SAMPLE REPORT / SAMPLE-2026-001 / FICTIONAL DATA

Anonymized WordPress Incident Report

Transparency notice: All names, timestamps, systems, and findings in this document are fictional. This example is not a customer case or proof of delivered work.

1. Management summary

Unauthorized spam pages and an external redirect were identified on the example site. The baseline was preserved, active impact was contained, and file, database, account, and scheduler persistence were reviewed. A definitive data-exfiltration conclusion was not possible because of a logging gap.

2. Scope and limitations

In scope	WordPress installation, database, accounts, schedulers, available hosting logs
Out of scope	Operating-system forensics, external email accounts, legal assessment
Log coverage	Web server: 7 days; WAF: 30 days; SFTP: unavailable

3. Incident timeline

T+00:00	baseline.captured	Baseline and logs preserved
T+00:45	redirect.contained	External redirect disabled
T+03:20	persistence.removed	File and database finding removed
T+06:10	verification.complete	Functional and integrity checks

4. Findings and classification

FINDING	Modified plugin file with executable redirect code; hash and trusted comparison source documented.
INDICATOR	Unrecognized administrator without a documented purpose; created within the incident window.
LIMIT	Web-server logs covered only seven days; earliest access remained unresolved.

5. Actions completed

OK	Preserved baseline and relevant logs before changes
OK	Contained the active redirect
OK	Replaced the affected component from a verified source
OK	Reviewed files, database, accounts, sessions, and cron jobs
OK	Rotated credentials and secrets in an agreed sequence
OK	Tested frontend, login, REST, forms, and core functions

6. Data-exfiltration indicators

No confirmed export was found in the available records. The malicious code could access application configuration, and log coverage was incomplete. Result: no confirmed exfiltration, but no dependable negative conclusion.

7. Remaining actions and sign-off

OK	Extend log retention and central alerting
OK	Enable MFA for privileged identities
OK	Document a restore test for the separated backup
OK	Perform a control review after 30 days

FINAL STATUS: REMEDIATED AND TECHNICALLY VERIFIED.
Point-in-time assessment - not a promise that the system can never be attacked again.