Module 09: Investigating Web Attacks

Lab Scenario

Forensic investigators need to investigate web attacks on a web server to identify the type of web attack and its severity. As a part of this investigation, investigators must analyze the web server's log files, IDS, and SIEM tools which contains the IP address, browser, and system information of the attacker. An example of a severe, large-scale web attack would be a scenario where the website of a renowned banking organization is brought down by attackers and the entire data on it, including account holders' details, employers' and employees' details, etc., is leaked online on the dark web. To investigate this web attack, investigators would need to analyze the IDS logs, web server logs, and SIEM alerts. By analyzing these details, they can determine the types of web attacks that have been attempted by the attackers. These may include cross-site scripting, SQL injection, brute-force, and various other attacks.

As an expert forensic investigator, you should know how to investigate web-related attacks.

Lab Objectives

The objective of this lab is to help the students understand how to investigate various types of web attacks, including:

- Detection and analysis of an XSS attack by examining Apache logs

Overview of Investigating Web Attacks

Web attacks are of different types. A denial-of-service (DoS) attack can be cited as an example of a web attack. In DoS attacks, visitors to a website are denied access to any information or services available on the website. In such cases, visitors may report the unavailability of online services which they were trying to access. Attackers can also use other techniques, such as SQL injection, command injection, brute-force attacks etc., to exploit any vulnerable website.

An indication of a web attack can be the redirection of a user to an unknown website. Unusually slow network performance and frequent server reboots may also indicate a web attack. In case a web attack is suspected, investigators need to examine the log data from various sources to understand where the attack originated and mitigate it at the earliest.

Lab Tasks

Recommended lab to assist you in investigating web attacks:

- Identifying and investigating web application attacks using Splunk

Lab 1: Identifying and Investigating Web Application Attacks Using Splunk

Lab Scenario

An e-commerce company has suffered a cyber-attack on its web application that lists and sells various goods/products. The attackers not only took down the website but also stole personally identifiable information of its users/customers. The company sought the services of the cyber-forensics wing of the state law enforcement department to crack the case, retrieve customer-specific stolen information, secure its systems and all customer-related information, and thus help restore the customers' faith in their business.

To investigate the case and determine the types of web attacks that have been carried out by the attackers on the company's web application, Robert, the forensic investigator, now needs to examine and analyze log files from the Apache server, IIS server, and ModSecurity web application firewall using SIEM tool.

