ENGAGEMENT AVH-2026-09 / FINAL REPORT

Infrastructure & WordPress security audit

Prepared for Aster Vale Hospitality Group
Prepared by WPServerGuard/G.Schad

ONE HOST. EIGHT SITES. SHARED BUSINESS RISK.

VPS / Linux / WHM
8 WordPress installations

FICTIONAL EXAMPLE

ENGAGEMENT	RECORD
Assessment period	14-18 September 2026 / UTC
Retest and issue date	22 September 2026 / Version 1.1 / Final
Lead assessor	G.Schad / WPServerGuard
Client sponsor	Evan Cole, Head of Technology
Assessment boundary	1 VPS, its Linux operating system, WHM/cPanel and 8 hosted WordPress installations.

Fictional scenario notice
A fully fictional worked example. The client organization, client personnel, assets, observations, evidence, dates of testing and retest outcomes are invented. No live audit was performed. Domains use .example and the IP address is reserved for documentation.

Written in the form of a completed client engagement. The notice and centered background watermark apply to the whole document, including all evidence and closure statements.

01 / EXECUTIVE SUMMARY

Shared hosting risk is the central concern

Initial posture: HIGH RISK / Residual posture after retest: HIGH RISK

5	6	1
HIGH / INITIAL FINDINGS	MEDIUM / INITIAL FINDINGS	LOW / INITIAL FINDINGS

Business impact

Aster Vale operates seven public hospitality websites and one staging installation on a single VPS. The assessment identified routes to server administration, unauthorized guest-data access and compromise spreading between four sites that share one operating-system account. A host outage could interrupt all eight installations at once.

Highest-priority findings

Internet-facing root SSH password access and incomplete WHM MFA created management-plane exposure. An events-site backup and a custom booking export exposed guest information. Four production sites shared one filesystem identity, so a compromise of one could affect the others.

Progress at the 22 September retest

Eight findings were resolved and verified within the scenario. Three remain open: site isolation, independent recovery capability and central monitoring. One low-severity metadata finding was accepted. The remaining isolation weakness keeps residual risk High despite the immediate exposure reductions.

> **Decision required from the client sponsor**
> Approve account separation by 2 October, fund independent backup storage and a restore exercise by 6 October, and complete alert routing by 29 September. Evan Cole is accountable for the remaining risk until verification.

Assurance limit: no affirmative indicators of compromise were found in the sampled records. Seven days of local authentication logs and incomplete application history prevent a conclusion that compromise never occurred. This was a security assessment, not a forensic investigation.

FICTIONAL EXAMPLE

02 / SCOPE AND ENGAGEMENT

What was assessed

Objective: evaluate practical compromise, cross-site impact, data exposure and recoverability across the shared hosting environment.

SCOPE	DETAIL
VPS and network	vps01.astervale.example / 203.0.113.42. Virtual allocation, provider firewall, host ingress controls, management ports and snapshot configuration.
Linux operating system	AlmaLinux 9, x86_64. Privileged access, SSH effective settings, package updates, service ownership, filesystem boundaries and logging.
Hosting control plane	WHM/cPanel, Apache, PHP-FPM pools, MariaDB, account privileges, MFA, backups and security-related settings.
WordPress portfolio	W01-W08: all eight installations. Authentication, roles, components, selected custom code, public files, error handling and backup exposure.
Access supplied	Temporary sudo account, supervised root WHM access, read access to provider settings, application admin accounts and test subscriber accounts.

Methods and safe-test boundaries

Configuration review, external service checks, authenticated application testing, targeted source inspection and non-destructive proof of access. Cross-site access used harmless marker files. Export tests used synthetic canary records in a controlled clone; production impact was determined from matching code and configuration.

Exclusions

Provider hypervisor and physical infrastructure; corporate endpoints; registrar and email tenancy; third-party payment processing; denial-of-service; social engineering; full malware forensics; exhaustive source review. Provider snapshots were reviewed as a recovery dependency, not a provider security audit.

Chronology: kickoff 14 September; technical checks 14-17 September; initial findings issued 18 September; agreed changes 19-21 September; targeted retest 22 September. All timestamps in this report use UTC.

FICTIONAL EXAMPLE

03 / ASSET INVENTORY

Eight installations, five hosting accounts

All sites share VPS-01, WHM-01 and the same MariaDB service. There are seven production sites and one staging site; each has a separate database.

