Security Compromise Analysis Report

Summary

System Compromised : YES
Severity : CRITICAL
Final Decision : CONFIRMED SYSTEM COMPROMISE
Anomaly Score : 1.0

Attack Details

Entry Point : Web Application
Attack Type : SQL Injection / XSS
Privilege Escalation : User → Root

Attack Timeline

- Privilege escalation attempt by user www-data using command /bin/bash
- Kernel-level security event detected
- Privilege escalation attempt by user www-data using command /usr/bin/id
- SSH login success for user user1 from IP 198.51.100.123
- Privilege escalation attempt by user user1 using command /usr/bin/python3 /tmp/exploit.py
- Kernel-level security event detected
- Login failed from IP 198.51.100.77
- Login failed from IP 198.51.100.77
- Login failed from IP 198.51.100.77
- Login failed from IP 198.51.100.77
- Login failed from IP 198.51.100.77
- Login failed from IP 198.51.100.77
- Login failed from IP 198.51.100.77
- SQL Injection attempt on /login?user=admin'-- from IP 198.51.100.99
- XSS payload detected on /profile?name=%3Cimg%20src%3Dx%20onerror%3Dalert(1)%3E fro