

# **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

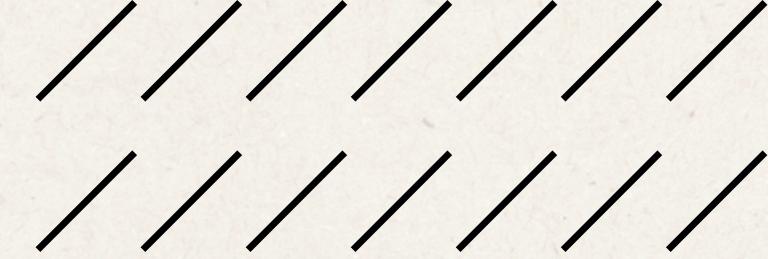
**Target URL:** <https://demo.owasp-juice.shop>

**Assessment Type:** Vulnerability Assessment

**Tool Used:** OWASP ZAP

**Date:** 24-12-25

# Agenda



01	<b>Introduction</b>
02	<b>scope of testing</b>
03	<b>test and methodology</b>
04	<b>Vulnerability Findings</b>
05	<b>conclusion</b>
06	<b>Thank you</b>

# 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**

Your future awaits! Search | Splunk 10.2

http://127.0.0.1:8000/en-US/app/search/search?q=search%20action%3Dlogin&earliest=0&latest=&display.page.search.mode=smart&display.page.list.mode=table

12/25/25 11:21:00 AM No Event Sampling Job

Items Statistics Visualization

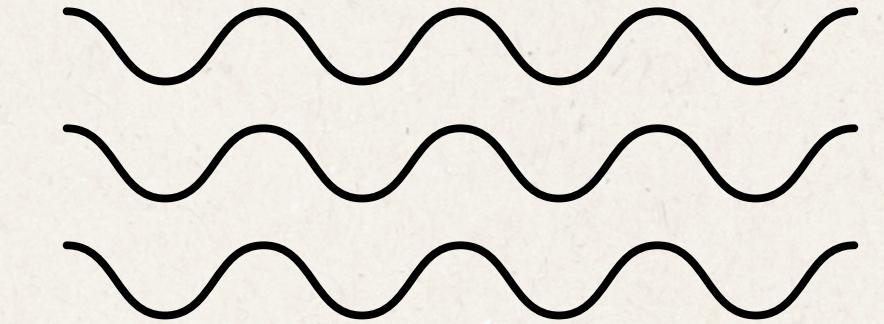
- Zoom Out + Zoom to Selection X Deselect

Format Show: 20 Per Page View: List

All Fields i Time Event

>	7/3/25 9:07:14:000 AM	2025-07-03 09:07:14   user=eve   ip=203.0.113.77   action=login success
>	7/3/25 9:02:14:000 AM	host = DESKTOP-734OL40 source = SOC_Task2_Sample_Logs.txt sourcetype = soc_sample_logs
>	7/3/25 8:30:14:000 AM	2025-07-03 08:30:14   user=eve   ip=172.16.0.3   action=login success
>	7/3/25 8:00:14:000 AM	host = DESKTOP-734OL40 source = SOC_Task2_Sample_Logs.txt sourcetype = soc_sample_logs
>	7/3/25 7:46:14:000 AM	2025-07-03 07:46:14   user=alice   ip=198.51.100.42   action=login success
>	7/3/25 7:02:14:000 AM	host = DESKTOP-734OL40 source = SOC_Task2_Sample_Logs.txt sourcetype = soc_sample_logs
>	7/3/25 6:21:14:000 AM	2025-07-03 06:21:14   user=alice   ip=203.0.113.77   action=login success
>	7/3/25 5:18:14:000 AM	host = DESKTOP-734OL40 source = SOC_Task2_Sample_Logs.txt sourcetype = soc_sample_logs

arch



# Vulnerability Findings

Don't miss opportunities! Search | Splunk 10.2

http://127.0.0.1:8000/en-US/app/search/search?q=search%20action%3Dconnection&earliest=0&latest=&display.page.search.mode=smart&display.page.list.mode=table