ID / HOSTNAME	BUSINESS PURPOSE	CPANEL USER / PHP
W01 / www.astervale.example	Corporate site and enquiry forms	avweb / 8.3
W02 / book.astervale.example	Booking portal; guest records; payment-provider redirect	avbook / 8.3
W03 / marina.astervale.example	Marina House property site	avweb / 8.3
W04 / ridge.astervale.example	Ridge Lodge property site	avweb / 8.3
W05 / journal.astervale.example	Editorial and destination content	avweb / 8.3
W06 / partners.astervale.example	Partner application portal	avpartners / 8.2
W07 / events.astervale.example	Events registration and enquiries	avevents / 8.3
W08 / stage.astervale.example	Staging copy of the booking portal	avstage / 8.3

FICTIONAL EXAMPLE

Host profile

VPS-01: 8 vCPU, 16 GB RAM and 320 GB SSD. AlmaLinux 9 with cPanel-managed Apache/PHP-FPM and local MariaDB. Site DNS is externally managed. Remote mailbox hosting is outside scope; the VPS retains application mail-delivery functionality.

Data and recovery expectations

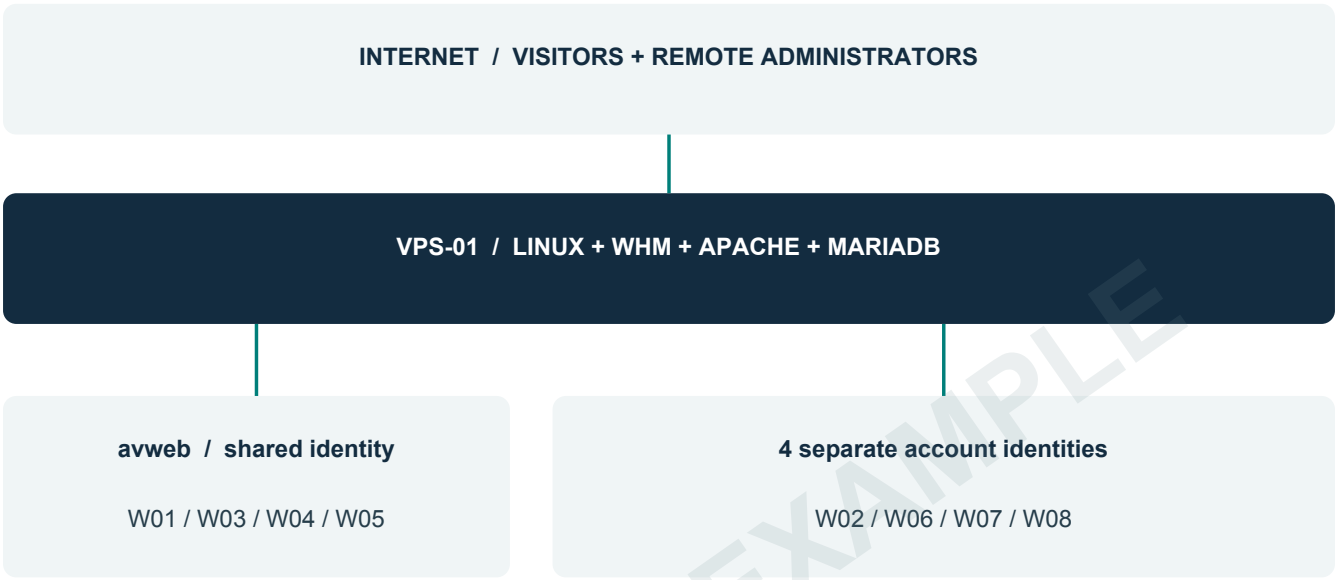
The booking portal holds guest contact and reservation details; the events site holds contact and attendance records. Cardholder data is handled by the external payment provider. The client target is a 24-hour recovery point and an 8-hour recovery time for all production sites.

Inventory basis: E-00, synthetic asset and version manifest dated 14 September. Public component version numbers are omitted because no finding depends on an asserted vendor release or CVE. Fictional custom component versions are identified where relevant.

04 / ARCHITECTURE AND METHODOLOGY

Where trust boundaries fail

The following diagram represents the assessed configuration before remediation.



FICTIONAL EXAMPLE

Blast radius

Root or privileged WHM access can affect every site. The shared avweb identity creates a narrower but still serious path among four production sites. Separate databases do not provide adequate isolation if the same Unix user can read each site's database configuration.

Test approach and confidence

Observations combine configuration review with bounded behavioral checks. Each finding includes a synthetic evidence identifier, the affected scope and the conditions required for impact. No production destructive payload, malware or high-volume credential attack was used in the scenario.

Rating model

High: a plausible route to privileged control, sensitive data disclosure or multi-site compromise. Medium: a material weakness with narrower impact or additional prerequisites. Low: limited direct impact. No Critical finding was established. Ratings are contextual judgments, not CVSS calculations or compliance scores.

