UNIVERSITY OF SCIENCE AND TECHNOLOGY OF HANOI

Information and Communication Technology Department

Investigating Web Attacks

Module 09 - Digital Forensic

Name - ID: **Đào Ngọc Tùng** **BA12-185**

Trần Đức Trung **BA12-179**

Phạm Phú Hưng **BA12-081**

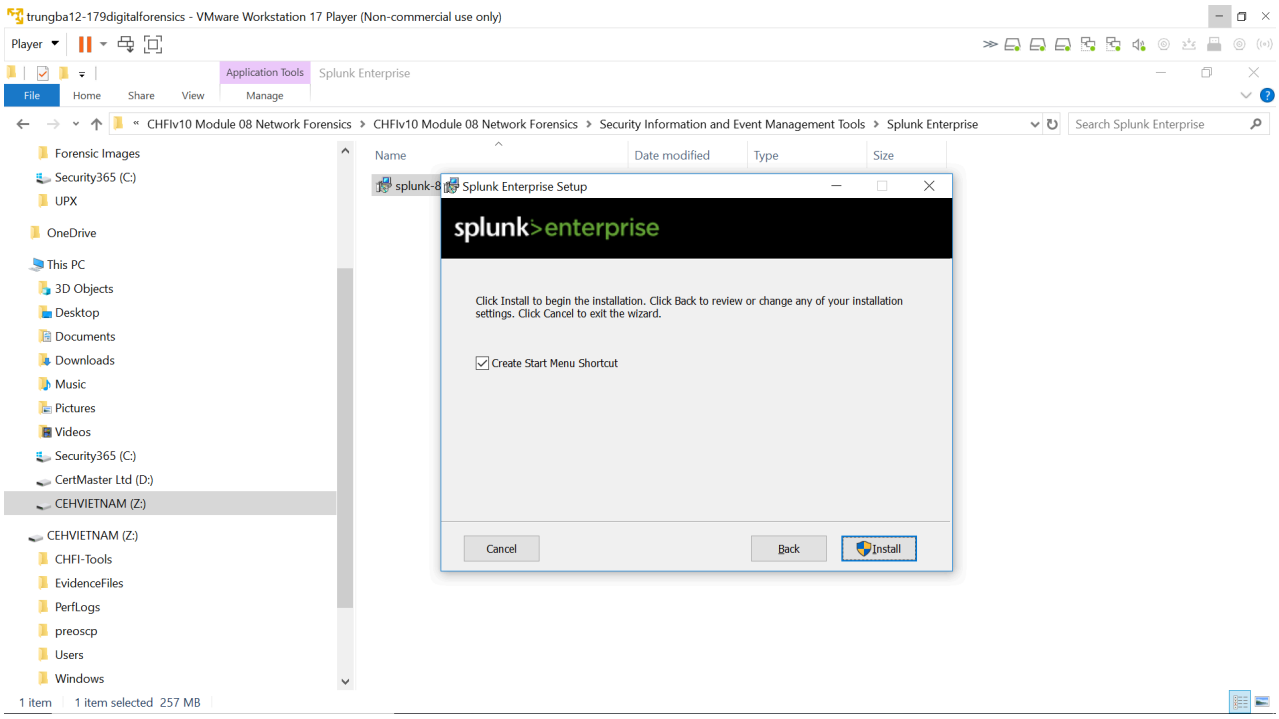
Nguyễn Tiến Ngọc **BA12-140**

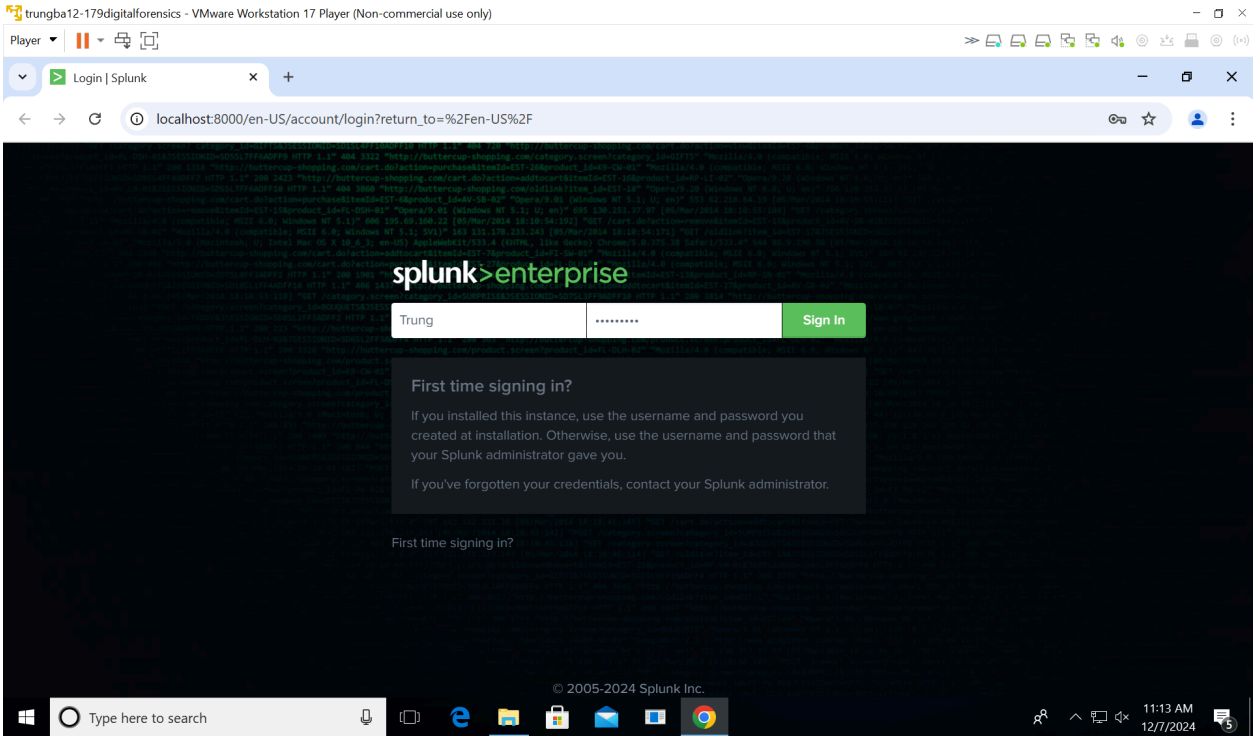
Ha Noi, Dec 07 2024

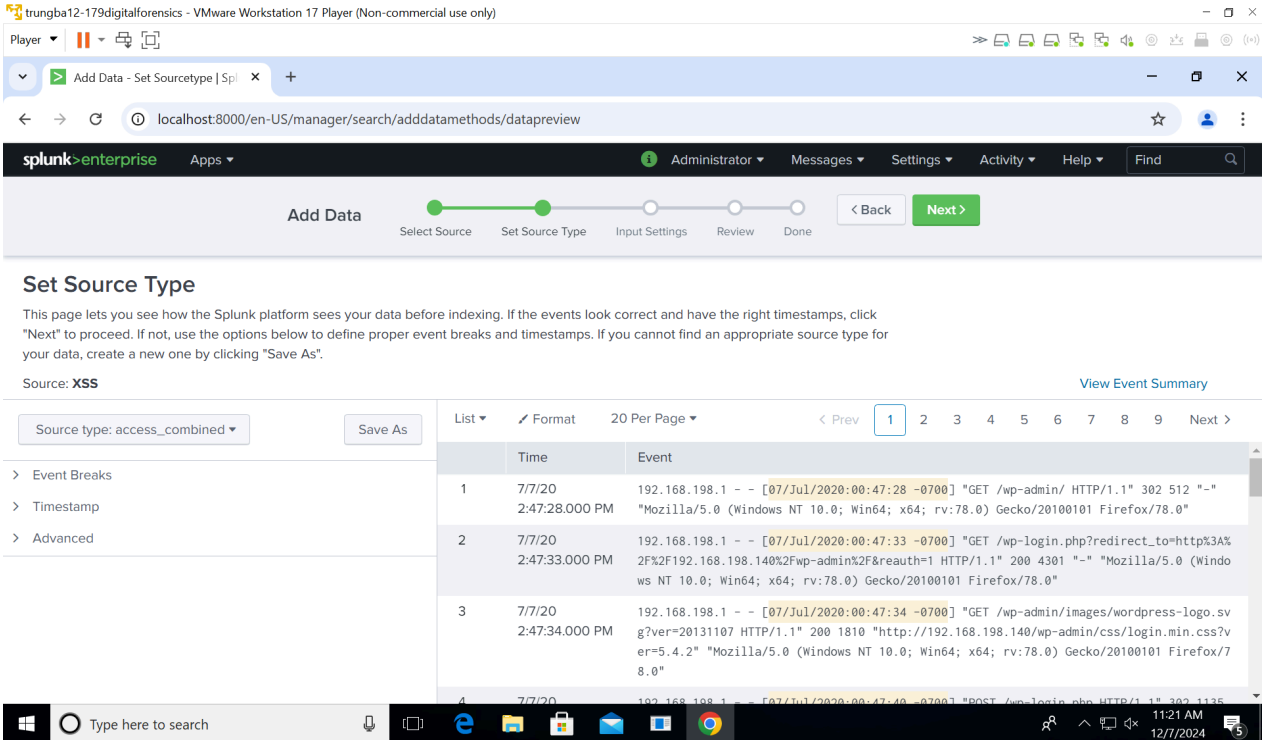
I. XSS (Apache Logs)

