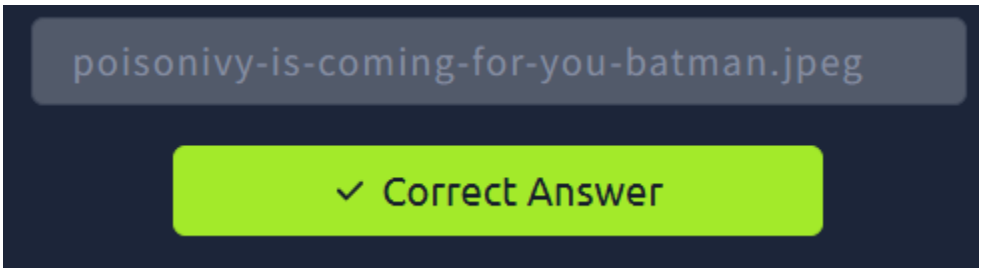
SPLUNK ACTION ON OBJECTIVES 2025/12/14

Action on Objective

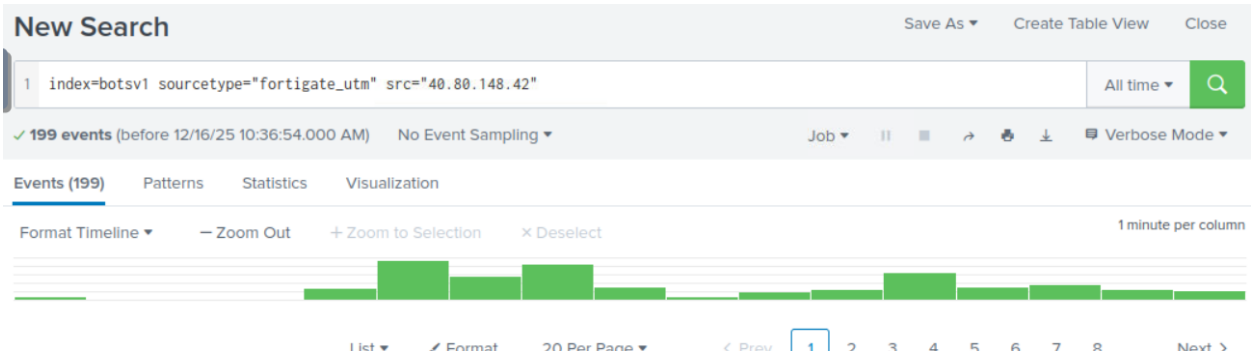
As the website was defaced due to a successful attack by the adversary, it would be helpful to understand better what ended up on the website that caused defacement.

As an analyst, our first quest could be to figure out the traffic flow that could lead us to the answer to this question. There can be a different approach to finding the answer to this question. We will start our investigation by examining the **Suricata** log source and the IP addresses communicating with the webserver 192.168.250.70.

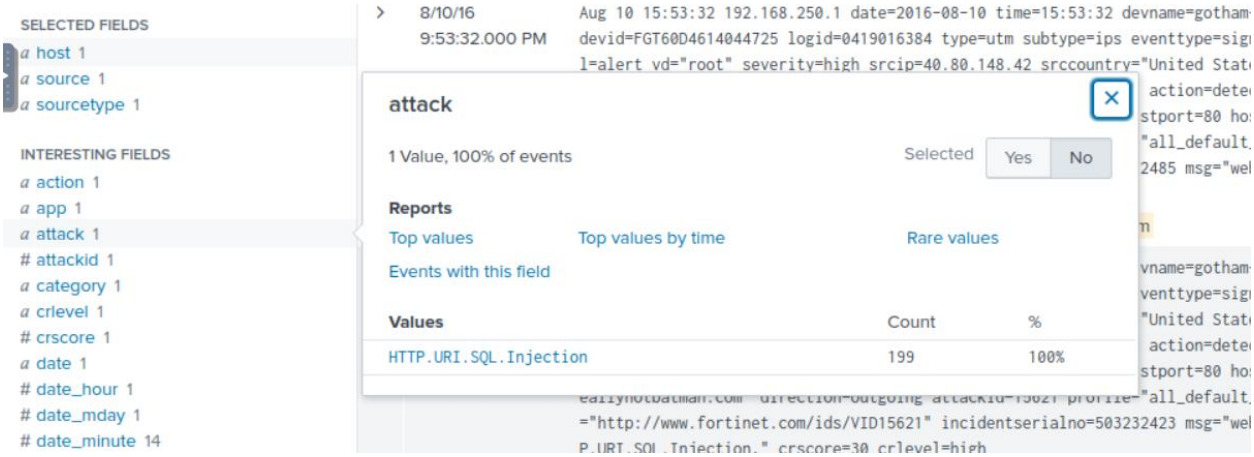
STEP 1: What is the name of the file that defaced the imreallynotbatman.com website?



Fortigate Firewall 'fortigate_utm' detected SQL attempt from the attacker's IP 40.80.148.42. What is the name of the rule that was triggered during the SQL Injection attempt?



I went back and changed the sourcetype in the fields and selected '**fortigate_utm'**. I scrolled down the fields again and clicked on src to select the ip – 40.80.148.42. I then clicked on the attack field.



Here is where I found the value – **HTTP.URI.SQL.Injection.**

Summary Conclusion

In this Action on Objectives phase, the investigation focused on identifying the activity that led to the successful website defacement. By analysing Suricata and FortiGate firewall logs in Splunk, the traffic targeting the web server 192.168.250.70 was reviewed. The attacker IP 40.80.148.42 was linked to malicious activity, with the FortiGate UTM detecting a SQL injection attempt. The triggered rule, HTTP.URI.SQL.Injection, confirmed that the attacker leveraged web-based exploitation techniques to achieve their objective, providing clear evidence of how the defacement was carried out.