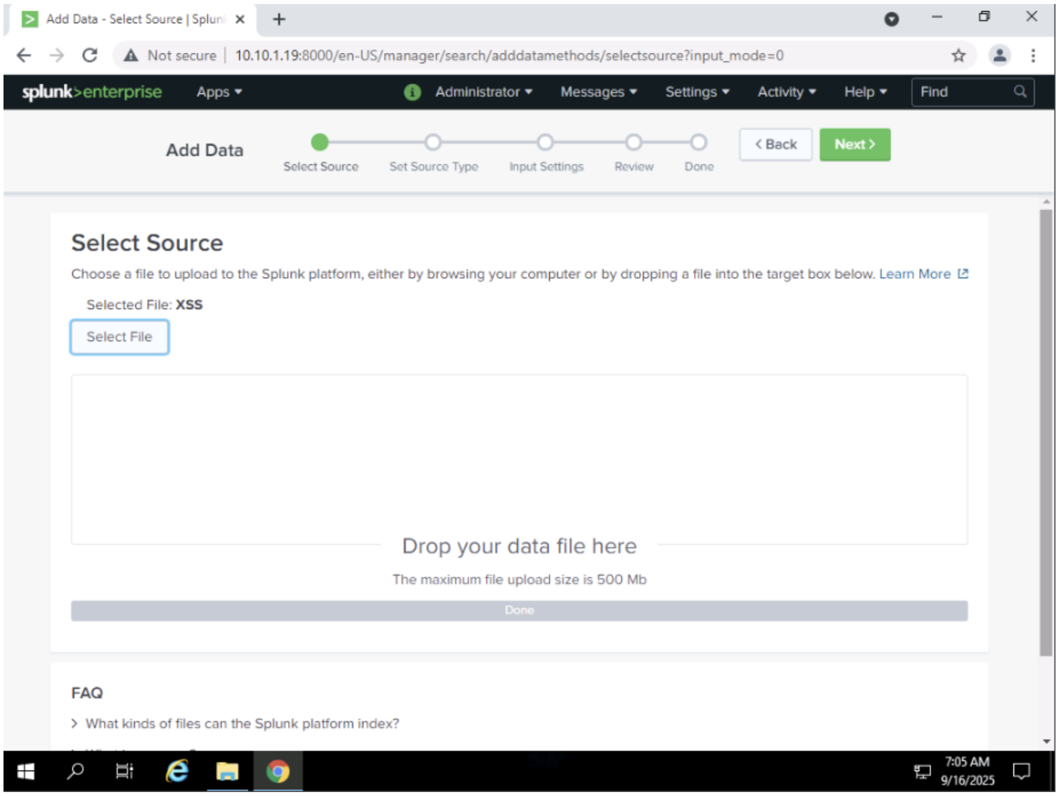
Lab Objectives

Log files record events and activities that take place in an operating system or during the runtime of a computer software or service. Forensic examination of these log files help investigator identify malicious activities that take place on the web server.

The objective of this lab is to help you understand how to examine log files and look for artifacts pertaining to web application attacks with SIEM tool.

Overview of the Lab

This lab familiarizes you with the process of examining log files generated by servers and web application firewalls to check for indicators of web attacks using SIEM tools like **Splunk Enterprise**.