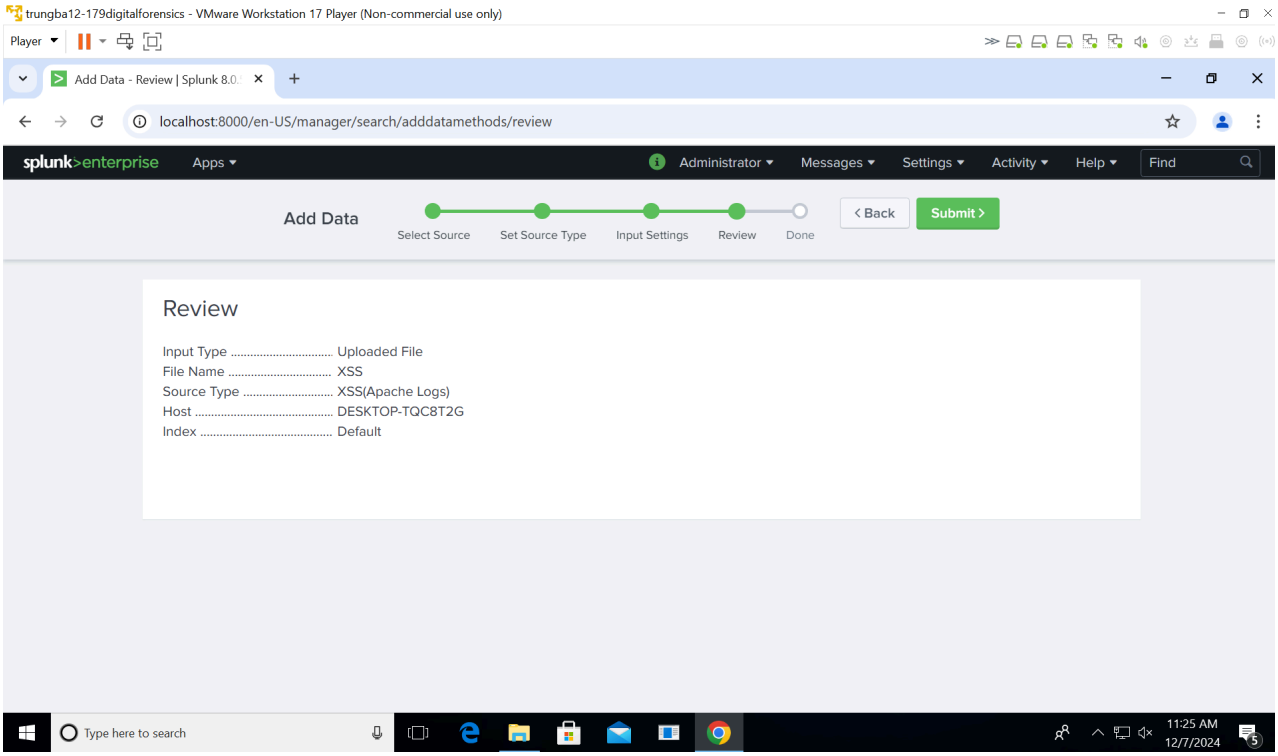
These images show how to detect an XSS attack by examining log files from the Apache server. You filtered for malicious scripts and decoded them to identify a potential XSS attack. The script found in the log file contains JavaScript that, when executed, may exploit vulnerabilities in the web application. This type of attack usually aims to execute scripts in the context of a victim's browser, which could steal information or perform unintended actions.

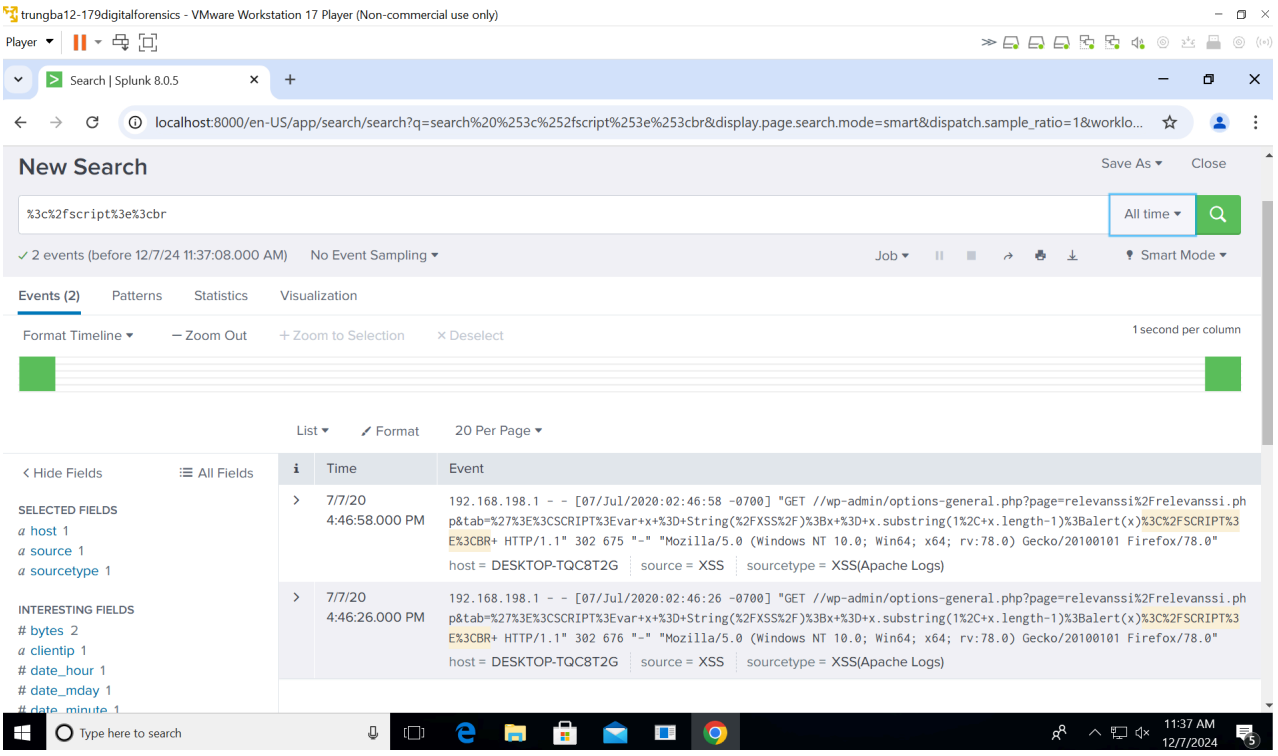
***Key Insights*: The images visually demonstrate filtering through logs in Splunk and detecting the attack via specific markers like `%3Cscript%3E` in the log entries. The presence of a suspicious script indicates the nature of the attack.**

