# OSINT Security Investigation Report

Prepared by: Shaik Abdul Rehman | Role: SOC Analyst (Aspiring) | Date: March 2026

### Executive Summary

This investigation was conducted to analyze the URL http://testphp.vulnweb.com/ using open-source intelligence tools. The purpose was to identify any potential malicious activity and validate the results using multiple trusted sources, similar to a real SOC workflow.

### Project Objective

The objective of this investigation is to evaluate the security posture of the given URL, identify any indicators of compromise, and determine whether the detection is legitimate or a false positive.

### System Approach

The analysis follows a structured SOC approach including data collection, threat validation, correlation of findings, and final decision-making based on evidence from multiple tools.

### Methodology

The URL was first submitted to VirusTotal for threat detection. URLScan.io was used to observe the behavior of the webpage. WHOIS lookup was performed to verify domain age and infrastructure. All findings were compared to reach a final conclusion.

### Tools & Technologies

VirusTotal, URLScan.io, and WHOIS Lookup (DomainTools) were used during the investigation.

### Investigation Findings

The URL http://testphp.vulnweb.com/ was analyzed across multiple platforms. VirusTotal showed 1 out of 95 detections, which suggests a low-confidence alert. URLScan did not return a screenshot, likely due to access restrictions, and showed no suspicious activity. WHOIS data indicates the domain has been active since 2010 and is hosted on AWS, which supports its legitimacy.

### SOC Output

- Indicators of Compromise: URL analyzed
- Threat Type: No confirmed threat
- Severity Level: Low (False Positive Suspected)
- Recommendation: No action required

### Practical Relevance

This investigation reflects real SOC responsibilities such as validating alerts, analyzing threat intelligence, and making decisions based on evidence.

### Conclusion

The analysis confirms that the URL appears safe. The detection from VirusTotal is likely a false positive as it is not supported by other tools.

### Incident Timeline

10:30 AM – URL submitted
10:32 AM – VirusTotal scan completed
10:35 AM – URLScan performed
10:38 AM – WHOIS reviewed
10:40 AM – Final analysis completed

### Indicators of Compromise (IOCs)

- URL: http://testphp.vulnweb.com/
- Detection: 1/95
- Behavior: Normal
- Infrastructure: AWS hosted

### Recommended Actions

- No immediate action required
- Monitor if needed
- Validate with additional tools if required

---

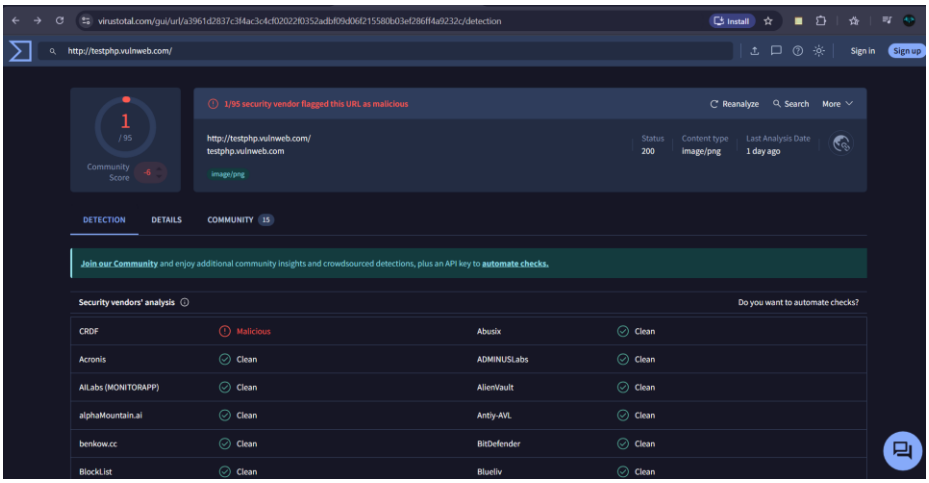
### Appendix – Supporting Evidence

https://www.virustotal.com/gui/url/a3961d2837c3f4ac3c4cf02022f0352adbf09d06f215580b03ef286ff4a9232c/detection

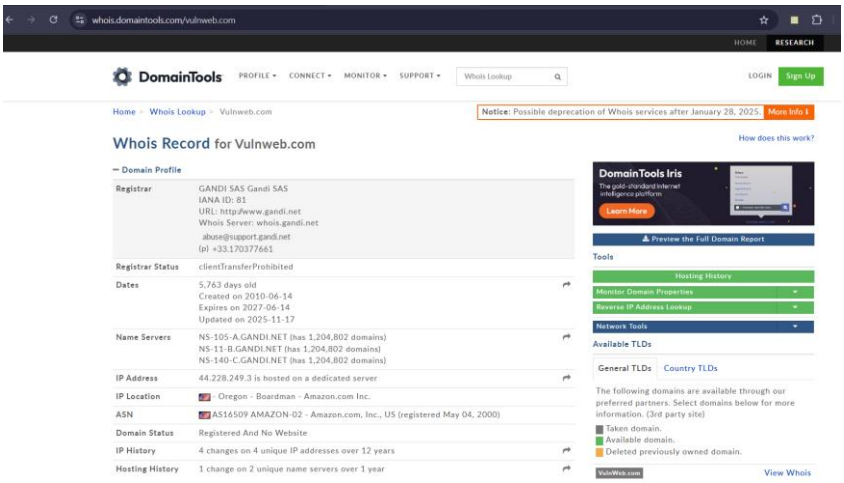
https://urlscan.io/result/019d2493-ab68-72fa-8ff6-58228c8b0842/

https://whois.domaintools.com/vulnweb.com

## -Figure 1: Virus Total Detection Result




## -Figure 2: -Whois.domain tool




## Figure 3: URLScan Analysis