# BTLO Lab Report: Middle Mayhem

## 1. Introduction

This report provides an analysis and summary of the 'Middle Mayhem' challenge from Blue Team Labs Online (BTLO). The objective of the lab was to simulate a real-world scenario where an attacker compromises a web application, exploits a known vulnerability, and then attempts lateral movement across the network. The investigation involves identifying various indicators of compromise (IOCs), vulnerabilities, and attacker techniques using SIEM logs.

## 2. Web Application Framework

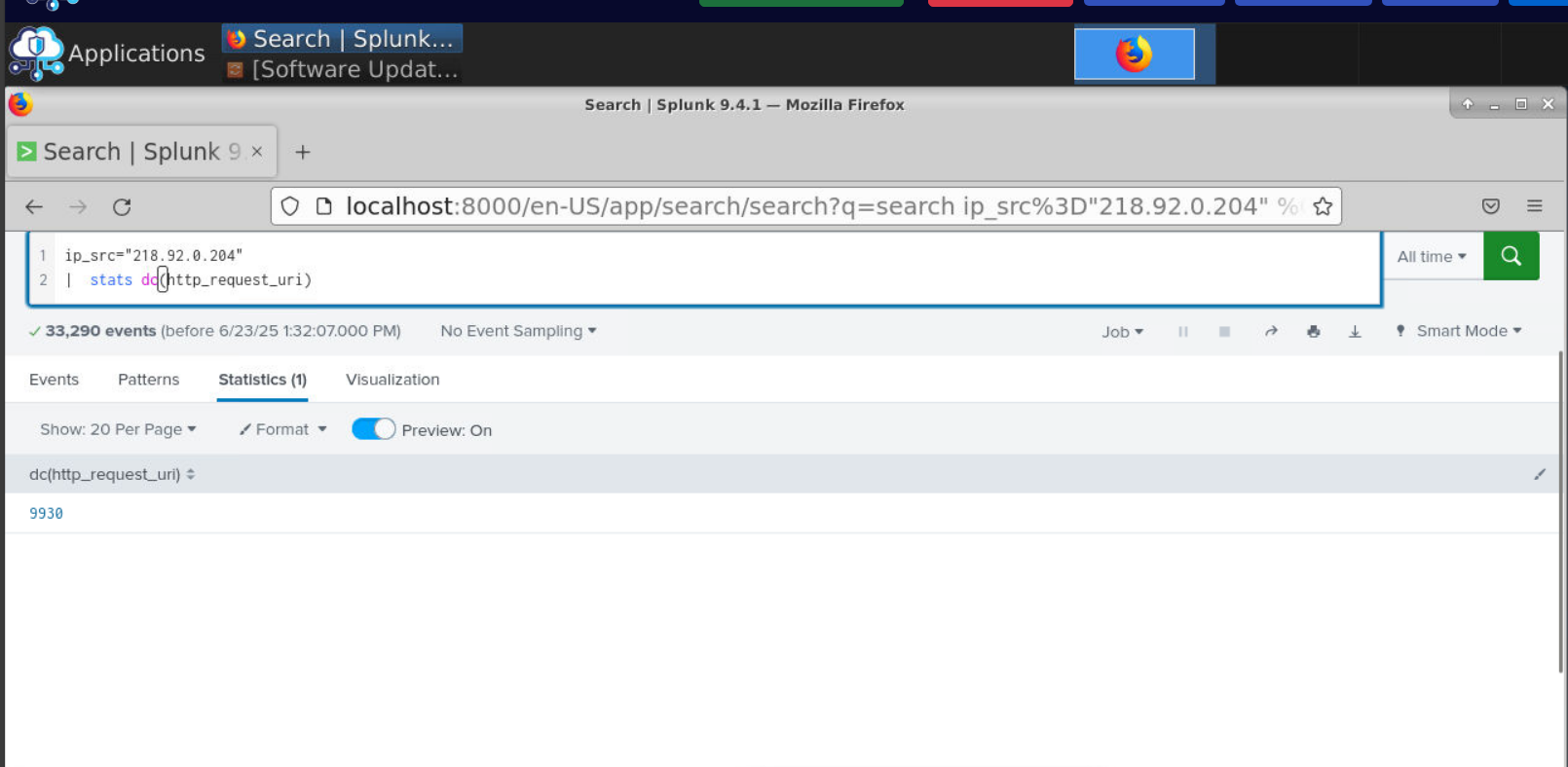
The frontend framework used by the compromised web application was identified as Next.js version 15.0.0.