10.10.1.19:8000/en-US/manager/search/adddatamethods/selectsource?input_mode=0

Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. Learn More

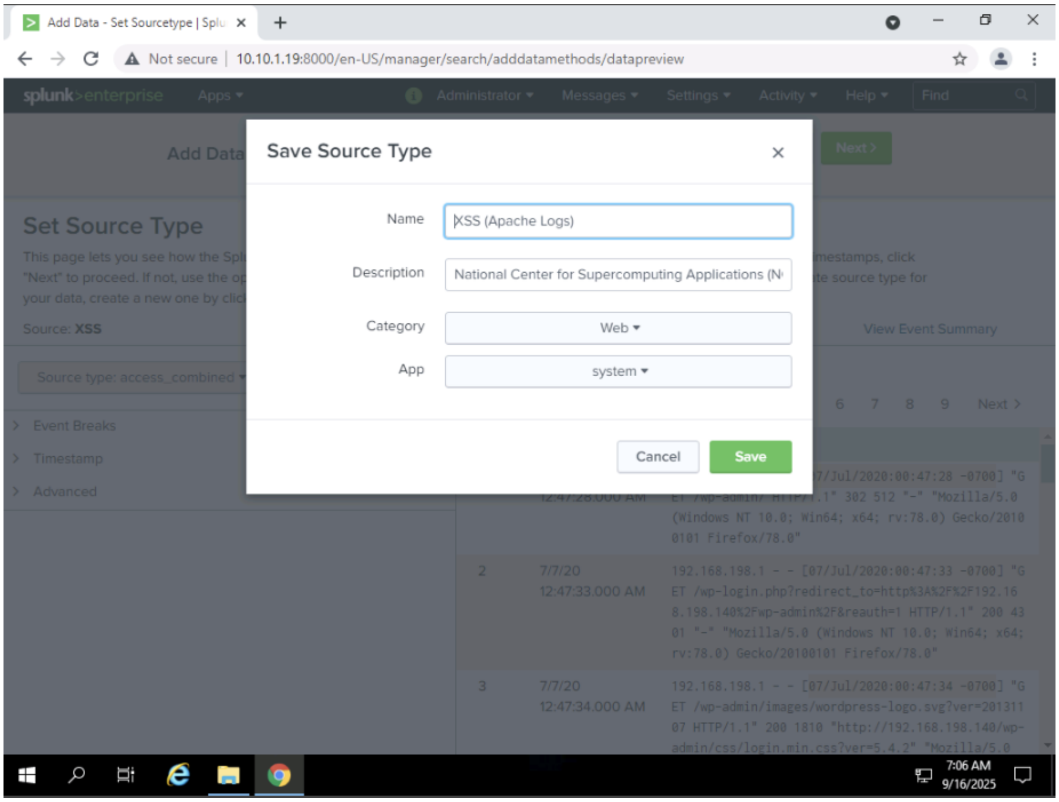
Selected File: **XSS**

Drop your data file here

The maximum file upload size is 500 Mb

FAQ

› What kinds of files can the Splunk platform index?



10.10.1.19:8000/en-US/manager/search/adddatamethods/datapreview

Set Source Type

This page lets you see how the Spl... timestamps, click "Next" to proceed. If not, use the op... te source type for your data, create a new one by clic...

Source: XSS

Source type: access_combined

Save Source Type

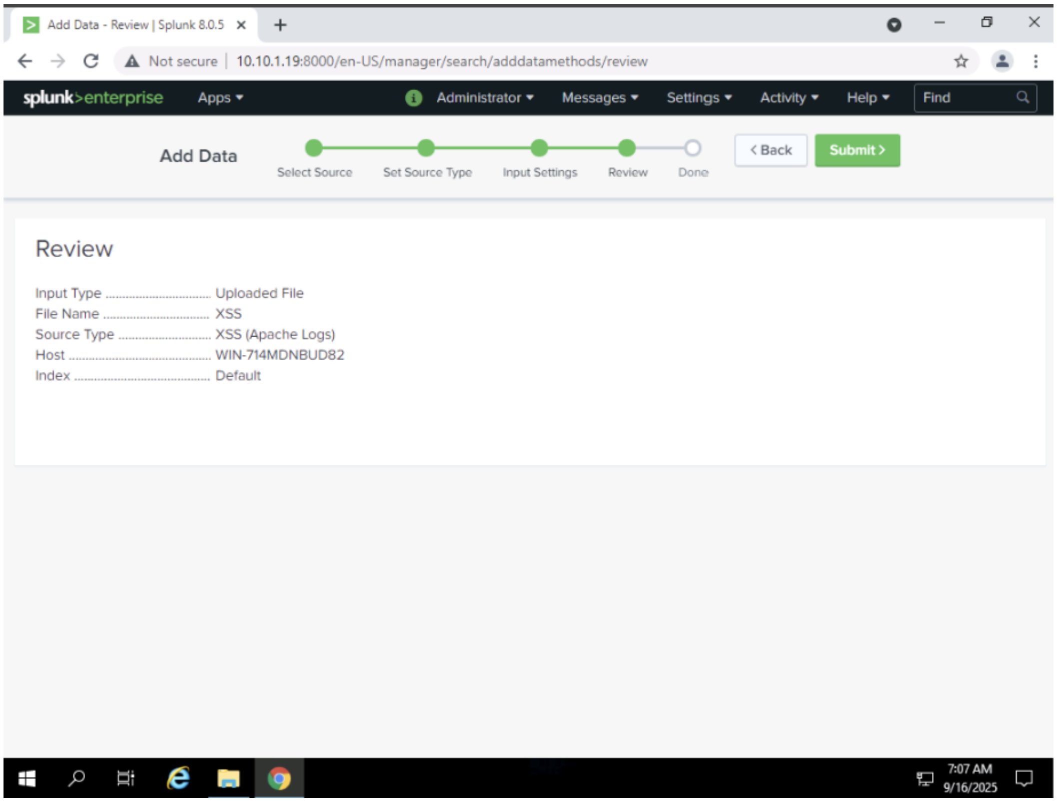
Name: XSS (Apache Logs)