12/25/25 11:19:15:000 AM No Event Sampling Job

Items Statistics Visualization

- Zoom Out + Zoom to Selection X Deselect

Format Show: 20 Per Page View: List

All Fields i Time Event

>	7/3/25 8:21:14:000 AM	2025-07-03 08:21:14   user=david   ip=172.16.0.3   action=connection attempt
>	7/3/25 8:20:14:000 AM	host = DESKTOP-734OL40 source = SOC_Task2_Sample_Logs.txt sourcetype = soc_sample_logs
>	7/3/25 7:44:14:000 AM	2025-07-03 07:44:14   user=bob   ip=192.168.1.101   action=connection attempt
>	7/3/25 7:44:14:000 AM	host = DESKTOP-734OL40 source = SOC_Task2_Sample_Logs.txt sourcetype = soc_sample_logs
>	7/3/25 7:38:14:000 AM	2025-07-03 07:38:14   user=charlie   ip=172.16.0.3   action=connection attempt
>	7/3/25 7:36:14:000 AM	host = DESKTOP-734OL40 source = SOC_Task2_Sample_Logs.txt sourcetype = soc_sample_logs
>	7/3/25 7:22:14:000 AM	2025-07-03 07:22:14   user=charlie   ip=192.168.1.101   action=connection attempt

arch

Vulnerability 1 :Malware Alert  
Severity:high  
Action:Isolate system & perform deep scan  
immediately

