TASK 2: SECURITY ALERT MONITORING & INCIDENT RESPONSE

Intern Name: Shahidul Hasan

Track Code: FUTURE_CS_02

Domain: Cyber Security

Internship Provider: Future Interns

Duration: June,2025

Tools Used: Splunk Enterprise, Browser, Sample Logs (access.log)

Submission Type: Task Report

AIM:

To analyze logs from a web server using a SIEM tool (Splunk), detect potential security incidents such as SQL Injection, XSS, and Brute-Force attacks, and respond with appropriate mitigation strategies.

TOOLS USED:

- Splunk Enterprise: For indexing, searching, and analyzing logs.
- access.log: Contains simulated HTTP requests with malicious payloads.
- Browser + VS Code: To view logs, edit reports, and push to GitHub.

LOG FILE ANALYZED:

- File Name: access.log
- Total Events Indexed: 50
- Time Range Covered: 24 June 2025

VULNERABILITIES TESTED:

1. SQL Injection

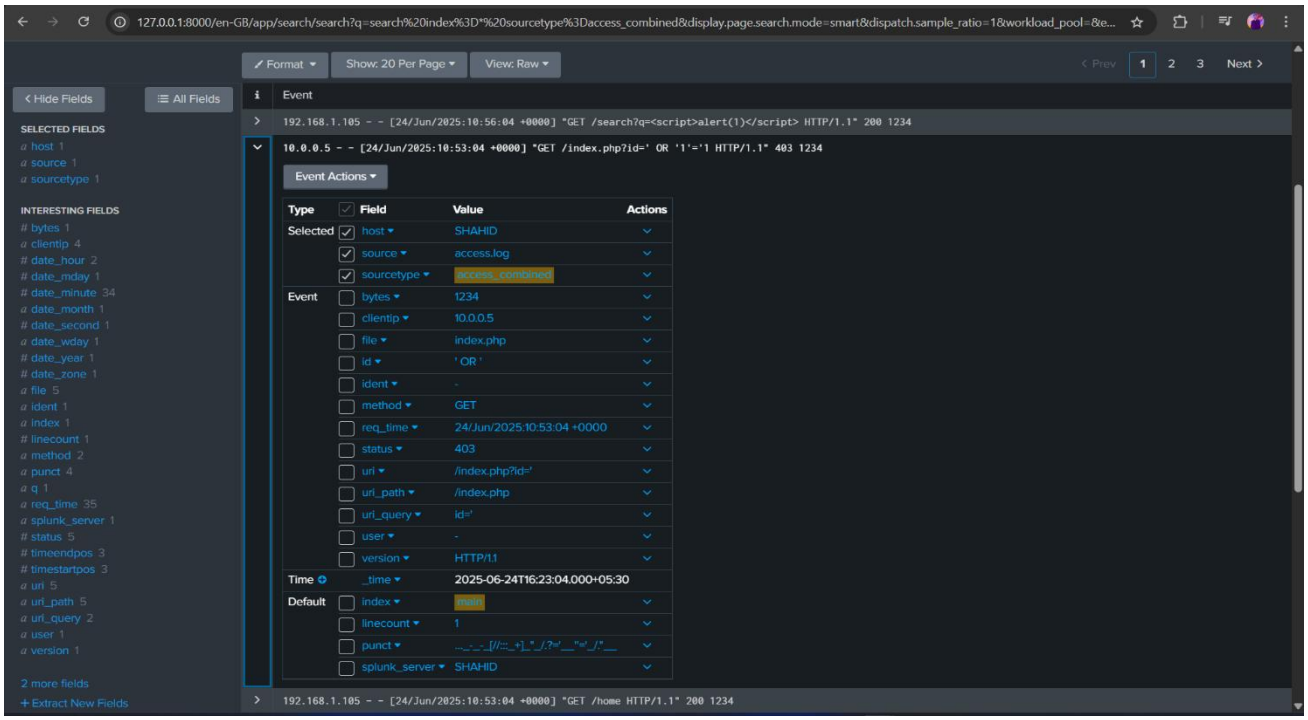
Log Sample:

GET /index.php?id=' OR '1'='1 HTTP/1.1" 403

- IP Address: 10.0.0.5
- Timestamp: 24/Jun/2025 10:53:04
- Description:
  The query parameter contained an SQL Injection payload

which could bypass authentication or dump database data. Server responded with 403, indicating partial protection.

