PROJECT:
SECURITY OPERATION CENTER

By Aditya Sathyan | +91-8904597554

Red Team Academy – CICSA 2022

TABLE OF CONTENTS

A Security Operations Center (SOC) is a centralized unit that deals with the **monitoring, detection, analysis, and response to security threats.** It is typically responsible for protecting an organization's information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The SOC can be operated by an internal team or by an external third-party service provider, and it typically uses a combination of technology, processes, and people to provide round-the-clock surveillance and protection for an organization's network and systems.

SIEM (Security Information and Event Management) tools are software solutions that provide organizations with real-time analysis of security-related data from various sources, such as network devices, servers, and applications. SIEM tools are designed to help **organizations detect, investigate, and respond to cyber security threats** by providing a central location for security information from different systems.

They collect, analyze and correlate log data from different sources, like firewalls, intrusion detection systems (IDS), and antivirus software, to identify potential security threats and provide alerts. SIEM tools also provide incident response, reporting, and compliance capabilities. Some examples of SIEM tools are:

- Splunk Enterprise Security
- LogRhythm
- IBM QRadar
- McAfee Enterprise Security Manager
- RSA NetWitness
- AlienVault USM
- ArcSight
- LogPoint
- SolarWinds
- Wazuh.

Splunk Enterprise Security.

Splunk is a software platform that is used for **analyzing, monitoring, and visualizing machine-generated data, such as log files and performance metrics, in real-time**. It allows users to search, correlate, and analyze data from a wide variety of sources, including network devices, servers, applications, and cloud services. Splunk is commonly used in IT operations, security, and compliance, as well as for business intelligence and big data analytics.

1. IT operations and infrastructure monitoring: Splunk can be used to monitor log files and performance metrics from servers, network devices, and applications, providing real-time visibility into the health and performance of IT systems.

2. Security and threat detection: Splunk can be used to collect and analyze security-related data, such as firewall logs, intrusion detection system alerts, and network traffic, to detect and respond to security incidents.

3. Compliance and regulatory reporting: Splunk can be used to collect and analyze data from various sources, such as network devices, servers, and applications, to meet compliance and regulatory requirements.

4. Business intelligence and analytics: Splunk can be used to analyze large volumes of structured and unstructured data, such as customer data, financial data, and website analytics, to gain insights and improve business performance.

5. Application performance management: Splunk can be used to monitor and analyze the performance of applications, including web applications, mobile apps, and microservices.

6. Network performance monitoring: Splunk can be used to monitor and analyze network traffic and performance metrics, such as network latency and throughput, to troubleshoot and optimize network performance.

7. Internet of Things (IoT) data: Splunk can be used to collect, store, and analyze data from IoT devices and sensors, such as temperature and humidity sensors, to gain insights and improve operational efficiencies.

8. Cloud monitoring: Splunk can be used to monitor and analyze data from cloud services, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform, to ensure performance and security.

9. Fraud detection: Splunk can be used to analyze large volumes of transactional and behavioral data, such as credit card transactions and website activity, to detect and prevent fraudulent activities.

10. Machine learning and Artificial Intelligence: Splunk can be used to collect and analyze large volumes of data, such as log files and sensor data, to train machine learning and AI models, and to make predictions and gain insights

To add a new device to Splunk, you will typically need to perform the following steps:

1. Install and configure the Splunk Universal Forwarder on the device you want to add. The Universal Forwarder is a lightweight version of the Splunk software that can be installed on remote systems to collect and forward data to a central Splunk indexer.

2. Configure the Universal Forwarder to forward the data you want to collect from the device. This can be done by editing the inputs.conf file, which is located in the etc/system/local directory of the Universal Forwarder installation.

3. Configure the central Splunk indexer to accept data from the new device. This can be done by editing the inputs.conf file on the indexer, which is located in the etc/system/local directory of the Splunk installation.

4. Restart the Universal Forwarder and the central Splunk indexer to apply the changes.

5. Verify that data is being received from the new device by searching for data in the Splunk Web interface or by using the command-line interface.

Note that the above steps are a general overview, and the specific steps may vary depending on the version of Splunk you are using and the type of device you are adding. It's important to consult the Splunk documentation or seek help from a Splunk administrator or professional for detailed instructions on adding new devices to Splunk.

To find a report on failed login attempts in Splunk

We can use the search functionality in the Splunk Web interface. Here are the general steps to create a report on failed login attempts:

1. In the Search bar, type in a search query that will return the failed login attempts events. For example, you can use the following query to search for failed login attempts in your authentication log:

   ```
   index=<your_index> sourcetype=<your_sourcetype> "failed login" OR
   "authentication failure"
   ```

2. Use the "time picker" on the top-right corner of the search bar to select the time range for which you want to see the failed login attempts.

3. Once you have the search results, you can use the "Stats" command to group the results by a specific field, such as the user or IP address, and get the count of failed login attempts.

   stats count by user

4 To create a report, you can use the "Save As" option in the "Actions" menu and select "Report" . This will create a new report with the search results, which you can then schedule, export, or share with others.

5 To view the report, you can go to the "Reports" section of the Splunk Web interface, where you will find the saved reports.

Note: The above steps are a general overview and the specific steps may vary depending on the version of Splunk you are using and the type of log files you have. It's important to consult the Splunk documentation or seek help from a Splunk administrator or professional for detailed instructions on creating reports in Splunk.

Search and Reporting Examples.

- Splunk report on failed login attempts

  The data contains Windows Event Codes, such as:

  - **540 Successful Network Logon**
  - **4624 Successful Network Logon**
  - **4625 Failure**
  - **4634 Successful Network Logoff**
- If you want to find events with "error", start by typing in the keyword.
  - *Error*
- To make the searches more efficient, use as many keywords as possible to describe the event. For example, to find specific errors described by a phrase, use the entire phrase.
  - "sshd error"
  - "login failed"
  - "failed password"
  - "access denied"

EXAMPLE 1:

USING SPLUNK TO LOCATE UNSUCCESSFUL LOGIN ATTEMPTS IN A SYSTEM.

To install Splunk on a Windows system, follow these steps:

1. Download the Splunk Enterprise installer from the Splunk website.: https://www.splunk.com/en_us/download.html

2. Register in the Splunk Website. Note: Save the username, email address and password https://www.splunk.com/en_us/sign-up.html

3. Run the installer and select the destination folder for the installation.

4. Follow the prompts in the installer to complete the installation process.

5. Once the installation is complete, open the Splunk Enterprise command prompt by clicking Start > All Programs > Splunk > Command Prompt.

6. Start the Splunk service by typing "splunk start" in the command prompt and pressing enter.

7. Open a web browser and go to "http://localhost:8000" to access the Splunk web interface.

8. Log in to Splunk using the email address and password used while registering in the splunk website.

Once you are logged in, you can start adding data to Splunk and using its various features.

NOTE:

Splunk Ports

8000 – Splunk Webserver Port

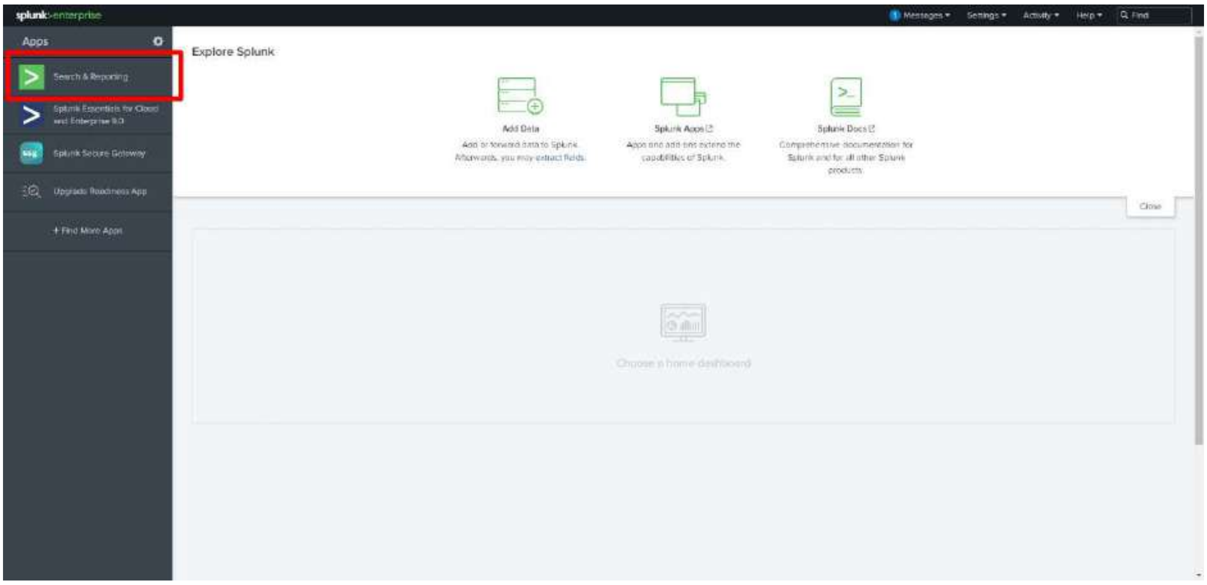
9997 – Receiving Port

8089 – Forwarder MGMT port

1. In the browser type: http://127.0.0.1:8000/

Enter in the email address and password used while registering in the splunk website

2. Once you login you will see the following screen. Click on the Search & Reporting Link on the left



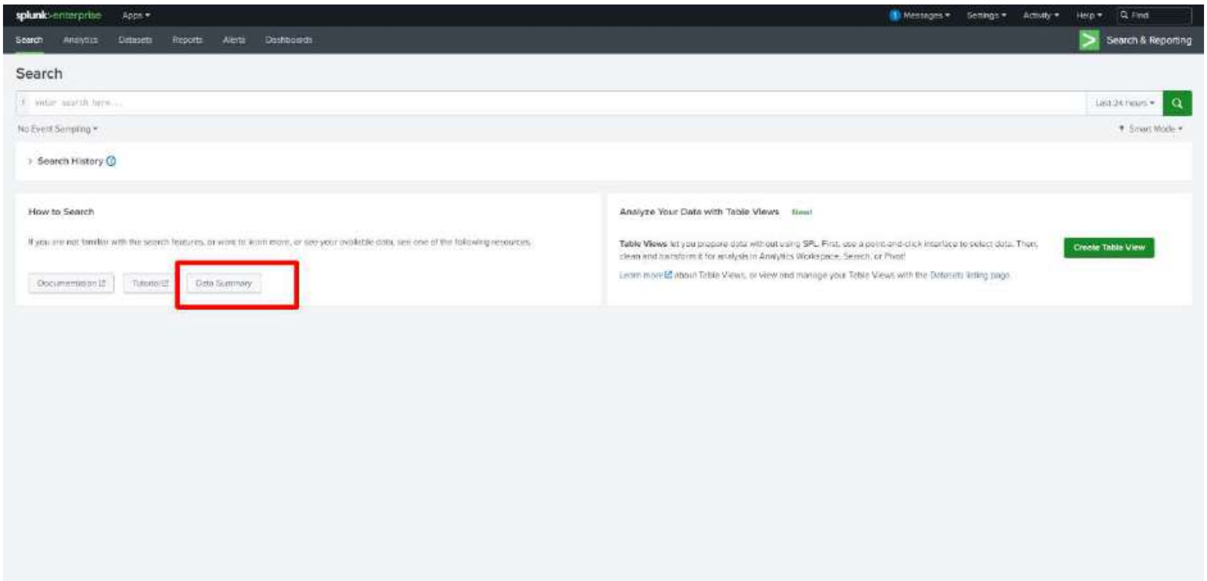
Add or forward data to Splunk. Afterwards, you may extract fields.

Apps and add-ons extend the capabilities of Splunk.

Comprehensive documentation for Splunk and for all other Splunk products.

Figure 1

3. Click on Data Summary



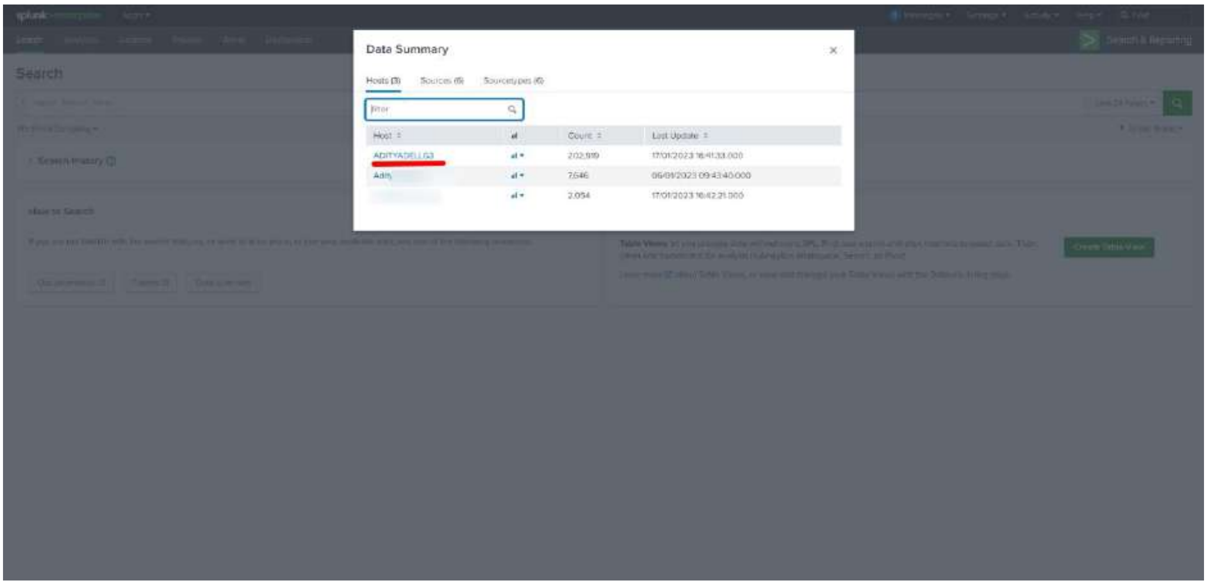
If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.