## 3. Attacker Source IP

The attack originated from the IP address: 218.92.0.204.

## 4. Unique URIs Accessed

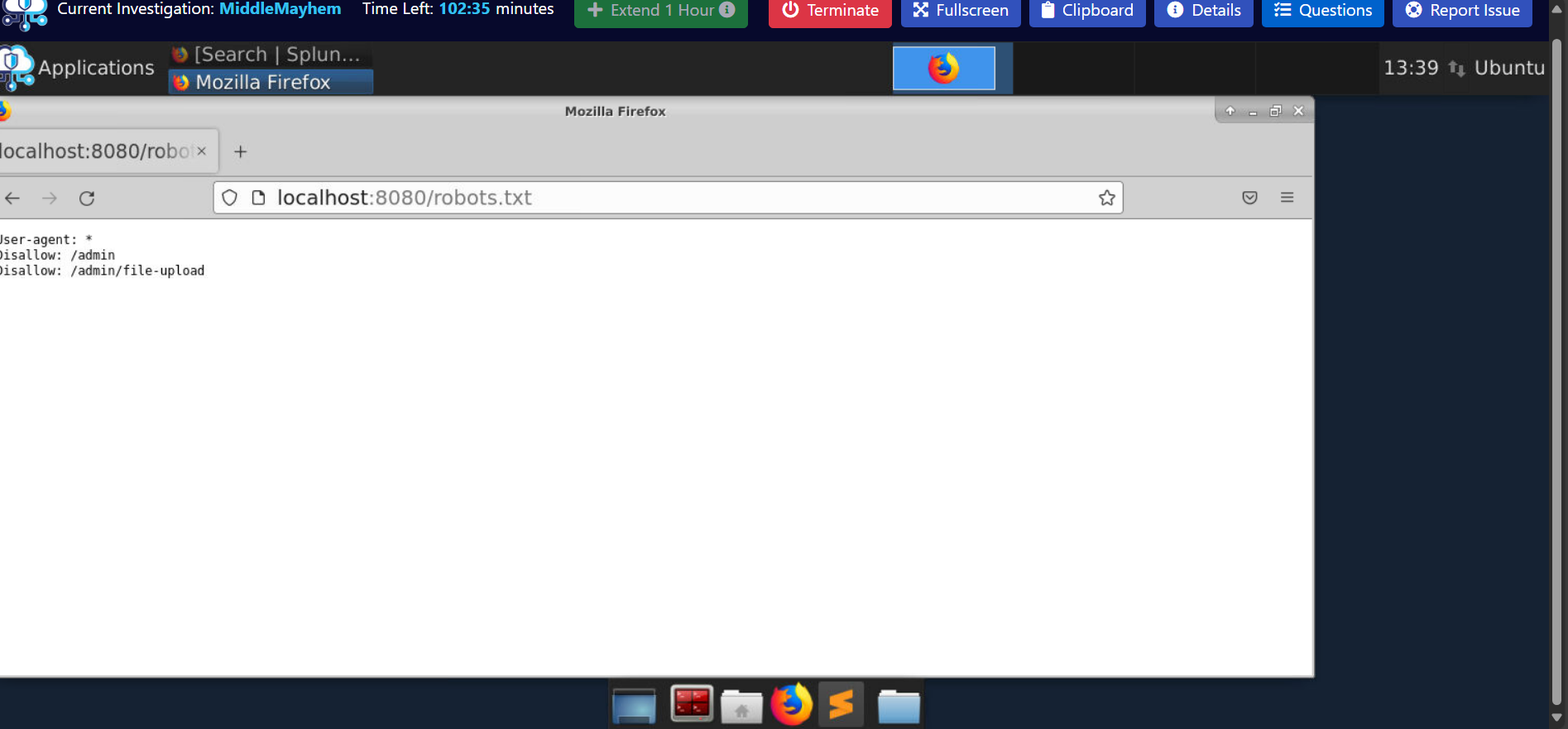
The attacker accessed a total of 9,930 unique URIs during the scan and exploitation phase.