- **Screenshot:**



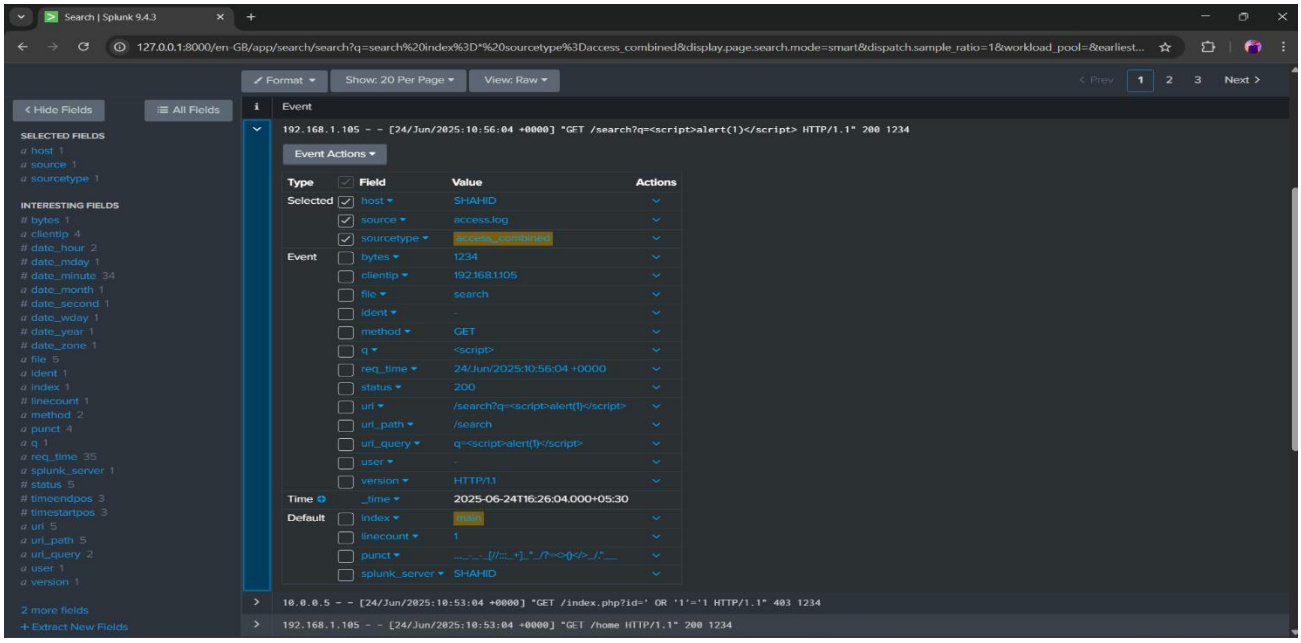
2. Reflected XSS

Log Sample:

GET /search?q=<script>alert(1)</script> HTTP/1.1" 200

- **IP Address:** 192.168.1.105
- **Timestamp:** 24/Jun/2025 10:56:04
- **Description:**
  A script tag was passed via the query string and successfully reflected in the browser. Response status 200 confirms payload was rendered without sanitization.

