Case Study

CyberArt Solutions Pvt. Ltd.

Hacked WordPress Website Restoration & VA/PT Engagement

I worked as a Cyber Forensics Investigator on a critical incident response and recovery project involving a compromised WordPress-based web application. The engagement required a combination of digital forensics, vulnerability assessment, penetration testing (VA/PT), and secure restoration practices to bring a hacked and damaged website back to a trusted operational state.

Project Overview

The client reported unauthorized modifications, defacement, and intermittent downtime on their WordPress website. Initial indicators suggested a successful compromise that impacted core files, plugins, and possibly sensitive data. The primary objectives of this project were:

- Investigate and identify the root cause of the compromise
- Preserve and analyze forensic evidence
- Remove malicious artifacts and restore the website
- Conduct a comprehensive VA/PT to identify existing vulnerabilities
- Strengthen the application against future attacks

his project required a structured incident response lifecycle approach, ensuring that emediation efforts did not destroy critical forensic evidence while restoring business continuity.

Roles and Responsibilities

1. Incident Identification & Evidence Preservation

- Collected and preserved forensic evidence including server logs, access logs, database snapshots, and file system artifacts
- Ensured integrity of evidence using hashing techniques to maintain chain of custody
- Created forensic copies of the compromised environment for offline analysis

2. Forensic Analysis

- Performed deep-dive analysis to identify:
- Initial entry point of the attacker
- Timeline of the attack
- Persistence mechanisms used
- Investigated indicators such as:
- Suspicious admin account creation
- Malicious PHP scripts embedded in theme and plugin files
- Unauthorized cron jobs and backdoors
- Correlated logs to trace attacker activity, IP patterns, and exploited vulnerabilities

3. Malware Identification & Removal

- Conducted file integrity checks to detect tampered core WordPress files
- Identified and removed:
- Web shells
- Obfuscated malicious scripts
- Injected spam or SEO poisoning content
- Cleaned database entries affected by malicious injections

4. Secure Restoration

- Restored the website using verified clean backups where applicable
- Rebuilt compromised components ensuring integrity and security
- Validated functionality post-restoration to ensure minimal business disruption

5. Vulnerability Assessment & Penetration Testing (VA/PT)

- Performed a full-scale security assessment of the restored application
- Identified vulnerabilities such as:
- Outdated plugins and themes
- Weak authentication mechanisms
- Misconfigured file permissions
- Exposure of sensitive endpoints
- Conducted penetration testing to validate exploitability and real-world impact

6. Hardening & Security Implementation

- Implemented security best practices, including:
- Enforcing strong password policies and MFA
- Restricting admin access and disabling unnecessary services
- Securing wp-config and sensitive files
- Configuring Web Application Firewall (WAF) rules
- Recommended regular patching and monitoring mechanisms

7. Reporting & Recommendations

- Delivered a detailed forensic report covering:
- Root cause analysis
- Attack timeline and techniques used
- Impact assessment
- Provided a VA/PT report with:
- Risk ratings and proof of concepts
- Prioritized remediation steps
- Shared actionable recommendations for long-term security improvement

Key Achievements

- Successfully identified the root cause of the breach, enabling targeted remediation
- Restored the compromised WordPress application with minimal downtime
- Eliminated multiple persistence mechanisms used by the attacker
- Strengthened the platform through comprehensive security testing and hardening
- Improved the client’s ability to detect and respond to future incidents

Impact

This engagement significantly enhanced the security posture of the client’s web application. By combining forensic investigation with proactive VA/PT, the project ensured not only recovery from the attack but also long-term resilience. The organization was able to:

- Regain control over its digital assets
- Prevent recurrence of similar attacks
- Build confidence among users and stakeholders
- Establish stronger monitoring and incident response practices

Skills and Expertise Demonstrated

- Digital forensics and incident response
- Log analysis and attack timeline reconstruction
- Malware analysis and removal
- WordPress security and hardening
- Web application VA/PT
- Risk assessment and technical reporting

Conclusion

This project showcased the importance of integrating cyber forensics with security testing in incident response scenarios. As a Cyber Forensics Investigator, I played a key role in not only uncovering how the breach occurred but also ensuring that the system was securely restored and hardened against future threats.

The experience reinforced the critical need for proactive security, continuous monitoring, and a well-defined incident response strategy—especially for widely used platforms like WordPress, which are frequent targets for attackers.