

# **PROJECT:** SECURITY OPERATION CENTER

By Aditya Sathyan | +91-8904597554 Red Team Academy - CICSA 2022

# TABLE OF CONTENTS

SI No	Content	Page No
1	Security Operations Center (SOC)	01
2	SIEM	01
3	Splunk Enterprise Security.	02
4	Add a new device to Splunk	03
5	Search and Reporting Examples	04
6	Example 1: Using Splunk to locate unsuccessful login attempts in a System	05
7	Generated Report- PDF	11
8	Example 2: The following is a challenge from blueteamlabs.online	13
9	Reference	22

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 securityrelated 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.: <u>https://www.splunk.com/en\_us/download.html</u>
- 2. Register in the Splunk Website. Note: Save the username, email address and password <a href="https://www.splunk.com/en\_us/sign-up.html">https://www.splunk.com/en\_us/sign-up.html</a>
- 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: <u>http://127.0.0.1:8000/</u>

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

splunk-enterprise		🚺 Messages *	Settings • Activity •	Help + Q Find
Apps O Explore Splunk				ĺ
Search & Reporting		5		
> Splank Expendeds for Good well Enterprise 8:0	Add Data Soluria Acco (2	Spinole Does 12		
Epilenk Sebure Goteway	Aon or torward data to Splans. Appe and add one extensione Alterwards, you may estated fields. capabilities of Splans.	Comprehensive documentation for Splank and for all other Splank		
SQ. Uppfada Roodmens App		(account)		day .
+ Find March Appl				
				,

Figure 1

3. Click on Data Summary

splunkt-enterprise Apps -	Messages + Sentings + Activity + Herp + Q. Find
Scench Analysius Dictasets Reports Allerta Dashbaanda	🚬 Search & Reporting
Search	
3 while south here	List24 mars + Q
No Evelt Sempting *	* Smurs Mode *
> Sourch History ()	
How to Search	Analyze Your Date with Table Views tiens
Byos on not builds with the search busines, or some to wom norm, or see your available data, see one of the following resources.	Table Views kit you propore data with out using SPL. First, see a point and click instruction to select data. Then, clean and astroform it for workylois in AnnyNics Workspace, Select), or Phont
Documentation (2) Tutute (2) Onto Summery	Enorm move 🖾 About Table Mews, or view and manage your Table Mews 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

plank						
And I setting the first the setting of	Data Summary				×	
Search	Houts (3) Socions (6)	Sourcet/pes-Kb				
(1) what have ( ) and (	Peter	9				Destroyer Q
distanting and the second seco	Law -		Course +	Last Harman #		A low trace
Construction 2	ADITYADELLG3	at =	202,910	17/01/2023 16:41:33.000		
( - MCMINITERED AND	Adm	al +	7.(546	064992923 09:43:40:000		
		al +	2.054	17/01/2023 16/42/21 000		
Hard to have the						
Two results in the second						-Over Still Val-
(Anternal Court) (Server of )						

Figure 3

5. This will show all the events in the system

splunk-enterprise	Appn.=				D Messages * Settings * Activity * Help * Q Find
Search Analytics					Search & Reporting
New Search					Save As + Cruster Table View Close
host-ADTIVADEUL	51				Last 24 bases + Q.
2,301 events (16/03)	202116:30 00.000	111-17/0	12023 1205 05	2000 No Event Simpling •	Job * II II # 8 🔟 🕈 Seiert Made *
Events (2,301) Put	tavni Skotučci	6 V	NGE22TON		
Formul Timeline *	-Zoom Out		are the Same sport	*Descire	these par potent
	1	_			
		i.e	· / Fami	20 Per Phys •	1 Prov 1 2 3 4 5 6 7 8 Next 3
CHide Fisials	I At Treids	4	Time	Event	
SELECTED PRIDE # host 1 # source 3 # sourcetype 3 INTERSTING RELDS # Account_Domain 7		3.	0/01/2023 15:41/01/000	6/17/2023 (BLR):31 PF Exection/10 Exection/300 Cooptentan-Microsofta Salawia & ADTMARCLICA Teach & TEACH & TEACH & TEACH & TEACH TEACH & TEACH	
o Account, Namis IB o ComputerNerse: 1 # date_hour 10 # date_moust 50 # date_moust 50 # date_second NB # date_second NB # date_second NB		3	1710112023 1641130.000	0/////2013 B4-Ct 10 PF Exercicity.com Exercicity.com Constanting.com Constanti	
# date_year 1 e date_year 1 # EventCode 100+ # EventCybe 4 e ndox 1 e Keywords 5 # Weecount 24		3	17/00/2023 18:41:20:000	BI/T/7023 49441158 FM Laphan-Malitation Exemitance Exemitance Comparisonae Additionality (1921) Since ADTARDELISS Incore - Windowstudy Application	
a imme ID 20		5	17/01/2023	87717/2023 881311-38 99	

