# WEB APPLICATION SECURITY TESTING

**Security Alert Monitoring & Incident Response Simulation**

**INTERN NAME:** RISHIKA JOSHI
**INTERNSHIP PROGRAM:** CYBER SECURITY INTERNSHIP – FUTURE INTERNS
**TASK: –** WEB APPLICATION SECURITY TESTING
**TARGET APPLICATION:** OWASP JUICE SHOP

**Target URL:** https://demo.owasp-juice.shop
**Assessment Type:** Vulnerability Assessment
**Tool Used:** OWASP ZAP
**Date:** 24-12-25

# Agenda

| | |
|---|---|
| 01 | Introduction |
| 02 | scope of testing |
| 03 | test and methadology |
| 04 | Vulnerability Findings |
| 05 | conclusion |
| 06 | Thank you |

# INTRODUCTION

This project simulates the real-world activities performed inside a Security Operations Center (SOC). As a SOC analyst intern, my role was to monitor security alerts, analyze suspicious events, and simulate an appropriate incident response using a SIEM platform – in this case, Splunk.
Using simulated enterprise security logs, I monitored system activity such as user logins, authentication failures, network connections, and malware alerts. The main objective was to detect potential security threats early, assess their severity, and recommend suitable response actions – similar to how real SOC teams protect organizations from cyberattacks 24/7.
.

# scope of testing

The scope of this SOC security monitoring project included:

## In-Scope

Log ingestion into a SIEM (Splunk)

All publicly accessible pages and directories

## Out-Scope

External domains (Google, GitHub, CDN links, social media)

Third-party services

# TOOLS

- **Splunk Enterprise (Free Trial) – SIEM log monitoring & search**
- **Sample SOC Logs (SOC_Task2_Sample_Logs) – Simulated event data**
- **Windows Machine – Environment**
- **MS Word / PPT – Documentation & reporting**