Description: National Center for Supercomputing Applications (N

Category: Web

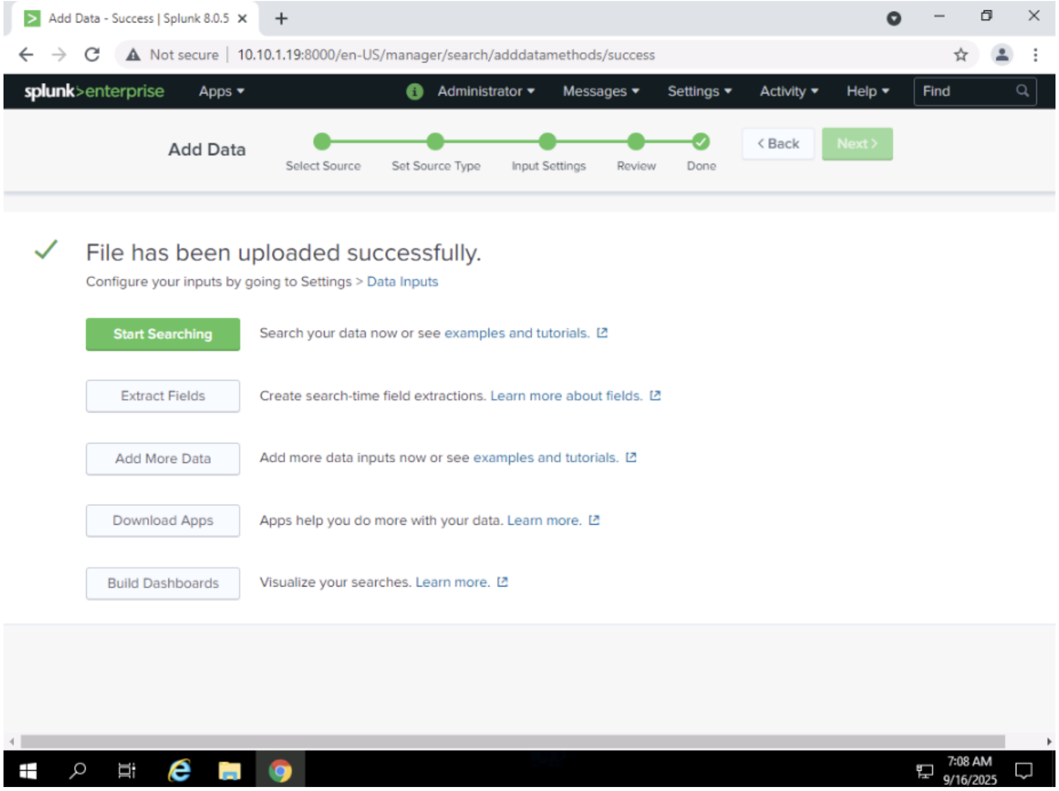
App: system

```
            ...7/Jul/2020:00:47:28 -0700] "G
12:47:28.000 AM  ET /wp-admin/ HTTP/1.1" 302 512 "-" "Mozilla/5.0
                 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/2010
                 0101 Firefox/78.0"
2   7/7/20       192.168.198.1 - - [07/Jul/2020:00:47:33 -0700] "G
    12:47:33.000 AM  ET /wp-login.php?redirect_to=http%3A%2F%2F192.16
                 8.198.140%2Fwp-admin%2F&reauth=1 HTTP/1.1" 200 43
                 01 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64;
                 rv:78.0) Gecko/20100101 Firefox/78.0"
3   7/7/20       192.168.198.1 - - [07/Jul/2020:00:47:34 -0700] "G
    12:47:34.000 AM  ET /wp-admin/images/wordpress-logo.svg?ver=201311
                 07 HTTP/1.1" 200 1810 "http://192.168.198.140/wp-
                 admin/css/login.min.css?ver=5.4.2" "Mozilla/5.0
```



Review

Input Type .... Uploaded File
File Name .... XSS
Source Type .... XSS (Apache Logs)
Host WIN-714MDNBUD82
Index .... Default



✓ File has been uploaded successfully.