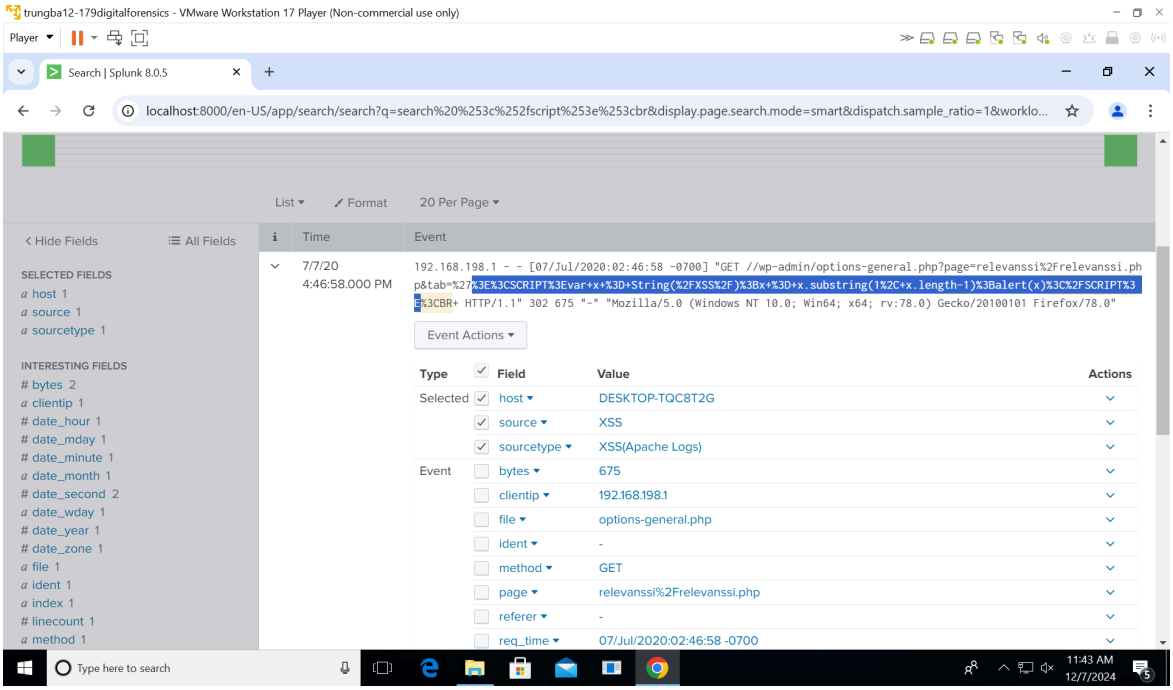



trungba12-179digitalforensics - VMware Workstation 17 Player (Non-commercial use only)
Player
Login | Splunk
localhost:8000/en-US/account/login?return_to=%2Fen-US%2F
splunk>enterprise
Trung
Sign In
First time signing in?
If you installed this instance, use the username and password you created at installation. Otherwise, use the username and password that your Splunk administrator gave you.
If you've forgotten your credentials, contact your Splunk administrator.
First time signing in?
© 2005-2024 Splunk Inc.
Type here to search
11:13 AM
12/7/2024


trungba12-179digitalforensics - VMware Workstation 17 Player (Non-commercial use only)
Player
Add Data - Set Sourcetype | Spl
localhost:8000/en-US/manager/search/adddatamethods/datapreview
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Next >
Set Source Type
This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".
Source: XSS
View Event Summary
Source type: access_combined
Save As
Event Breaks
Timestamp
Advanced
List
Format
20 Per Page
< Prev
1
2
3
4
5
6
7
8
9
Next >
Time
Event
1
7/7/20 2:47:28.000 PM
192.168.198.1 - - [07/Jul/2020:00:47:28 -0700] "GET /wp-admin/ HTTP/1.1" 302 512 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0"
2
7/7/20 2:47:33.000 PM
192.168.198.1 - - [07/Jul/2020:00:47:33 -0700] "GET /wp-login.php?redirect_to=http%3A%2F%2F192.168.198.140%2Fwp-admin%2F&reauth=1 HTTP/1.1" 200 4301 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0"
3
7/7/20 2:47:34.000 PM
192.168.198.1 - - [07/Jul/2020:00:47:34 -0700] "GET /wp-admin/images/wordpress-logo.svg?ver=20131107 HTTP/1.1" 200 1810 "http://192.168.198.140/wp-admin/css/login.min.css?ver=5.4.2" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0"
Type here to search
11:21 AM
12/7/2024


trungba12-179digitalforensics - VMware Workstation 17 Player (Non-commercial use only)
Player
Add Data - Review | Splunk 8.0.
localhost:8000/en-US/manager/search/adddatamethods/review
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
Back
Submit
Review
Input Type ..... Uploaded File
File Name ..... XSS
Source Type ..... XSS(Apache Logs)
Host DESKTOP-TQC8T2G
Index ..... Default
Type here to search
11:25 AM
12/7/2024

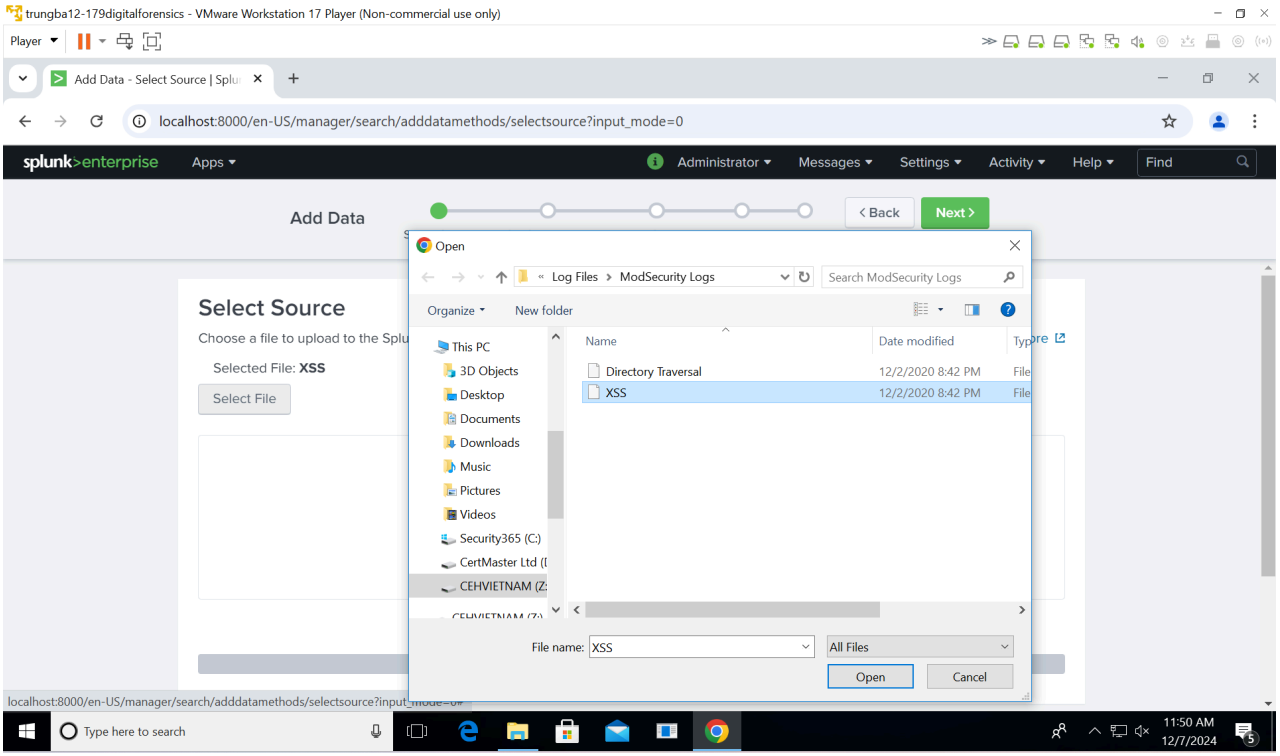

trungba12-179digitalforensics - VMware Workstation 17 Player (Non-commercial use only)
Player
Search | Splunk 8.0.5
localhost:8000/en-US/app/search/search?q=search%20%253c%252fscript%253e%253cbr&display.page.search.mode=smart&dispatch.sample_ratio=1&worklo...
New Search
Save As
Close
%3c%2fscript%3e%3cbr
All time
2 events (before 12/7/24 11:37:08.000 AM)
No Event Sampling
Job
Smart Mode
Events (2)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 second per column
List
Format
20 Per Page
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
bytes 2
a clientip 1
date_hour 1
date_mday 1
Time
Event
7/7/20 4:46:58.000 PM
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 = DESKTOP-TQC8T2G source = XSS sourcetype = XSS(Apache Logs)
7/7/20 4:46:26.000 PM
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) Gecko/20100101 Firefox/78.0"
host = DESKTOP-TQC8T2G source = XSS sourcetype = XSS(Apache Logs)
Type here to search
11:37 AM
12/7/2024