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

splunk-enterprise Apps *			Stitlings * Activity * Hop * Q Find
Search Analytics Datasets	Reports Alerts	Ashbords	🚬 Search & Reportin
New Search			Sove As - Create Table View Close
) host-ADITVADELLG) EventLade-263			Load 20 boars - Q
- 4 events (18/01/2023 15:30:00,000 to 1	7/012023 15:30:11:000;	nu Event Sempting *	Job + H R A & Smart Mode +
Event (4) Paterios Statutos	Vecalizion		
Pormut Timeline • - Zoom Out	+ Yours to Splantar	+ Common	Time provident
	Liat • 🖉 Forma	20 Per Page *	
$\varepsilon$ inder Fields $$\equiv\Delta 0.7{\rm km}s$$	1. Time	Event	
SALACTED FILLIDS IN NUTURE 1 IN SUITORYDIE 1 INTERESTING PIECOS I ACCOUNT, DOMORY 2	> 17/01/2023 15:58 40:000	el (177)222 30:58 48 PF Lapter-Security Exectode-H25 Exectode-H25 Exectode-H25 Exectode-H26 Exec	type - WritEventug/Security
a Account, Norm 7 a Authenticition, Protoge 1 a Cather Process, John a Cather Process, John 1 Cather Process, Norme 1 4 ComputerName 1 8 Cather Joan 1 8 Cather, Joan 1 8 Cather, Joan 1	<ul> <li>170/2028</li> <li>18:58.39.000</li> </ul>	et (7)7/2021 85:081/09 PH LogBeen-Vecifi (1) EventStyle-VE(2) EventStyle-V	non - WieBvaritagSecurity
# bace_means # date_mounts 1 # date_second 4 # date_second 4 # date_second 7 # date_second 7 # date_second 7 # date_second 7 # bacest_baces 1 # bacest_baces 1 # bacest_baces 1	> 17042028 16:98 37000	el/77/2023 e)/50.57 PH Lappower/sourity Exectors-405 Konst Type=0 Comparing=-xiting/balleti Show of all most Konst - AD/TARTILGI Sames - VortherdingSecurity same	nppe = World vortiling decumy
<pre>v Fair vs_Pression 1 v Fair vs_Pression 1 v Fair vs_Pression 1 v Ksoveron 1 v Ksoveron 1 v (source 1 v)) vsource 1 v (source 1 v)) vsource 1 v (source 1 v)) vsource 1 v)</pre>	<ul> <li>1703/2023</li> <li>18:58:35.000</li> </ul>	ef/17/2023 e5.5k155 /h Leptanineo Ity Sectopa-Hoo Sectopa-Hoo Creater Haw-Aki (sec100) Down at 64 Heo Hoo - Abd Trabellog Hoo - Abd Trabellog Sector - WetVenLog Security - Source	ljare - WirBverik.agBecunty

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

splunk-enterprise Apen •			💷 Messages 👻 Settings 👻 Activity 👻 🖡	Help • 9 Find
Search Analytics Datasets	Raporti Allerti	Distroranti		Search & Reporting
New Search			Save AL* C	uate Table View Choic
host-ADITVADELLS) ExertCode+462	i		Report -	Last 24 hours + Q
4 events (6.012022 15.30 00.000 to 1	7012023172317000)	Ja Hew Destinated	🚊 🕴 Seier Voor -	
ventu (4) Puztarres Statuzica	Weakingcookin		Event Type	
formut Timeline Zoom Out	+ Provide Telestor	*Descript		Arrest pair point
NUCTED PRIDE	) 07/01/2023 15:58:40.000	0//17/2003 05:96-48-791 Laghane-Security		
	i.ez • Z Formal	20 Per Phoe •		
BUTCTID PRIDE	37/01/2023 15:58:40.000	81717/2003 82:56-48 PM ContractSecuritize		
hoit 1 source 1		EventCade=0.025 EventType10		
suurselvise 1		ConstantNan+Artityze103 Snow mi481net		
Account_Doman 3		host + ADITYADELLG3   source + WebsentLogSecurity   sourcesper + WebsentLogSecurity		
Account_Name 2 Authentication_Package 1	> 17/01/2023 15/58/39.000	8//17/2023 Binlar 19 PM LophawristorTty		
Caller, Process, JD 1 Caller, Process, Name 1		EventCode=4035 EventSysemi		
ComputerName 1 date hour 1		Cossular/Anne-Mittys/Dell/El Snow di Allines		
date_movy 1 date_movts 1		nost = AbitYADBLLG3 unuse = WinEventLogSacumy sourcesyle = WinEventLogSacumy		
date_month 1 date_second 4	> 17/002023 15/56/37/000	BF7/F7/903 Assistanty Met Lociane-Security		
tioto, swiny 1 nate_year 1		River(Code=#A)(3) EventTape=0		
date zone 1 EventCode 1		Computeritate=Rel tysCe1101 Since all 48 (new		
Dentifype 1		Host - ADITVADELIGI Source - WinEventLigSeculty sourcetype - WinEventLogSeculty		
wident 3	5 17002023	01/11/2021 03-50:05 PH		

#### Figure 6

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

denue a la conserva de la conserva d							
See See Terry 1			Save As Report		,		
New Search			-				
I American Statistics (Section 1977)		TRO	Logen Failured				
other designation of the local division of t	Description	optional			Carlo II. A CARLA MANAGAM		
Annald Parson Street			Content	I Events		·	
Sentimer desta			Time Range Picker	Yes	240	1	
					Concel		
Western Street			_				
Second State Hard and Art Hard A.         Second State Hard And Art Hard A.           Second State Hard And Art Hard And Art Hard A.         Second State Hard And Art Hard And Art Hard And Art Hard Art Hard Art Hard And Art Hard Art Hard And Art Hard Art Hard And Art Hard Art Hard And Art Hard Art Hard Art Hard Art Art Hard Art Hard Art Art Hard Art Hard Art Art Hard Art Hard Art Art Hard Art Art Hard Art Hard Art Hard Art Art Hart Art Hard Art Hard Art Art Hard Art Hard Art Hard Art Art Hard Art Hard Art Art Hard Art Hard Art Hard Art Art Hard Art Hard Art Hard Art Hard Art Art Hard Art Hard Art Hard Art Art Hart Har Art Hart Hard Art Art Hard Art Hard Art Art Hard Art Art							
A final start of a max start							