Configure your inputs by going to Settings > Data Inputs

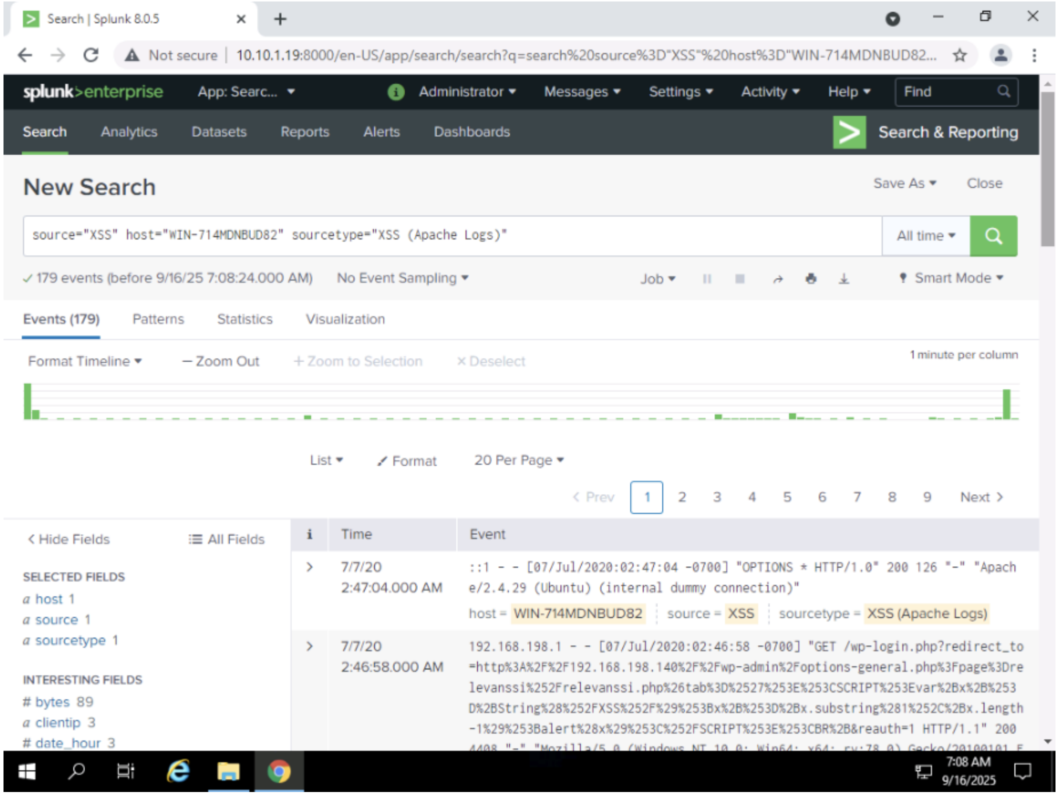
Start Searching — Search your data now or see examples and tutorials.

Extract Fields — Create search-time field extractions. Learn more about fields.

Add More Data — Add more data inputs now or see examples and tutorials.

Download Apps — Apps help you do more with your data. Learn more.

Build Dashboards — Visualize your searches. Learn more.



```
source="XSS" host="WIN-714MDNBUD82" sourcetype="XSS (Apache Logs)"
```

