — Referrer-Policy is missing
- Low — Server software versions are advertised
- Low — Cookies have no SameSite attribute

WordPress / Joomla

- Medium — WordPress login usernames can be listed by anyone
- Medium — WordPress XML-RPC is enabled
- Informational — WordPress version is visible to visitors
- Informational — WordPress login page is at the default address