#### 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).

```
ADITYA SATHYAN
```

**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

Logon Failures	
Time	Event
2023-01-17T15:58:40+0530	017/74ZZ4 UZB-SSI PM LogName-Security
	EventOpe=-0
	ComputerName-AdaptaketSi Sourchame-Manot Windows security auding.
	ype-reformance RecordNather-1904
	Taska happn-kagon DeCode bijn
	Message-An account failed to tog on.
	Subject: Searby D2-16-18
	Account Name:ADTVADELLQ3 Account Name:ADTVADELLQ3
	Logon D0:387
	Logn Type2
	Account of which Lgon Fastet: Security D2-You D4
	Account Damain-
	False Morrado:
	Shate Account of a segment of the segmento of the segmento of the segment of the segment of the
	Pocess Infomation:
	Caler Process ID:06:do Caler Process Ima: C:WindowSystem22exchost.exe
	Network Momalian:
	Wokatian Nane:- Source Network (dates 127.0.1
	Source Port 0
	Detained Automatation Information: Logon Process Lond 2
	Autentiaaion Vaolaga Vaojaalo Taranida Salvosta
	· Podgi dramo (v LLA dray) Kogli dramo (v LLA dray)
	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 Service service, or a local process such as Winlogon.axe or Services.service.
	The Legon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (interact
	The Process Momation fields indicate which account and process on the system requested the logon.
	The Network Information fields induce 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. - Transiend services integrated services have participated in this population.
	- vacage name matcakes who as protocil was used among the NTLM potocia. - Key integrit inclusions the length of the generated assessine's private length of the generated assessine's privated assessine's privated assessine's privated asses
2023-01-17T15:58:39+0530	01/7/22/21058:29 PM
	EventOpe=402 EventOpe=0
	ComputerName-AdiyaDelIC3 SourceName-Morear Windows security auding.
	Type-Information Reconstrumter-4960
	Keywords-Audi Falue TaskChäpery-Logon
	QpCode-info Message-An account failed to log on.
	Subject
	Security User-SP (Security Security Sec
	Logen Dåd&7
	Logon Type 2
	Account for Which Logon Falset Security D3-10-0
	Account Names
	Falue Information:
	Falur Peason/H Error courced during Logon. Shark 3rc/C0000D
	Sub Status 0x0000080
	Process Information: Caller Process Dubated
	Caller Process Name D:Windows/System 32exchost.ase
	Network Mormation:
	Souter Review Address: 27.0.0.1 Souter Review Address: 27.0.1 Souter Review Address: 2
	Debide Automotication Information: Learne Oncerent Intel?
	Authentication Psychogenhegolates Transferd Services
	Padaga Nama MTLM any)- Kar Landho
	This event is generated when a logon request fails. It is generated on the computer where access was attempted.
	The Subjectifields indicate the account on the local system which requested the logon. This is most commonly a service such as the Service serve.
	The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).
	The Process Mormation fields indicate which account and process on the system requested the logon.
	The Network Information lields 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.
	- Intrafed service indicate which internedate services have participated in the sign request. - Package many many factors which are participated in the sign request.
2023-01-17T15:58:37+0530	- Ay ingin inclusis the engin and established by the state of the stat
	LopIane-Security EventCa54-e425
	Event/pse-0 CompletAmar-Advp2elG3
	avacementermenuose minore secuti 2007g. Type=atomasian minore avacementermenuose minore avacementerme
	Nagawada Anda Dahan Tada Dahangan angan
	Application of a second label to a second l
	incomparison to constant and a fing out.
	Security DC-1-5-18 Account Network/DVGELLGS
	Account Dramin WORKGROUP Learn Dravid? Learn Dravid?
	Logon Type2
	Account For Which Logon Failed:
	Security Ds-1+0 Account Name>
	Acout Umanity
	False Research Error scaned during Logor.
	Poser Momalani Coder Poses Duble
	Caller Process Name C:Windows/System 32 enclosed
	Network Wormation: Workation Network
	Source Network Address127.0.1 Source Portu
	Debied Authoritation Information:
	Logo Process Hand2 Auther Kalon Papage Registed
	Tranita Gavias- Padaga Name (PLL Avity)
	Key Lengh 0
	This event is generated when a logon request laits. 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 Service such as Winlegon are or Service servic.
	The Legon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).
	The Process Montation fields understanding and process on the system requested the login.
	The environment measurement where a memory and proof register organization. However, and campter and many be left bank in some case.
	- Transible stockes indicate witch interacted services tay angebras logarities against against against again tegers.
	- Kay length indicates the length of the generated session Key <sup>2</sup> . This will be 0 if no session key was requested.

 Event

 01170000\_000000

 EventOx=Gased

 EventOx=Gased

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 main indicates which also proceed was used among the NTM protocol was use

splunk>

Time 2023-01-17T15:58:35+0530

2023-01-17 16:07:02 India Standard Time Page 12

# 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





3. Upload files for computer



Figure 2

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

splunkt-enterprise Apps -		(1) Messages +	Settings *	AdMity #	Help +	Q, Find
	Add Data Searce Sector States Type Providency Review Date					
[	Select Source Drose is file to splate to the Splank plattane will be by branking your comparise or by disparing a file entro the larged back before. Leven More 22 Selected File Balact File					
	Drop your data file here					
	The maximum file upload sea 6 500 MB					
	FAQ > Yolliut lance of flow can the Splure platform tasks? > What is a source?					
	Provida Tget remate data anta my Seluns plattam instance?					

#### Figure 3

5. Click on Next

splunk-enterprise Apps *		,	Messeges *	Settings *	Activity *	Help 🔻	Q. Find
	Add Data O O O	-O Clack Nort2					
	Select Source Classes of the to upload to the Space plottern, where to knowing your computer or by the Solvert of the needs log Solver file	upping a fe into the larget has before. Learn More 12					
	Drop your data file here						
	The meanment for upheat size is 500.0	Ab					