✓ 179 events (before 9/16/25 7:08:24.000 AM) No Event Sampling

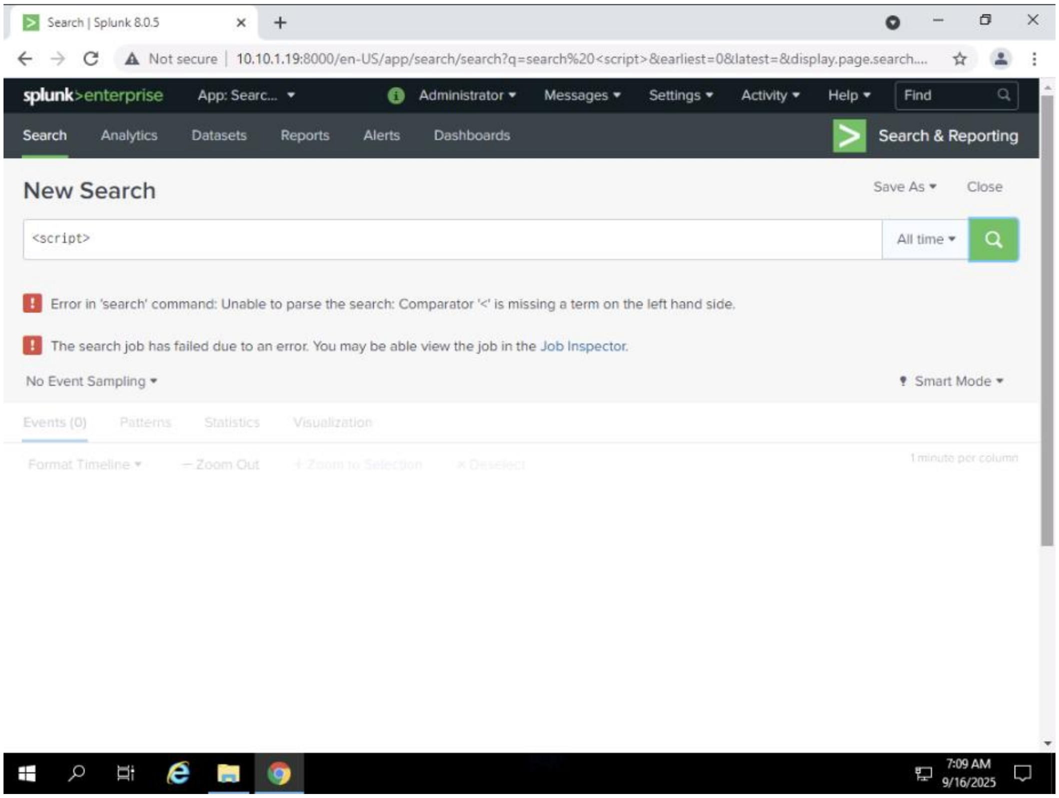
SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- # bytes 89
- a clientip 3
- # date_hour 3

i	Time	Event

>	7/7/20
	2:47:04.000 AM
		`::1 - - [07/Jul/2020:02:47:04 -0700] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.29 (Ubuntu) (internal dummy connection)"`
		host = WIN-714MDNBUD82 source = XSS sourcetype = XSS (Apache Logs)