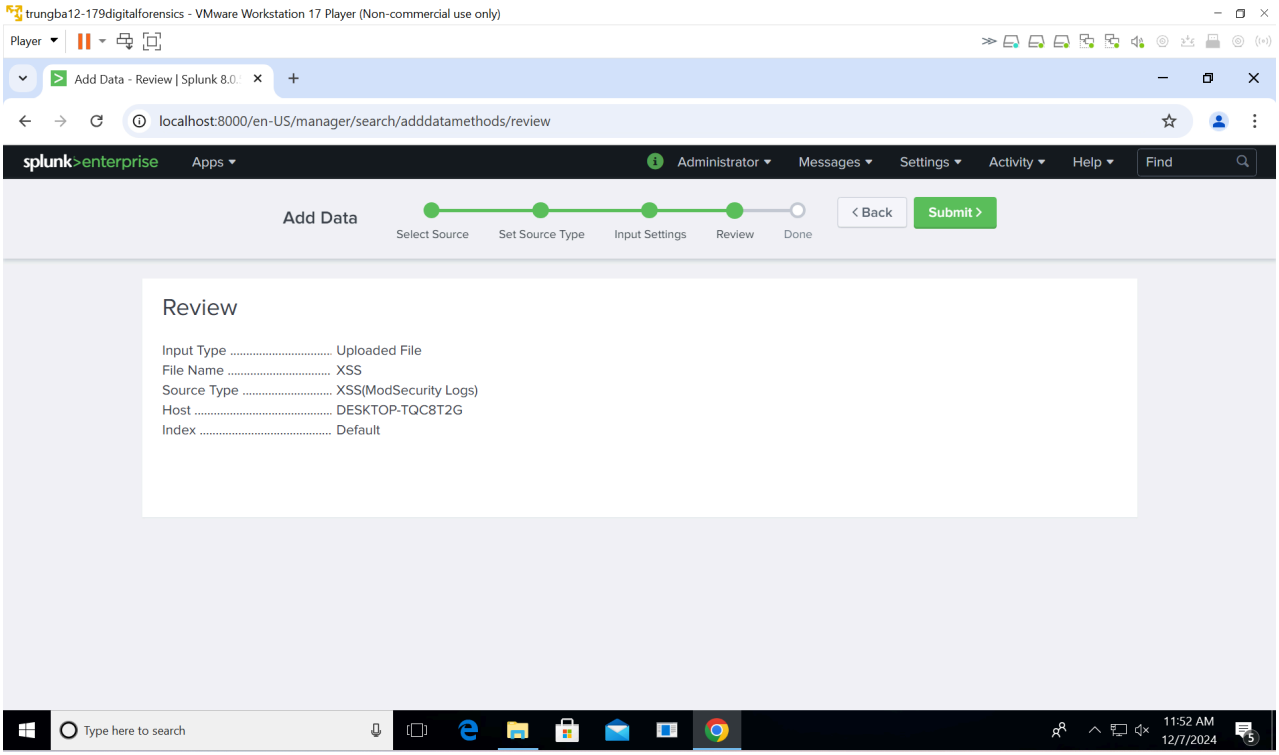

trungba12-179digitalforensics - VMware Workstation 17 Player (Non-commercial use only)
Player
Search | Splunk 8.0.5
localhost:8000/en-US/app/search/search?q=search%20%253c%252fscript%253e%253cbr&display.page.search.mode=smart&dispatch.sample_ratio=1&worklo...
List
Format
20 Per Page
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
bytes 2
a clientip 1
date_hour 1
date_mday 1
date_minute 1
a date_month 1
date_second 2
a date_wday 1
date_year 1
date_zone 1
a file 1
a ident 1
a index 1
linecount 1
a method 1
Time
Event
7/7/20
4:46:58.000 PM
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"
Event Actions
Type
Field
Value
Actions
Selected
host
DESKTOP-TQC8T2G
source
XSS
sourcetype
XSS(Apache Logs)
Event
bytes
675
clientip
192.168.198.1
file
options-general.php
ident
-
method
GET
page
relevanssi%2Frelevanssi.php
referer
-
req_time
07/Jul/2020:02:46:58 -0700
Type here to search
11:43 AM
12/7/2024

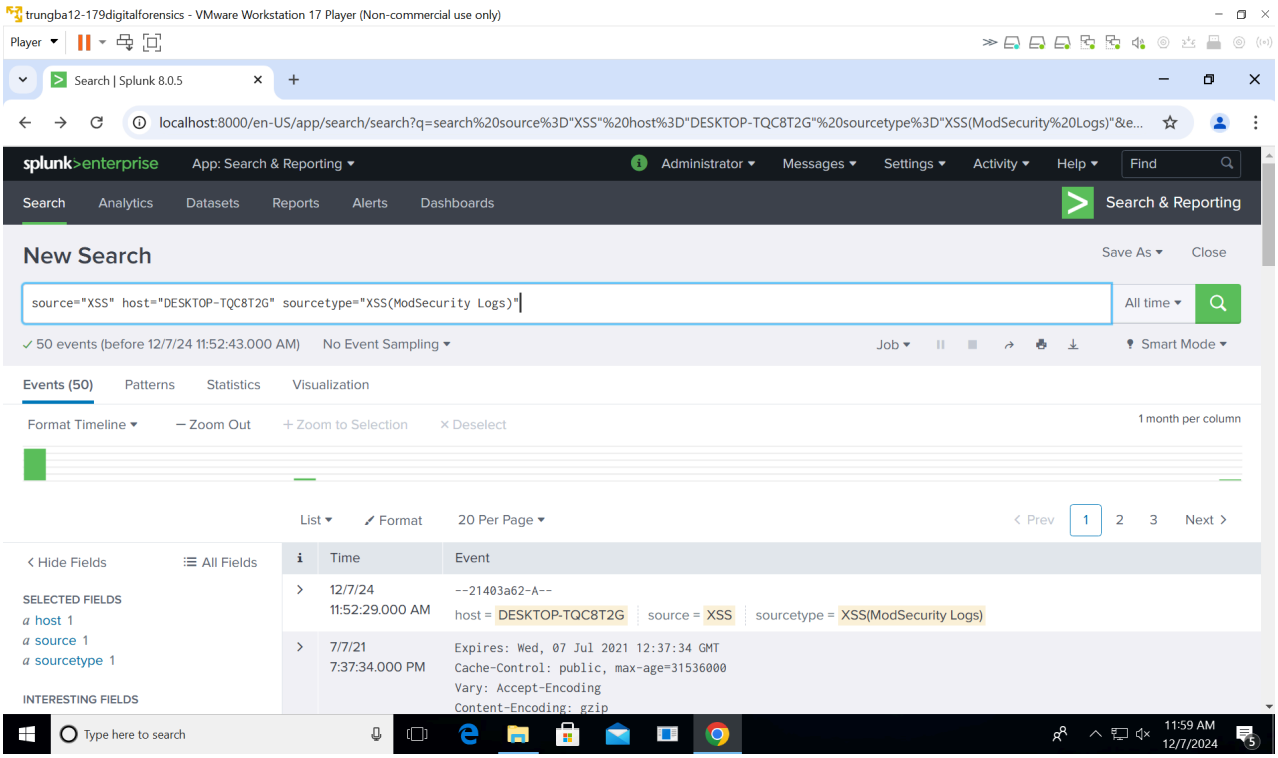
II. XSS (ModSecurity Logs)