## 5. Hidden/Internal Endpoints

Two hidden endpoints discovered from the application were:

* /admin
* /admin/file-upload

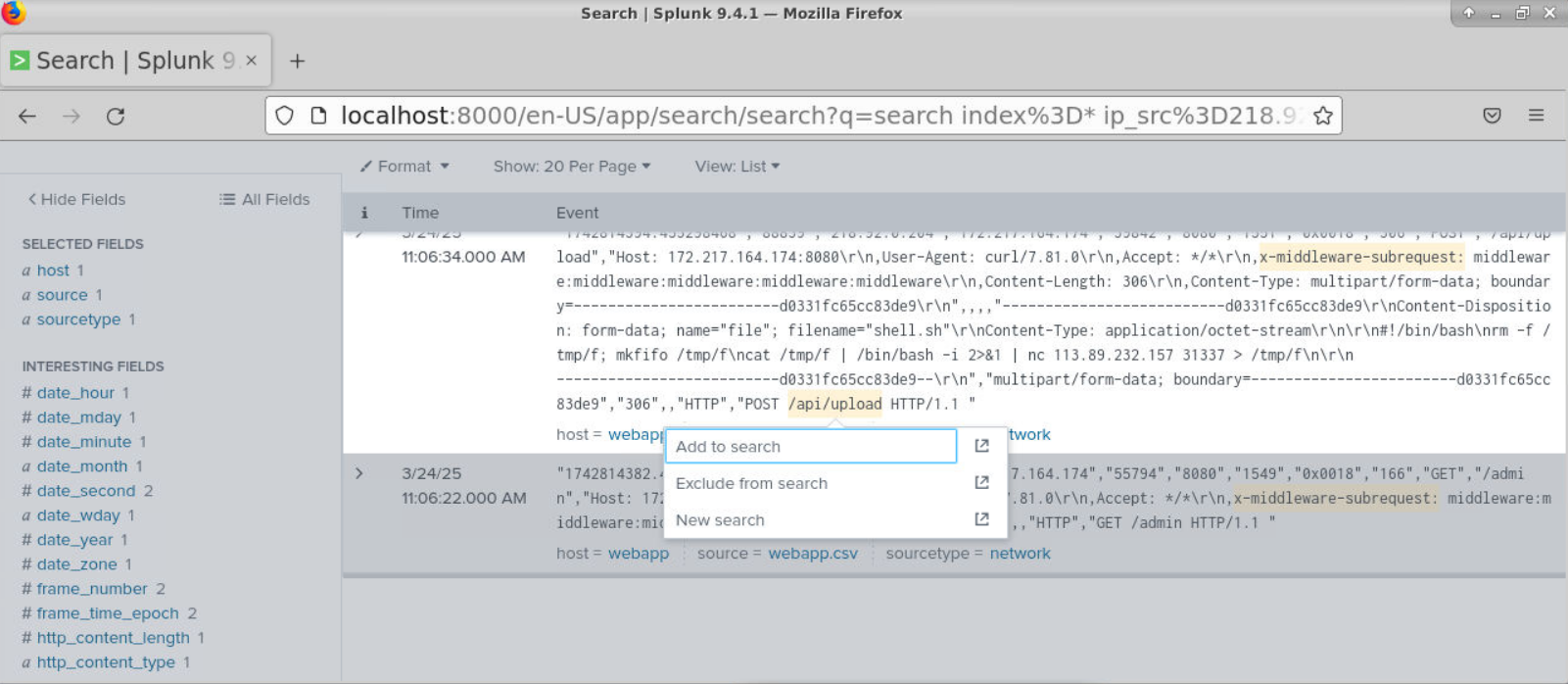


## 6. Vulnerability Exploited

The attacker exploited a vulnerability in Next.js identified as CVE-2025-29927, which allows bypassing authorization mechanisms.

