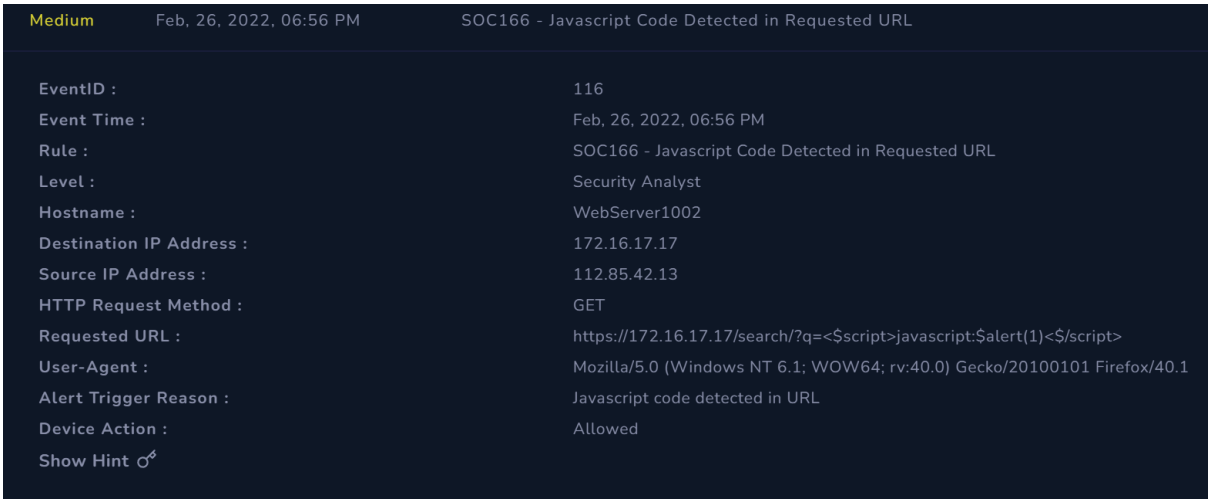
What is Cross Site Script (XSS) ?

- Cross site Scripting is a type of computer security vulnerability that enables an attacker to inject malicious code into a web page viewed by other users.
- This can allow the attacker to steal sensitive information such as
    - Login credentials (e.g username and password)
    - Personal information
    - Financial information
    - Session cookies
    - Website content

How to Detect XSS?

- Look for keywords such as “alert” and “script”.
- Also check presents of characters like greater than (>) or lesser than (<) are present.

Now look into alert



- The Source IP address (112.85.42.13) sending the request with javascript code to the Web Server 1002 (172.16.17.17)
- Requested URL : https://172.16.17.17/search/?q=<$script>javascript:$alert(1)<$/script>

We can start our investigation with Source IP address :

- We can clearly see that IP address (112.85.42.13) was Malicious

Now looking in to Log Management for what are the activity done by 112.85.42.13 so far,

DATE ↑	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Feb, 26, 2022, 06:34 PM	Firewall	112.85.42.13	49183	172.16.17.17	443	
Feb, 26, 2022, 06:35 PM	Firewall	112.85.42.13	49182	172.16.17.17	443	
Feb, 26, 2022, 06:45 PM	Firewall	112.85.42.13	48189	172.16.17.17	443	
Feb, 26, 2022, 06:46 PM	Firewall	112.85.42.13	49183	172.16.17.17	443	
Feb, 26, 2022, 06:46 PM	Firewall	112.85.42.13	47283	172.16.17.17	443	
Feb, 26, 2022, 06:50 PM	Firewall	112.85.42.13	49243	172.16.17.17	443	
Feb, 26, 2022, 06:53 PM	Firewall	112.85.42.13	49263	172.16.17.17	443	
Feb, 26, 2022, 06:56 PM	Firewall	112.85.42.13	49283	172.16.17.17	443	

- Attacker made several XSS attacks , but all of the attempts were redirected by the server with HTTP status 302.

Request URL: https://172.16.17.17/search/?q=<$img%20src%20=q%20onerror=prompt(8)$>

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

Request Method: GET

Device Action: Permitted

HTTP Response Size:: 0

HTTP Response Status: 302

- Here we can compare the 200 HTTP Response Status and 302 HTTP Response status which server responds to an attacker while making a non malicious and malicious request.
- From this response we can say the attack was unsuccessful.

Request URL: https://172.16.17.17/

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

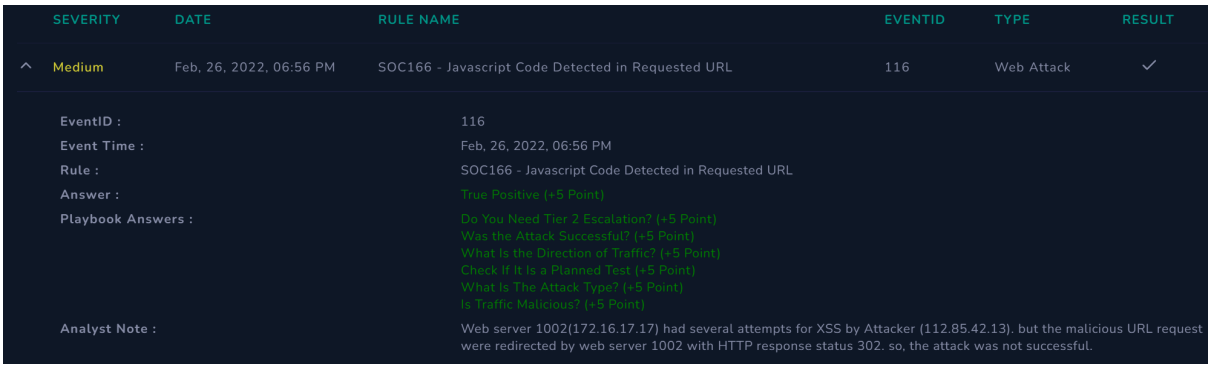
Request Method: GET

Device Action: Permitted

HTTP Response Size:: 1024

HTTP Response Status: 200

Playbook Answers:



SEVERITY	DATE	RULE NAME	EVENTID	TYPE	RESULT
Medium	Feb, 26, 2022, 06:56 PM	SOC166 - Javascript Code Detected in Requested URL	116	Web Attack	✓

EventID :	116
Event Time :	Feb, 26, 2022, 06:56 PM
Rule :	SOC166 - Javascript Code Detected in Requested URL
Answer :	True Positive (+5 Point)
Playbook Answers :	Do You Need Tier 2 Escalation? (+5 Point) Was the Attack Successful? (+5 Point) What Is the Direction of Traffic? (+5 Point) Check If It Is a Planned Test (+5 Point) What Is The Attack Type? (+5 Point) Is Traffic Malicious? (+5 Point)
Analyst Note :	Web server 1002(172.16.17.17) had several attempts for XSS by Attacker (112.85.42.13). but the malicious URL request were redirected by web server 1002 with HTTP response status 302. so, the attack was not successful.

- No need to Tier 2 Escalation
- The attack was not successful
- The direction of Traffic : internet to company network
- Not a Planned test (attack)
- Cross site scripting XSS attack.
- Yes, the traffic has Malicious code.