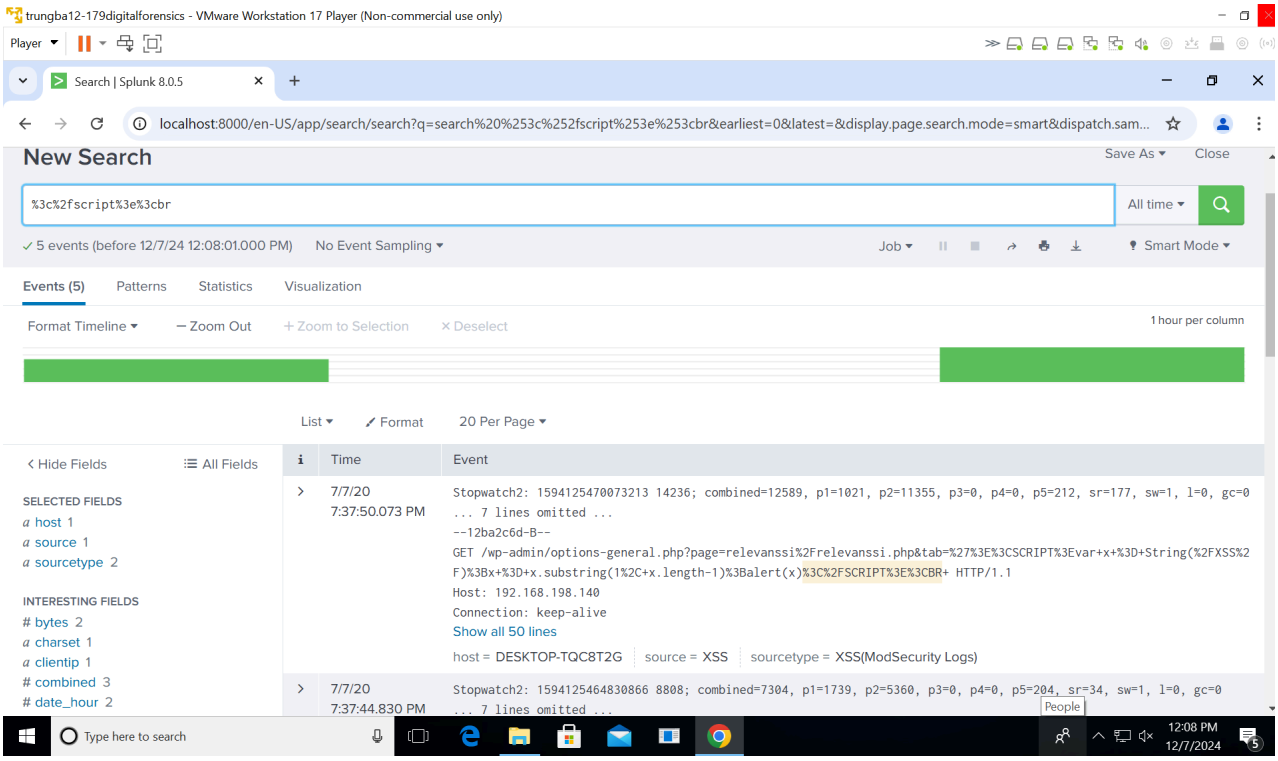
The analysis of ModSecurity logs reveals similar patterns in XSS attacks, with the added layer of security offered by ModSecurity, which tries to block such attacks. The images here show how the attack was detected and the firewall's response to it, with HTTP 403 errors indicating that access to the resource was blocked.

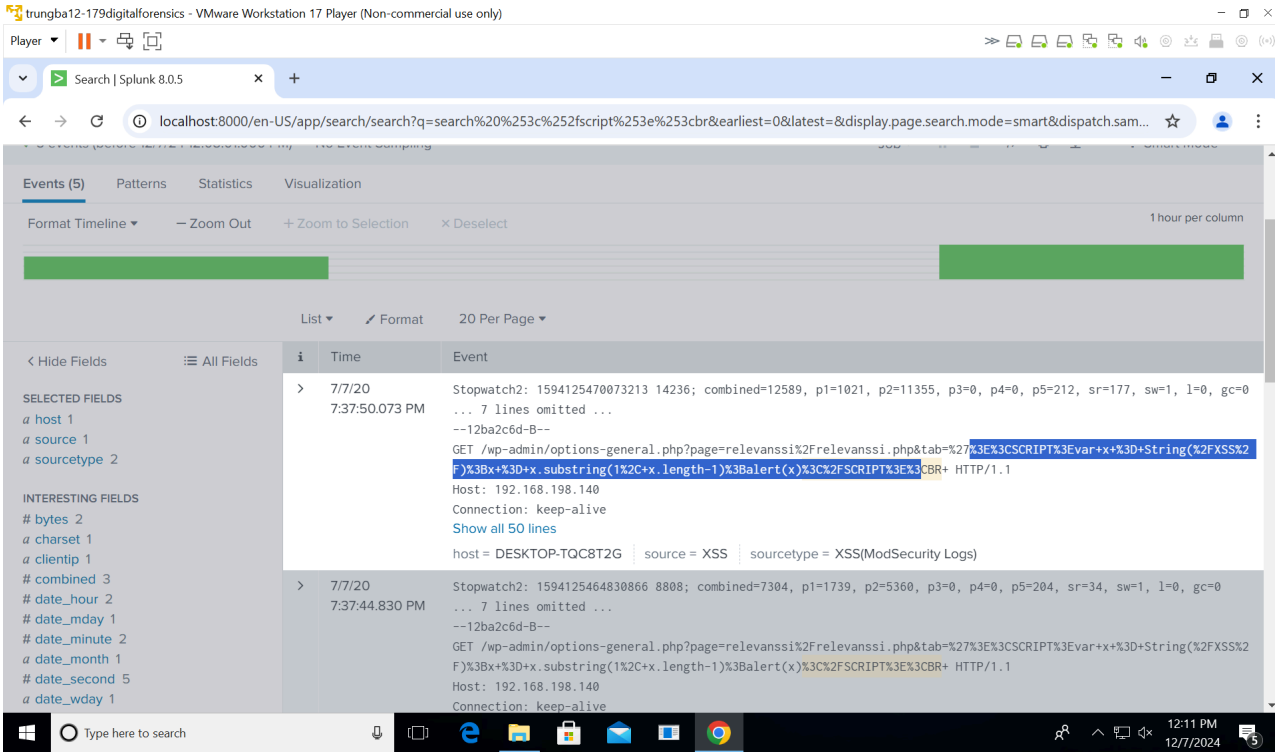
***Key Insights*: The images help visualize how web application firewalls (WAFs) like ModSecurity attempt to prevent these attacks by blocking malicious input.**




trungba12-179digitalforensics - VMware Workstation 17 Player (Non-commercial use only)
Player
Add Data - Review | Splunk 8.0.
localhost:8000/en-US/manager/search/adddatamethods/review
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
Back
Submit
Review
Input Type ..... Uploaded File
File Name ..... XSS
Source Type ..... XSS(ModSecurity Logs)
Host DESKTOP-TQC8T2G
Index ..... Default
Type here to search
11:52 AM
12/7/2024


trungba12-179digitalforensics - VMware Workstation 17 Player (Non-commercial use only)
Player
Search | Splunk 8.0.5
localhost:8000/en-US/app/search/search?q=search%20source%3D"XSS"%20host%3D"DESKTOP-TQC8T2G"%20sourcetype%3D"XSS(ModSecurity%20Logs)"&e...
splunk>enterprise
App: Search & Reporting
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Close
source="XSS" host="DESKTOP-TQC8T2G" sourcetype="XSS(ModSecurity Logs)"
All time
50 events (before 12/7/24 11:52:43.000 AM)
No Event Sampling
Job
Smart Mode
Events (50)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 month per column
List
Format
20 Per Page
Prev
1
2
3
Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
Time
Event
12/7/24
11:52:29.000 AM
--21403a62-A--
host = DESKTOP-TQC8T2G
source = XSS
sourcetype = XSS(ModSecurity Logs)
7/7/21
7:37:34.000 PM
Expires: Wed, 07 Jul 2021 12:37:34 GMT
Cache-Control: public, max-age=31536000
Vary: Accept-Encoding
Content-Encoding: gzip
Type here to search
11:59 AM
12/7/2024