Table Views let you prepare data without using SPL. First, use a point-and-click interface to select data. Then, clean and transform it for analysis in Analytics Workspace, Search, or Pivot!

Learn more about Table Views, or view and manage your Table Views with the Datasets listing page.

Figure 2

4. If the system is properly configured the Device will be shown in the Host section. In this case 3 sources are shown. We will be selecting ADITYADELLG3



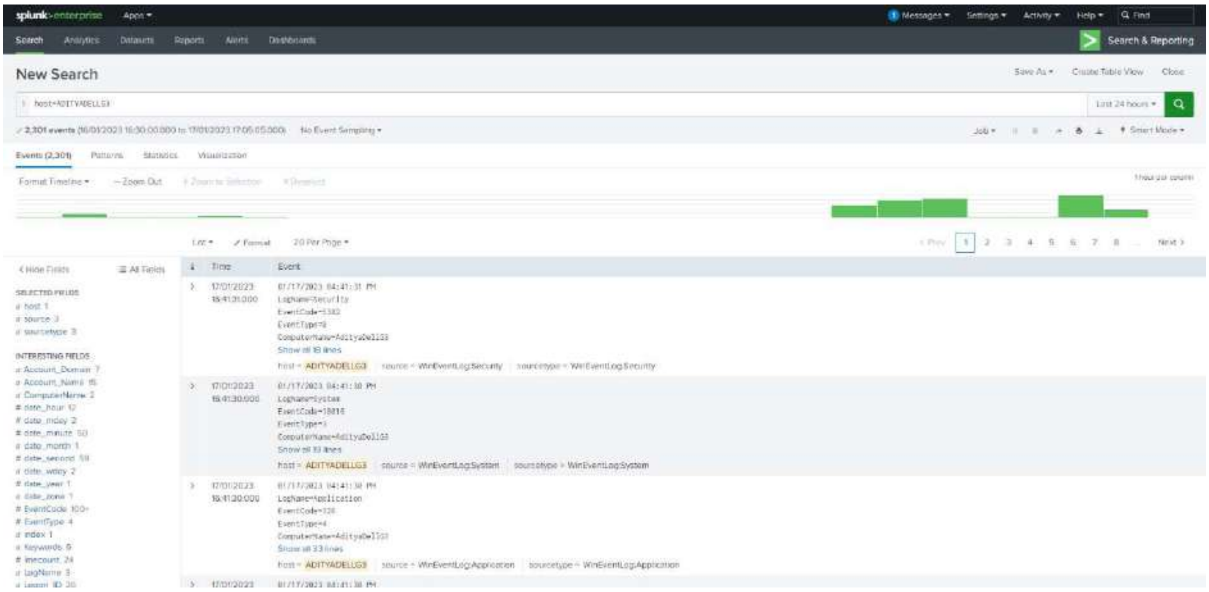
Data Summary

Hosts (3) Sources (6) Sourcetypes (6)

Host		Count	Last Update
ADITYADELLG3		202,919	17/01/2023 16:41:33.000
Adit[redacted]		7,646	06/01/2023 09:43:40.000
[redacted]		2,054	17/01/2023 16:42:21.000

Figure 3

5. This will show all the events in the system



New Search

host=ADITYADELLG3

✓ 2,301 events (16/01/2023 16:30:00.000 to 17/01/2023 17:06:05.000) No Event Sampling

SELECTED FIELDS
a host 1
a source 3
a sourcetype 3

INTERESTING FIELDS
a Account_Domain 7
a Account_Name 15
a ComputerName 2
# date_hour 12
# date_mday 2
# date_minute 50
a date_month 1
# date_second 59
a date_wday 2
# date_year 1
a date_zone 1
EventCode 100+
EventType 4
a index 1
a Keywords 6
# linecount 24
a LogName 3
a Logon_ID 20

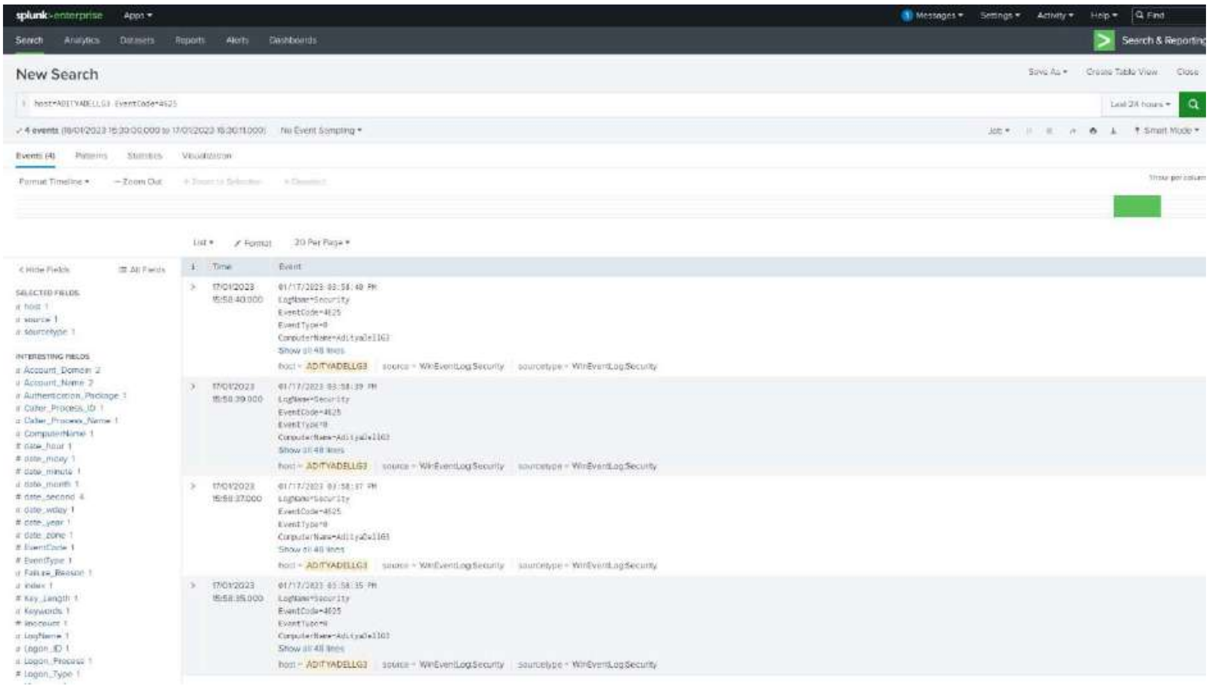
```
i  Time                     Event
>  17/01/2023               01/17/2023 04:41:31 PM
   16:41:31.000             LogName=Security
                            EventCode=5382
                            EventType=0
                            ComputerName=AdityaDellG3
                            Show all 18 lines
                            host = ADITYADELLG3   source = WinEventLog:Security   sourcetype = WinEventLog:Security
>  17/01/2023               01/17/2023 04:41:30 PM
   16:41:30.000             LogName=System
                            EventCode=10016
                            EventType=3
                            ComputerName=AdityaDellG3
                            Show all 33 lines
                            host = ADITYADELLG3   source = WinEventLog:System   sourcetype = WinEventLog:System
>  17/01/2023               01/17/2023 04:41:30 PM
   16:41:20.000             LogName=Application
                            EventCode=326
                            EventType=4
                            ComputerName=AdityaDellG3
                            Show all 33 lines
                            host = ADITYADELLG3   source = WinEventLog:Application   sourcetype = WinEventLog:Application
>  17/01/2023               01/17/2023 04:41:30 PM
```

Figure 4

In this Example we will find Login Failures that has occurred in this system.
Note: For reference 4 times an incorrect password was used

6. Search for :
   host:ADITYADELLG3 EventCode=4625

We get 4 Events as shown below



New Search

```
host=ADITYADELLG3 EventCode=4625
```

✓ 4 events (16/01/2023 15:30:00.000 to 17/01/2023 15:30:11.000)   No Event Sampling ▾

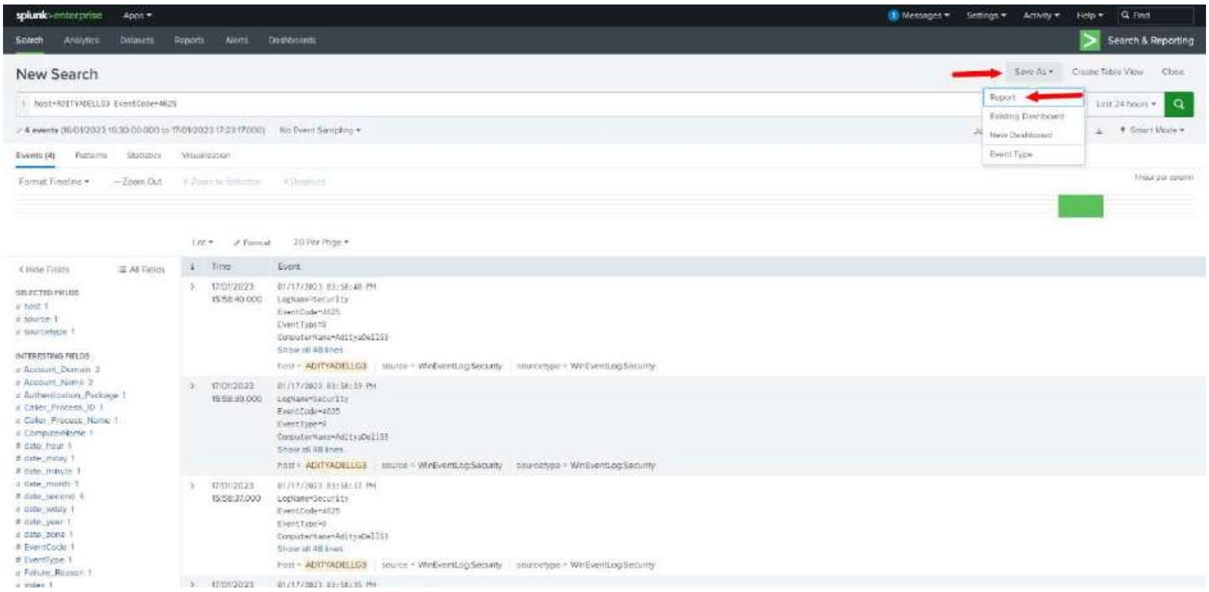
```
17/01/2023 15:58:40.000   01/17/2023 03:58:40 PM
                          LogName=Security
                          EventCode=4625
                          EventType=0
                          ComputerName=AdityaDellG3
                          Show all 48 lines
                          host = ADITYADELLG3   source = WinEventLog:Security   sourcetype = WinEventLog:Security
17/01/2023 15:58:39.000   01/17/2023 03:58:39 PM
                          LogName=Security
                          EventCode=4625
                          EventType=0
                          ComputerName=AdityaDellG3
                          Show all 48 lines
                          host = ADITYADELLG3   source = WinEventLog:Security   sourcetype = WinEventLog:Security
17/01/2023 15:58:37.000   01/17/2023 03:58:37 PM
                          LogName=Security
                          EventCode=4625
                          EventType=0
                          ComputerName=AdityaDellG3
                          Show all 48 lines
                          host = ADITYADELLG3   source = WinEventLog:Security   sourcetype = WinEventLog:Security
17/01/2023 15:58:35.000   01/17/2023 03:58:35 PM
                          LogName=Security
                          EventCode=4625
                          EventType=0
                          ComputerName=AdityaDellG3
                          Show all 48 lines
                          host = ADITYADELLG3   source = WinEventLog:Security   sourcetype = WinEventLog:Security
```

Figure 5

Note: Event Code 4625
https://docs.splunk.com/Documentation/SplunkLight/7.3.6/Examples/Reportonfailedloginattempts

The same is mentioned in the above section.

