SOC166 - Javascript Code Detected in Requested URL

SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
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
Level :	Security Analyst
Hostname :	WebServer1002
Destination IP Address :	172.16.17.17
Source IP Address :	112.85.42.13
HTTP Request Method :	GET
Requested URL :	https://172.16.17.17/search/?q=<$script>javascript:$alert(1)<$/script>
User-Agent :	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1
Alert Trigger Reason :	Javascript code detected in URL
Device Action :	Allowed
Show Hint	

Click on >> and create case and click Continue.

Incident Details

Incident Name:	**EventID: 116 - [SOC166 - Javascript Code Detected in Requested URL]**
Description:	**EventID: 116**
Incident Type:	**Web Attack**
Created Date:	**Jan, 14, 2024, 12:27 PM**

Start Playbook!

Let's look at the info we have with us before we start the playbook. Since the attack type is WEB ATTACK with JavaScript code detected in URL, our priorities would be to look at the endpoint and the log management. One look at the requested URL, gives an indication of a possible XSS attack with the JavaScript code embedded in the URL.

https://172.16.17.17/search/?q=<$script>javascript:$alert(1)<$/script> ... Let's dig further

Lookup data results for IP Address

112.85.42.13

Search by IP, domain, or network owner for real-time threat data.

IP & Domain Reputation Overview | File Reputation Lookup | Email & Spam Data

LOCATION DATA

Shanghai, China

OWNER DETAILS

IP ADDRESS	112.85.42.13
FWD/REV DNS MATCH	No data
HOSTNAME	-
DOMAIN	-
NETWORK OWNER	china unicom jiangsu province network

REPUTATION DETAILS

SENDER IP REPUTATION	Poor	Submit Sender IP Reputation Ticket
WEB REPUTATION	Unknown	Submit Web Reputation Ticket

EMAIL VOLUME DATA

	LAST DAY	LAST MONTH
EMAIL VOLUME	0.0	0.0
VOLUME CHANGE	0%	
SPAM LEVEL	Critical	

Upon checking the Source address on Talos, the location is Shanghai, China with IP Reputation as POOR and Spam Level as CRITICAL.

The endpoint **WebServer1002** was checked and no related information could be found there. The last time the admin logged into the machine was over 20 days prior to the event date.

Checking the logs, we see there are quite a few listings with source IP as 112.85.42.13

Basic Pro

Show Filter

Search

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	47283	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, 06:53 PM	Firewall	112.85.42.13	49263	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, 06:56 PM	Firewall	112.85.42.13	49283	172.16.17.17	443	

After checking all the logs, it can be understood that the attacker was trying to perform reconnaissance on the server with the first three responses and the actual attack started at Feb, 26, 2022, 06:46 PM

Feb, 26, 2022, 06:46 PM	Firewall	112.85.42.13	47283	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, 06:53 PM	Firewall	112.85.42.13	49263	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, 06:56 PM	Firewall	112.85.42.13	49283	172.16.17.17	443	

Post URL decoding, the prompts are as follows:

https://172.16.17.17/search/?q=prompt(8)

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

https://172.16.17.17/search/?q=<$svg><$script ?>$alert(1)

https://172.16.17.17/search/?q=<$script>$for((i)in(self))eval(i)(1)<$/script>

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

For all the prompts, the HTTP Response Size was 0 & HTTP Response Status: 302, which meant that server was able to actively avoid the injection of the code and redirect the attacker elsewhere. Hence, the attack was not successful.

Let’s start the Playbook!

Understand Why the Alert Was Triggered

In order to perform a better analysis and to determine whether the triggered alert is false positive, it is first necessary to understand why the rule was triggered. Instead of starting the analysis directly, first understand why this rule was triggered.

- Examine the rule name. Rule names are usually created specifically for the attack to be detected. By examining the rule name, you can understand which attack you are facing.
- Detect between which two devices the traffic is occurring. It's a good starting point to understand the situation by learning about the direction of traffic, what protocol is used between devices, etc.

Next

Collect Data

Gather some information that can be gathered quickly to get a better understanding of the traffic. These can be summarized as follows.