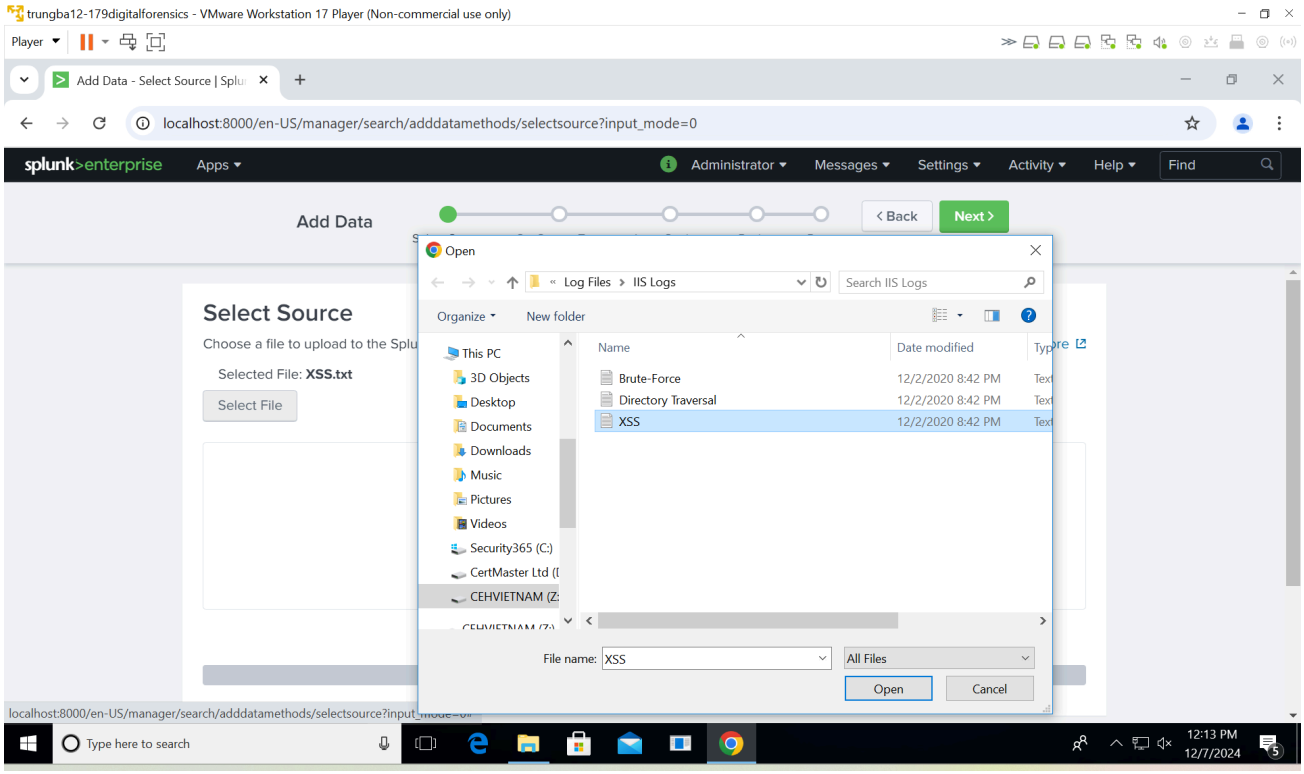

trungba12-179digitalforensics - VMware Workstation 17 Player (Non-commercial use only)
Player
Search | Splunk 8.0.5
localhost:8000/en-US/app/search/search?q=search%20%253c%252fscript%253e%253cbr&earliest=0&latest=&display.page.search.mode=smart&dispatch.sam...
New Search
Save As
Close
%3c%2fscript%3e%3cbr
All time
5 events (before 12/7/24 12:08:01.000 PM)
No Event Sampling
Job
Smart Mode
Events (5)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
List
Format
20 Per Page
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 2
INTERESTING FIELDS
bytes 2
a charset 1
a clientip 1
combined 3
date_hour 2
Time
Event
7/7/20
7:37:50.073 PM
Stopwatch2: 1594125470073213 14236; combined=12589, p1=1021, p2=11355, p3=0, p4=0, p5=212, sr=177, sw=1, l=0, gc=0
... 7 lines omitted ...
--12ba2c6d-B--
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
Host: 192.168.198.140
Connection: keep-alive
Show all 50 lines
host = DESKTOP-TQC8T2G
source = XSS
sourcetype = XSS(ModSecurity Logs)
7/7/20
7:37:44.830 PM
Stopwatch2: 1594125464830866 8808; combined=7304, p1=1739, p2=5360, p3=0, p4=0, p5=204, sr=34, sw=1, l=0, gc=0
... 7 lines omitted ...
People
Type here to search
12:08 PM
12/7/2024

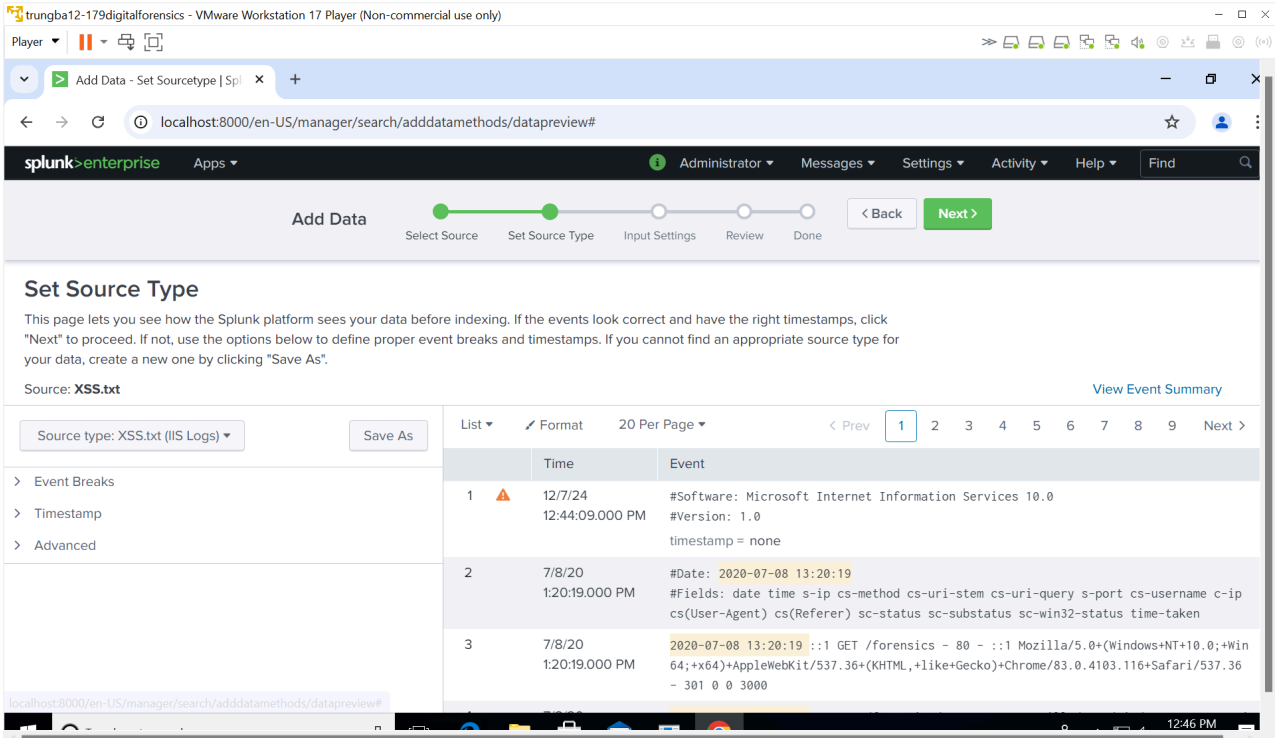

trungba12-179digitalforensics - VMware Workstation 17 Player (Non-commercial use only)
Player
Search | Splunk 8.0.5
localhost:8000/en-US/app/search/search?q=search%20%253c%252fscript%253e%253cbr&earliest=0&latest=&display.page.search.mode=smart&dispatch.sam...
Events (5)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
List
Format
20 Per Page
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 2
INTERESTING FIELDS
bytes 2
a charset 1
a clientip 1
combined 3
date_hour 2
date_mday 1
date_minute 2
a date_month 1
date_second 5
a date_wday 1
Time
Event
7/7/20
7:37:50.073 PM
Stopwatch2: 1594125470073213 14236; combined=12589, p1=1021, p2=11355, p3=0, p4=0, p5=212, sr=177, sw=1, l=0, gc=0
... 7 lines omitted ...
--12ba2c6d-B--
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
Host: 192.168.198.140
Connection: keep-alive
Show all 50 lines
host = DESKTOP-TQC8T2G
source = XSS
sourcetype = XSS(ModSecurity Logs)
7/7/20
7:37:44.830 PM
Stopwatch2: 1594125464830866 8808; combined=7304, p1=1739, p2=5360, p3=0, p4=0, p5=204, sr=34, sw=1, l=0, gc=0
... 7 lines omitted ...
--12ba2c6d-B--
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
Host: 192.168.198.140
Connection: keep-alive
Type here to search
12:11 PM
12/7/2024

