SOC Incident Report

Web Application Attack – DVWA Lab Environment

Incident Overview

A Security Operations Center investigation was conducted following the detection of malicious web activity targeting a vulnerable web application (DVWA) hosted on a Windows 10 system. The activity involved SQL Injection and Command Injection techniques executed from a Kali Linux host within a controlled lab environment.

Incident Details

Incident ID: SOC-WEB-2025-001
Severity: High
Status: Resolved (Lab)
Target System: Windows 10 + XAMPP + DVWA
Target IP: 10.10.10.10
Port: 8080

Detection Summary

The incident was detected through analysis of Apache web server logs. Indicators included repeated URL-encoded SQL payloads, automated scanning behavior, and command execution attempts.

Indicators of Compromise

- Repeated SQL injection payloads ('OR 1=1', UNION SELECT)
- Automated exploitation using sqlmap (identified via User-Agent)
- Command injection via vulnerable application parameters

Attack Timeline

Initial reconnaissance was observed, followed by successful SQL injection exploitation. Database enumeration and credential hash extraction occurred shortly thereafter. Command injection attempts confirmed operating system–level access.

Technical Analysis

SQL injection vulnerabilities allowed the attacker to enumerate databases and extract credential hashes. Command injection vulnerabilities enabled execution of system commands via unsanitized input fields.

Impact Assessment

Confidentiality: Compromised
Integrity: Potentially compromised
Availability: Not impacted
Business Risk: High if in production

Root Cause

- Lack of input validation
- Absence of parameterized queries
- Unsafe PHP functions enabled
- Weak application security configuration

MITRE ATT&CK; Mapping

- T1190 – Exploit Public-Facing Application
- T1059 – Command and Scripting Interpreter
- T1552 – Credential Access

Response Actions

Simulated containment actions included isolating the affected host, disabling vulnerable endpoints, and resetting compromised credentials.

Recommendations

- Implement prepared statements and input validation
- Deploy web application firewall rules
- Centralize logging and alerting
- Perform regular security testing

Analyst

Ismail Imam
SOC / Security Analyst (Lab Simulation)