> **Report navigation**
> Read the finding register on page 6, detailed findings on pages 7-18, the action plan on page 19, control assurance on page 20, and final dispositions on page 21. References and evidence handling are on page 22.

05 / FINDINGS REGISTER

Twelve findings, one accountable plan

Ratings describe the initial condition. Status reflects the final scenario retest on 22 September 2026.

ID / RISK	FINDING	STATUS	PAGE
VPS-01 **High**	Root SSH password access	Resolved	7
WHM-01 **High**	Privileged WHM access without enrolled MFA	Resolved	8
HOST-01 **High**	Four sites share one filesystem identity	Open	9
WP-01 **High**	Events backup available without authentication	Resolved	10
WP-02 **High**	Booking export lacks server-side authorization	Resolved	11
OS-01 **Medium**	Security updates deferred and kernel reboot pending	Resolved	12
WP-03 **Medium**	Gaps in WordPress privileged account hygiene	Resolved	13
BCP-01 **Medium**	Recovery relies on the same provider account	Open	14
MON-01 **Medium**	Security events are local and alerts lack ownership	Open	15
DATA-01 **Medium**	Staging exposes copied guest contact records	Resolved	16
CFG-01 **Medium**	Public debug log exposes operational data	Resolved	17
INFO-01 **Low**	Public component version information	Accepted	18

Initial: 5 High / 6 Medium / 1 Low. **Final:** 8 resolved / 3 open / 1 accepted.
Residual open findings: HOST-01 (High), BCP-01 (Medium), MON-01 (Medium).

FICTIONAL EXAMPLE

06 / FINDING 01 OF 12

VPS-01 | Root SSH password access

HIGH RISK / RESOLVED AT RETEST

Affected: VPS-01 / all eight sites indirectly
Owner: Infrastructure Lead · **Observed:** 15 Sep 09:20 2026 UTC

Observation

SSH was reachable from arbitrary external addresses. Effective configuration permitted root login with a password, and an authorized test login succeeded. The shared root credential was held by two operational staff, reducing individual accountability.

Impact and prerequisites

The attacker must obtain or guess a valid root password; exposure alone does not establish compromise. A successful login would provide host-wide control of websites, databases, backup files and logs. The impact and direct privileged authentication path justify High.

EVIDENCE E-01 / SYNTHETIC NORMALIZED EXTRACT

```
Source: external test network
TCP/22: reachable
Effective: permitrootlogin yes; passwordauthentication yes
Authorized root password login: accepted
```

FICTIONAL EXAMPLE

Remediation

Create individual key-based administrator accounts with reviewed sudo rights. Disable direct root SSH and password authentication, including equivalent keyboard-interactive paths if enabled. Restrict SSH to the approved administrative network and verify the provider console before reloading configuration. [R1]

Acceptance test

From an unapproved network, SSH is blocked. From the approved network, named key-based access and sudo work; direct root and password-based sessions fail. The emergency console remains usable.

> **Retest / final disposition**
> 22 Sep: verified. RT-01 records the network, authentication and recovery tests; no public site regression observed.

06 / FINDING 02 OF 12

WHM-01 | Privileged WHM access without enrolled MFA

HIGH RISK / RESOLVED AT RETEST

Affected: WHM-01 / root and reseller avops
Owner: Infrastructure Lead · **Observed:** 15 Sep 11:05 2026 UTC

Observation

WHM on TCP/2087 was publicly reachable. The server-level two-factor feature was enabled, but root and the avops reseller account had no enrolled second factor. The reseller could create and modify hosting accounts. Both accounts authenticated using only their passwords.

Impact and prerequisites

A stolen privileged control-panel password could enable account changes and access affecting the hosted portfolio. A server toggle showing MFA enabled did not demonstrate enrollment or protection for these accounts.

EVIDENCE E-02 / SYNTHETIC NORMALIZED EXTRACT

```
WHM: Two-Factor Authentication security policy = enabled
Account enrollment: root = absent; avops = absent
Approved password-only login: accepted for both
TCP/2087: reachable from external test network
```

Remediation

Enroll both privileged accounts using supported TOTP, secure recovery handling and verify fresh login challenges. Limit WHM network access to approved administrators. Review reseller privileges, API tokens and password-authenticated API access separately; browser MFA does not establish token protection. [R2]

Acceptance test

Both privileged accounts require a valid second factor on fresh sessions. Unapproved networks cannot reach WHM. Needed API integrations still work using reviewed, least-privilege credentials.

