

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:**

The screenshot shows a Splunk search interface with the following details:

- Selected Fields:** host, source, sourcetype (access_combined).
- Interesting Fields:** bytes, clientip, date_hour, date_mday, date_minute, date_month, date_second, date_wday, date_year, date_zone, file, ident, index, linecount, method, punct, q, req_time, status, timeendpos, timestartpos, uri, url_path, url_query, user, version.
- Event Actions:** A table showing event details:

Type	Field	Value	Actions
Selected	host	SHAHID	▼
	source	access.log	▼
	sourcetype	access_combined	▼
Event	bytes	1234	▼
	clientip	10.0.0.5	▼
	file	index.php	▼
	id	' OR '	▼
	ident	-	▼
	method	GET	▼
	req_time	24/Jun/2025:10:53:04 +0000	▼
	status	403	▼
	uri	/index.php?id=	▼
	url_path	/index.php	▼
	url_query	id='	▼
	user	-	▼
	version	HTTP/1.1	▼
Time	_time	2025-06-24T16:23:04.000+05:30	▼
Default	index	main	▼
	linecount	1	▼
	punct	..._-_-_[/..._+]+_?=_^=_/?=_	▼
	splunk_server	SHAHID	▼
- Log Sample:** 192.168.1.105 -- [24/Jun/2025:10:53:04 +0000] "GET /search?q=<script>alert(1)</script> HTTP/1.1" 200 1234

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:**

The screenshot shows the Splunk 9.4.3 search interface. The search bar at the top contains the query: `search%20index%3D%20sourcetype%3Daccess_combined&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&earliest...`. The results pane displays an event for a host named "SHAHID" with source "access.log" and sourcetype "access_combined". The event details show a GET request to "/search?q=<script>alert(1)</script>" with status 200. The event actions panel is open, showing the selected host, source, and sourcetype, along with other event fields like bytes, clientip, file, ident, method, q, req_time, status, url, url_path, url_query, user, and version. The time range is set to 2025-06-24T16:26:04.000+05:30. The default index is "main", linecount is 1, and punct is "...". The Splunk server is listed as "SHAHID". Below the main event, there are two more events: one from IP 10.0.0.5 and another from host 192.168.1.105.

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:

The screenshot shows the Splunk 9.4.3 search interface. The search bar at the top contains the same query as the previous screenshot. The results pane displays an event for host "SHAHID" with source "access.log" and sourcetype "access_combined". The event details show a GET request to "/admin/login" with status 404. The event actions panel is open, showing the selected host, source, and sourcetype, along with other event fields like bytes, clientip, file, ident, method, q, req_time, status, url, url_path, url_query, user, and version. The time range is set to 2025-06-24T16:18:04.000+05:30. The default index is "main", linecount is 1, and punct is "...". The Splunk server is listed as "SHAHID". Below the main event, there are two more events: one from IP 10.0.0.5 and another from host 192.168.1.105.

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

FINDINGS SUMMARY:

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.