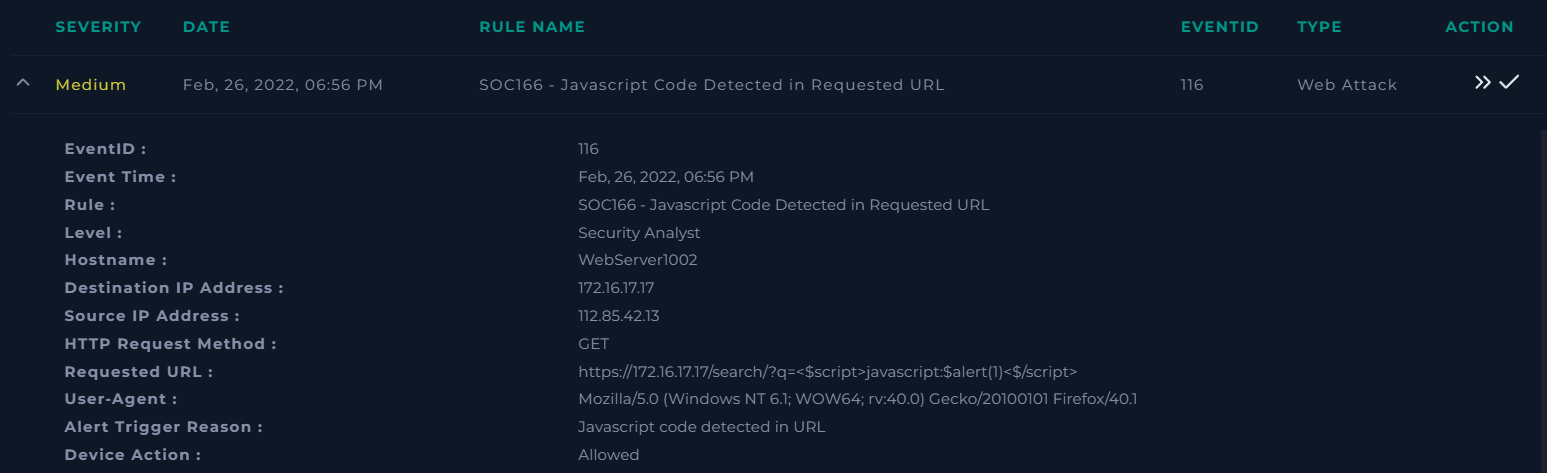
I will be investigating the Cross-site scripting alert “SOC166 - Javascript Code Detected in Requested URL” from letsdefend.

Cross-site scripting (XSS) is a type of attack which allows a threat actor to inject malicious code into a web application.



First it is important to gather important information from the alert itself.

When did the event occur?

Feb, 26, 2022, 06:56 PM

What was the threat’s IP?

112.85.42.13

What was the target?

One of our web servers (WebServer 1002), IP: 172.16.17.17

Who was the potential attacker?

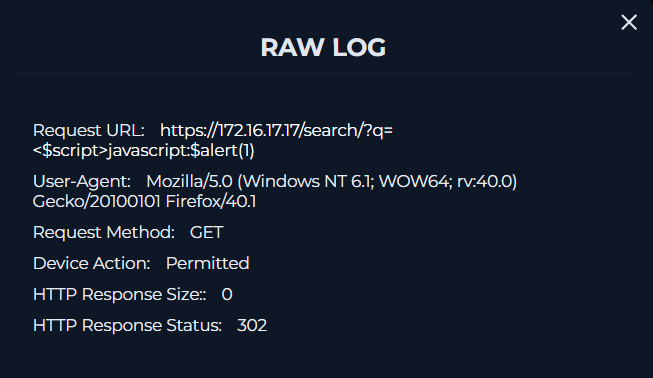
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1