> **Retest / final disposition**
> 22 Sep: verified. RT-02 confirms both enrollments, network restriction and integration checks. Client-side cPanel MFA remains separately administered.

FICTIONAL EXAMPLE

06 / FINDING 03 OF 12

HOST-01 | Four sites share one filesystem identity

HIGH RISK / OPEN AT RETEST

Affected: W01, W03, W04, W05 / account avweb
Owner: Web Engineering Lead · **Observed:** 16 Sep 10:10 2026 UTC

Observation

Four independently maintained production sites run under avweb. A controlled PHP process in W05 could read a harmless configuration-adjacent marker under W01 and modify a designated test file under W03. No cross-account access to the other four hosting users was demonstrated.

Impact and prerequisites

This issue requires code execution or equivalent access in one of the shared sites. Once that occurs, the same identity can reach sibling content and potentially configuration secrets. Separate directories and databases do not stop this within-account movement.

EVIDENCE E-03 / SYNTHETIC NORMALIZED EXTRACT

```
PHP-FPM user: avweb on W01 / W03 / W04 / W05
W05 -> W01 audit marker read: allowed
W05 -> W03 designated test-file write: allowed
W05 -> avbook marker read: denied
```

Remediation

Move W01, W03, W04 and W05 into distinct cPanel accounts and PHP-FPM identities. Separate deployment and database credentials; verify ownership, cron jobs, redirects, mail routing and backup coverage after migration. Preserve functioning account-boundary protections. [R3]

Acceptance test

A process in each migrated site cannot read another site's configuration marker or write its files. All four sites pass smoke tests, scheduled jobs and backup/restore checks under their new accounts.

> **Retest / final disposition**
> 22 Sep: open. A staging migration passed, but production still uses avweb. Target 2 Oct 2026. Reduced deploy access is interim mitigation, not closure.

FICTIONAL EXAMPLE

06 / FINDING 04 OF 12

WP-01 | Events backup available without authentication

HIGH RISK / RESOLVED AT RETEST

Affected: W07 / events.astervale.example
Owner: Web Engineering Lead · **Observed:** 16 Sep 13:30 2026 UTC

Observation

A plugin-generated backup archive was stored in a public uploads directory and returned directly to an unauthenticated request. In the scenario, inventory of the owner-supplied matching archive showed 8,642 contact records and wp-config.php containing the site database credential.

Impact and prerequisites

Anyone who knew or discovered the path could obtain contact records and configuration secrets without a WordPress account. The backup was a full site archive, so database credential exposure is supported here. The finding does not imply root or access to every site.

EVIDENCE E-04 / SYNTHETIC NORMALIZED EXTRACT

```
GET /wp-content/uploads/backup/events-full.zip
Authentication: none -> HTTP 200 / application/zip
Matching archive contents: database dump + wp-config.php
Affected contact rows: 8,642; DB credential present
```

Remediation

Deny access, remove the archive and correct the backup destination. Purge relevant cached copies, rotate the exposed database password and WordPress salts, and verify application connectivity. Preserve available access records and have the data owner assess the disclosure; do not assume deletion reverses exposure.

Acceptance test

The original path and approved variants return no archive to anonymous clients. A fresh backup is created in private storage. The old database credential fails, the new credential works, and active sessions are invalidated as intended.

> **Retest / final disposition**
> 22 Sep: verified. RT-04 records retrieval denial, private backup creation and rotation checks. Historical third-party access remains undetermined due to limited logs.

FICTIONAL EXAMPLE

06 / FINDING 05 OF 12

WP-02 | Booking export lacks server-side authorization

HIGH RISK / RESOLVED AT RETEST

Affected: W02 / fictional AV Reservation Tools 1.4.0
Owner: Application Development Lead · **Observed:** 17 Sep 09:45 2026 UTC

Observation

The fictional custom AV Reservation Tools plugin registered a booking export route with an always-allow permission callback. A controlled clone running the same code and settings returned seeded reservation details without authentication. The production dataset held 1,246 reservations.

Impact and prerequisites

The missing authorization check exposed a route intended for booking managers. The affected fields included guest names, emails, stay dates and booking references. Card numbers were not stored. The custom component and version are fictional; this is not an allegation against a real plugin.

EVIDENCE E-05 / SYNTHETIC NORMALIZED EXTRACT

```
Route: GET /wp-json/av-reservations/v1/export
Permission callback: unconditional allow
Unauthenticated clone request: 200; canary row returned
Production match: same plugin source and route settings
```

Remediation

Remove unconditional access and enforce an explicit booking-export capability on the server. Validate authenticated requests using the selected WordPress authentication mechanism. Treat nonces as CSRF protection where applicable, not as a substitute for authorization. Review related export routes and log approved exports. [R4]

Acceptance test

Anonymous callers receive 401 or 403; subscribers and ordinary editors are denied. An authorized booking manager can export only intended fields. Alternate route forms and related endpoints do not bypass the capability check.