7. A report can be generated on the same. Click on Save As > Report



New Search

```
host=ADITYADELLG3 EventCode=4625
```

✓ 4 events (16/01/2023 15:30:00.000 to 17/01/2023 17:23:17.000) No Event Sampling

i	Time	Event

>	17/01/2023
	15:58:40.000
		01/17/2023 03:58:40 PM
		LogName=Security
		EventCode=4625
		EventType=0
		ComputerName=AdityaDell G3
		Show all 48 lines
		host = ADITYADELLG3 source = WinEventLog:Security sourcetype = WinEventLog:Security

>	17/01/2023
	15:58:39.000
		01/17/2023 03:58:39 PM
		LogName=Security
		EventCode=4625
		EventType=0
		ComputerName=AdityaDell G3
		Show all 48 lines
		host = ADITYADELLG3 source = WinEventLog:Security sourcetype = WinEventLog:Security

>	17/01/2023
	15:58:37.000
		01/17/2023 03:58:37 PM
		LogName=Security
		EventCode=4625
		EventType=0
		ComputerName=AdityaDell G3
		Show all 48 lines
		host = ADITYADELLG3 source = WinEventLog:Security sourcetype = WinEventLog:Security

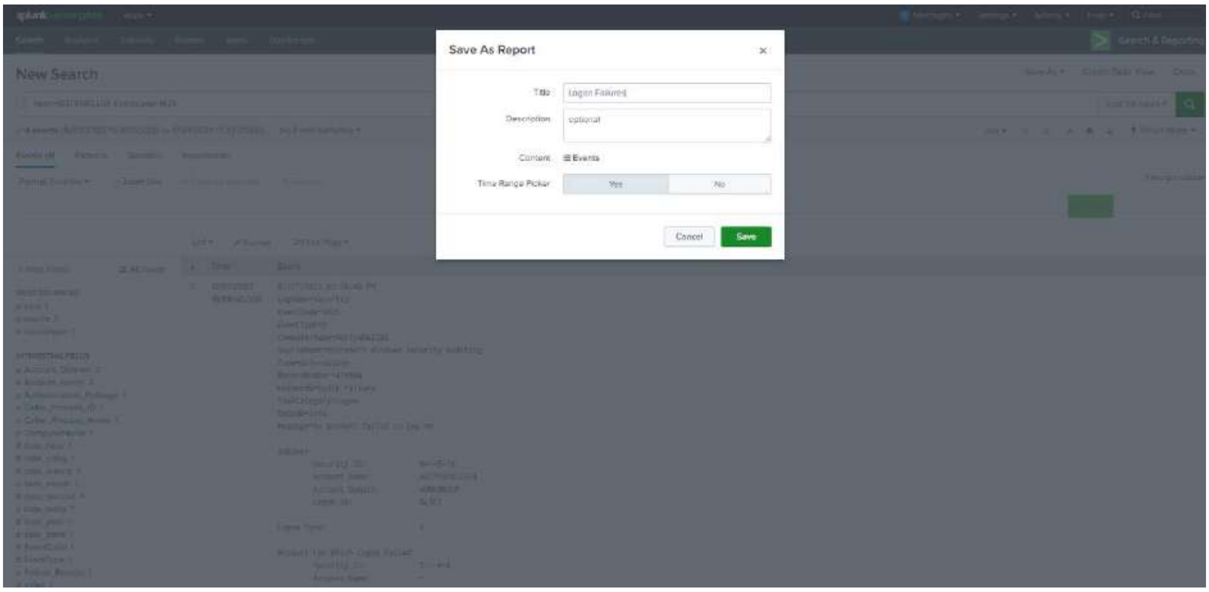
>	17/01/2023	01/17/2023 03:58:35 PM

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a Account_Domain 2
a Account_Name 2
a Authentication_Package 1
a Caller_Process_ID 1
a Caller_Process_Name 1
a ComputerName 1
# date_hour 1
# date_mday 1
# date_minute 1
a date_month 1
# date_second 4
a date_wday 1
# date_year 1
a date_zone 1
EventCode 1
EventType 1
a Failure_Reason 1
a index 1

Figure 6

8. Name is Appropriately. In this case we have named it as “Logon Failures”



Title: Logon Failures

Description: optional

Content: Events

Time Range Picker: Yes No

Figure 7

Save the Files as per the requirement

PDF: Accessible documents that are "Read-Only" on computers, laptops, tablets, and mobile phones. Most web browsers can now display PDF files without the requirement for a PDF viewer to be set up on your computer.

JSON: Using human-readable typefaces, JSON (JavaScript Object Notation) stores and transmits data items made up of attribute-value combinations and ranges. JSON is a well-established standardised data type (or other serializable values).

CSV: A text format called a CSV (Comma-separated Values) document uses commas to separate variables. There is an information set associated with each entry in the document. Every document has multiple sections that are separated by commas. This data type's name derives from the fact that it employs a period to demarcate sections. Statistical data, both quantitative and textual, is typically recorded in a CSV format as simple text, with the precise number of sections on each line.

XML: The XML format is perfect for processing complex information because it fully supports nested data types. Additionally, it is very human-understandable. Almost all browsers come with built-in XML readers that let users study XML data. Since XML was the first ever worldwide hierarchical data structure, a number of APIs support converting XML data files into objects in regional programming languages.

The below two pages are the splunk report generated in a pdf format.

Logon Failures

Time	Event
2023-01-17T15:58:40+0530	01/17/2023 03:58:40 PM LogName=Security EventCode=4625 EventType=0 ComputerName=AdityaDellG3 SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=419604 Keywords=Audit Failure TaskCategory=Logon OpCode=Info Message=An account failed to log on. Subject: Security ID:S-1-5-18 Account Name:ADITYADELLG3$ Account Domain:WORKGROUP Logon ID:0x3E7 Logon Type:2 Account For Which Logon Failed: Security ID:S-1-0-0 Account Name:- Account Domain:- Failure Information: Failure Reason:An Error occured during Logon. Status:0xC000006D Sub Status:0xC0000380 Process Information: Caller Process ID:0x6dc Caller Process Name:C:\Windows\System32\svchost.exe Network Information: Workstation Name:- Source Network Address:127.0.0.1 Source Port:0 Detailed Authentication Information: Logon Process:User32 Authentication Package:Negotiate Transited Services:- Package Name (NTLM only):- Key Length:0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
2023-01-17T15:58:39+0530	01/17/2023 03:58:39 PM LogName=Security EventCode=4625 EventType=0 ComputerName=AdityaDellG3 SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=419601 Keywords=Audit Failure TaskCategory=Logon OpCode=Info Message=An account failed to log on. Subject: Security ID:S-1-5-18 Account Name:ADITYADELLG3$ Account Domain:WORKGROUP Logon ID:0x3E7 Logon Type:2 Account For Which Logon Failed: Security ID:S-1-0-0 Account Name:- Account Domain:- Failure Information: Failure Reason:An Error occured during Logon. Status:0xC000006D Sub Status:0xC0000380 Process Information: Caller Process ID:0x6dc Caller Process Name:C:\Windows\System32\svchost.exe Network Information: Workstation Name:- Source Network Address:127.0.0.1 Source Port:0 Detailed Authentication Information: Logon Process:User32 Authentication Package:Negotiate Transited Services:- Package Name (NTLM only):- Key Length:0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
2023-01-17T15:58:37+0530	01/17/2023 03:58:37 PM LogName=Security EventCode=4625 EventType=0 ComputerName=AdityaDellG3 SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=419598 Keywords=Audit Failure TaskCategory=Logon OpCode=Info Message=An account failed to log on. Subject: Security ID:S-1-5-18 Account Name:ADITYADELLG3$ Account Domain:WORKGROUP Logon ID:0x3E7 Logon Type:2 Account For Which Logon Failed: Security ID:S-1-0-0 Account Name:- Account Domain:- Failure Information: Failure Reason:An Error occured during Logon. Status:0xC000006D Sub Status:0xC0000380 Process Information: Caller Process ID:0x6dc Caller Process Name:C:\Windows\System32\svchost.exe Network Information: Workstation Name:- Source Network Address:127.0.0.1 Source Port:0 Detailed Authentication Information: Logon Process:User32 Authentication Package:Negotiate Transited Services:- Package Name (NTLM only):- Key Length:0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

Time	Event
2023-01-17T15:58:35+0530	01/17/2023 03:58:35 PM LogName=Security EventCode=4625 EventType=0 ComputerName=AdityaDellG3 SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=419595 Keywords=Audit Failure TaskCategory=Logon OpCode=Info Message=An account failed to log on. Subject: Security ID:S-1-5-18 Account Name:ADITYADELLG3$ Account Domain:WORKGROUP Logon ID:0x3E7 Logon Type:2 Account For Which Logon Failed: Security ID:S-1-0-0 Account Name:- Account Domain:- Failure Information: Failure Reason:An Error occured during Logon. Status:0xC000006D Sub Status:0xC0000380 Process Information: Caller Process ID:0x6dc Caller Process Name:C:\Windows\System32\svchost.exe Network Information: Workstation Name:- Source Network Address:127.0.0.1 Source Port:0 Detailed Authentication Information: Logon Process:User32 Authentication Package:Negotiate Transited Services:- Package Name (NTLM only):- Key Length:0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

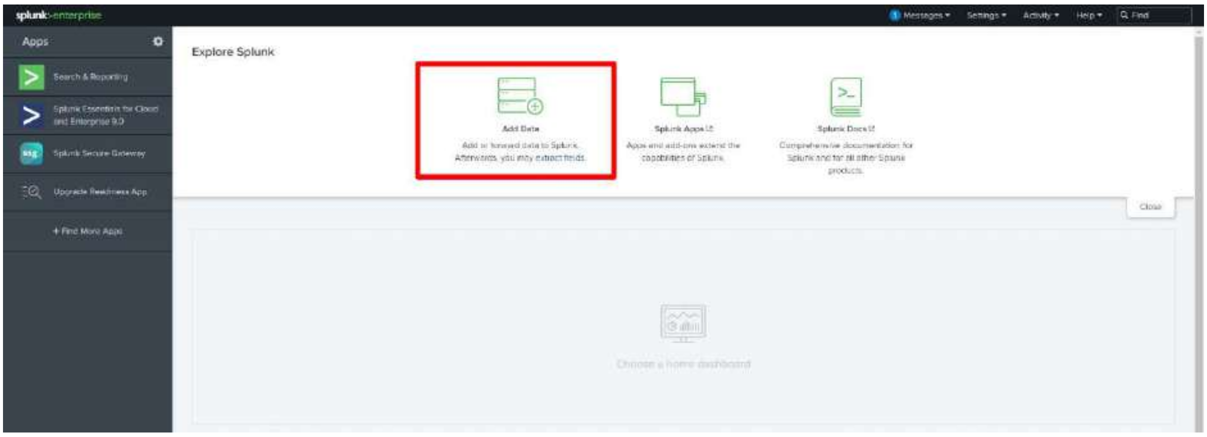
EXAMPLE 2:

THE FOLLOWING IS A CHALLENGE FROM HTTPS://BLUETEAMLABS.ONLINE/

Log Analysis – Compromised WordPress (to analyse log files)

One of our WordPress sites has been compromised but we're currently unsure how. The primary hypothesis is that an installed plugin was vulnerable to a remote code execution vulnerability which gave an attacker access to the underlying operating system of the server.

1. Download the access.log file and upload it to splunk
2. Click on add data



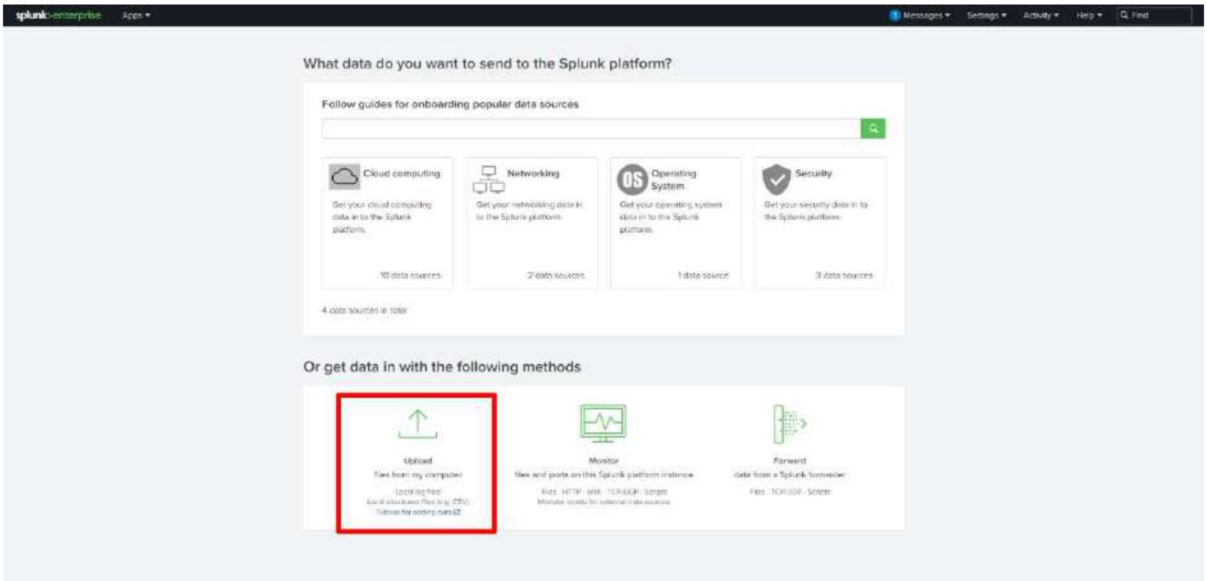
Add or forward data to Splunk. Afterwards, you may extract fields.

Apps and add-ons extend the capabilities of Splunk.

Comprehensive documentation for Splunk and for all other Splunk products.

Figure 1

3. Upload files for computer



What data do you want to send to the Splunk platform?

Follow guides for onboarding popular data sources

Get your cloud computing data in to the Splunk platform.

Get your networking data in to the Splunk platform.

Get your operating system data in to the Splunk platform.

Get your security data in to the Splunk platform.