# vulnerability 2: login failed

severity:medium

action:Monitor user & enforce MFA

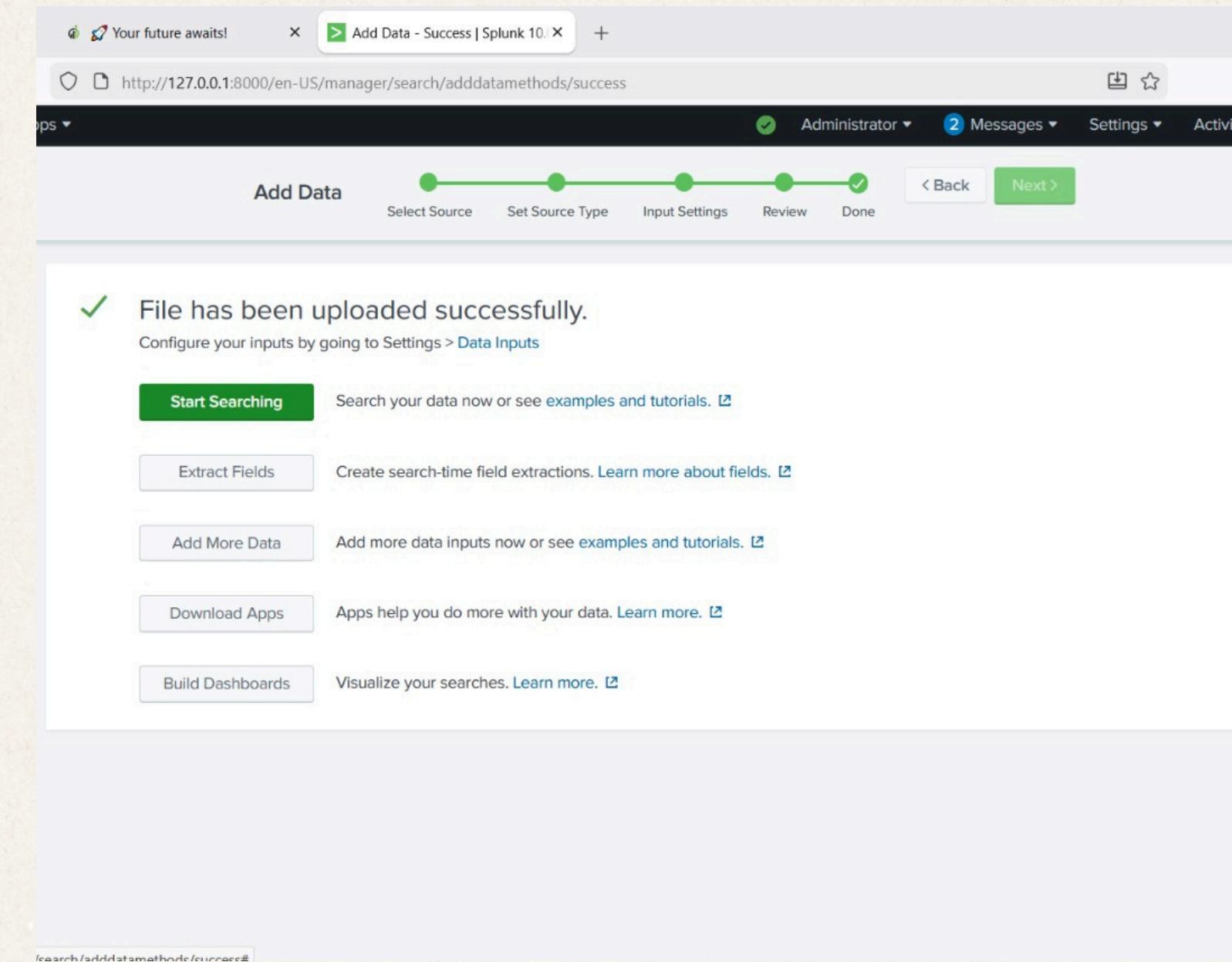
The screenshot shows a Splunk search results page. The top navigation bar includes tabs for 'Search' and 'Splunk 10.0.2'. The URL in the address bar is <http://127.0.0.1:8000/en-US/app/search/search?q=search%20action%3Dlogin&earliest=0&latest=&display.page.search.mode=smart&display.page=search>. The main area displays a table of log events. The table has three columns: 'Time' (sorted by descending timestamp), 'Event' (containing log details), and a small icon column. The log entries show various users (eve, david, alice, bob, charlie) attempting to log in from different IP addresses (203.0.113.77, 172.16.0.3, 198.51.100.42, 10.0.0.5) at different times on July 3, 2025. Some entries indicate a 'login success' while others show a 'login failed' status.

i	Time	Event
>	7/3/25 9:07:14.000 AM	2025-07-03 09:07:14   user=eve   ip=203.0.113.77   action=login success host = DESKTOP-734OL4O   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs
>	7/3/25 9:02:14.000 AM	2025-07-03 09:02:14   user=david   ip=203.0.113.77   action=login failed host = DESKTOP-734OL4O   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs
>	7/3/25 8:30:14.000 AM	2025-07-03 08:30:14   user=eve   ip=172.16.0.3   action=login success host = DESKTOP-734OL4O   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs
>	7/3/25 8:00:14.000 AM	2025-07-03 08:00:14   user=alice   ip=198.51.100.42   action=login success host = DESKTOP-734OL4O   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs
>	7/3/25 7:46:14.000 AM	2025-07-03 07:46:14   user=bob   ip=10.0.0.5   action=login success host = DESKTOP-734OL4O   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs
>	7/3/25 7:02:14.000 AM	2025-07-03 07:02:14   user=alice   ip=203.0.113.77   action=login failed host = DESKTOP-734OL4O   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs
>	7/3/25 6:21:14.000 AM	2025-07-03 06:21:14   user=alice   ip=203.0.113.77   action=login success host = DESKTOP-734OL4O   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs
>	7/3/25 5:18:14.000 AM	2025-07-03 05:18:14   user=charlie   ip=172.16.0.3   action=login success host = DESKTOP-734OL4O   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs

# vulnerability 3: Successful login

## severity: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 system 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**

---