



FUTURE INTERNS

SECURITY ALERT MONITORING & INCIDENT RESPONSE

Task 2: Incident response report with alert analysis, incident classification, and remediation recommendations

Author

Shaheer Ali

Date

August 11, 2025

Tools Used

Splunk (Search, Field
Extraction, Event Review)

Author
Shaheer Ali

Task
**Task 2 — SECURITY ALERT
MONITORING & INCIDENT
RESPONSE**

Date
August 11, 2025

Executive Summary

Methodology

Dashboard Summary

Alert Analysis

Incident Classification

Evidence (Screenshots)

Recommendations

What I Learned

Conclusion

Executive Summary

High-level overview of what was monitored, what was found, and the actions proposed.

Using Splunk, I monitored HTTP access patterns and highlighted potentially malicious requests targeting administrative endpoints and attempting SQL injection. From the provided event samples, at least three unique external IPs probed endpoints such as /admin and /phpmyadmin, and one request used an injection payload resembling ' OR '1'='1 with a tool signature similar to sqlmap/1.4. The affected host in the samples is **DESKTOP-H9J6DRG**.

The incidents are classified as reconnaissance and injection attempts. Immediate mitigations include enforcing WAF rules, hardening authentication, and blocking abusive sources while improving detection fidelity in Splunk.

Methodology


How the data was collected, filtered, and analyzed within Splunk.

- Collected HTTP access events into the index: security_test.
- Filtered by host, source, and sourcetype as shown in the screenshot panel (host: DESKTOP-H9J6DRG, source: security_logs.log, sourcetype: testing).
- Queried suspicious URIs including /admin, /phpmyadmin, and parameterized search endpoints containing single-quote patterns.
- Flagged user-agents indicating automated tools (e.g., curl/7.68.0,sqlmap/1.4).
- Extracted fields to identify unique source IPs, response codes, and timestamps.

- Summarized findings and prepared evidence screenshots directly from Splunk.


Dashboard Summary

Key indicators extracted from the provided samples.

Unique Source IPs (sample)


≥ 3

203.0.113.77, 198.51.100.45, 198.51.100.23

Blocked Admin Probes


2+

403 responses to /admin, /phpmyadmin

SQLi Attempt

1

GET /search.php?q=' OR '1'='1 (500/600)

Affected Host (sample)

DESKTOP-H9J6DRG

source: security_logs.log

Note: KPIs reflect the provided screenshots/snippets and represent a sample, not full environment counts.

Alert Analysis

Details of notable events observed.

Observed Patterns

- Repeated access to administrative paths with 403 responses suggesting blocked or unauthorized probes.
- SQL injection style query parameter containing single quotes and a tool user-agent indicating automated testing.
- Requests originated from multiple external IPs in test networks (e.g., 203.0.113.77, 198.51.100.45, 198.51.100.23).

Risk Assessment

- **Reconnaissance/Enumeration:** Medium — Attempts to locate admin panels are common precursors to intrusion.
- **SQL Injection Attempt:** High — If exploitable, could lead to data exfiltration or privilege escalation.

Potential Impact

Successful exploitation could expose sensitive data or grant unauthorized access. Even failed attempts increase operational noise and can mask more targeted attacks.