4 data sources in total

Or get data in with the following methods

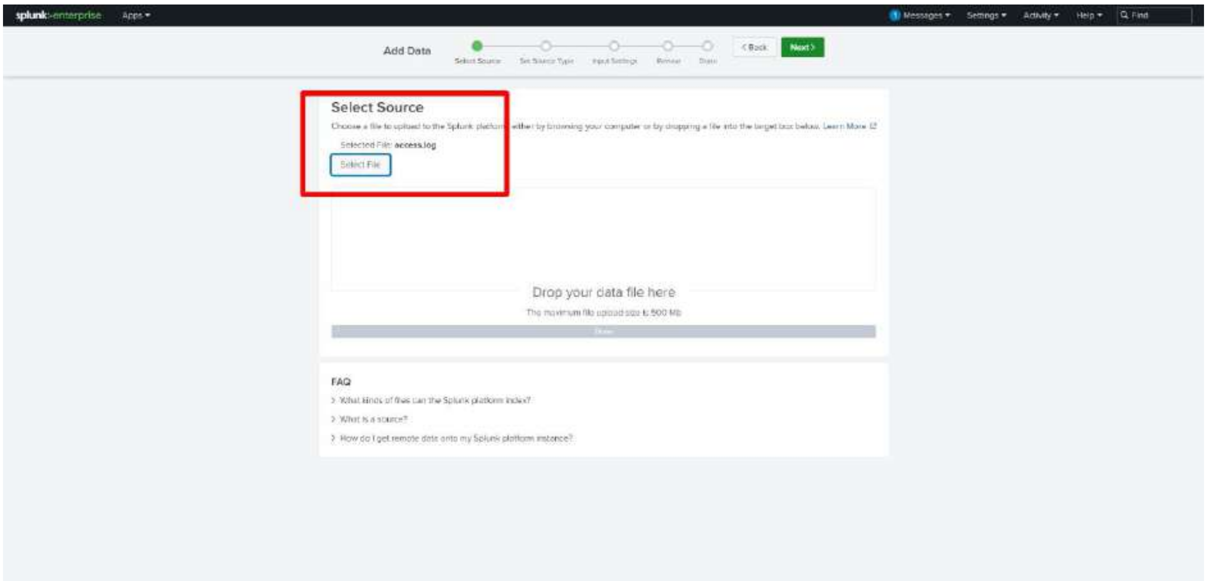
files from my computer
Local log files
Local structured files (e.g. CSV)
Tutorial for adding data

files and ports on this Splunk platform instance
Files · HTTP · WMI · TCP/UDP · Scripts
Modular inputs for external data sources

data from a Splunk forwarder
Files · TCP/UDP · Scripts

Figure 2

4. Upload the file by: Select file button or drop the file in the given area.



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: **access.log**

Select File

Drop your data file here

The maximum file upload size is 500 Mb

FAQ

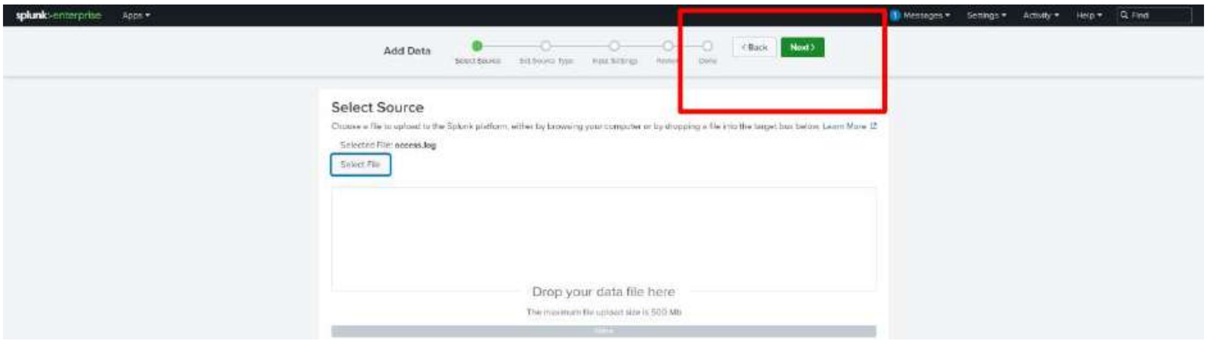
> What kinds of files can the Splunk platform index?

> What is a source?

> How do I get remote data onto my Splunk platform instance?

Figure 3

5. Click on Next



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: **access.log**

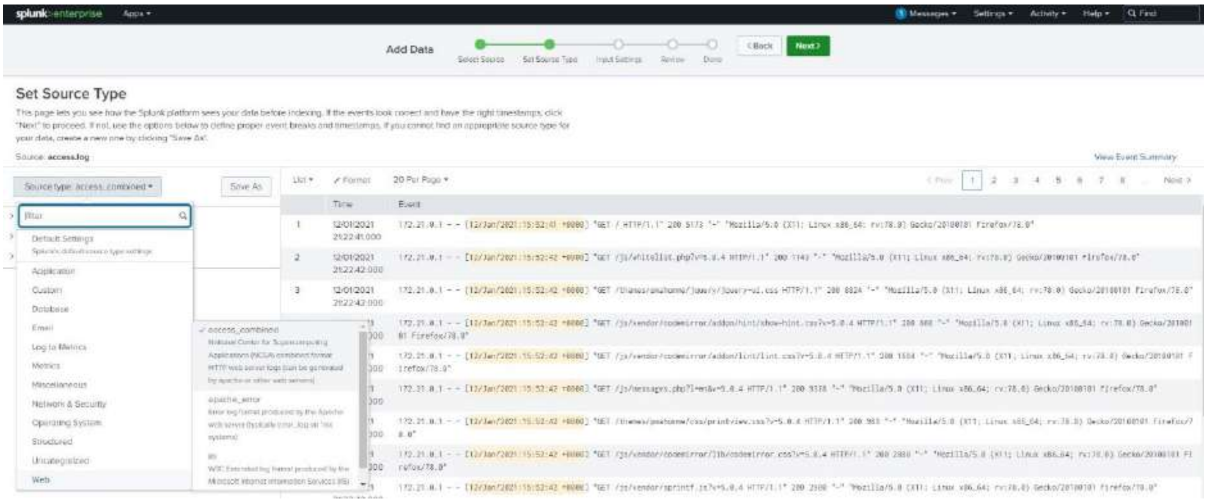
Select File

Drop your data file here

The maximum file upload size is 500 Mb

Figure 4

6. Set Source Type: Splunk automatically has selected this file as : access_combined. If required we can manually select as per the file source.



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: **access.log**

Source type: access_combined ▾

✓ access_combined
National Center for Supercomputing Applications (NCSA) combined format HTTP web server logs (can be generated by apache or other web servers)

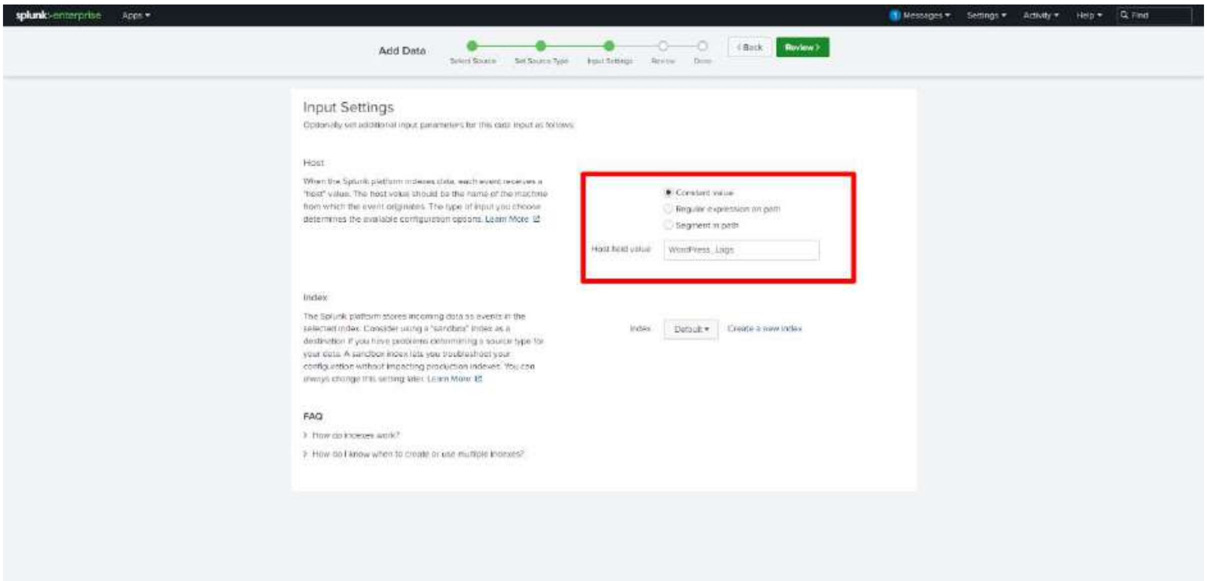
apache_error
Error log format produced by the Apache web server (typically error_log on *nix systems)

iis
W3C Extended log format produced by the Microsoft Internet Information Services (IIS)

	Time	Event
1	12/01/2021 21:22:41.000	172.21.0.1 - - [12/Jan/2021:15:52:41 +0000] "GET / HTTP/1.1" 200 5173 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
2	12/01/2021 21:22:42.000	172.21.0.1 - - [12/Jan/2021:15:52:42 +0000] "GET /js/whitelist.php?v=5.0.4 HTTP/1.1" 200 1143 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
3	12/01/2021 21:22:42.000	172.21.0.1 - - [12/Jan/2021:15:52:42 +0000] "GET /themes/pmahomme/jquery/jquery-ui.css HTTP/1.1" 200 6824 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
[illegible]	[illegible]	172.21.0.1 - - [12/Jan/2021:15:52:42 +0000] "GET /js/vendor/codemirror/addon/hint/show-hint.css?v=5.0.4 HTTP/1.1" 200 668 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
[illegible]	[illegible]	172.21.0.1 - - [12/Jan/2021:15:52:42 +0000] "GET /js/vendor/codemirror/addon/lint/lint.css?v=5.0.4 HTTP/1.1" 200 1504 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
[illegible]	[illegible]	172.21.0.1 - - [12/Jan/2021:15:52:42 +0000] "GET /js/messages.php?l=en&v=5.0.4 HTTP/1.1" 200 3378 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
[illegible]	[illegible]	172.21.0.1 - - [12/Jan/2021:15:52:42 +0000] "GET /themes/pmahomme/css/printview.css?v=5.0.4 HTTP/1.1" 200 983 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
[illegible]	[illegible]	172.21.0.1 - - [12/Jan/2021:15:52:42 +0000] "GET /js/vendor/codemirror/lib/codemirror.css?v=5.0.4 HTTP/1.1" 200 2880 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
[illegible]	[illegible]	172.21.0.1 - - [12/Jan/2021:15:52:42 +0000] "GET /js/vendor/sprintf.js?v=5.0.4 HTTP/1.1" 200 2300 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"

Figure 5

Put the relevant Name in the host filed value: we have used WordPress_Logs



Input Settings

Optionally set additional input parameters for this data input as follows:

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More

● Constant value
○ Regular expression on path
○ Segment in path

Host field value: WordPress_Logs

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More

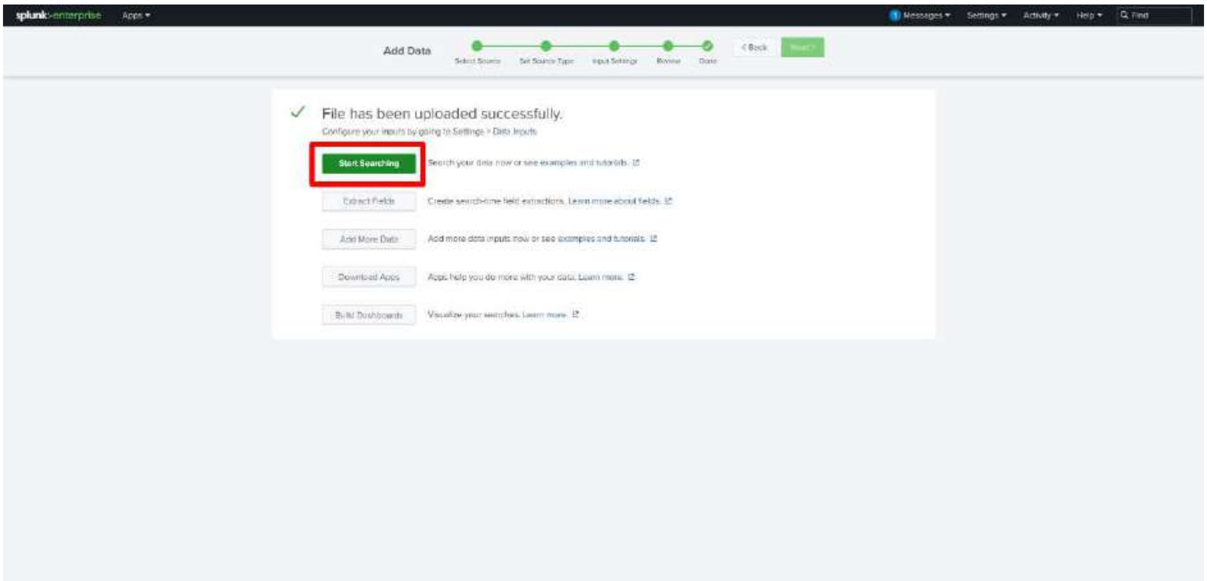
Index: Default ▾ Create a new index

FAQ

- How do indexes work?
- How do I know when to create or use multiple indexes?