#### 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.

splunk-enterprise Aeex •					1 Messeger - Sellings - Activity - Help - Q Fact
				Add Data	Gent Status Set Source Tax Input Sectors Review Does
Set Source Type This page lets you see how the Splark platt "Next" to proceed. If not, use the options be your deta, create a new one top clicking "Six	lorm sees your date low to define prope re dat.	before indexing in event breaks a	If the events to addimentarizes	ak coolect and have Eyou connot lind a	erve the right threatenings, click of an ingerepative source ages for
Source accessiog					Vew Even Summary
Source type access composed •	Sove As	* 1912 N	✓ Format	20 Pur Pago +	(The 1 2 3 4 5 8 7 8 . Not
	1		Trie	Event	
Pittar Q	9	<u>, t</u>	12/01/2021 21/22/41.000	172.21.0.1 -	(12/20/202115:52(0-4000) 16ET / ATTH/1,1" 200 5175 1-* "Moziliz/5:0 (201) Linox x80 50: nv176.0) Socia/2010010 Fzrefox/78.01
Spinnin defaulteners type settinge     Application	_	2	\$2401(2021 21:22:42:000	172,21.9,1 -	[ <mark>1//มม/วันการกรรร: -พพพวิ "นกา (</mark> 1//ปกรไปน.405/05.0.4 พทพ) ก" 100 กรร "- "พนปไม้สร.พ (การ เป็นมาพบ.54) กรรมขาง (ประกัตน) (ประกัตนตร ประกัตนตร
Custom		э	12/01/2021 21/22/42/000	172,21.0.1 -	(11/1a/1821) (5.52-2 - 6860) *627 / Ulanszimakons/ Jan/9/ Jan/9/ Jan/9/ Jan/9/ 1, ** 306 8234 *** ********************************
Ernail Log fo Metrica Herrica	er ancente, conte Notassa Conte Applications (M HTTY web Serie	Red for Sciencerpolit Sch comberet for in togs (sum beiger	19 1000 ner 17 1000	172,21.8.1 - 81 Firefox/28 122.21.8.1 - 1refox/28.01	[11/de/18111512] 40001 "WT /]//eede/indefrec/abbe/int/dow-bin/.tr/v=1.0.4 WTF/17 180 AM <sup></sup> * <sup>1</sup> 0pilla/1.0 (VI) (inex 48,44) +: TE B Geo/2010 20.9* (11/de/2011152:0 4000) "WT /p/vede/indefrec/abbe/int/int/ab-bin/.tr/v=1.0.4 MTF/1.7* 200 1014 *- <sup>-</sup> Texille/5.0 (VI), inex 48,44) +: 7.0 (abbe/2010/11 (11/de/2011152:0 4000) "WT /p/vede/indefrec/abbe/int/int/int/ab-bin/.tr/v=1.0.4 MTF/1.7* 200 1014 *- <sup>-</sup> Texille/5.0 (VI), inex 48,44) +: 7.0 (abbe/2010/11
Miscellaneous Network & Security	by apache or of opache jerror	epathe_enter		172.31.8,1 -	(1)/3m/303 15:52:42 10003 '001 /js/mages.ph/?emaes.a.4.00770.15 200 3338 555 'mecillars.a.(01); Linux 306.04; cs/78.0) deda/20100101 freefor/38.0*
Operating System with revently: Structured rystems		with server (typically cross-loop on "not- systems):		122.21.0.1 - 8.0*	-> (17/Jer/20131122501 4000) 4E1 /memor/motore/conference/conf
Unicategratized	galized BS WSC Extended log Network produced by Net		eny tra 200	172.21.0.1 - refox/78.0*	(1)/10/2011515142 +0001 "GT/51/0000/00001/0/130/00001/0/ 50/053.8.4 010/0.1" 300 200 "** "POTITATS # (0.1) (Jaux x06.84] PC10.0) Sector2000101
Web	Millipsolt Velans	at internation Serv	COL 1981	172.21.0.1 -	(122/an/2021)15:52:42 +9000) *GET /22/vendor/motionsf julyes.0.4 +179/1.1* 200 2300 *_* *Postilia/5.0 (XII: Linux x06.64) +++30.0) Secto/2010010 /irefox/10.0*

#### Figure 5

Put the relevant Name in the host filed value: we have used WordPress\_Logs

splunk-enterprise Apps *			👔 Messages 🕶 Settings 🕶 Activity 🖛 Help 🐐 🔍 Find
	Add Data Select South Set South Type	Hant Server Doop	aw 5
	Input Settings Optionally with additional input parameters, the this case input as follows:		
	When the Spinch platform indexes that, each event receives a fract value. The next value tribulat to the ranker of the machine new when the event originates. The spin of their up on the observances the available compareture options. Learn More 12	Constant value     Regular expression on part     Begreen in part     Hold Netrystue     WomtPress_Logs	
	Index The Source particum scores incoming data as swents in the relevant robe: Coopsign using a "sarchbar" holes as a definition or "year data in produce other scores ingo to you data A and bon score it is your include all data your coopsign action within incoming monotonic in indexet. You con unless the output this action grant within Moner 12	Index Datack • Create 3 new Index	
	FAQ 1. How do homes work? 2. How do homes when to create or use multiple increases?		

Figure 6

7. Click on Start Searching

<image/> <image/>	splunkt-enterprise Apps +		Messages + Settings + Adivity + Hep + C, Find
Figure 1		Add Data Salat Sines Set Scars Type east Setting Rowe Date	•
Figure 7		<ul> <li>File has been uploaded successfully. Configurity our multi by going to Settings + Data Houte</li> </ul>	
Figure 7		: Stort Syarching Sept[K yotil divisition on side examples and tudo tab. 15	
Figure 7		Extend fields Create servici-time field extinctions. Learn more about fields. 15	
Tigure 7		Acts More Data Act more dota inputs new or see examples and futures.	
Tigure 7		Deventional Apps: Apps help you do more with your data. Learn menu. 12	
≒igure 7		Build Doubboards Viscolize your searches Learn more I2	
Figure 7			
	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