## 7. Exploited HTTP Header

The HTTP header used by the attacker to exploit the application was: X-Middleware-Subrequest.

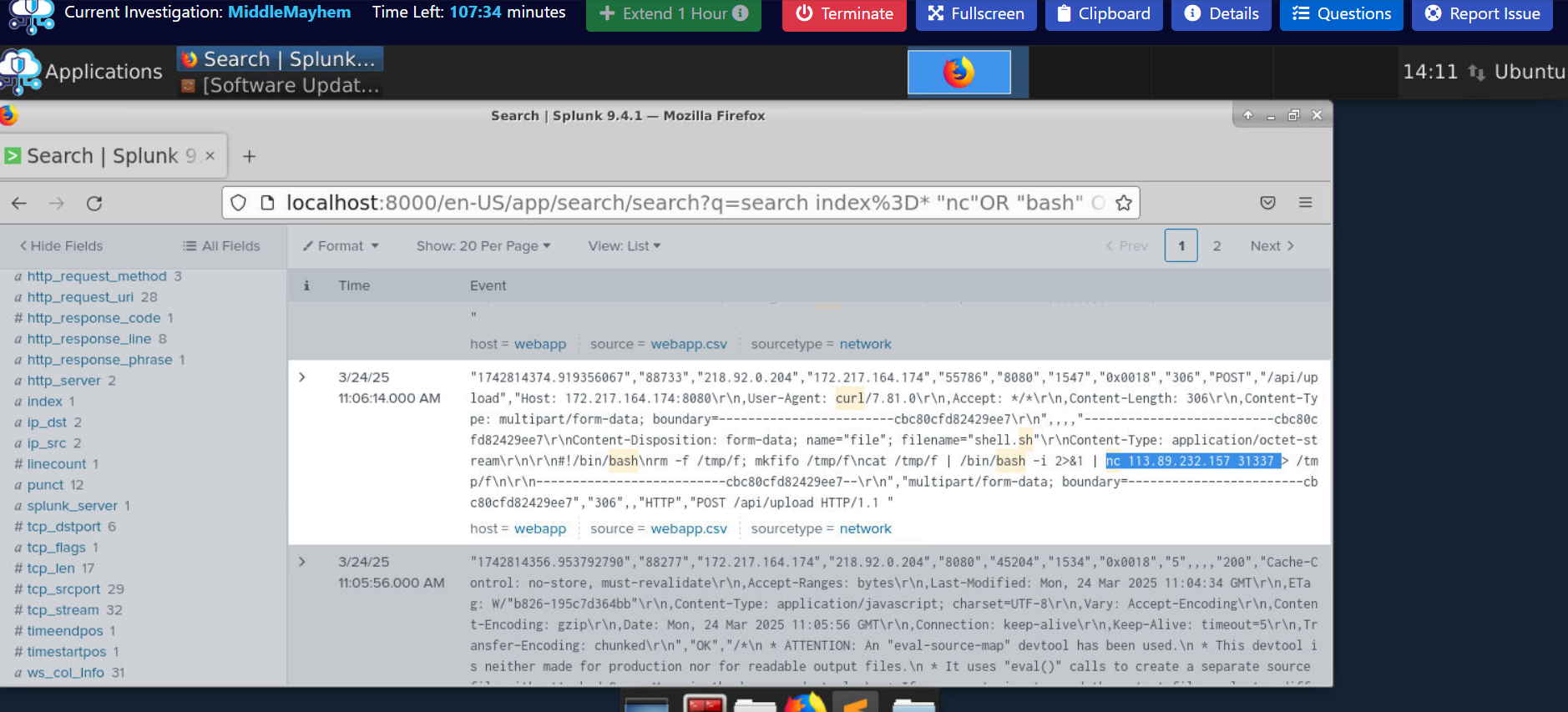


## 8. Endpoint Accessed Post-Exploitation

After the exploitation, the attacker accessed the endpoint: /api/upload. As shown in the previous image .