Figure 6

7. Click on Start Searching



✓ 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.

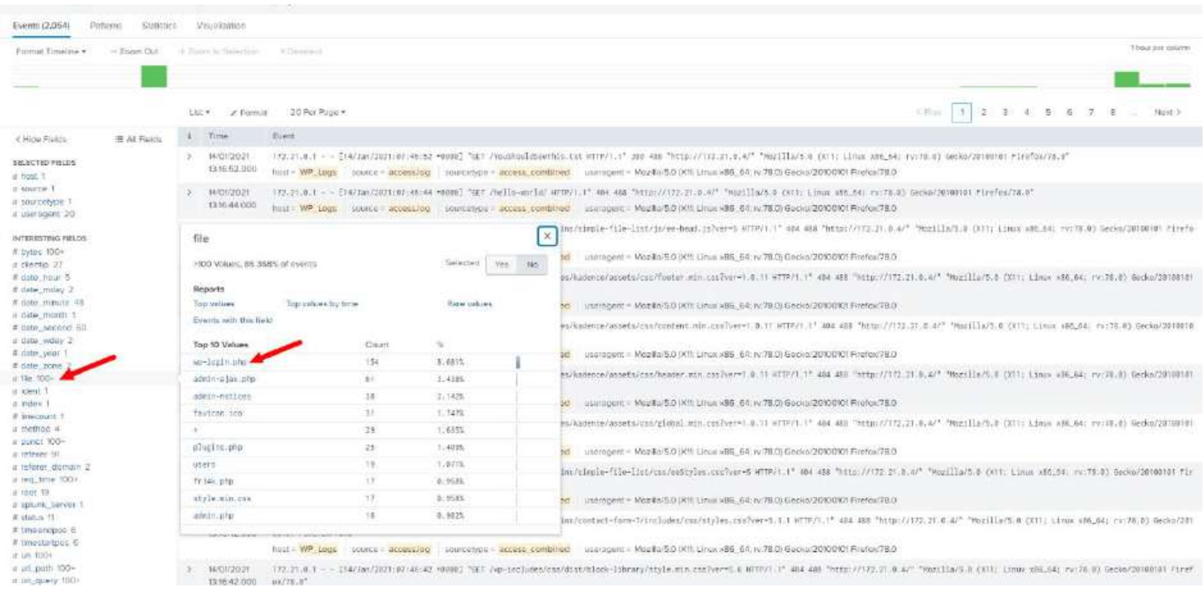
Build Dashboards — Visualize your searches. Learn more.

Figure 7

Q1: Identify the URI of the admin login panel that the attacker gained access to (include the token)

Solution.:

A. Select File> wp-login.php



file

>100 Values, 85.388% of events

Reports

Top values | Top values by time | Rare values

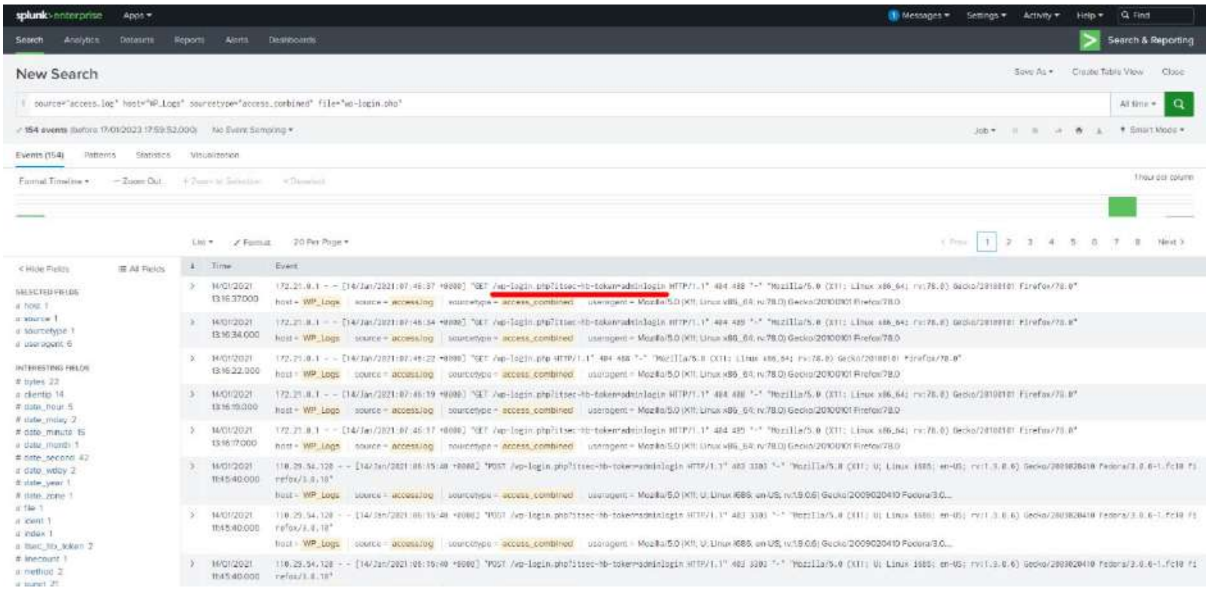
Events with this field

Top 10 Values	Count	%
wp-login.php	154	8.681%
admin-ajax.php	61	3.438%
admin-notices	38	2.142%
favicon.ico	31	1.747%
/	29	1.635%
plugins.php	25	1.409%
users	19	1.071%
fr34k.php	17	0.958%
style.min.css	17	0.958%
admin.php	16	0.902%

```
14/01/2021 13:16:52.000  172.21.0.1 - - [14/Jan/2021:07:46:52 +0000] "GET /youshouldseethis.txt HTTP/1.1" 200 488 "http://172.21.0.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
14/01/2021 13:16:44.000  172.21.0.1 - - [14/Jan/2021:07:46:44 +0000] "GET /hello-world/ HTTP/1.1" 404 488 "http://172.21.0.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
14/01/2021 13:16:42.000  172.21.0.1 - - [14/Jan/2021:07:46:42 +0000] "GET /wp-includes/css/dist/block-library/style.min.css?ver=5.6 HTTP/1.1" 404 488 "http://172.21.0.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
```

Figure 8

B. The uri and token is displayed



New Search

source="access.log" host="WP_Logs" sourcetype="access_combined" file="wp-login.php"

✓ 154 events (before 17/01/2023 17:59:52.000) No Event Sampling

Events (154)

```
14/01/2021 13:16:37.000  172.21.0.1 - - [14/Jan/2021:07:46:37 +0000] "GET /wp-login.php?itsec-hb-token=adminlogin HTTP/1.1" 404 488 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
14/01/2021 13:16:34.000  172.21.0.1 - - [14/Jan/2021:07:46:34 +0000] "GET /wp-login.php?itsec-hb-token=adminlogin HTTP/1.1" 404 489 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
14/01/2021 13:16:22.000  172.21.0.1 - - [14/Jan/2021:07:46:22 +0000] "GET /wp-login.php HTTP/1.1" 404 488 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
14/01/2021 13:16:19.000  172.21.0.1 - - [14/Jan/2021:07:46:19 +0000] "GET /wp-login.php?itsec-hb-token=adminlogin HTTP/1.1" 404 488 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
14/01/2021 13:16:17.000  172.21.0.1 - - [14/Jan/2021:07:46:17 +0000] "GET /wp-login.php?itsec-hb-token=adminlogin HTTP/1.1" 404 489 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
14/01/2021 11:45:40.000  110.29.54.120 - - [14/Jan/2021:06:15:40 +0000] "POST /wp-login.php?itsec-hb-token=adminlogin HTTP/1.1" 403 3303 "-" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.6) Gecko/2009020410 Fedora/3.0.6-1.fc10 Firefox/3.0.10"
14/01/2021 11:45:40.000  110.29.54.120 - - [14/Jan/2021:06:15:40 +0000] "POST /wp-login.php?itsec-hb-token=adminlogin HTTP/1.1" 403 3303 "-" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.6) Gecko/2009020410 Fedora/3.0.6-1.fc10 Firefox/3.0.10"
14/01/2021 11:45:40.000  110.29.54.120 - - [14/Jan/2021:06:15:40 +0000] "POST /wp-login.php?itsec-hb-token=adminlogin HTTP/1.1" 403 3303 "-" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.6) Gecko/2009020410 Fedora/3.0.6-1.fc10 Firefox/3.0.10"
```

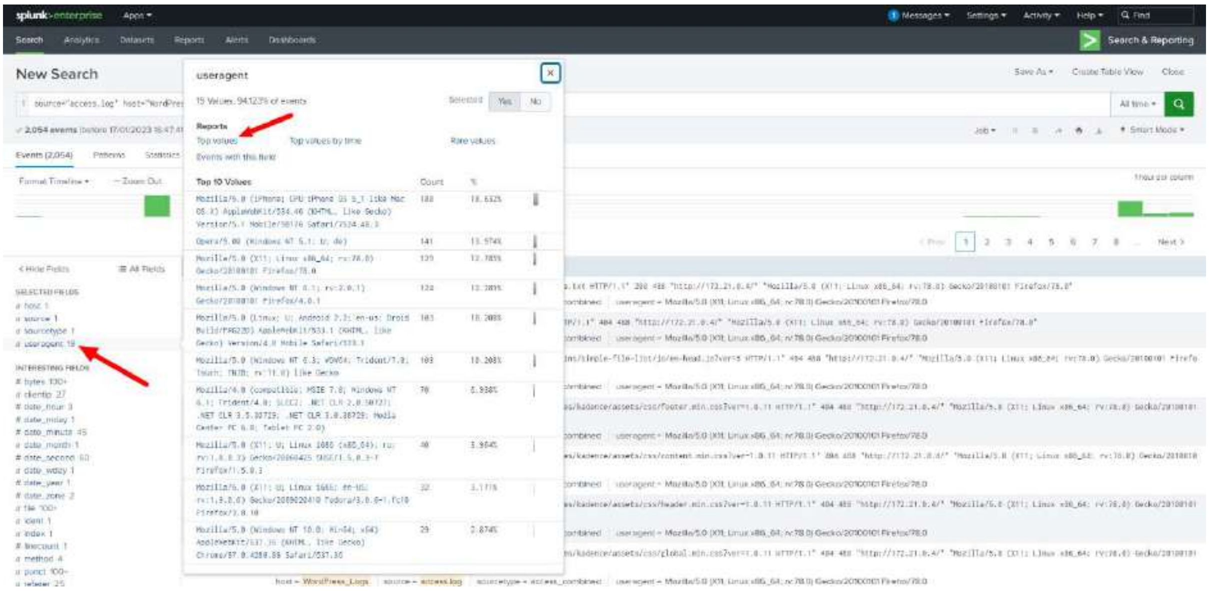
Figure 9

Answer: /wp-login.php?itsec-hb-token=adminlogin

Q2: Can you find two tools the attacker used?

Solution:

A. Select User Agents > Top Value



useragent

15 Values, 94.123% of events

Reports

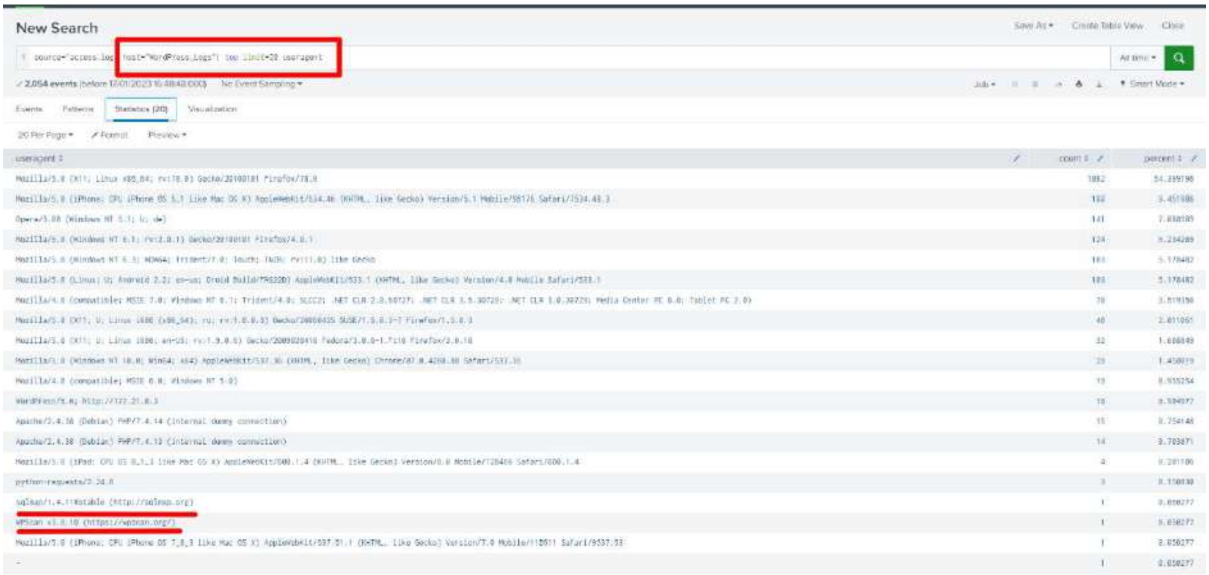
Top values   Top values by time   Rare values