- **Screenshot:**

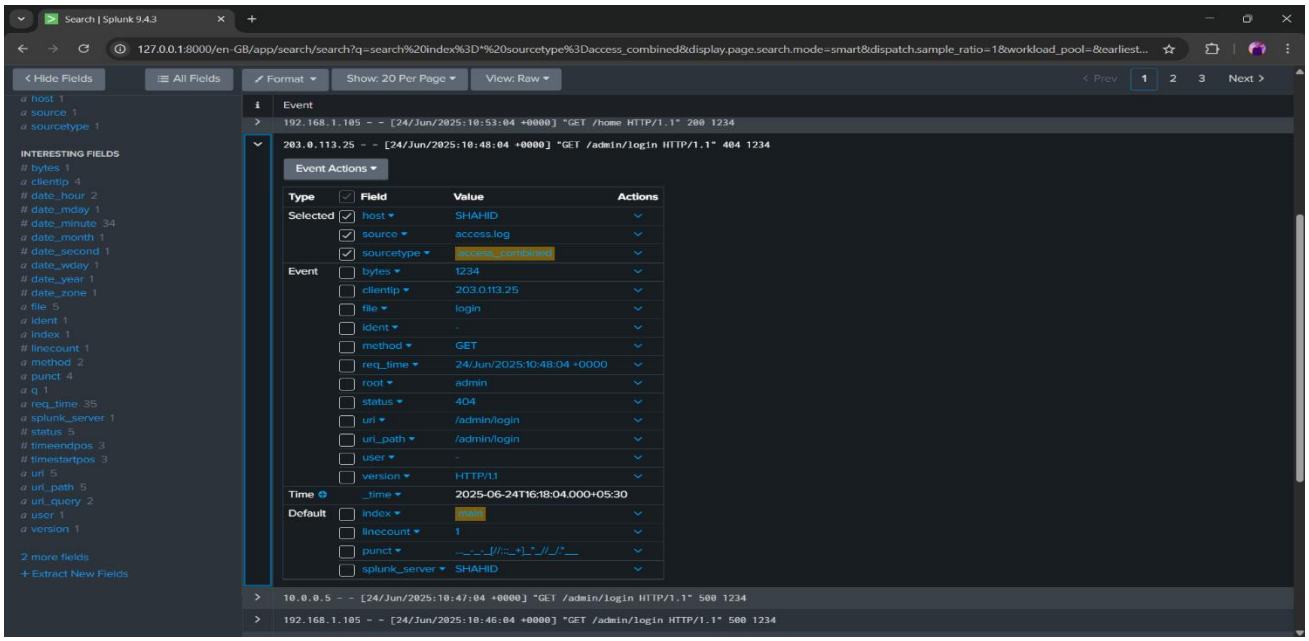


3. Brute-Force Login Attempt

Log Sample:

GET /admin/login HTTP/1.1" 401 / 500 / 404

- IP Address: 203.0.113.25, 10.0.0.5
- Multiple Attempts Detected:
  Logs show repeated login attempts across failed status codes indicating password guessing attempts.
- Screenshot:



FINDINGS SUMMARY:

Vulnerability	IP Address	Status	Risk
SQL Injection	10.0.0.5	403	High
Reflected XSS	192.168.1.105	200	Critical
Brute Force Login	203.0.113.25	401/500	Medium

RECOMMENDATIONS:

- ✅ Implement input sanitization and parameterized queries.
- ✅ Use output encoding and CSP headers.
- ✅ Enable brute-force protection (rate limiting, fail2ban).
- ✅ Log and monitor failed login attempts in real-time.
- ✅ Regularly update and patch web applications.

LEARNING OUTCOME:

Through this task, I learned to:

- Use **Splunk** for real-time log analysis
- Detect **common attack patterns** like SQLi and XSS
- Simulate **SOC workflows** like triaging and documenting incidents
- Write structured reports for cybersecurity findings

CONCLUSION:

This exercise demonstrated how logs can expose critical attack patterns and how SIEM tools like Splunk empower defenders to detect them early. By working on real-world attack traces, I've strengthened my capability to handle web security incidents and respond effectively with actionable intelligence.