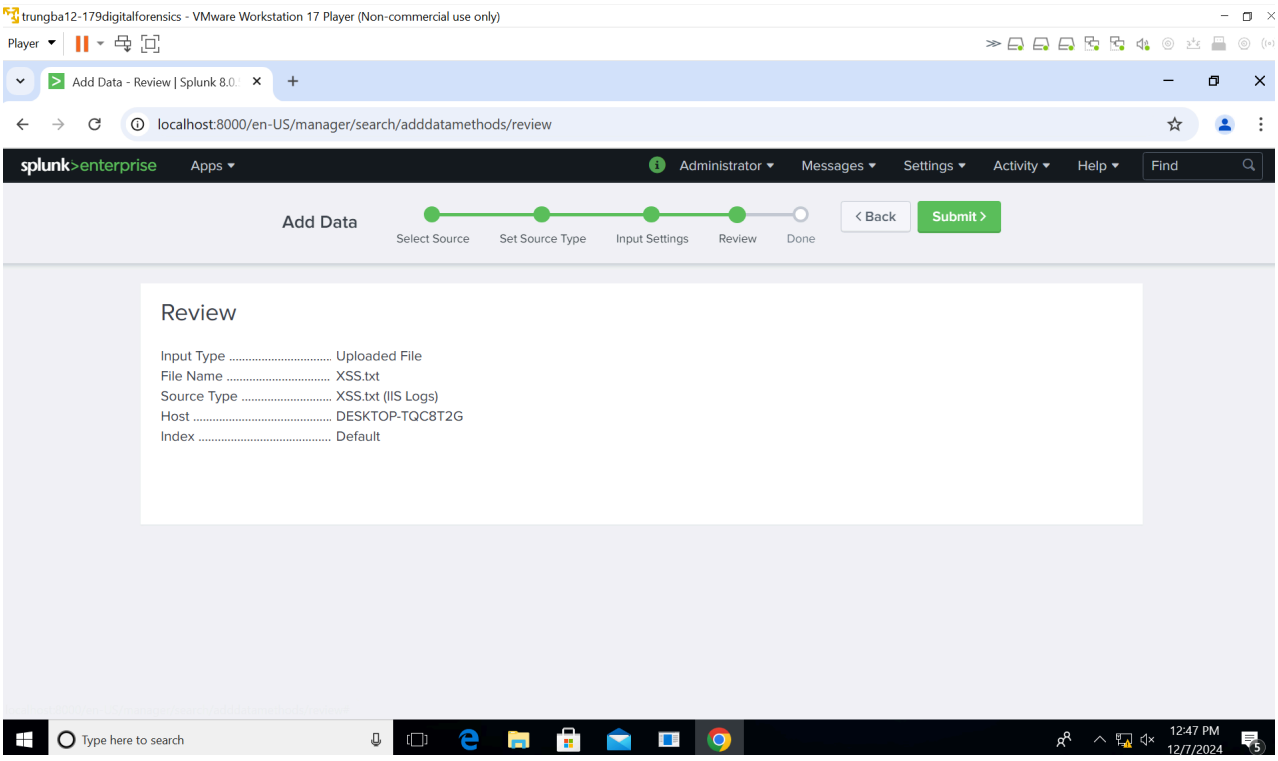
III. XSS.txt (IIS Logs)

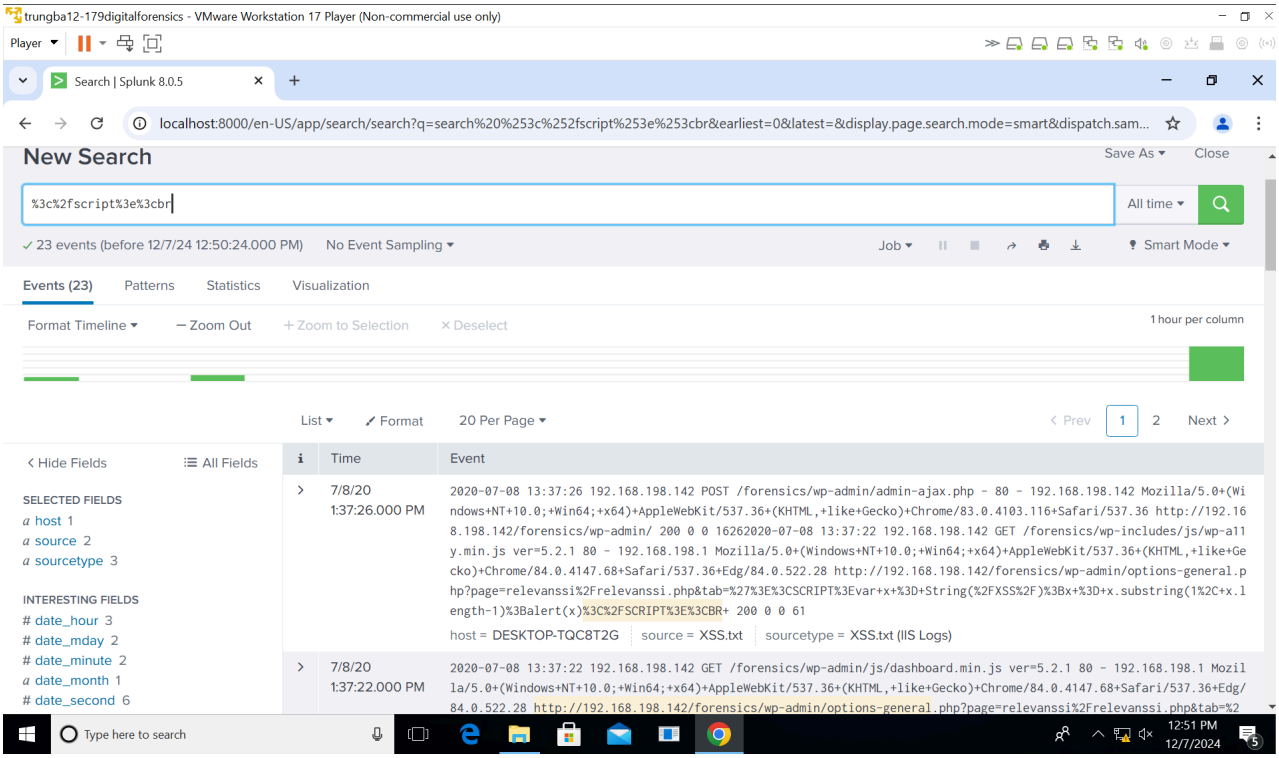
This part involves examining IIS logs for the same XSS attack. Similar to the Apache and ModSecurity logs, we can see the attacker using encoded scripts to inject malicious JavaScript. The key here is recognizing that different web servers (Apache, ModSecurity, IIS) may log different data, and understanding these variations is critical for an in-depth forensic investigation.