Events with this field

Top 10 Values	Count	%
Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48.3	188	18.632%
Opera/9.80 (Windows NT 5.1; U; de)	141	13.974%
Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0	129	12.785%
Mozilla/5.0 (Windows NT 6.1; rv:2.0.1) Gecko/20100101 Firefox/4.0.1	124	12.289%
Mozilla/5.0 (Linux; U; Android 2.2; en-us; Droid Build/FRG22D) AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1	103	10.208%
Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; Touch; TNJB; rv:11.0) like Gecko	103	10.208%
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)	70	6.938%
Mozilla/5.0 (X11; U; Linux i686 (x86_64); ru; rv:1.8.0.3) Gecko/20060425 SUSE/1.5.0.3-7 Firefox/1.5.0.3	40	3.964%
Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.6) Gecko/2009020410 Fedora/3.0.6-1.fc10 Firefox/3.0.10	32	3.171%
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36	29	2.874%

Figure 10

B. At the bottom of the list we can see the user: sqlmap and WPScan



```
source="access.log" host="WordPress_Logs" | top limit=20 useragent
```

2,054 events (before 17/01/2023 16:48:48.000)   No Event Sampling

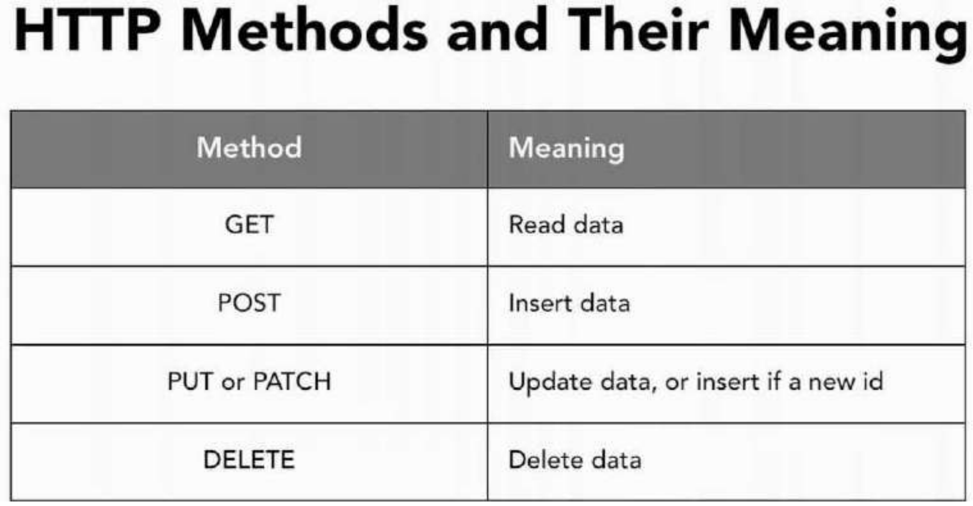
useragent	count	percent
Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0	1082	54.399198
Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48.3	112	5.451886
Opera/9.80 (Windows NT 5.1; U; de)	141	7.038389
Mozilla/5.0 (Windows NT 6.1; rv:2.0.1) Gecko/20100101 Firefox/4.0.1	124	6.234289
Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; Touch; TNJB; rv:11.0) like Gecko	103	5.178482
Mozilla/5.0 (Linux; U; Android 2.2; en-us; Droid Build/FRG22D) AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1	103	5.178482
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)	70	3.519358
Mozilla/5.0 (X11; U; Linux i686 (x86_64); ru; rv:1.8.0.3) Gecko/20060425 SUSE/1.5.0.3-7 Firefox/1.5.0.3	40	2.011061
Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.6) Gecko/2009020410 Fedora/3.0.6-1.fc10 Firefox/3.0.10	32	1.608849
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36	29	1.458019
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)	19	0.955254
WordPress/5.6; http://172.21.0.3	18	0.904977
Apache/2.4.38 (Debian) PHP/7.4.14 (internal dummy connection)	15	0.754148
Apache/2.4.38 (Debian) PHP/7.4.13 (internal dummy connection)	14	0.703871
Mozilla/5.0 (iPad; CPU OS 8_1_3 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12B466 Safari/600.1.4	4	0.201106
python-requests/2.24.0	3	0.150830
sqlmap/1.4.11#stable (http://sqlmap.org)	1	0.050277
WPScan v3.8.10 (https://wpscan.org/)	1	0.050277
Mozilla/5.0 (iPhone; CPU iPhone OS 7_0_3 like Mac OS X) AppleWebKit/537.51.1 (KHTML, like Gecko) Version/7.0 Mobile/11B511 Safari/9537.53	1	0.050277
-	1	0.050277

Figure 11

Answer: WPScan sqlmap

Q3: The attacker tried to exploit a vulnerability in ‘Contact Form 7’. What CVE was the plugin vulnerable to? (Do some research!)

Since the attacker has found some vulnerability we can assume we can get the data from the POST method

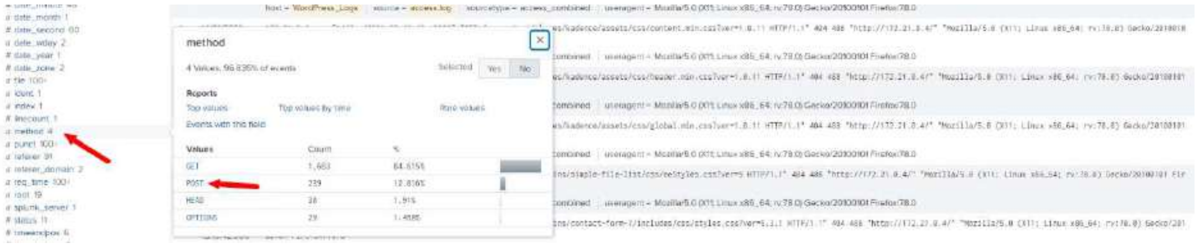


HTTP Methods and Their Meaning

Method	Meaning
GET	Read data
POST	Insert data
PUT or PATCH	Update data, or insert if a new id
DELETE	Delete data

Figure 12

A. In the Method > POST



method

4 Values, 96.836% of events

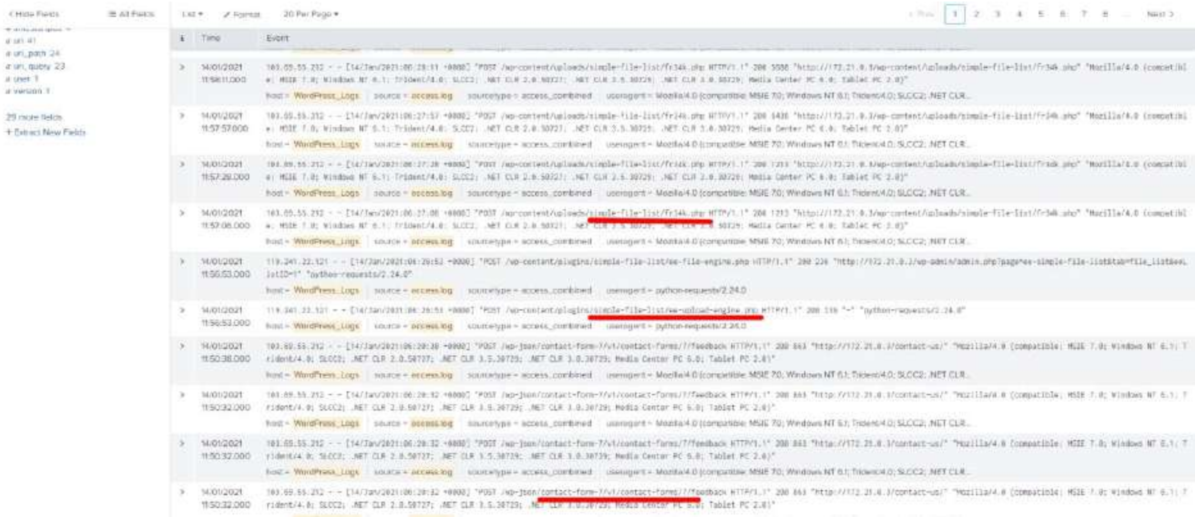
Selected: Yes No

Reports: Top values · Top values by time · Rare values · Events with this field

Values	Count	%
GET	1,663	84.615%
POST	239	12.816%
HEAD	38	1.91%
OPTIONS	29	1.458%

Figure 13

B. We can a list of files that could have been modified

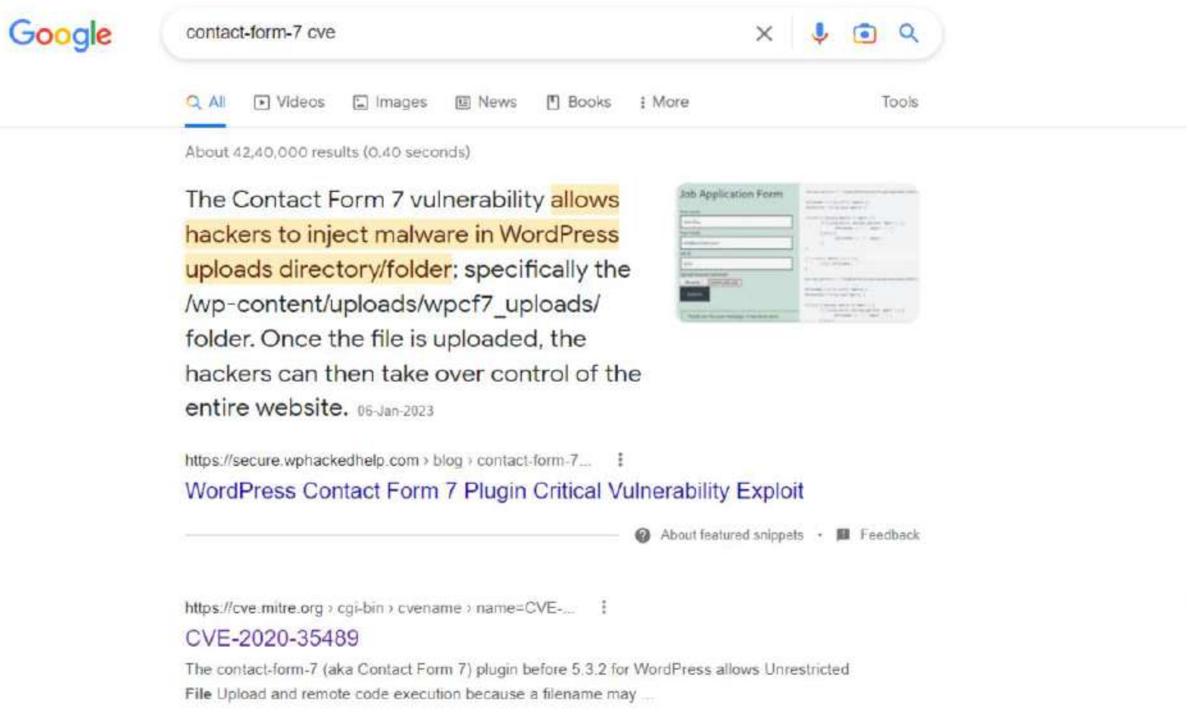


i	Time	Event
>	14/01/2021 11:58:11.000	103.69.55.212 - - [14/Jan/2021:06:28:11 +0000] "POST /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 5586 "http://172.21.0.3/wp-content/uploads/simple-file-list/fr34k.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)" host = WordPress_Logs · source = access.log · sourcetype = access_combined · useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...
>	14/01/2021 11:57:57.000	103.69.55.212 - - [14/Jan/2021:06:27:57 +0000] "POST /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 1436 "http://172.21.0.3/wp-content/uploads/simple-file-list/fr34k.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)" host = WordPress_Logs · source = access.log · sourcetype = access_combined · useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...
>	14/01/2021 11:57:28.000	103.69.55.212 - - [14/Jan/2021:06:27:28 +0000] "POST /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 1213 "http://172.21.0.3/wp-content/uploads/simple-file-list/fr34k.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)" host = WordPress_Logs · source = access.log · sourcetype = access_combined · useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...
>	14/01/2021 11:57:08.000	103.69.55.212 - - [14/Jan/2021:06:27:08 +0000] "POST /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 1213 "http://172.21.0.3/wp-content/uploads/simple-file-list/fr34k.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)" host = WordPress_Logs · source = access.log · sourcetype = access_combined · useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...
>	14/01/2021 11:56:53.000	119.241.22.121 - - [14/Jan/2021:06:26:53 +0000] "POST /wp-content/plugins/simple-file-list/ee-file-engine.php HTTP/1.1" 200 226 "http://172.21.0.3/wp-admin/admin.php?page=ee-simple-file-list&tab=file_list&eeListID=1" "python-requests/2.24.0" host = WordPress_Logs · source = access.log · sourcetype = access_combined · useragent = python-requests/2.24.0
>	14/01/2021 11:56:53.000	119.241.22.121 - - [14/Jan/2021:06:26:53 +0000] "POST /wp-content/plugins/simple-file-list/ee-upload-engine.php HTTP/1.1" 200 116 "-" "python-requests/2.24.0" host = WordPress_Logs · source = access.log · sourcetype = access_combined · useragent = python-requests/2.24.0
>	14/01/2021 11:50:38.000	103.69.55.212 - - [14/Jan/2021:06:20:38 +0000] "POST /wp-json/contact-form-7/v1/contact-forms/7/feedback HTTP/1.1" 200 663 "http://172.21.0.3/contact-us/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)" host = WordPress_Logs · source = access.log · sourcetype = access_combined · useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...
>	14/01/2021 11:50:32.000	103.69.55.212 - - [14/Jan/2021:06:20:32 +0000] "POST /wp-json/contact-form-7/v1/contact-forms/7/feedback HTTP/1.1" 200 663 "http://172.21.0.3/contact-us/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)" host = WordPress_Logs · source = access.log · sourcetype = access_combined · useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...
>	14/01/2021 11:50:32.000	103.69.55.212 - - [14/Jan/2021:06:20:32 +0000] "POST /wp-json/contact-form-7/v1/contact-forms/7/feedback HTTP/1.1" 200 663 "http://172.21.0.3/contact-us/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)" host = WordPress_Logs · source = access.log · sourcetype = access_combined · useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...
>	14/01/2021 11:50:32.000	103.69.55.212 - - [14/Jan/2021:06:20:32 +0000] "POST /wp-json/contact-form-7/v1/contact-forms/7/feedback HTTP/1.1" 200 663 "http://172.21.0.3/contact-us/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"

Figure 14

C. As figure 21 and the time stamp on the left, the plugin: **contact form 7** has request

D. A quick search in google gives us:



contact-form-7 cve

About 42,40,000 results (0.40 seconds)

The Contact Form 7 vulnerability allows hackers to inject malware in WordPress uploads directory/folder; specifically the /wp-content/uploads/wpcf7_uploads/ folder. Once the file is uploaded, the hackers can then take over control of the entire website. 06-Jan-2023

https://secure.wphackedhelp.com › blog › contact-form-7...