> **Retest / final disposition**
> 22 Sep: verified. RT-05 covers role-based negative tests and the permitted manager flow for fictional version 1.4.1. Production validation used an authorized canary record only.

FICTIONAL EXAMPLE

06 / FINDING 06 OF 12

OS-01 | Security updates deferred and kernel reboot pending

MEDIUM RISK / RESOLVED AT RETEST

Affected: VPS-01 / AlmaLinux 9
Owner: Infrastructure Lead · **Observed:** 15 Sep 14:15 2026 UTC

Observation

The patch review recorded six packages with available security updates and a newer installed kernel that was not running. The previous routine maintenance window had been missed; the host had 96 days of uptime. No individual unpatched CVE was exploited during testing.

Impact and prerequisites

Delayed patching extends exposure to known software weaknesses, while an installed kernel does not protect a running older kernel until the required restart occurs. Medium reflects a demonstrated process and runtime gap without a proven direct exploit path in this engagement.

EVIDENCE E-06 / SYNTHETIC NORMALIZED EXTRACT

```
Security-update inventory: 6 packages pending
Installed kernel differs from running kernel: yes
Reboot requirement: reported by maintenance checks
Last planned window: missed; host uptime = 96 days
```

Remediation

Apply compatible OS updates through the supported package-management workflow, coordinate with cPanel requirements and reboot during an approved window. Verify the running kernel and service health. Establish recurring maintenance, exception ownership and alerts for missed windows. [R5]

Acceptance test

Security-update review shows no unapproved pending items; the intended kernel is running. WHM, database access, all eight web frontends and scheduled jobs pass post-reboot checks. Exceptions, if any, have dates and owners.

> **Retest / final disposition**
> 22 Sep: verified. RT-06 records the completed 20 Sep maintenance window, running-kernel comparison and post-restart checks. No vendor release or CVE claim is made in this fictional example.

FICTIONAL EXAMPLE

06 / FINDING 07 OF 12

WP-03 | Gaps in WordPress privileged account hygiene

MEDIUM RISK / RESOLVED AT RETEST

Affected: W01, W03, W05, W07 / 7 account records
Owner: Site Operations Lead · **Observed:** 16 Sep 15:10 2026 UTC

Observation

Seven of 19 administrator account records across the eight installations had no MFA. They were distributed across W01, W03, W05 and W07. Three of the seven belonged to departed contractors and remained enabled. Login rate controls were present, but did not address credential reuse or retained access.

Impact and prerequisites

A valid stolen password or a former contractor's retained access could allow site administration. Existing rate controls reduce guessing risk; they do not establish that privileged identities remain authorized. The shared hosting identity can increase consequences for W01, W03 and W05.

EVIDENCE E-07 / SYNTHETIC NORMALIZED EXTRACT

```
Privileged account records reviewed: 19
MFA absent: W01=2; W03=2; W05=1; W07=2
Departed-contractor accounts still enabled: 3 of 7
Bounded login-rate control check: protection triggered
```

Remediation

Remove access for departed contractors after reassigning owned content. Enroll MFA for the remaining four affected administrator records and review all privileged roles. Revoke stale sessions and application passwords where relevant. Add account-owner approval and an offboarding checklist.

Acceptance test

The three departed accounts cannot authenticate; content ownership remains intact. All 16 remaining administrator records require MFA. Recovery, rate controls and ordinary publishing operate correctly.

> **Retest / final disposition**
> 22 Sep: verified. RT-07 confirms three account removals, four new MFA enrollments and the 16-account final inventory. Counts refer to site account records, not unique people.

FICTIONAL EXAMPLE

06 / FINDING 08 OF 12

BCP-01 | Recovery relies on the same provider account

MEDIUM RISK / OPEN AT RETEST

Affected: VPS-01 / backups for W01-W08
Owner: Infrastructure Lead · **Observed:** 17 Sep 11:00 2026 UTC

Observation

Daily WHM account backups completed locally. Daily provider snapshots were also configured, but both remained within the same provider account and administrative recovery boundary. No independent remote destination was configured. A staged W02 restore took 11 hours because integration settings needed manual reconstruction.

Impact and prerequisites

A single provider-account compromise or prolonged provider unavailability could affect both production and its recovery copies. The tested restoration exceeded the 8-hour target. Successful local backup jobs and provider snapshots do not prove independent recovery capability.