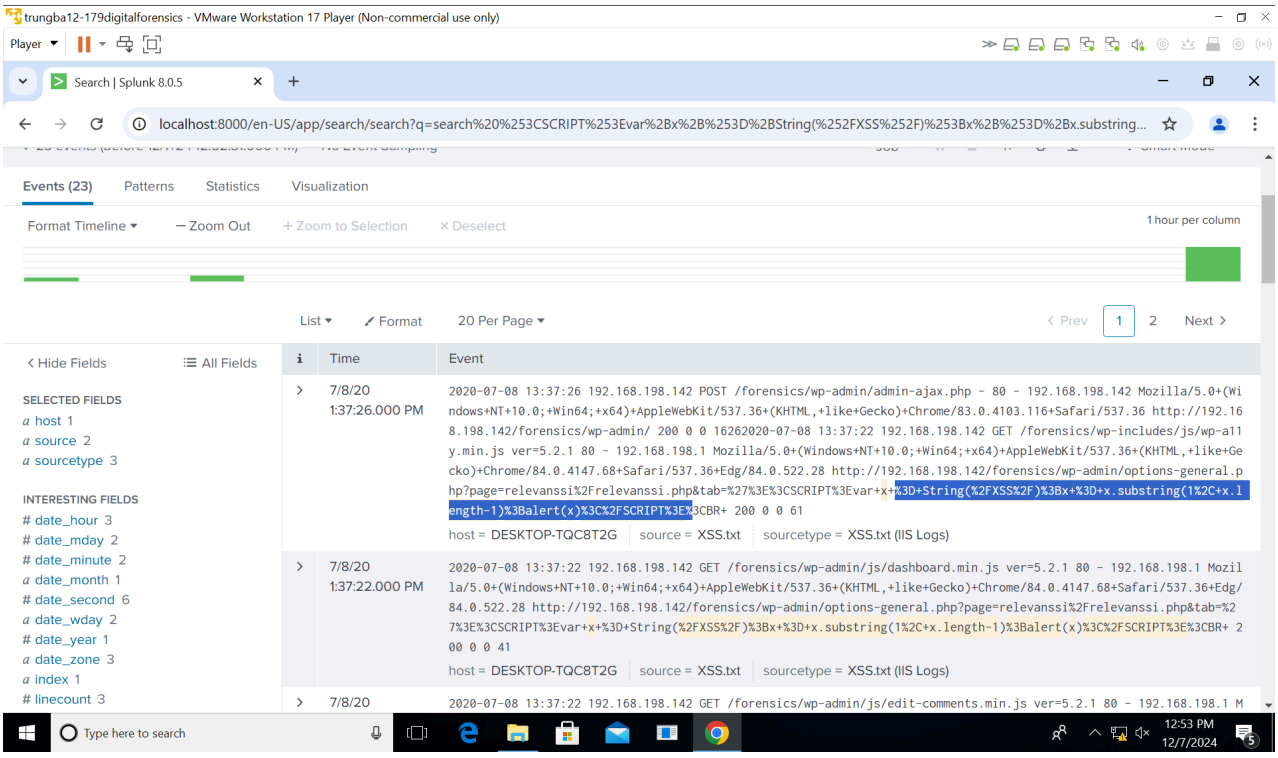
The IIS logs highlight that despite the firewall's response, the attacker was able to launch an attack, which emphasizes the need for multiple layers of defense.




trungba12-179digitalforensics - VMware Workstation 17 Player (Non-commercial use only)
Player
Add Data - Set Sourcetype | Spl
localhost:8000/en-US/manager/search/adddatamethods/datapreview#
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Next >
Set Source Type
This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".
Source: XSS.txt
View Event Summary
Source type: XSS.txt (IIS Logs)
Save As
List
Format
20 Per Page
Prev
1
2
3
4
5
6
7
8
9
Next >
Event Breaks
Timestamp
Advanced
Time
Event
1
12/7/24
12:44:09.000 PM
#Software: Microsoft Internet Information Services 10.0
#Version: 1.0
timestamp = none
2
7/8/20
1:20:19.000 PM
#Date: 2020-07-08 13:20:19
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) cs(Referer) sc-status sc-substatus sc-win32-status time-taken
3
7/8/20
1:20:19.000 PM
2020-07-08 13:20:19 ::1 GET /forensics - 80 - ::1 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/83.0.4103.116+Safari/537.36 - 301 0 0 3000
12:46 PM


trungba12-179digitalforensics - VMware Workstation 17 Player (Non-commercial use only)
Player
Add Data - Review | Splunk 8.0
localhost:8000/en-US/manager/search/adddatamethods/review
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Submit >
Review
Input Type ..... Uploaded File
File Name ..... XSS.txt
Source Type ..... XSS.txt (IIS Logs)
Host DESKTOP-TQC8T2G
Index ..... Default
Type here to search
12:47 PM
12/7/2024


trungba12-179digitalforensics - VMware Workstation 17 Player (Non-commercial use only)
Search | Splunk 8.0.5
localhost:8000/en-US/app/search/search?q=search%20%253c%252fscript%253e%253cbr&earliest=0&latest=&display.page.search.mode=smart&dispatch.sam...
New Search
Save As
Close
%3c%2fscript%3e%3cbr
All time
23 events (before 12/7/24 12:50:24.000 PM)
No Event Sampling
Job
Smart Mode
Events (23)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
List
Format
20 Per Page
Prev
1
2
Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 2
a sourcetype 3
INTERESTING FIELDS
date_hour 3
date_mday 2
date_minute 2
a date_month 1
date_second 6
Time
Event
7/8/20 1:37:26.000 PM
2020-07-08 13:37:26 192.168.198.142 POST /forensics/wp-admin/admin-ajax.php - 80 - 192.168.198.142 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/83.0.4103.116+Safari/537.36 http://192.168.198.142/forensics/wp-admin/ 200 0 0 16262020-07-08 13:37:22 192.168.198.142 GET /forensics/wp-includes/js/wp-a11y.min.js ver=5.2.1 80 - 192.168.198.1 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/84.0.4147.68+Safari/537.36+Edg/84.0.522.28 http://192.168.198.142/forensics/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+ 200 0 0 61
host = DESKTOP-TQC8T2G
source = XSS.txt
sourcetype = XSS.txt (IIS Logs)
7/8/20 1:37:22.000 PM
2020-07-08 13:37:22 192.168.198.142 GET /forensics/wp-admin/js/dashboard.min.js ver=5.2.1 80 - 192.168.198.1 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/84.0.4147.68+Safari/537.36+Edg/84.0.522.28 http://192.168.198.142/forensics/wp-admin/options-general.php?page=relevanssi%2Frelevanssi.php&tab=%2
Type here to search
12:51 PM
12/7/2024


trungba12-179digitalforensics - VMware Workstation 17 Player (Non-commercial use only)
Search | Splunk 8.0.5
localhost:8000/en-US/app/search/search?q=search%20%253CSCRIPT%253Evar%2Bx%2B%253D%2BString(%252FXSS%252F)%253Bx%2B%253D%2Bx.substring...
Events (23)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
List
Format
20 Per Page
Prev
1
2
Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 2
a sourcetype 3
INTERESTING FIELDS
date_hour 3
date_mday 2
date_minute 2
a date_month 1
date_second 6
a date_wday 2
date_year 1
a date_zone 3
a index 1
linecount 3
Time
Event
7/8/20 1:37:26.000 PM
2020-07-08 13:37:26 192.168.198.142 POST /forensics/wp-admin/admin-ajax.php - 80 - 192.168.198.142 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/83.0.4103.116+Safari/537.36 http://192.168.198.142/forensics/wp-admin/ 200 0 0 16262020-07-08 13:37:22 192.168.198.142 GET /forensics/wp-includes/js/wp-a11y.min.js ver=5.2.1 80 - 192.168.198.1 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/84.0.4147.68+Safari/537.36+Edg/84.0.522.28 http://192.168.198.142/forensics/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+ 200 0 0 61
host = DESKTOP-TQC8T2G
source = XSS.txt
sourcetype = XSS.txt (IIS Logs)
7/8/20 1:37:22.000 PM
2020-07-08 13:37:22 192.168.198.142 GET /forensics/wp-admin/js/dashboard.min.js ver=5.2.1 80 - 192.168.198.1 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/84.0.4147.68+Safari/537.36+Edg/84.0.522.28 http://192.168.198.142/forensics/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+ 200 0 0 41
host = DESKTOP-TQC8T2G
source = XSS.txt
sourcetype = XSS.txt (IIS Logs)
7/8/20
2020-07-08 13:37:22 192.168.198.142 GET /forensics/wp-admin/js/edit-comments.min.js ver=5.2.1 80 - 192.168.198.1 M
Type here to search
12:53 PM
12/7/2024

Meaning of the Lab Work:

The primary goal of this lab is to teach the practical skills needed for investigating web attacks, specifically XSS. By analyzing the logs from different sources (Apache, ModSecurity, IIS), you learn how to:

- **Identify Web Attacks: XSS attacks are detected through log analysis by recognizing malicious scripts or unusual patterns in the logs.**
- **Understand Log Data: The lab demonstrates how various systems log data differently. Apache, ModSecurity, and IIS each have distinct log formats, and understanding these can help in tracing back the steps of an attack.**
- **Practical Forensic Skills: The lab emphasizes hands-on experience with tools like Splunk Enterprise, which is used to search and analyze logs, allowing you to track down the source of the attack and understand its impact.**
- **Improve Web Security: By simulating and detecting attacks in a controlled environment, you gain knowledge of how to prevent, detect, and mitigate web vulnerabilities in real-world applications.**

The significance of this lab is that it equips you with the skills to conduct forensic investigations into web-based attacks, which is a crucial part of cybersecurity. Understanding these types of attacks, especially XSS, is important for developing secure applications and systems, as well as for responding to incidents involving web vulnerabilities.