nmat Timelitie • - Zoom Out	+ Zone ho Selection - Alberton			Theat put only						
	Lkz.+ ∠ Formit 20 Per	Pupe *		(Far 1 2 3 4 5 6 7 8 - Not)						
Hoe Fields III All Fields	1 Time Event									
ected vectos ost. 1	> 14/01/2021 172, 21, 0, 1 13 16 62, 000 hmt - WP	Et4/Jan/JUJ1:0/ Logs tource - acce	(46:52 -40082] "akt /Youshoulds malog   sourcetype + access, co	erhás, tat mitr/), 1° 380-488 "http://itz.m.e.4/* "NotTII/5.8 (Art) Lina: Are_61: rv.78.8) (eska/antenet Firefau/a.4" Millión - Millión						
wreitie 1 wreitigen, 20	> ##00/2021 177.21.0.1 13:36:44:000 hutt = WP	E14/Jas/207110/	iasiaa +somi "ser /mello-anri sourceype = access co	al HETY), 1,1 484 485 (HTE)/(172.21.0.4) (HOLILLAS 6 (KTE) LINUX AS (AL IN:TAG) Geola/2010111 (Inters/78.0) HENRO: Demogram: Mouthe 50 (KT Linux 486 61 N.TED) Geola:2010/01 Finder/78.0						
RESTING PIELOS	file			x Instrimute-file-instrimate-head.jp?ver=0.000000.0000000000000000000000000000						
tec 150+ entre 27 to frour 5 te mile 2 for manuf 48 to manuf 48	HOD Waters, 85 35855 of events		Selected Ves No.	36 usaragent = Nozāc-E0 (Xft. Unus x85_54 n/ 78.0) Gacko/20100101 Firefox/78.0						
	Reports			<pre>se/kadence/acode/cos/footer.min.cos?ver=1.6.11 #TTP/1.1* 484 488 "http://172.21.0.4/* "hozilla/5.6 (X11: Linex 486,64; rv:76.8) Gecko/20108</pre>						
	Top values Top sale	and a locy for the	Razie unteres	ed Usenhgent = Metille/50 (Ktt: Unuil x86, 64; N/78 0) Geole/20100101 Frefex/78.0						
inv_second BU	Events with this lield			es/kadense/assets/cun/content.min.cun/ver-0.0.11 #TTP/1.11 ADE 488 "http://122.31.0.4/" "http://122.31.0.4(" "http://122.31.0.4/" http://122.31.0.4/"						
te wday 2 te waar 1	Top 50 Values	Cisart	5	Manager - Manager - Manager - Manager - All and the state of the state						
te zone 2	ser-login.she	154	3,4815							
100-	adedini-a janphp	. 61	1.4385	Exploration approximation and contraction of the state of						
tex 1	admin-netices	34	211425	10 Juliagent - MecRa 5.0 (XII) Linux X85, 64, iv 78.0) Geolo 2010/001 Filofox/78.0						
count 1	favicat: 1co	31	1, 1478	aukanente/assets/cst/vinsi.min.cst/vervi.0.71 eTE/1.1* 404 400 "http://172.21.0.0/* "MortHa/6.5 (211: Linux 406.64: rv:01.0) Gerkn/20100						
mod +-	1	- 24	1,6355							
ever W	blacterbob	23	1.402%	nd ustragent = Mar#a/5.0 KM Linux x85_64, w/RL0g Gocka/2010001 Firefax/78.0						
erer_domain 2	users	19.	1,870.	Ins/elepie-file-list/cas/eeStyles.csc?ver-5 4TTP/1.1* 404 488 "http://172 24.8.4/* "Mozilla/5.8 (Mit: Linux 486,54: nv.78.8) Secko/20100101						
of 19	Tr 14k ptp	. 17	0.9538							
LUTR_BATYON 1.	style.min.com		0.15365	ad statisgent + Notifinitis (Nith Line) HBL_66; (N/180) Geole/2000003 Firefax(78.0)						
illus 11 Incommunic E	10010-020	14	9.9925	Ins/contact=form=3/includes/cos/styles.iss?ver=5.1.1 WTTP/1.1* 484 488 "http://172.21.0.4/" "Mozilla/S.0 (XT1) Linux 406_04; rx:76.0) Gecko/S						
estartpes 6	burt ND	Tour comments area	The memory water of	100000 - 1000000 - Month & 0.000 1000 - 000 64 to 20 0. Govern 2000000 Exchar 20 0						
1004	figure me	Polity - Andrew - Monte	name poncetton - access co							