EVIDENCE E-08 / SYNTHETIC NORMALIZED EXTRACT

```
WHM local backups: 5 cPanel accounts / daily / success
Independent additional destination: none
Provider snapshots: daily; same provider account
W02 restore: 11h actual vs 8h target; data age = 19h
```

Remediation

Add an independently controlled private backup destination, separate backup administration and protect retained copies from routine deletion where supported. Document rebuild steps for Linux, WHM configuration and site integrations. Validate destination connectivity and then perform actual restores; these are different checks. [R6]

Acceptance test

All five current hosting accounts, and new accounts after separation, are covered. Restore a representative site and required host configuration into an isolated environment within 8 hours with data no older than 24 hours.

> **Retest / final disposition**
> 22 Sep: open. Destination procurement and credentials approved, but no full independent restore completed. Target 6 Oct 2026. Daily local copies and snapshots remain interim controls.

FICTIONAL EXAMPLE

06 / FINDING 09 OF 12

MON-01 | Security events are local and alerts lack ownership

MEDIUM RISK / OPEN AT RETEST

Affected: VPS-01, WHM-01 / all sites indirectly
Owner: Infrastructure Lead · **Observed:** 17 Sep 14:20 2026 UTC

Observation

Authentication records were retained locally for seven days and were not forwarded off-host. An approved repeated-failure test generated a log event but no notification to a named responder. Critical WordPress role-change events were not consistently retained across the portfolio.

Impact and prerequisites

An attacker with host control could tamper with local evidence. Short retention and incomplete alert routing delay detection and limit the ability to determine exposure after an incident. This weakness increases uncertainty; it does not prove an intrusion occurred.

EVIDENCE E-09 / SYNTHETIC NORMALIZED EXTRACT

```
Authentication retention: 7 days / local only
Off-host forwarding: absent
Approved failure test: event logged; alert not received
WordPress role-change coverage: inconsistent
```

FICTIONAL EXAMPLE

Remediation

Forward relevant OS, WHM and application security events to restricted off-host storage. Set proportionate retention and redact secrets or unnecessary personal data. Define alerts for privileged login anomalies, new administrators and backup failures, with a named on-call owner and escalation path.

Acceptance test

Controlled events arrive off-host with synchronized timestamps, trigger a notification received by the responder and survive local log rotation. Verify least-privilege access and complete a timed acknowledgement exercise.

> **Retest / final disposition**
> 22 Sep: open. Forwarding agent installed on a test configuration, but end-to-end production alert delivery and retention were not demonstrated. Target 29 Sep 2026.

06 / FINDING 10 OF 12

DATA-01 | Staging exposes copied guest contact records

MEDIUM RISK / RESOLVED AT RETEST

Affected: W08 / staging clone of W02
Owner: Application Development Lead · **Observed:** 17 Sep 15:05 2026 UTC

Observation

The staging site was internet-accessible and relied on a noindex directive rather than authentication. A migration-test CSV in its uploads directory contained 37 copied guest contact records and could be retrieved without a session. Live email-delivery settings were also retained in the clone.

Impact and prerequisites

The copied records included names, emails and telephone numbers. The limited dataset supports Medium in this scenario, but access was unauthenticated and required prompt containment. The retained mail configuration also created a risk of test messages reaching real guests.

EVIDENCE E-10 / SYNTHETIC NORMALIZED EXTRACT

```
GET /wp-content/uploads/test-data/guests.csv -> 200
Authentication: none; records = 37
Indexing control: noindex only
Clone mail configuration: production delivery enabled
```

Remediation

Put staging behind authentication or an approved access gateway, remove the exported file and replace copied personal data with generated test data. Isolate staging mail and external integrations. Review relevant access records and include the exposure in the data owner's incident assessment.

Acceptance test

Unapproved visitors cannot access staging pages or files. The CSV is unavailable, a data review finds only generated test records, and test mail reaches a controlled sink. Production booking workflows remain unaffected.

> **Retest / final disposition**
> 22 Sep: verified. RT-10 confirms the access gate, file removal, synthetic data replacement and mail isolation. Prior external retrieval cannot be excluded from the available logs.

FICTIONAL EXAMPLE

06 / FINDING 11 OF 12

CFG-01 | Public debug log exposes operational data

MEDIUM RISK / RESOLVED AT RETEST

Affected: W06 / partner application portal
Owner: Application Development Lead · **Observed:** 16 Sep 16:40 2026 UTC

Observation

W06 stored its WordPress debug log under a publicly served directory. An unauthenticated request returned stack traces, filesystem paths and partner-applicant email addresses recorded by a custom form handler. No password, API token or payment data was identified in the reviewed excerpt.