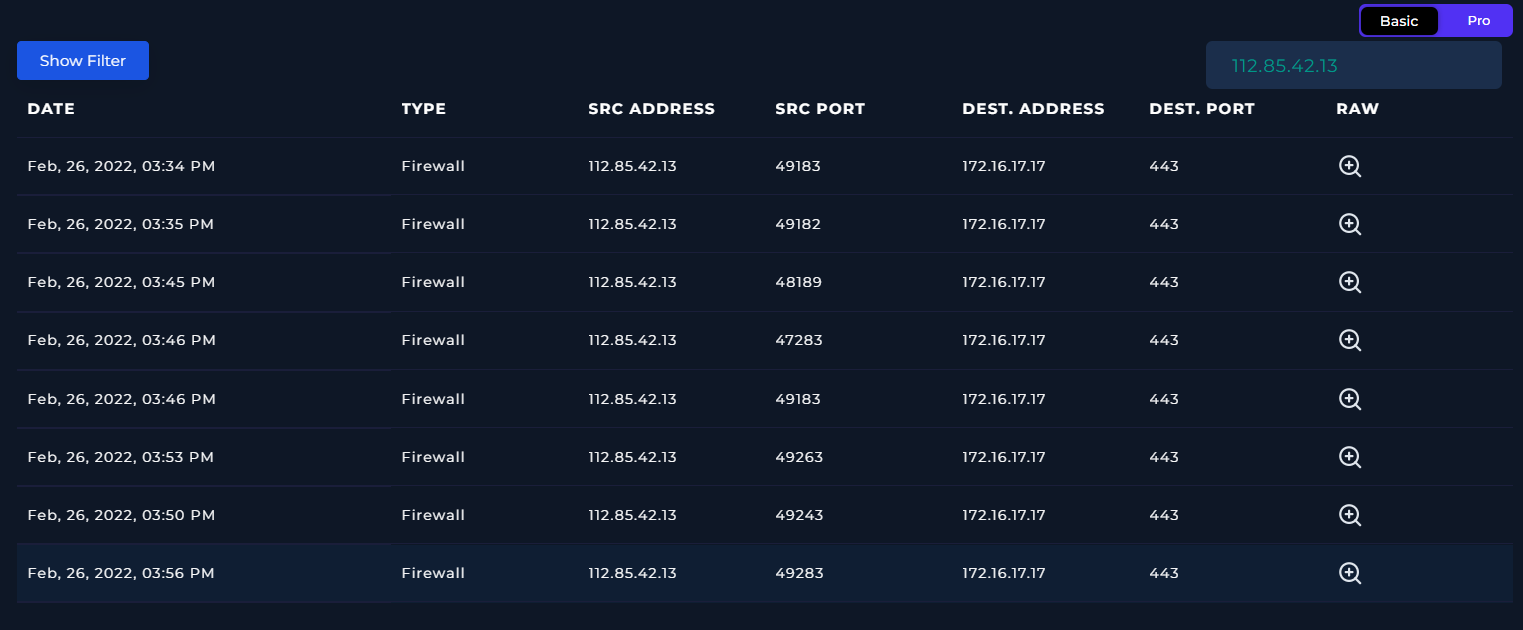
What URL was requested?  
https://172.16.17.17/search/?q=<$script>javascript:$alert(1)<$/script>

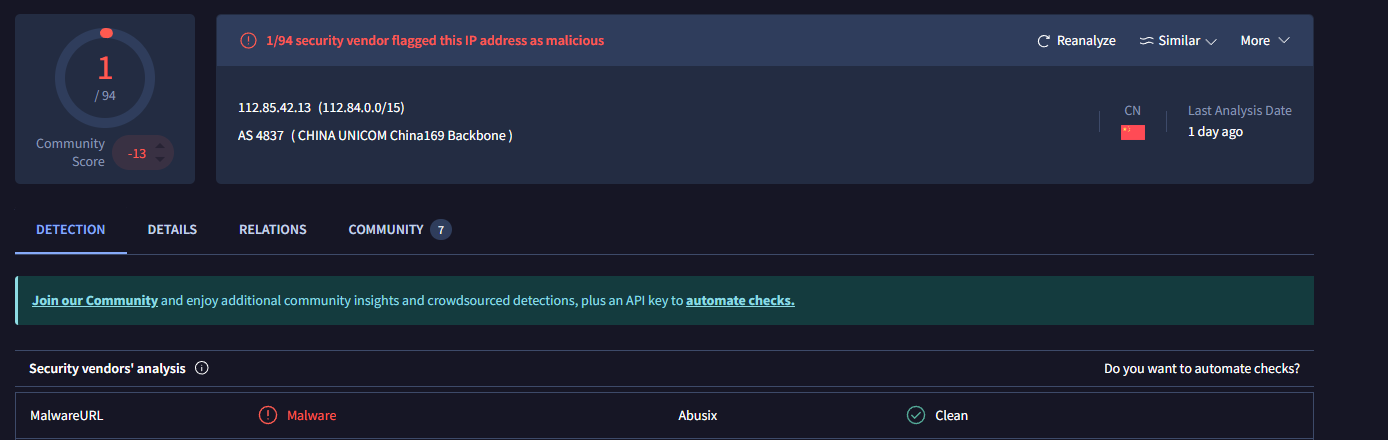
Why did the alert trigger?

A possible XSS attack, supported by <$script> within the url.

Next I searched the logs for a matching source IP. Strangely, in the logs the attack seems to happen three hours earlier than the report, though all other information matches and their is no alert for 6:56PM. From this I decided to investigate the matching 3:56PM alert.



The attacker 112.85.42.13 sent multiple requests to the web server. 

After searching the source address on our endpoint devices, I find it does not belong within our network. Analysing the source IP 112.85.42.13 in multiple engines found that it was potentially malicious. According to the WhoIs lookup the IP is from China with a DNS of “chinaunicom.cn”. 



When considering the Direction of traffic in this attack, It is from the internet (China) to the company network (WebServer1002).

The attack itself was unsuccessful, as the HTTP response size is 0 and the HTTP response status was 300 (Redirection message). As this was an unsuccessful attack, according to our policy it does not need tier 2 escalation.

Notable artifacts used in investigation:



Analysis note:

Potential cross-site scripting attack from China. According to logs, it was unsuccessful and was redirected. No need for tier two escalation.