WordPress Contact Form 7 Plugin Critical Vulnerability Exploit

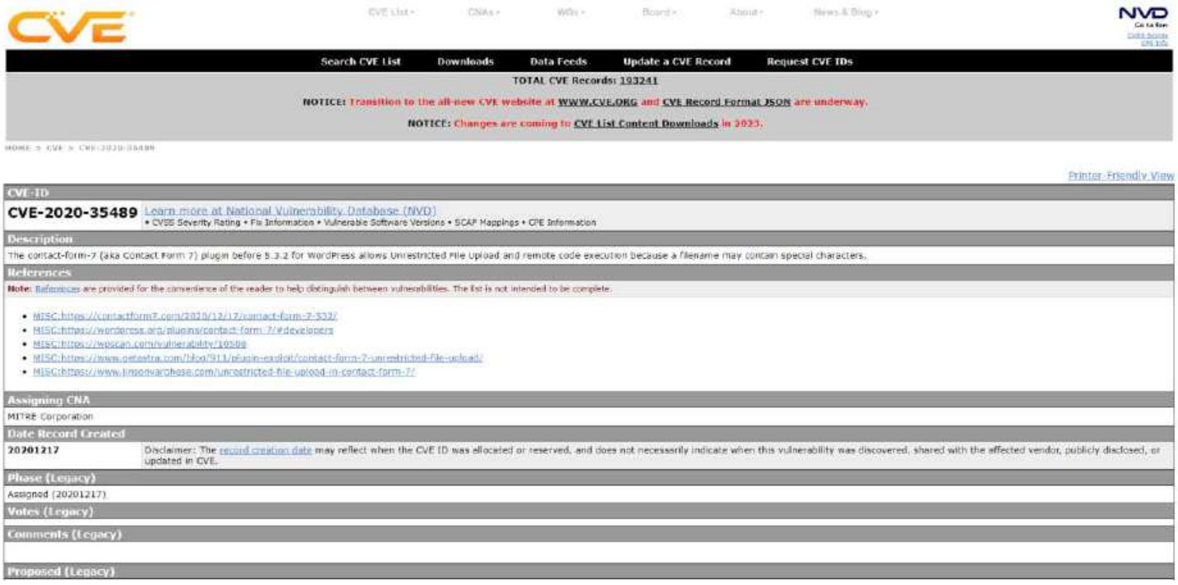
https://cve.mitre.org › cgi-bin › cvename › name=CVE-...

CVE-2020-35489

The contact-form-7 (aka Contact Form 7) plugin before 5.3.2 for WordPress allows Unrestricted File Upload and remote code execution because a filename may ...

Figure 15

E. And in the https://cve.mitre.org/ more details are found



TOTAL CVE Records: 193241

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.

NOTICE: Changes are coming to CVE List Content Downloads in 2023.

HOME > CVE > CVE-2020-35489

CVE-ID

CVE-2020-35489 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

The contact-form-7 (aka Contact Form 7) plugin before 5.3.2 for WordPress allows Unrestricted File Upload and remote code execution because a filename may contain special characters.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://contactform7.com/2020/12/17/contact-form-7-532/
- MISC:https://wordpress.org/plugins/contact-form-7/#developers
- MISC:https://wpscan.com/vulnerability/10508
- MISC:https://www.getastra.com/blog/911/plugin-exploit/contact-form-7-unrestricted-file-upload/
- MISC:https://www.jinsonvarghese.com/unrestricted-file-upload-in-contact-form-7/

Assigning CNA

MITRE Corporation

Date Record Created

20201217 Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20201217)

Votes (Legacy)

Comments (Legacy)

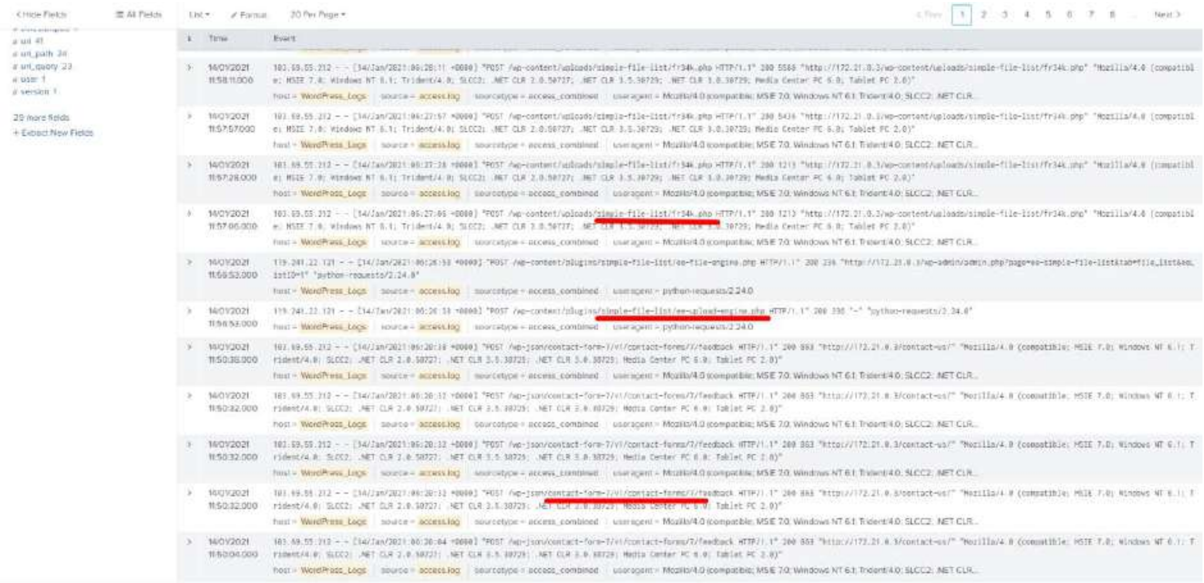
Proposed (Legacy)

Figure 16

Answer: CVE-2020-35489

Q4 : What plugin was exploited to get access?

In the screen shot taken form POST we can see the Plugin name



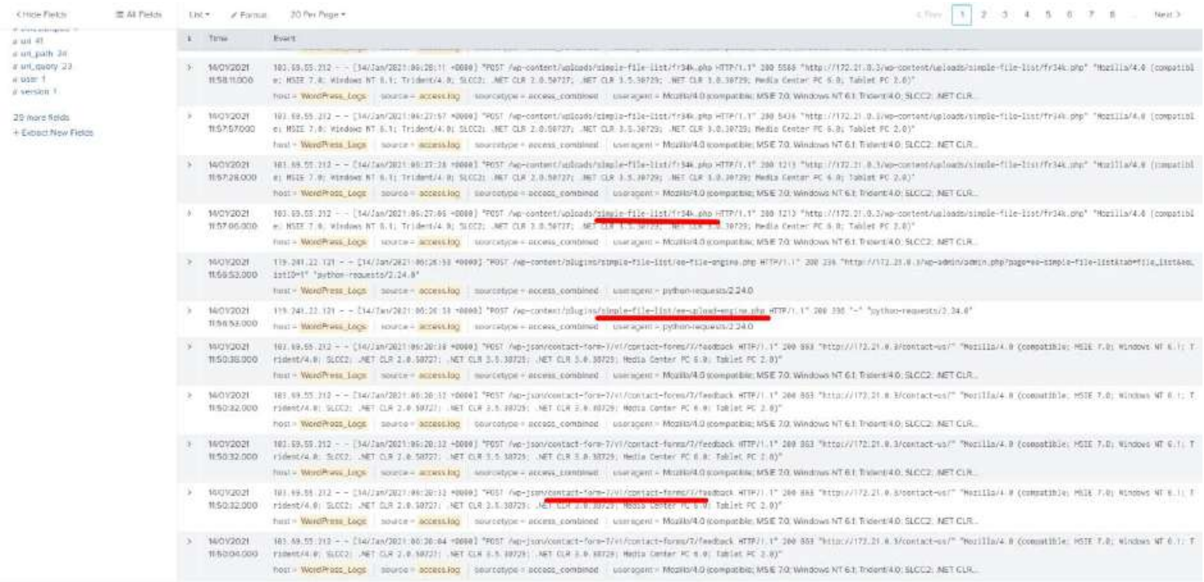
```
> 14/01/2021    103.69.55.212 - - [14/Jan/2021:06:28:11 +0000] "POST /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 5566 "http://172.21.0.3/wp-content/uploads/simple-file-list/fr34k.php" "Mozilla/4.0 (compatibl
  11:58:11.000  e; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
                host = WordPress_Logs   source = access.log   sourcetype = access_combined   useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...
> 14/01/2021    103.69.55.212 - - [14/Jan/2021:06:27:57 +0000] "POST /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 5436 "http://172.21.0.3/wp-content/uploads/simple-file-list/fr34k.php" "Mozilla/4.0 (compatibl
  11:57:57.000  e; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
                host = WordPress_Logs   source = access.log   sourcetype = access_combined   useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...
> 14/01/2021    103.69.55.212 - - [14/Jan/2021:06:27:28 +0000] "POST /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 1213 "http://172.21.0.3/wp-content/uploads/simple-file-list/fr34k.php" "Mozilla/4.0 (compatibl
  11:57:28.000  e; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
                host = WordPress_Logs   source = access.log   sourcetype = access_combined   useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...
> 14/01/2021    103.69.55.212 - - [14/Jan/2021:06:27:06 +0000] "POST /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 1213 "http://172.21.0.3/wp-content/uploads/simple-file-list/fr34k.php" "Mozilla/4.0 (compatibl
  11:57:06.000  e; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
                host = WordPress_Logs   source = access.log   sourcetype = access_combined   useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...
> 14/01/2021    119.241.22.121 - - [14/Jan/2021:06:26:53 +0000] "POST /wp-content/plugins/simple-file-list/ee-file-engine.php HTTP/1.1" 200 236 "http://172.21.0.3/wp-admin/admin.php?page=ee-simple-file-list&tab=file_list&eeL
  11:56:53.000  istID=1" "python-requests/2.24.0"
                host = WordPress_Logs   source = access.log   sourcetype = access_combined   useragent = python-requests/2.24.0
> 14/01/2021    119.241.22.121 - - [14/Jan/2021:06:26:33 +0000] "POST /wp-content/plugins/simple-file-list/ee-upload-engine.php HTTP/1.1" 200 336 "-" "python-requests/2.24.0"
  11:56:33.000  host = WordPress_Logs   source = access.log   sourcetype = access_combined   useragent = python-requests/2.24.0
> 14/01/2021    103.69.55.212 - - [14/Jan/2021:06:20:38 +0000] "POST /wp-json/contact-form-7/v1/contact-forms/7/feedback HTTP/1.1" 200 863 "http://172.21.0.3/contact-us/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; T
  11:50:38.000  rident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
                host = WordPress_Logs   source = access.log   sourcetype = access_combined   useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...
> 14/01/2021    103.69.55.212 - - [14/Jan/2021:06:20:32 +0000] "POST /wp-json/contact-form-7/v1/contact-forms/7/feedback HTTP/1.1" 200 863 "http://172.21.0.3/contact-us/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; T
  11:50:32.000  rident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
                host = WordPress_Logs   source = access.log   sourcetype = access_combined   useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...
> 14/01/2021    103.69.55.212 - - [14/Jan/2021:06:20:32 +0000] "POST /wp-json/contact-form-7/v1/contact-forms/7/feedback HTTP/1.1" 200 863 "http://172.21.0.3/contact-us/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; T
  11:50:32.000  rident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
                host = WordPress_Logs   source = access.log   sourcetype = access_combined   useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...
> 14/01/2021    103.69.55.212 - - [14/Jan/2021:06:20:32 +0000] "POST /wp-json/contact-form-7/v1/contact-forms/7/feedback HTTP/1.1" 200 863 "http://172.21.0.3/contact-us/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; T
  11:50:32.000  rident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
                host = WordPress_Logs   source = access.log   sourcetype = access_combined   useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...
> 14/01/2021    103.69.55.212 - - [14/Jan/2021:06:20:04 +0000] "POST /wp-json/contact-form-7/v1/contact-forms/7/feedback HTTP/1.1" 200 863 "http://172.21.0.3/contact-us/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; T
  11:50:04.000  rident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
                host = WordPress_Logs   source = access.log   sourcetype = access_combined   useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...
```

Figure 17

Answer: Simple File List 4.2.2

Q5: What is the name of the PHP web shell file?