Impact and prerequisites

The log provided both internal application detail and personal contact data to anonymous readers. This is more material than a path-only error disclosure, but evidence did not establish credential leakage or direct code execution.

EVIDENCE E-11 / SYNTHETIC NORMALIZED EXTRACT

```
GET /wp-content/debug.log -> HTTP 200
Observed: stack trace + absolute paths + applicant email
WP_DEBUG=true; WP_DEBUG_LOG=true
WP_DEBUG_DISPLAY=false; public log access not blocked
```

Remediation

Disable unnecessary production debugging and move required logs outside publicly served paths. Correct the form handler's logging to avoid personal data and secrets, apply restricted permissions and retention, and remove exposed historical logs after evidence preservation. [R7]

Acceptance test

Public requests cannot retrieve current or rotated debug logs. A safe application error produces a generic response and a useful restricted log entry without applicant data. Form submission and support diagnostics still function.

> **Retest / final disposition**
> 22 Sep: verified. RT-11 records blocked public retrieval, private logging and a regression check on the partner form.

FICTIONAL EXAMPLE

06 / FINDING 12 OF 12

INFO-01 | Public component version information

LOW RISK / ACCEPTED AT RETEST

Affected: W01-W08 / selected HTTP headers and metadata
Owner: Head of Technology · **Observed:** 17 Sep 16:10 2026 UTC

Observation

Public response metadata disclosed component version information on the host and several sites. No exploitable vulnerability was established from the disclosed values. The information can help an attacker narrow reconnaissance, but does not bypass authentication or permissions.

Impact and prerequisites

Direct business impact is limited. Removing these signals can reduce easy fingerprinting but cannot guarantee that software versions are hidden, and is less valuable than maintaining supported, patched software.

EVIDENCE E-12 / SYNTHETIC NORMALIZED EXTRACT

```
HTTP and page metadata sample: versions present
Observed surfaces: server response / generator metadata
Matched exploitable weakness from disclosure alone: none
Coverage: host configuration and eight site samples
```

Remediation

Remove unnecessary headers and generator details where operationally safe. Continue patching and inventory management regardless of disclosure. Avoid fragile changes that interfere with cache behavior, support diagnostics or updates.

Acceptance test

For technical closure, verify selected metadata reductions and regression-test caching and updates. For acceptance, retain a named approver, rationale, compensating practices and a review date.

> **Retest / final disposition**
> 22 Sep: risk accepted by Evan Cole, Head of Technology. Review due 22 Dec 2026 or earlier if a relevant exploitable version is identified. Acceptance does not mean the metadata was removed.

FICTIONAL EXAMPLE

07 / ACTION PLAN

Close the remaining shared-environment risks

The client sponsor owns the risk decision; technical leads own implementation and evidence. Dates are committed targets within the fictional scenario.

DUE / OWNER	DELIVERABLE	ACCEPTANCE
29 Sep Infrastructure Lead	MON-01: centralize security events and complete on-call routing.	Controlled OS, WHM and WordPress events trigger received, acknowledged alerts.
2 Oct Web Engineering Lead	HOST-01: separate the four avweb sites into independent hosting identities.	All cross-site marker tests fail safely; site workflows, cron jobs and backups pass.
6 Oct Infrastructure Lead	BCP-01: independent backup destination and timed recovery drill.	Restore within 8h; recovered data no older than 24h; migrated accounts included.
22 Dec Head of Technology	INFO-01: review accepted version metadata exposure.	Acceptance renewed with rationale or targeted reduction completed.

Sequence and dependencies

Complete account separation before the final full recovery drill so the backup inventory reflects the new hosting layout. Establish alerts for backup failures as the independent destination is introduced. Track each migrated site's DNS, certificates, database credentials and scheduled jobs.

Completed immediate actions

Root SSH password access and exposed WHM access were restricted; privileged MFA was configured. The public events backup, unauthorized booking export, staging dataset and debug log were contained. Patch maintenance and WordPress administrator cleanup were verified.

> **Change safety**
> Before migrating, create recoverable backups and define rollback criteria. Validate each site with its business owner. Do not retire the previous account layout until the new site, background jobs and recovery path have passed acceptance checks.

FICTIONAL EXAMPLE

08 / POSITIVE CONTROLS AND COVERAGE

Controls that worked

These controls passed the bounded checks in the scenario. They reduce specific risks and should be preserved through remediation.

