SOC Lab Write Up. Splunk investigation of a Joomla admin brute force attempt

Overview

In this Blue Team Level 1 practice lab, I investigated suspicious HTTP POST activity targeting a Joomla administrator login endpoint. The goal was to confirm the behavior in logs, attribute the primary source, identify the internal target, extract request artifacts that prove brute force attempts, and build a simple timeline of the earliest password attempts for escalation and response.

SOC handoff summary

Classification: Suspicious authentication attack, web admin brute force attempt
Severity: Medium, escalate to High if any successful authentication is confirmed
Confidence: High
Target: Joomla administrator login endpoint
Primary attacker source IP: 23.22.63.114
Destination web server IP: 192.168.250.70
Event volume: 425 malicious POST events total, 412 tied to the primary attacker
Credential artifacts observed: username admin, example password baby, earliest password in sequence 12345678

Environment and data sources

Platform: Splunk Search and Reporting
Telemetry: Web request events containing form submission data for HTTP POST requests to the Joomla administrator login endpoint
Key fields used: timestamp, form_data, source IP, destination IP

Investigation workflow

1. Triage
   I started with a narrow detection focused on HTTP POST requests to the Joomla administrator login endpoint. The intent was to confirm this was an authentication attack pattern before expanding scope.

2. Scope and attribution
   I counted total matching events, then pivoted on source IP to identify the dominant origin. This isolated the primary attacker and reduced noise from minor background activity.

Evidence

Total malicious POST events to the Joomla admin endpoint: 425
Primary attacking source IP: 23.22.63.114
Events after filtering to the primary attacker IP: 412

3. Identify the targeted asset
   I pivoted on destination IP to confirm which internal web server was receiving the requests.

Evidence
Destination IP of the web server: 192.168.250.70

4. Validate attack content using request artifacts
   To prove the behavior was brute force and not normal traffic, I examined the form_data field from representative events to extract attempted credentials.

Evidence
Attempted username observed in form_data: admin
Example attempted password observed in form_data: baby

5. Build a timeline of earliest attempts
   I used a table view of timestamp and form_data, sorted oldest first, to identify the earliest password in the observed brute force sequence. This supports reporting, containment timing, and downstream hunting.

Evidence
Earliest brute force password after sorting by oldest timestamp: 12345678

Outcome and determination
Log evidence confirms a high volume brute force attempt against a Joomla administrator login endpoint, primarily from a single external source IP. The investigation produced actionable artifacts for escalation and response, including attacker attribution, internal target identification, and credential attempt evidence extracted directly from form submissions.

Recommended response actions, production safe guidance

Immediate actions
Block or rate limit 23.22.63.114 at the perimeter if business impact is acceptable
Confirm whether any authentication succeeded by reviewing Joomla authentication logs and web server logs for the same time window
Force password reset for any impacted admin accounts if success is confirmed

Hardening actions
Enable account lockout or throttling for repeated failed logins
Enforce strong admin passwords and add MFA for admin access where possible
Restrict administrator portal access by IP allow list, VPN, or internal only access if feasible
Review patch posture for Joomla and related components

Detection and hunting improvements

Alert on repeated POST requests to admin login endpoints with high failure rates from a single source

Track password spraying and brute force patterns by counting attempts per source IP and per destination host over short windows

Hunt across other web assets for the same source IP and similar form_data patterns

Skills demonstrated

Front line SIEM triage and rapid scoping in Splunk

Log pivoting and correlation using source and destination analysis

Evidence based validation using request artifacts in form_data

Timeline reconstruction to support escalation and incident response actions

Clear incident style reporting aligned to SOC workflows