- Ownership of the IP addresses and devices.
- If the traffic is coming from outside (Internet);
  - Ownership of IP address (Static or Pool Address? Who owns it? Is it web hosting?)
  - Reputation of IP Address (Search in VirusTotal, AbuseIPDB, Cisco Talos)

- If the traffic is coming from company network;
  - Hostname of the device
  - Who owns the device (username)
  - Last user logon time

Next

Ownership of the IP addresses and devices.: china unicom jiangsu province network

If the traffic is coming from outside (Internet); Yes

Ownership of IP address (Static or Pool Address? Who owns it? Is it web hosting?): 112.85.42.13(112.84.0.0/15). Pool address

Reputation of IP Address (Search in VirusTotal, AbuseIPDB, Cisco Talos): Poor

If the traffic is coming from company network; No

Hostname of the device: WebServer1002

Who owns the device (username): webadmin15

Last user logon time: Feb, 02, 2022, 03:40 PM

Examine HTTP Traffic

Check the traffic content for any suspicious conditions such as web attack payloads (SQL Injection, XSS, Command Injection, IDOR, RFI/LFI).

Examine all the fields in the HTTP Request. Since the attackers do not only attack through the URL, all the data from the source must be examined to understand whether there is really a cyber attack.

You can review the Web Attacks 101 tutorial for information about attacks on web applications and how to detect these attacks.

- Web Attacks 101

Next

Already examined.

Is Traffic Malicious?

Decide whether the traffic is malicious or not based on your investigations.

You can find our related training below.

- Web Attacks 101

Malicious | Non-malicious

Selecting **Malicious** as the prompts in the log management direct towards an intended XSS attack.

What Is The Attack Type?

Which of the following is the attack vector in the malicious traffic you have detected as a result of your investigations?

Command Injection | IDOR | LFI & RFI | Other | SQL Injection | XML Injection | XSS

Selecting **XSS** here.

Check If It Is a Planned Test

Penetration tests or attack simulation products can trigger False Positive alarms if the rules are not set correctly. Check whether the malicious traffic is the result of a planned test.

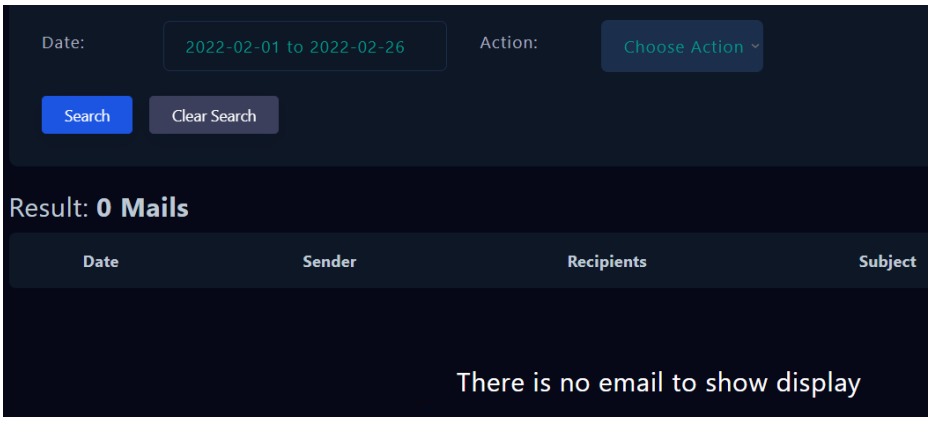
- Check if there is an email showing that there will be planned work by searching for information such as hostname, username, IP address on the mailbox.
- Check if the device generating malicious traffic belongs to attack simulation products. If the Hostname contains the name of Attack Simulation products (such as Verodin, AttackIQ, Picus...), these devices belong to Attack Simulation products within the framework of LetsDefend simulation and it is a planned work.

Is the malicious traffic caused by a planned test?

Not Planned | Planned

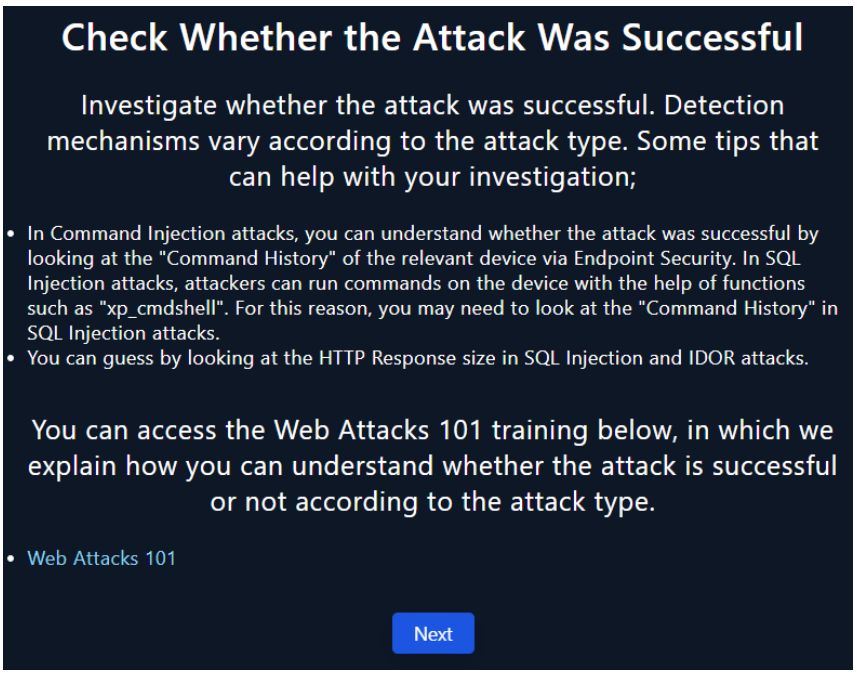
Checking in Email Security and filtering by date to check if any emails arrived indicating a planned test.