CONTROL	OBSERVED RESULT / LIMIT
TLS and redirect behavior	All eight web frontends redirected HTTP to HTTPS and presented valid certificates during testing. This is a dated observation, not a renewal guarantee.
Database network exposure	MariaDB accepted local application connections; public TCP/3306 was not reachable in the external check. Separate schemas existed for all eight sites.
Independent account boundaries	Marker tests from avweb into avbook, avpartners, avevents and avstage were denied. Within avweb, isolation failed as described in HOST-01.
Login rate controls	Bounded WordPress failure tests triggered configured protections. This did not replace MFA or offboarding, addressed in WP-03.
Core integrity and updates	Core checksum checks reported no mismatches in the eight installations. Automatic minor core updates were configured. These checks did not attest to custom plugin safety.
Local backup scheduling	Daily account backups completed for all five cPanel accounts. Independence and recovery-time requirements remained unmet under BCP-01.

Portfolio coverage summary

All eight sites received checks of authentication, privileged accounts, public files, visible errors, plugin/theme inventory and core integrity. Targeted custom-code review focused on booking exports and partner-form logging. No claim of exhaustive review is made for every theme, plugin or business workflow.

Evidence: E-00 contains the synthetic asset/control matrix. A successful core checksum test does not rule out malicious files elsewhere, compromised credentials or an application-level flaw.

FICTIONAL EXAMPLE

09 / RETEST RECORD

Eight resolved. Three open. One accepted.

Targeted retest completed 22 September 2026 by WPServerGuard/G.Schad (fictional retest scenario). The register records scenario outcomes rather than treating every implemented change as closed.

FINDING	DISPOSITION	EVIDENCE / NEXT ACTION
VPS-01	Resolved	RT-01 / acceptance checks passed
WHM-01	Resolved	RT-02 / acceptance checks passed
HOST-01	Open	Production separation pending / 2 Oct
WP-01	Resolved	RT-04 / acceptance checks passed
WP-02	Resolved	RT-05 / acceptance checks passed
OS-01	Resolved	RT-06 / acceptance checks passed
WP-03	Resolved	RT-07 / acceptance checks passed
BCP-01	Open	Independent recovery test pending / 6 Oct
MON-01	Open	Alert delivery not demonstrated / 29 Sep
DATA-01	Resolved	RT-10 / acceptance checks passed
CFG-01	Resolved	RT-11 / acceptance checks passed
INFO-01	Accepted	RA-01 / Evan Cole / review 22 Dec

FICTIONAL EXAMPLE

Closure standard

Resolved means the defined acceptance checks passed in the scenario and a reviewer recorded the result. Open means a material check is incomplete or the weakness remains. Accepted means the sponsor knowingly retains the exposure with a review trigger; it is not a technical fix.

Client acknowledgement: Evan Cole acknowledged the three remaining work items and accepted only INFO-01 on 22 September. No compliance certification or unconditional security assurance is implied.

10 / EVIDENCE AND REFERENCES

Traceable evidence, bounded conclusions

All report evidence and outcomes are synthetic. Documentation links support technical guidance; they do not substantiate an actual assessment.

Evidence index and handling

E-00: asset/control matrix. E-01-E-12: initial finding extracts. RT-01, RT-02, RT-04, RT-05, RT-06, RT-07, RT-10 and RT-11: successful retests. Open findings retain reviewer notes rather than closure records. RA-01: metadata risk acceptance. Extracts are normalized summaries, not raw terminal captures.

In the fictional engagement, detailed evidence is restricted to the client sponsor and named technical owners. Guest data and secrets are redacted from the report; controlled canary values support behavioral tests. The scenario retention period is 90 days after issue, followed by documented deletion unless the client approves a justified extension. No separate raw evidence bundle accompanies this example.

Technical references / consulted 22 September 2026

[R1] Red Hat: securing networks / OpenSSH

[R2] cPanel: two-factor authentication for WHM

[R3] cPanel: security best practices

[R4] WordPress: REST API endpoint permissions

[R5] cPanel: update preferences

[R6] cPanel: backup configuration and destination validation

[R7] WordPress: debugging in WordPress

Document control

Report ID AVH-2026-09 / Version 1.1 / issued 22 September 2026. Prepared by WPServerGuard/G.Schad for fictional Aster Vale Hospitality Group. This worked example expands the structure of the supplied WordPress sample. All assessment findings and retest outcomes are fictional examples, not observations from a live engagement.

> **End of fictional report**
> The .example hostnames, documentation IP address, custom plugin, client personnel, evidence and retest history exist only to demonstrate a credible report format. No claim about a real organization or system is intended.

FICTIONAL EXAMPLE