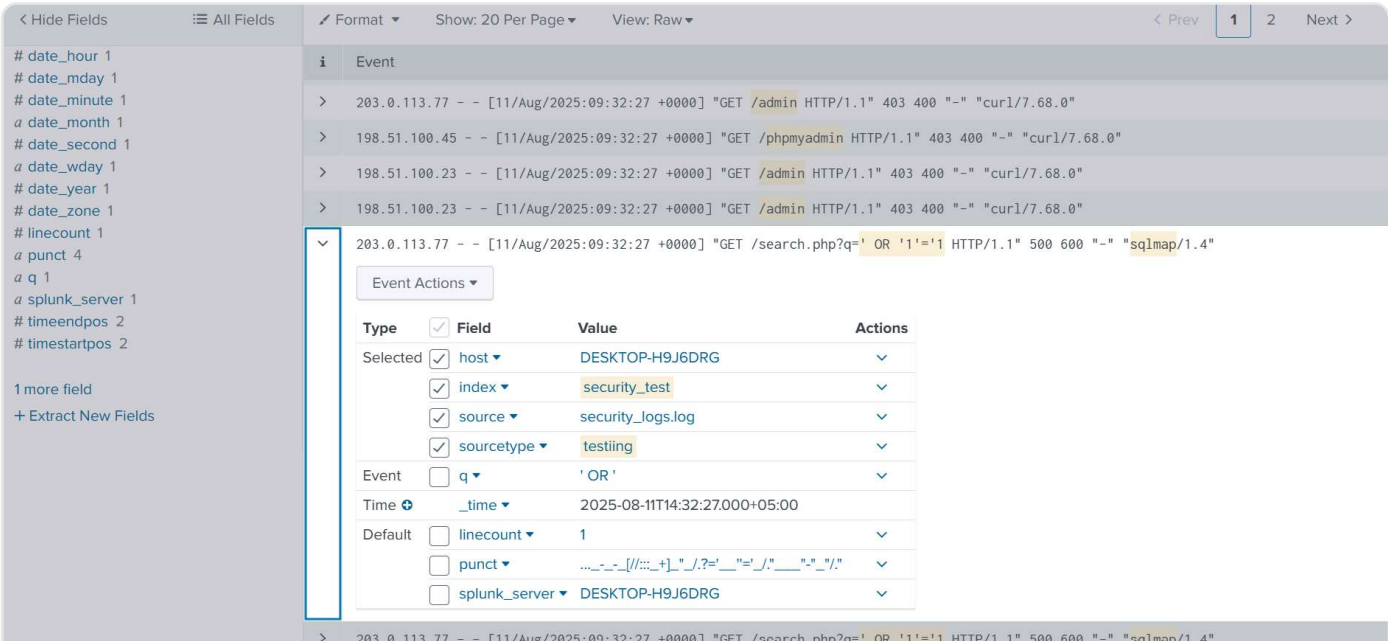
Incident Classification

Categorization aligned with common security taxonomies.

- **Type:** Web Application Attack — Reconnaissance and Injection.
- **Severity (sample context):** Medium-High (due to presence of SQLi attempt).
- **Status:** Detected and documented; further validation recommended against full dataset.
- **Affected Asset:** DESKTOP-H9J6DRG (from sample logs).

Evidence (Screenshots)

Screenshots from Splunk demonstrating the observed events and fields.



Splunk event view highlighting admin probes and SQLi-style request

Shows host, index, source, sourcetype filters and user-agent 'sqlmap/1.4'.

raw	raw	raw	raw	raw	raw	raw	raw	raw	eventtype	host	id	index	linecount	password	punct	q	source	sourcetype	splunk_se	splunk_se	timeendp	timestartp	username
198.51.101.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	45	19			
198.51.101.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	45	19			
198.51.101.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	45	19			
203.0.113.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	44	18			
198.51.101.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	45	19			
198.51.101.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	45	19			
203.0.113.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	44	18			
198.51.101.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	45	19			
198.51.101.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	45	19			
203.0.113.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	44	18			
203.0.113.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	44	18			
198.51.101.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	45	19			
198.51.101.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	45	19			
203.0.113.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	44	18			
198.51.101.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	45	19			
198.51.101.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	45	19			
203.0.113.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	44	18			
198.51.101.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	45	19			
198.51.101.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	45	19			
203.0.113.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	44	18			
192.168.1.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	44	18			
192.168.1.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	44	18			
203.0.113.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	44	18			
192.168.1.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	44	18			
192.168.1.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	44	18			
192.168.1.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	44	18			
192.168.1.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	44	18			
192.168.1.2025-08-1	9	11	32	august	27	monday	2025	0	DESKTOP-H9IGDRG	security_t	1	security_lctesting	DESKTOP-H9IGDRG	44	18			

Raw table extract with fields (raw, host, index, q, timestamps)

Demonstrates repeated patterns and multiple source IPs within the sample.

Remediation Recommendations

Immediate and longer-term actions to reduce risk.

Immediate

- Block or rate-limit abusive source IPs observed in logs.
- Enforce strong authentication and restrict access to admin endpoints behind VPN or allow-lists.
- Deploy or tighten WAF rules for SQL injection and generic injection payloads; validate on staging before production rollout.
- Review server responses producing 500/600 codes for error disclosure.

Detection & Monitoring

- In Splunk, add saved searches for admin path probes and SQLi signatures; schedule alerts with severity thresholds.
- Build dashboards tracking unique attacking IPs, top targeted endpoints, and response code distribution.
- Implement enrichment (GeoIP, ASN) for better triage context.

Hardening

- Ensure parameterized queries and input validation in all backend services.
- Hide default admin paths or use randomized/indirect administration endpoints.
- Keep frameworks and dependencies up to date to minimize known CVEs.

- What I Learned

Key takeaways from performing this task.

- Hands-on practice with Splunk search, field selection, and event inspection.
- Recognizing patterns of web reconnaissance versus active exploitation.
- Creating concise KPIs and a report-ready summary from raw logs.
- Formulating remediation steps and prioritizing actions by risk.

Conclusion

Final summary of findings and next steps.

The analysis confirms active probing of administrative endpoints and at least one SQL injection attempt. Controls appear to have blocked some access (403), but error responses and injection attempts indicate opportunities for further hardening. The recommended actions—WAF tuning, strict admin access, improved detection content, and application input validation—should be prioritized. Continuous monitoring in Splunk will help detect recurrence and measure control effectiveness.

Summary:

- Observed admin probes and SQLi attempt from multiple external IPs.
- Classified as Reconnaissance and Injection; severity Medium-High.
- Action plan: block abuse, WAF rules, harden app, strengthen Splunk detections.

Prepared by Shaheer Ali • August 11, 2025 • Future Interns

This report can be printed or saved as PDF via the browser.