RawatApp

business application care and upgrades

Application Security Audit Report

Static security and compatibility audit

A report from one of our clients. Client identity was anonymized before publishing.

Client	Client A, business site on shared hosting
Report date	12 May 2026
Document version	1.0
Classification	Confidential
Prepared by	RawatApp

3	5.289	1	Tier C
PHP files audited	lines of code	active webshell	risk level

Confidential. For the intended client only.

1. Executive Summary

The client site is a single-file PHP site on shared hosting. The main file index.php holds 5.181 lines. In total there are 3 PHP files and 5.289 lines of code.

The static scan found strong indicators of compromise. We found one active webshell disguised as a configuration file, one unknown entry file, and one attacker trace file.

File timestamps indicate the incident happened around early May 2026. Some protection was already applied days after the incident. PHP execution is blocked through server configuration.

CONCLUSION

Tier C. There are indicators of an active webshell. A full cleanup and hardening pass is required. Estimated at 8 to 15 working hours. A fixed price is given after the log review.

RISK IF LEFT UNTREATED

A webshell gives the attacker full control over the site and the server. Customer data and credentials stored on the hosting account are at risk of leakage. The hosting provider may suspend the account if it detects malicious activity.

2. Scope and Methodology

The audit ran on 12 May 2026 against every PHP file reachable in the hosting account, without running the application. Third-party vendor libraries were excluded.

The scan uses the four layers below.

- **PHPCompatibility**, line-by-line compatibility scan against PHP 8.3
- **Rector**, dry run to measure the automatic fixes that are possible
- **Pattern scan**, a fixed list of webshell and malicious-code markers, including password gates and download-then-execute patterns
- **Manual review**, analysis of scan results and suspicious files

3. Findings

The table below summarizes all findings. Details for each finding follow.

#	FINDING	LEVEL	LOCATION
1	**Active webshell** A password gate, then code is downloaded from a third-party server and executed through eval().	Critical	.env.php lines 44, 59, 60
2	**Unknown entry file** A new 30-line file, not part of the original site. The name mimics index.php to avoid suspicion.	High	indexx.php
3	**Attacker trace file** A text file holding a handwritten note from the attacker.	Medium	cmd.txt
4	**Two Search Console verification files** Two different verification files were found in the root directory.	Medium	root directory
5	**PHP 8.3 compatibility** PHPCompatibility found 0 errors and 2 minor warnings.	Clear	index.php

Temuan 1. Active webshell

Evidence. The .env.php file is not part of the original configuration. Line 44 checks a password from a hidden parameter. Lines 59 and 60 download code from a third-party server and execute it through eval().

Impact. The attacker can run arbitrary code. The attacker gets full control over the site and the hosting server.

Recommendation. Keep it as investigation evidence, then remove it. Rotate all credentials. Trace the entry point through access logs.

Temuan 2. Unknown entry file

Evidence. This file is never referenced anywhere in the site code. Its creation time lines up with the incident.

Impact. A potential entry point if PHP execution is re-enabled.

Recommendation. Remove it after preserving it as investigation evidence.

Temuan 3. Attacker trace file

Evidence. Files like this are commonly used to test write access on a server.

Impact. Confirms manual attacker activity on the server.

Recommendation. Remove it. Use it as a time anchor when reviewing logs.

Temuan 4. Two Search Console verification files

Evidence. The original site uses only one Search Console account.

Impact. The attacker may have claimed the site in Search Console.

Recommendation. Check the list of verified owners in Search Console. Revoke any unknown claim.

Temuan 5. PHP 8.3 compatibility

Evidence. Both minor warnings are recorded in the full scan output.

Impact. The original site runs safely on PHP 8.3.

Recommendation. Resolve the minor warnings if upgrade work is ordered.

PROTECTION ALREADY IN PLACE

The current server configuration blocks execution of all PHP files and denies access to hidden files. The webshell in finding 1 most likely can no longer execute. However, the file is still on the server and must be removed, because hosting configuration can change at any time.

4. Work Plan

The cleanup work is split into three phases. Total estimate is 8 to 15 working hours.

Phase 1. Evidence and cleanup

1. Take a full snapshot of code and database as investigation evidence.
2. Remove all attacker artifacts, findings 1 through 4, plus any other foreign files found in manual review.

Phase 2. Rotation and investigation

1. Rotate all credentials. This covers hosting, FTP, database, and admin account passwords.
2. Review access and error logs around the incident date to find the entry point.

Phase 3. Hardening and reporting

1. Permanent hardening. Server rules, security headers, and file integrity monitoring.
2. A written action report with recommendations for ongoing care.

5. Investment

PACKAGE	INCLUDES	PRICE
Full audit (this report)	Static scan, analyst review, a written report with risk levels and a work plan.	$200, credited toward a package below if ordered within 30 days
Cleanup and hardening	The full work plan above. A 14-day warranty on defects introduced by our work.	$300 to $500, confirmed after the log review
Monthly care (Caretaker)	Regular patches, uptime checks, priority queue. Annual contract.	$150 to $400 per month per application

- Payment is 50% upfront and 50% on handover of the action report.
- Work outside the scope above gets a new fixed quote before it starts.

6. Audit Limitations

This audit is based on static scanning. We did not run the application and did not read server logs. The incident time window was inferred from file modification times. The server access log review, part of the cleanup package, will verify these findings.

Contact

halo@rawatapp.com · rawatapp.com

WhatsApp +62 895-0646-188