#### Figure 8

splunk-onterprise	Apps *		🚺 Medsages 🖛 Settings 🖛 Activity	• Help • Q Find
Search Analytics	Dotesets I	leporti Alerta	Destrocardo	Search & Report
New Search			See As	Crushe Table View Close
f cource+"access.1	log* hist**₩.Log	r" sourcetype="acc	ess_porbined" file="wo-login.cho"	Al Sine + Q
r 154 avents (before 1	7/01/2023 17:59:52	000 No Event St	• # doL • # doL	* * Smart Moos -
Events (154) Patre	ints Statistics	Visualization		
Earnal Timeline •	- Zuom Out	+ Zene to Selected	e - Abundant	Those day poly
		Uni • Z Far	ад. 208н Аран (Ала 1) 2 3	4 5 6 7 8 Next)
< Hide Fields	III All Fields	1 Time	Event	
ALSO FED FELDS		> W/GI/2621 1316.37000	(72.2): 6.1 [1423a/221101.4537.4608] '987 Au-login pp/(100-th-tokan-addivlogin HTP/1.1". 44.488 '-" "Notilla/S.6 (X1): Linex 366,651 (V1)R.6) & dood/2018010 Fardren http://www.login.com/en/accession/com/en/acces	×78:0*
r source 1 r sourcetype 1 r uterscent 6		> H401/2021 (3:16:34.000	(72.21.8.1 - (14/)a/(2210) 44.54 4000) "927 Aprilogis phylitescho-dokenaktiologis mitter)." 444 489 "* "huzillab.# (311: Line etc.ps: rc:76.4) asis/22100101 Florin huzi - We_logi searce - accessing - secret, combined - usengent - Markillo (MLUsa 480, 64, n-780) Golo-220000 Refer (780)	/78.8*
NTHRESTING HELON		x H/01/2021 13/16/22.000	175,751.8.1 Div/Dav/2011:01:452:4522:40000 "925: April 2010;010:4111/1.1" 444-488.">" "Net/Dav/2011:Liteux Mol,452:4518.0; Gelon/2010001 Firefor/20.0" http://www.logs_cource=accesting_courceptor=accest.combined_uturopent=ModAls50.0%;Uhux 489,831;478.0;Gelon/2000001 Firefor/20.0"	
a clientio 14 a data, nour 5		3 M/01/2021 1316 19:000	172.21.0.1 C14/Jar/J22187-6119 9000 '9ET Ans-Legin phylitter-th-dakensekitalgin WTP71.1* 444 488 '' "Rezillar%.6 (311: Linux 66,64) rs:78.4) Gesd/J00101 Firefax host= WP_Logo_source=accession_source=access.combiner_userspeet=Wath/SD (WT,Linux 69, 54; nr/SD) Gesd/200001 Firefax/SD (WT,Linux 69, 54; nr/SD) Gesd	/72.8*
f date_minute_t5 i date_minute_t5 i date_minute_1		3 M/002020 13/16/7/000	(72,71.8,1 (14/16/101.8/.46.17.4008) VEC Ap-login phylicise: thirthdewidebiologis HITP/L1*.44.485 *** "Norzilla/S.0.(21): Linux 46.441.rs:78.0) Bebo/20100101 Firefox hore: WPLlogs: nource-accessing: nourcepta-access.combined: unsngent = Waths 50 (PEL Unix 466, 541 rs:78.0) Bebo/2010070 References.	278.R*
E date_second #2 r date_wday 2 t date_year 1		3 M/01/2021 11:45:40:001	116.25.36.128 [10:16/2011 00:15:00 H0052 P007 Jup-login phylites-th-toker-modulagin #70/1.3" 005 3380 C.* "Mozilla/6.0 (01) 0; Linux 4005; H0073 0; Crit.3.0.6) method.3.0%	2003020410 Pedicia/3.0.6-1.fc18
I date zone 1			hast - WP_Logs - some - accession - some - access combined - user up in - Mesta/50 (MT, U. Linux KBS, an VS; m. 15.0.5) Geula/2009620410 Fuorus/3.0	
cient 1 index 1		> 14/01/20/21 15/45/40.001	(10.2).54 (20 ~ 114/3m/2021.00.05.40 (4000) TWO Am-Ingta profitized the tokerholmlingth MINUL 11 483 3000 *** "RepEllarS.# (011) 01 Linux 4000; mol 3.0.6) Geom Préparit. 4, 78	2803828410 Federa/3 0.6-1.fc10
ther_thy_token 2			frait = WP_Logssource = accessingsource/pps = access _combinedusaragent = MosRut50 (KM, U. Unix KBS, an US, V.150.6) Gecks 2009020410 Poors/3.0	
inecount 1 method 2		) M/01/2021 8945-40.000	106/25.36/38 (14/16/301/08:36:00 4000) Wolf /ws-login.dublises-Ne-tokerezdeklogin stip/t.1" Hei Sku "+" Morilla/S.0 (01) U. Linus 1685; m-45; 19/1.3.0.6) Second 1 - refusil.4.10"	2003020410 fedbra/3.0.0-1.fc10