After filtering with date range Feb, 01, 2022 – Feb, 26, 2022, there are no emails listed.



So, this was not a planned test. Selecting **NOT PLANNED** here.

Selecting **Internet → Company Network** here.



Based on the HTTP Response Code, we have already determined that the attack was not successful.

Was the Attack Successful?

Select “Yes” if you found that the attack was successful as a result of your investigations, and “No” if you found that the attack was unsuccessful.

No Yes

Selecting **NO** here.

Add Artifacts

+

Value	Comment	Type	Remove
112.85.42.13	Malicious IP	IP Address	

Next

Adding the only artifact of the attack.

Do You Need Tier 2 Escalation?

Tier 2 escalation should be performed in the following situations.

- In cases where the attack succeeds,
- When the attacker compromises a device in the internal network (in cases where the direction of harmful traffic is from inside → inside),

Tier 2 escalation is not required in the following cases.

- In cases where attacks from the Internet do not succeed

** Institutions may have their own escalation procedure. Don't forget to learn about the escalation procedure in your institution.

Perform Tier 2 escalation?

No Yes

Selecting NO here since the attack was not successful, there is no need to escalate the issue.

Analyst Note

Please enter your analysis comments.

An XSS attack was attempted from 112.85.42.13 on WebServer1002 (172.16.17.17) on Feb, 26, 2022. The requests sent to the server were rejected with HTTP Response code 302 and the attack was averted.
The CIDR 112.84.0.0/15 should be added to the firewall logs.

259 / 3000

Next

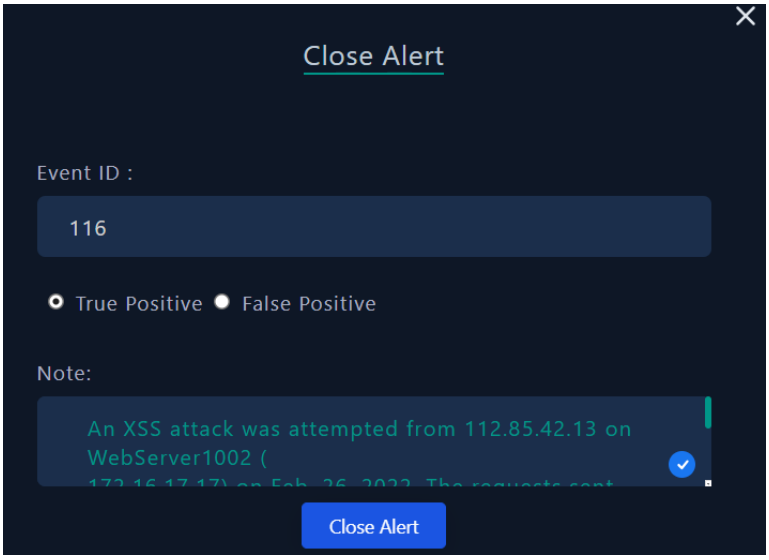
Add your finding as comments,

An XSS attack was attempted from 112.85.42.13 on WebServer1002 (

172.16.17.17) on Feb, 26, 2022. The requests sent to the server were rejected with HTTP Response code 302 and the attack was averted.

The CIDR 112.84.0.0/15 should be added to the firewall logs.

.. And click and confirm on FINISH PLAYBOOK and close the Alert.



Selecting as **True Positive** since there indeed was JavaScript code in the URL

Let's check the scores now.

SEVERITY	DATE CLOSED	RULE NAME	EVENTID	TYPE	RESULT
Medium	Jan, 14, 2024, 09:04 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 :	An XSS attack was attempted from 112.85.42.13 on WebServer1002 (172.16.17.17) on Feb, 26, 2022. The requests sent to the server were rejected with HTTP Response code 302 and the attack was averted. The CIDR 112.84.0.0/15 should be added to the firewall logs.

Hope this helped.