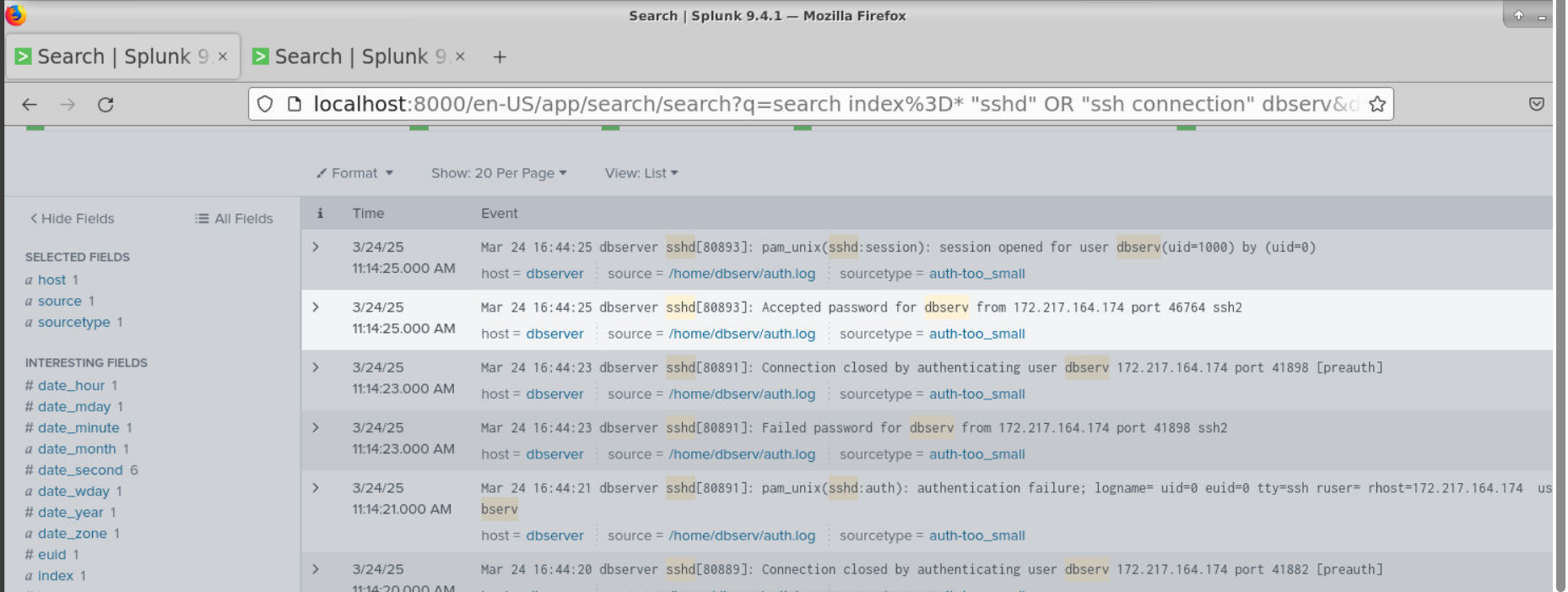
## 9. Reverse Shell Callback

The attacker established a reverse shell to the IP: 113.89.232.157 on port 31337.



## 10. Lateral Movement Technique

As seen in the SIEM logs, the attacker used SSH with a password-based login for lateral movement. The account used was 'dbserv', and the specific technique identified was: SSH Bruteforce.



## 11. Conclusion

The 'Middle Mayhem' lab demonstrates how a threat actor can exploit a web application vulnerability to gain access, escalate privileges, and move laterally across systems using brute force techniques. Identifying such attack patterns is critical for blue teamers to develop proactive detection and response mechanisms.