In the Same screen shot we can see the php file



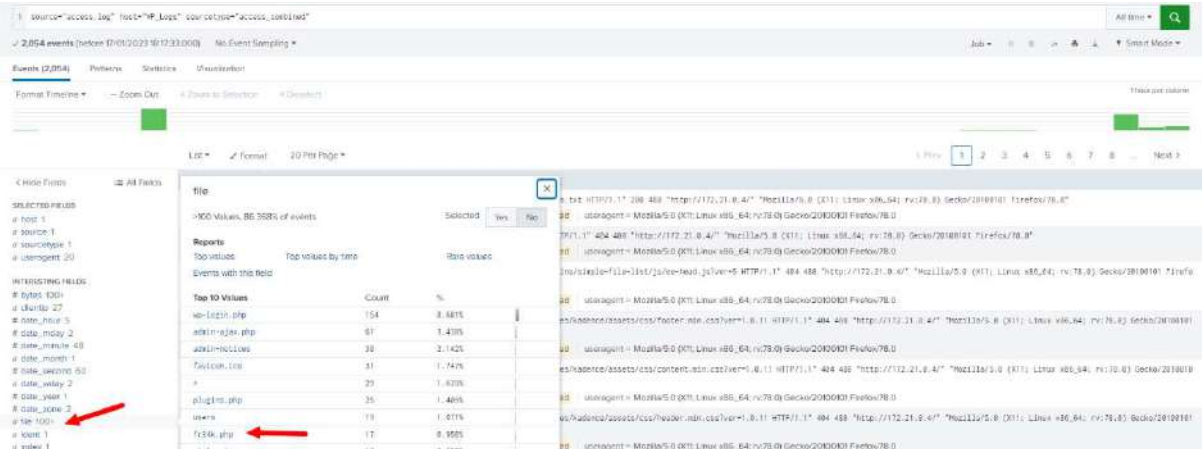
```
> 14/01/2021    103.69.55.212 - - [14/Jan/2021:06:28:11 +0000] "POST /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 5566 "http://172.21.0.3/wp-content/uploads/simple-file-list/fr34k.php" "Mozilla/4.0 (compatibl
  11:58:11.000  e; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
                host = WordPress_Logs   source = access.log   sourcetype = access_combined   useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...
> 14/01/2021    103.69.55.212 - - [14/Jan/2021:06:27:57 +0000] "POST /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 5436 "http://172.21.0.3/wp-content/uploads/simple-file-list/fr34k.php" "Mozilla/4.0 (compatibl
  11:57:57.000  e; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
                host = WordPress_Logs   source = access.log   sourcetype = access_combined   useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...
> 14/01/2021    103.69.55.212 - - [14/Jan/2021:06:27:28 +0000] "POST /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 1213 "http://172.21.0.3/wp-content/uploads/simple-file-list/fr34k.php" "Mozilla/4.0 (compatibl
  11:57:28.000  e; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
                host = WordPress_Logs   source = access.log   sourcetype = access_combined   useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...
> 14/01/2021    103.69.55.212 - - [14/Jan/2021:06:27:06 +0000] "POST /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 1213 "http://172.21.0.3/wp-content/uploads/simple-file-list/fr34k.php" "Mozilla/4.0 (compatibl
  11:57:06.000  e; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
                host = WordPress_Logs   source = access.log   sourcetype = access_combined   useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...
> 14/01/2021    119.241.22.121 - - [14/Jan/2021:06:26:53 +0000] "POST /wp-content/plugins/simple-file-list/ee-file-engine.php HTTP/1.1" 200 236 "http://172.21.0.3/wp-admin/admin.php?page=ee-simple-file-list&tab=file_list&eeL
  11:56:53.000  istID=1" "python-requests/2.24.0"
                host = WordPress_Logs   source = access.log   sourcetype = access_combined   useragent = python-requests/2.24.0
> 14/01/2021    119.241.22.121 - - [14/Jan/2021:06:26:33 +0000] "POST /wp-content/plugins/simple-file-list/ee-upload-engine.php HTTP/1.1" 200 336 "-" "python-requests/2.24.0"
  11:56:33.000  host = WordPress_Logs   source = access.log   sourcetype = access_combined   useragent = python-requests/2.24.0
> 14/01/2021    103.69.55.212 - - [14/Jan/2021:06:20:38 +0000] "POST /wp-json/contact-form-7/v1/contact-forms/7/feedback HTTP/1.1" 200 863 "http://172.21.0.3/contact-us/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; T
  11:50:38.000  rident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
                host = WordPress_Logs   source = access.log   sourcetype = access_combined   useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...
> 14/01/2021    103.69.55.212 - - [14/Jan/2021:06:20:32 +0000] "POST /wp-json/contact-form-7/v1/contact-forms/7/feedback HTTP/1.1" 200 863 "http://172.21.0.3/contact-us/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; T
  11:50:32.000  rident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
                host = WordPress_Logs   source = access.log   sourcetype = access_combined   useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...
> 14/01/2021    103.69.55.212 - - [14/Jan/2021:06:20:32 +0000] "POST /wp-json/contact-form-7/v1/contact-forms/7/feedback HTTP/1.1" 200 863 "http://172.21.0.3/contact-us/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; T
  11:50:32.000  rident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
                host = WordPress_Logs   source = access.log   sourcetype = access_combined   useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...
> 14/01/2021    103.69.55.212 - - [14/Jan/2021:06:20:32 +0000] "POST /wp-json/contact-form-7/v1/contact-forms/7/feedback HTTP/1.1" 200 863 "http://172.21.0.3/contact-us/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; T
  11:50:32.000  rident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
                host = WordPress_Logs   source = access.log   sourcetype = access_combined   useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...
> 14/01/2021    103.69.55.212 - - [14/Jan/2021:06:20:04 +0000] "POST /wp-json/contact-form-7/v1/contact-forms/7/feedback HTTP/1.1" 200 863 "http://172.21.0.3/contact-us/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; T
  11:50:04.000  rident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
                host = WordPress_Logs   source = access.log   sourcetype = access_combined   useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...
```

Figure 18

Answer: Fr34k.php

Q6: What was the HTTP response code provided when the web shell was accessed for the final time?

A. Click on File > Fr34k.php



```
source="access.log" host="WP_Logs" sourcetype="access_combined"
✓ 2,054 events (before 17/01/2023 18:12:33.000)   No Event Sampling ▾
```

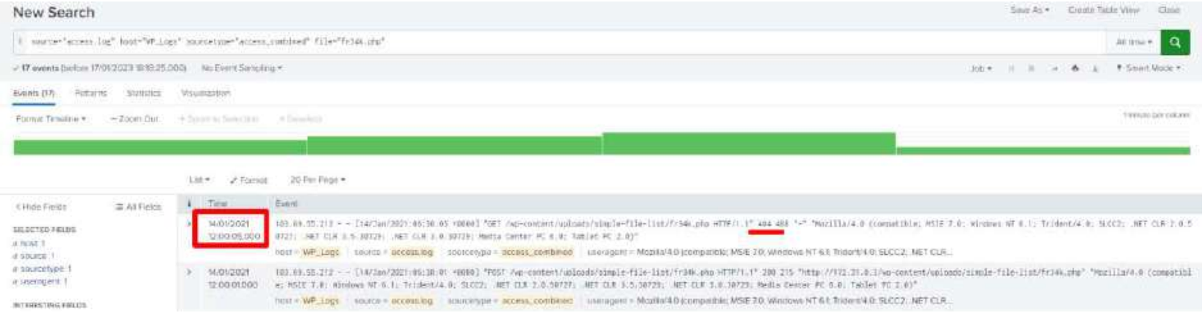
file

>100 Values, 86.358% of events

Top 10 Values	Count	%
wp-login.php	154	8.681%
admin-ajax.php	61	3.437%
admin-notices	38	2.142%
favicon.ico	31	1.747%
*	29	1.634%
plugins.php	26	1.465%
users	19	1.071%
fr34k.php	17	0.958%

Figure 19

B. We get the following. The Final time was 14/01/2021 12:00:05.000



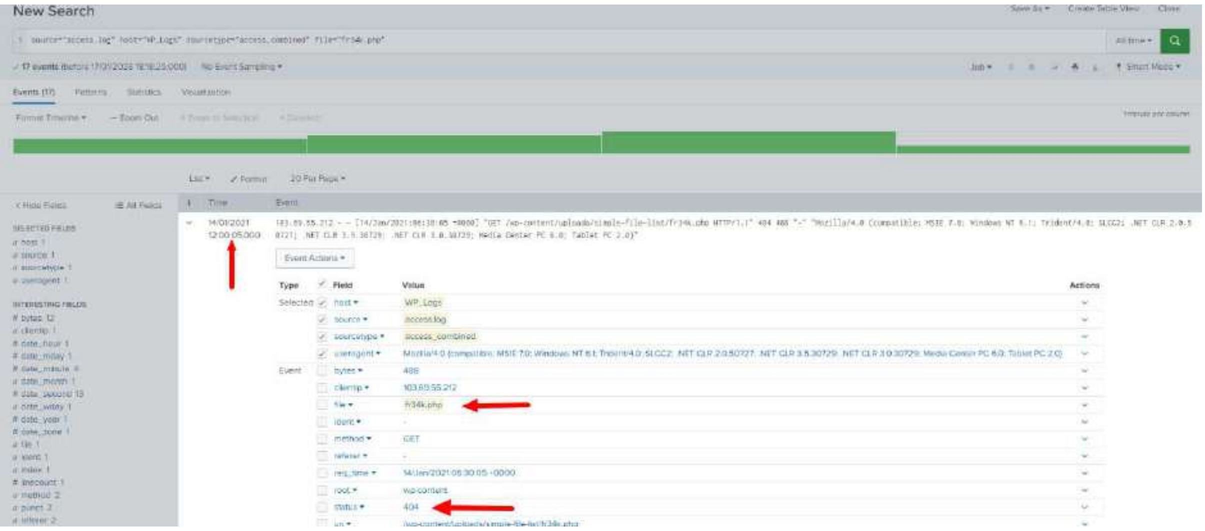
```
source="access.log" host="WP_Logs" sourcetype="access_combined" file="fr34k.php"
✓ 17 events (before 17/01/2023 18:18:25.000)   No Event Sampling ▾
```

```
14/01/2021   103.69.55.212 - - [14/Jan/2021:06:30:05 +0000] "GET /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 404 488 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.5
12:00:05.000 0727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
             host = WP_Logs   source = access.log   sourcetype = access_combined   useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...

14/01/2021   103.69.55.212 - - [14/Jan/2021:06:30:01 +0000] "POST /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 215 "http://172.21.0.3/wp-content/uploads/simple-file-list/fr34k.php" "Mozilla/4.0 (compatibl
12:00:01.000 e; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
             host = WP_Logs   source = access.log   sourcetype = access_combined   useragent = Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR...
```

Figure 20

C. When we expand we get the status code



```
14/01/2021   103.69.55.212 - - [14/Jan/2021:06:30:05 +0000] "GET /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 404 488 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.5
12:00:05.000 0727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
```

Type		Field	Value
Selected	☑	host	WP_Logs
	☑	source	access.log
	☑	sourcetype	access_combined
	☑	useragent	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Event	□	bytes	488
	□	clientip	103.69.55.212
	□	file	fr34k.php
	□	ident	-
	□	method	GET
	□	referer	-
	□	req_time	14/Jan/2021:06:30:05 -0000
	□	root	wp-content
	□	status	404
	□	uri	/wp-content/uploads/simple-file-list/fr34k.php

Figure 21

Answer: 404

Reference:

Soc
https://www.ibm.com/in-en/topics/security-operations-center

SIEM Tools
https://www.comparitech.com/net-admin/siem-tools/
https://www.softwaretestinghelp.com/siem-tools/

Splunk:
https://www.splunk.com/
https://www.splunk.com/en_us/sign-up.html?redirecturl=https://www.splunk.com/

Splunk Search and Reporting:
https://docs.splunk.com/Documentation/SplunkLight/7.3.6/Examples/Aboutthismanual

Report on failed login attempts

https://docs.splunk.com/Documentation/SplunkLight/7.3.6/Examples/Reportonfailedloginattempts
Search for Errors:
https://docs.splunk.com/Documentation/SplunkLight/7.3.6/Examples/Searchforerrors

BTLO
https://blueteamlabs.online/home/challenge/log-analysis-compromised-wordpress-ce000f5b59

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-35489