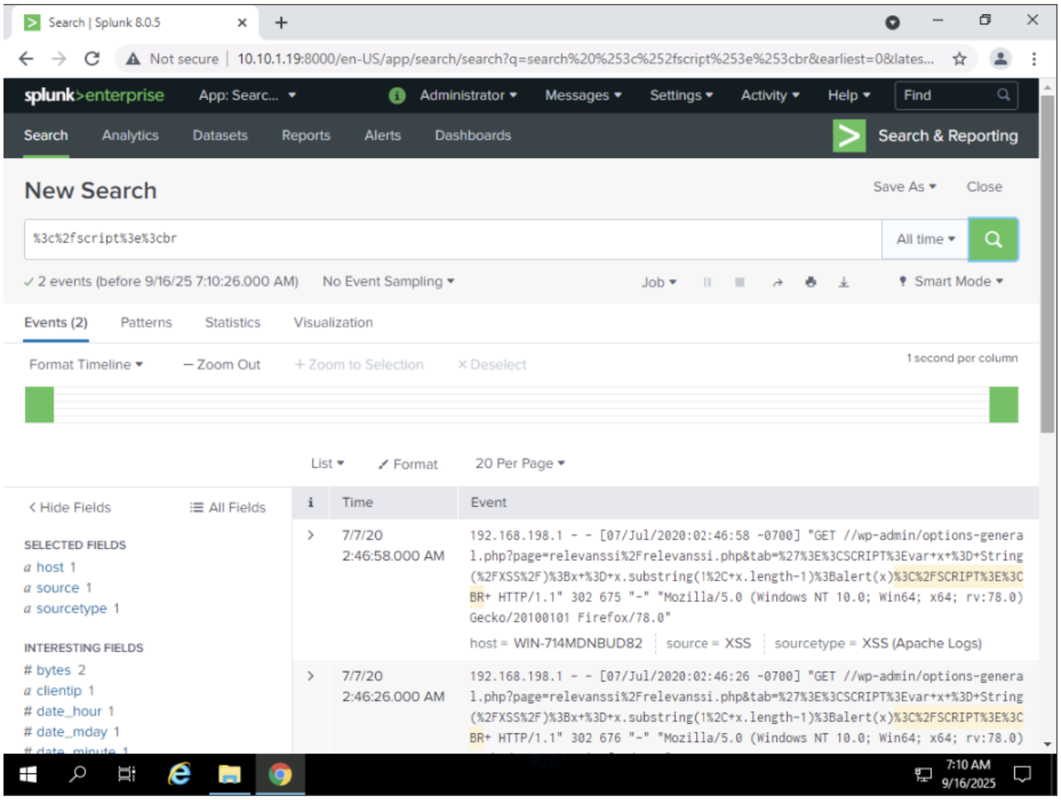
>	7/7/20 2:46:58.000 AM	`192.168.198.1 - - [07/Jul/2020:02:46:58 -0700] "GET /wp-login.php?redirect_to=http%3A%2F%2F192.168.198.140%2F%2Fwp-admin%2Foptions-general.php%3Fpage%3Drelevanssi%252Frelevanssi.php%26tab%3D%2527%253E%253CSCRIPT%253Evar%2Bx%2B%253D%2BString%28%252FXSS%252F%29%253Bx%2B%253D%2Bx.substring%281%252C%2Bx.length-1%29%253Balert%28x%29%253C%252FSCRIPT%253E%253CBR%2B&reauth=1 HTTP/1.1" 200 4408 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 F`



```
<script>
```

! Error in 'search' command: Unable to parse the search: Comparator '<' is missing a term on the left hand side.

! The search job has failed due to an error. You may be able view the job in the Job Inspector.



New Search

```
%3c%2fscript%3e%3cbr
```

✓ 2 events (before 9/16/25 7:10:26.000 AM)   No Event Sampling

i	Time	Event

>	7/7/20
	2:46:58.000 AM
		192.168.198.1 - - [07/Jul/2020:02:46:58 -0700] "GET //wp-admin/options-general.php?page=relevanssi%2Frelevanssi.php&tab=%27%3E%3CSCRIPT%3Evar+x+%3D+String(%2FXSS%2F)%3Bx+%3D+x.substring(1%2C+x.length-1)%3Balert(x)%3C%2FSCRIPT%3E%3CBR+ HTTP/1.1" 302 675 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0"
		host = WIN-714MDNBUD82 source = XSS sourcetype = XSS (Apache Logs)

>	7/7/20 2:46:26.000 AM	192.168.198.1 - - [07/Jul/2020:02:46:26 -0700] "GET //wp-admin/options-general.php?page=relevanssi%2Frelevanssi.php&tab=%27%3E%3CSCRIPT%3Evar+x+%3D+String(%2FXSS%2F)%3Bx+%3D+x.substring(1%2C+x.length-1)%3Balert(x)%3C%2FSCRIPT%3E%3CBR+ HTTP/1.1" 302 676 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0)

Module 09: Web Application Attacks – Lab 1 Summary

This lab focused on analyzing web server log files to detect and investigate web application attacks, particularly XSS attacks. Using Splunk Enterprise, the objectives were to upload Apache log files, apply plain-text and encoded filters, and examine events for evidence of malicious activity. The lab emphasized decoding encoded scripts, interpreting log data, and identifying critical indicators such as attacker IP, targeted webpage, and HTTP status codes. Through this process, the lab reinforced skills in log analysis, web attack detection, and practical use of SIEM tools for forensic investigation.