# B. The uri and token is displayed

#### 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

splunk-enterprise Apen *					🚺 Messages 🕶 Settings 👻 Activity 🕶 Help = 📿 Find
Scorch Analytics Datasets R	quorts Alertis Deskilooards				Search & Reporting
New Search	useragent			×	Save Au + Counte Table View Close
1 cource+"access.log" host+"WordPre	15 Willies, 94.123% of events	53	Serence Yes	NO.	Arme+ Q
< 2,054 events (before 17/01/2023 15:47.4	Reports				Job *
Events (2,054) Patterns Statistics	Events with this flexe		Kilke Askhez		
Finnel Timelère • Zuom Dut	Top 10 Values	Court	x		These gas spectra
_	Horilla's # (Phone: CPU thread is 5.1 like Nac 05.3) Applance#11/334.46 (HHTML, Like Secker) Version/5.1 Not124/38176 Safari/7324.48.3	188	18.6525	1	
	Opera/9.00 (Mindows 47 5.1; tz. do)	141	13.5748	1	(Prov 1 2 3 4 5 6 7 8 Next)
CHICE Pietra III Al Reida	Perille/5.0 (X11) time sNL_64; rs:70.0) Geoko/Obl00101 Fjrefes/75.0	120	12.7855	1	
SELECTED FREIDS	Hueilla/5.0 (Windows WT 0.1) rv:2.0.1) Gecko/20100101 fji-fox/4.0.1	122	12.2895	1	b. 101 (HTRP1), 11 288 488 (Http://122.21.4.47 ModELLA75.8 (011) Linux 388_64) (v) (8.8) 660028188101 Firefox/78.8 (http://doi.org/10.0001/000000000000000000000000000000
a source 1 a sourcetype 1 a scarcent 19	Morillo/5.0 (Linux: U. Android 2.1: Nn-WS: Droid Delid/198220) Analescentri/Stat. 1 (Setter, Line Sector) Version(4.0 Mobile Seferi/CDL1	185	18.2085	1	1971. (* 484 488. "NITE//172.21.9.41" "NEETERS.8 (*111) LINUE 385,84(*1212.8) GRANDERE (*1476a/24.8" ombere – usersejen – MacHallo DOL Linue 386,84(*178.0) Gedan20200019 Pertur/26.0
INTERESTING RELOW	Moziliz/5.0 (Windows WT 6.3; WOWGH; Trident/1.9; Isurh; TWIR; rv:11.0) Like Gecko	103	10.2081	1	ins/lingle-file-lins/idee-head.ph/erss/stre/1.1* ese ean "http://itplit.e.e// "Moglila/S.D. (xit) Linux add.pet re(ra.d) Gesa/autonot Firef
# tytes 130+	Mozilla/0.0 (compatible: MSIE 7.8; Windows W7	70	5.9381	1	z/mbinec usersgent - Manifa/Ed (XN, Linux 486, 64; nr/98.8) Gedan/20100001 Fineto/78.9
# date_four 1 # date_folgy 1	<ol> <li>I. Trident/4.8: SLECT. NET U.N.2.8: 507271 NET U.S.3.5.30715: NET U.S.3.8725; Hodla Center PC 5.8: Tablet PC 2.01</li> </ol>				as/labace/asses/sac/bater.six.cos/bater.s.ri.atto/1.r* 404.400 "http://itz.zi.a.e/* "http://itz.zi.atto/sac.atto.s.s
e date month 1 # date nordh 1 # date second 60 # date wday 1	<pre>Muzillu70.0 (X11:0; Linux 1000 (x00.04); ru; rv11.4.0.0; Derker700004425 500071.5,0.3-T r31070071(5:0.3</pre>	-18	2436.1	ġ.	oonteen isenegen: Mackela (DB Lauwalle, SH n788) (Seena200000 Parke/28) wakaannaamata/saa/enteet aan.saalaer1.8.11 HTP/1.11 88.481 Mate/2112.21.8.491 Mate/2181(111) Linux 486,48, nv(36.8) Seeha/20180
R date_peer 1 # date_peer 2 # the 100+	Mozilla/5.0 (2)1:01 Linux 1665; 45-05; rs:11.5.2.0 Secto/205922410 Todora/3.0.6-1.Fc10 riserov/3.8.0	32	1.175		bondnest interapent - Marchald B. DOL Lina x86, 301 (r/36.0) Geom/20100007FFe/si/26.0 av/balance/assistaryss/hauke-min.ust/werr.0.10.407971.1* 464.485 "Mbp///12.21.8.4/" "Resiltar%.6. (D11; Linus +BL66; IV-18.8) Geom/2010011
a dent 1 a index 1 & linecount 1 a method 4	Mozilla/5.0 (Windows 07 10.0; Hir54; x64) Ass(reextr/all in (WiNH, like leces) Chromp/57.0.4250.55 Satar1/537.30	29	2.874%		อกรณฑิษณ์ "เลลาญกร"- พิษร์ติงวิธ (PDL Druck RB, 64, 478) ( Geologizmond Revis/RB) หมายสามสระบังอาร์ไฟฟ์เป็นสว้างกราสาสามาราว" สม48. "ประชา/117, 21, 8, 47. "วิชย์[ไลวร์วิธ (2011)

Figure 10

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

New Search		Savi A	· Criste	Table View Close
▼ cource="scients.log "ost="Word#Tess_Logs"  too limit=10 iseragent				ALDON - Q
20054 events (before 10/01/2023 % 48448.0003) No Event Sampling *	+ dbit.	1.10		• Smart Woole •
Events Pettern Statistics (20) Visualization				
20 Per Poge * 🖉 Format - Preview *				
unsopri 1		1	court 5 J	percent ± /
NALIILISSE (N11, LINUX X85,84; PV17E,8) GecKel23108181 Pirufox/7E.8			103	54,259790
Narilla/5.# (IMPone: CM) iPhone (DS 5.1 Like Mac CG 8) Applement(2/LiA 40 (NMUM., Like Geoks) Verzion/5.1 Mabile/55176 Safar1/25)4.48.3			38	9.451995
Spere/3.08 (Winine: N 5.1) is, do)			34	7. #38/389
NULTIANS (NICHMENT NT 6.1. PC.I.6.1) GREAD FILTERS A. V			12	5.234289
RADILLAS. 8 (WINNER NT 8.3) NUMERI TEIDENTE (V. RALES, TATEL PVITT.8) LINE GESSE			10	5.178482
HALILACS # QLINA; U; MARVID 2.2; ex-as; Droid DollaCTRE2D) ApploVENTICTS.1 (NETW. like meska) Version/4.8 Maille Safar/251.1			10	5.176482
Murilla/4.8 Communible: MSIE 3.4: Vienna M7 8.1: Triemti4.4: SECEN ART CLR 2.0.80127: JBET ELR 3.5.30725: JRT CLR 1.0.30728: Weila Conter PE 0.4: Toblet PC 2.0)			7	3.819190
Marilla(5.4 (01), 0, Lines 146 (148,54), etc. etc.1.6.4.3) 0ecker/0405435 36527(13.8.9-7 FreeFau/1.3.4.1			1.4	2.011051
Ruilla/3.4 (VI), D. Line 1884; ev.1.3.6.8) Bicks/2009020418 Fadora/3.8.6+1.718 Firefox/3.8.18			3	1.008349
Section ( Minese W) 10.0, Mines ( 4.2) AppleAdd(1533) 30 (4004, 1340 Decks) Connector 8.4504.00 SectorS37.00			2	1.45009
Narilla/LR (compatible; MCTE 6.8, States NT 5.0)			1	0.1155254
WardDFennersteing, Nichartzer 201.01.3				8.104077
Aparhe/7.4.36 (Sublay) MMP/7.4.14 (Internal Games connection)			.1	1 (V. 75414)
Apuchar(1.6.38 (Dublin) WFF7.6.13 (Internal dammy commution)			- 1	9.763871
Norsila/S.# (1Pad: CPU 05 0.1.1 1946 Mar CS 4) AnnieWecktr/001.1.4 (NHM., 1946 Gerkel Verscov/0.0 Modele/120406 Safari/0000.1.4				10 10 201100
aptime requests/2.34.0				0.110130
salaan/1,4,119arahda (http://realmon.org)				0.050277
Witson VL 8:10 (https://witson.org/)				0.038272
Nec111/5.0 (IPhone: CFU IPhone 05 7.8.3 Ilke Nec 05 X) Applembel1/537.57.1 (BCTML, Ilke Becke) Version/7.4 Meb10/10571 Safar1/9537.53				8.856277
				2:050277