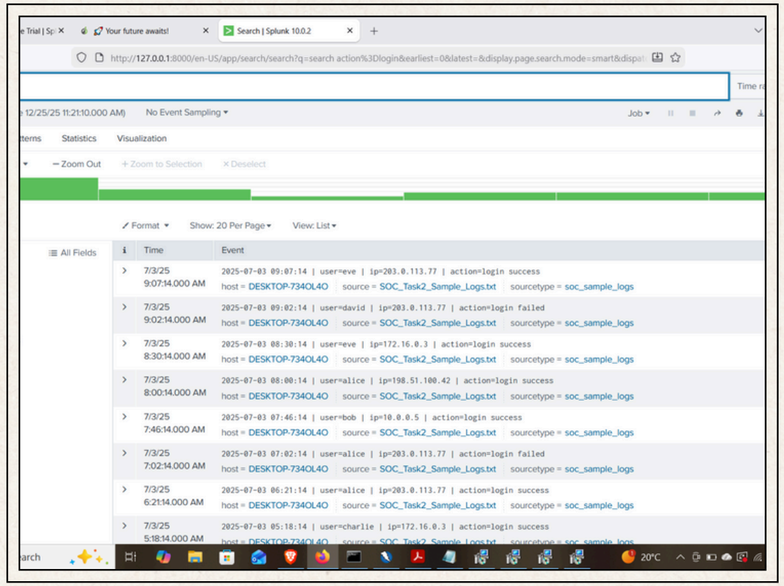
# METHODOLOGY

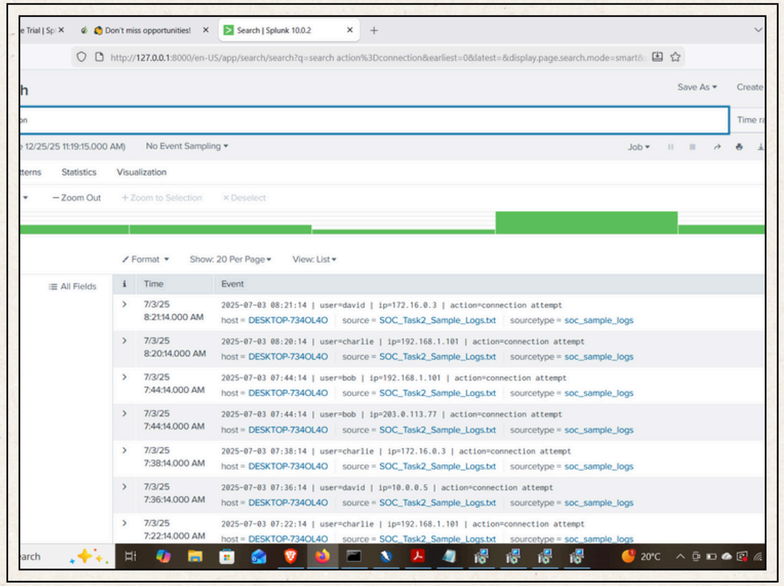
**Log Ingestion in Splunk**

**Log Search & Filtering**

**Event Review & Field Extraction**

**Threat Identification**




# Vulnerability Findings

Vulnerability 1 :Malware Alert

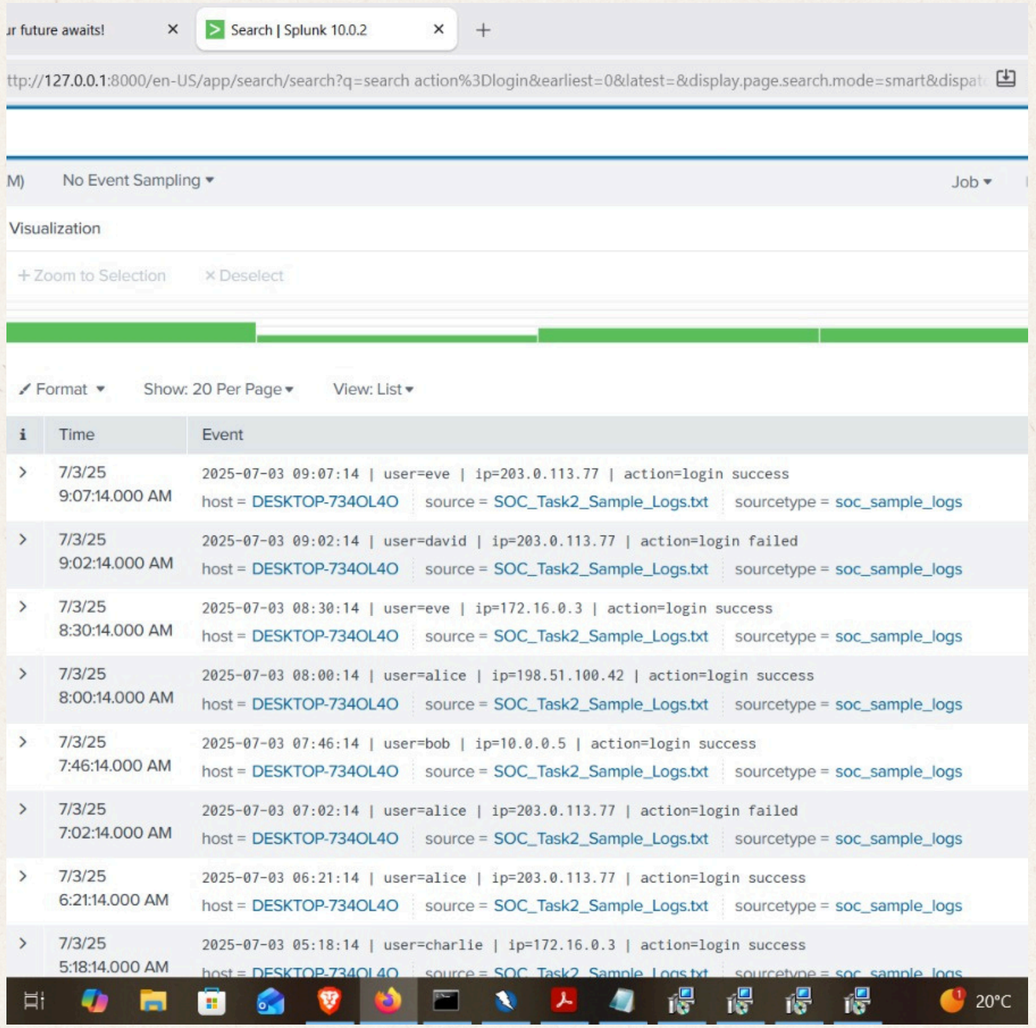
servity:high i

action:Isolate system & perform deep scan immediately

# vernability 2: login failed

# sevity:medium

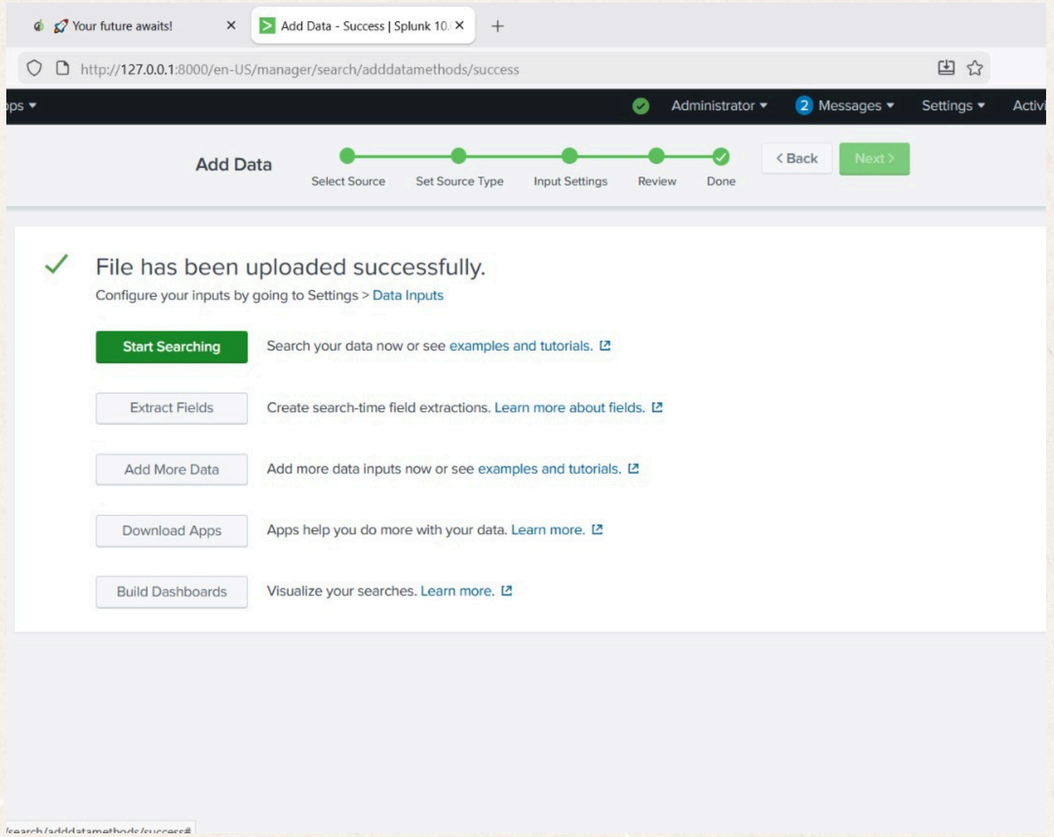
# action:Monitor user & enforce MFA



# vernabilty 3: Successful login

# sevity:low

# action:No action  baseline monitoring only



# conclusion

**This SOC internship simulation successfully demonstrated how SIEM-based security monitoring helps detect threats early and supports cybersecurity defense operations.**

| TIME | USER | IP ADDRESS | EVENT TYPE | DETAILS | SEVERITY | ACTION |
|---|---|---|---|---|---|---|
| 2025-07-03 09:10:14 | Bob | 172.16.0.3 | Malware alert | Ransomware detected | High | Isolate sysytem and scan |
| 2025-07-03 07:51:14 | Eve | 10.0.5 | Malware alert | Rootkit detected | High | Quarantine and deep scan |
| 2025-07-03 07:45:14 | Charlie | 172.16.0.3 | Malware alert | Trojan detected | High | Remove malware and block source |
| 2025-07-03 09:07:14 | David | 203.0.113.77 | Login-failed | Login failed | Medium | Monitor and enforce MFA |
| 2025- | Eve | 203.0.113.77 | Login- | Login | Low | No action |

# Thank you