#### 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

a state month 1		Nort - Northern Loge North - Northerne State State State Northerne - Northerne									
# date velocity 00 in date velocity 2 # date velocity 2 # date velocity 2 in the 1000 in the 1000 in the 100 in the 1 in	method 4 Values, 96 E395, 4 Reports Top values	of ecenta	Selected wes to	The desceed assets (cardinates cardinates (cardinates (cardin							
a method 4	Events with the field										
a laterer bt	Values	Court	<i>e</i>	International   wearagent - Meanlark 0 01tt Linux x85_ 64: IV:78.00 Getwol/2000101 Profee/78.0							
a toterer_domain 2	GET	1,683	84.6151	and a set of the feat of the set							
a req_time 900/	PÓST	239	12.8161	universe of a structure of a million of the second structure of the second structure of the structure of the second structure of the second structure of the structure of the second structure of the structure of							
a logi 19	HEND	38	1.915	conclused interrupert - Mozillarti G (01.1 interx85.64, vv.38.0) Geckor20100101 Firefox78.0							
# planes 11	ONTIONS	29 1.4585		ins/contact-form-//includes/cos/styles.cos/ver=6.11 WTF/1 17 484 486 "http://112.27.0.4/" "Mozilla/5.0 (011) Linux x86.64) rv1/0.0) Secto/201							
# interaction for	and the second sec	and the second s									

#### Figure 13

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

Childe Fields III & All freids	1.62	• Z Format	20 Per Page •		1 2	3.4	5.8	7 B	Next 5
4 10 14 14 14 14 14 14 14 14 14 14 14 14 14	×.	Time	Exert						
e uni pagn 24 e uni, gubey 23 e geet 1 e version 1	>	94/01/2021 11/98/11/202	101.05.05.25 / - Clubber/201100.01111.00002 /9000 /ap-content/aplass/simple-file-list/file.dos 0000/1.07.000 9000 /http:///17.1.0.1A el 0000 1.07.05.0012 - Clubber 0.0.012 / 000 0.002 / 000 0.002 / 000 0.0012 / 000 0.0012 / 000 0.0012 / 000 0.00	e-cootes(Aple 2 #}"	ado/eine	le-file-li	x1./Fr346ph	o" 'Marilla∕	4.0 (consist/ii)
			Note = Wwweenast_Logssource = accessingsource/ype = access_companed _ucoragent = woena.4.5 (companie Misle 76) Windows NT 61, choene	ADDESCORE INE	COL.				
29 more telds + Extract New Fields	2	11.57.57.000	103.05.35.312 - 114/Jmr/202100127537 400052 1937 (An-content/unloads/simile-lie-list/fr240.ptp HTD/1.1* 200 (4MM "http://173.27.0.7/ +) HDIE / D. Vindmon Mf 9.1: Trinkent/4.4: 55071 (ACT CCR 2.0.30721) ACT CCR 3.5.30229 (ACT CCR 3.0.30229) Helia Genter PC 0.0. Teller PC	p-content/valo 2.07"	ada/aina	ie-file-li	11/77240.3H	o" 'Mozilla/	<pre>#.0 (respirit)</pre>
			hosi - WoofFrest, Lags - source - infrest-log - source/pe - scorest, contributing - sensers - MoofAst 0-(competitie MSRE 70, Workes NT 0.). Tables	40.5CC2. NE	CLR.				
	2	90.010.021 1157:29.000	101.00.05.712 [14/14/3021100:17.30 +0006] "VOIT /Ap+ContextAugLowdor/redue=flim=lit/frids.prp.wrmv/ 1" 200 (213 "MCTpc///12/21 0.04 w/ MLE 7.0 Window W 5.11 Fridemi/4.01 50022) MET CUM 2.0 5022] /MET CUM 2.5 30725] /MET CUM 2.0 50725 Molia Conter PC 6.45 Tablet PC	p-content/usla 2-83 <sup>4</sup>	ab/sim	a-file-li	utifirada pe	o" "Morilla/	a.e (constibi
			hod - WordPress, Logs - source - broad, bg - sourcetype - sccess, combined - useingent - Medile-4.0 (competible: MBIE 70; Windows NT & 1; Trident	4.0; SLCC2: NE	FGER.				
	э.	14/01/2021 11:57:08.000	103.05.55.212 154/156/242100.27.00 100003 70007 Aurocontext/adias56/11016-(11-153/07144.dtm HTTV/1 1* 200 1213 "http://122.31.0.3A #. HDE 1 U; Windows NY 8.1. Tribent/4.8: 50002, VMT CAR 2.8:50021, VMT CAR 2.5:50027, VMT CAR 2.5:50027	orcontest/mla 2.03*	als/sim	e-file-li	n1/6-346_ab	o" "Mucilla/	A.D (competibl)
			had - WeinFrest Lings - sources and - sources per access continent - weingest - Wontask Digongurine MSRI 70; Windows NT 61; Diserc	4.0; %.CC2; NE	CER				
	2	11:56:53.000	<pre>10.30.20.20.4 - [14/38/2010012013:145.4000] "EGT /we contact/alugion/timele-file-list/se-file-engine.php.0709/1.1" 200.200 "http://02 latEP-1" "arthor resents/2.24.4"</pre>	.21.0.3/vp-sdr	in/amin	uto Teager	es-single-f	ile-liothtad	rtiie_liitkeel
			hust - WindPress Logs Nurce - ecores.log source/pe - scores.comblerd usemgert - python-equests/2.24.0						
	2	94/01/2021 11:56:53:000	119.241.22.121 ()4(1an/2011-04.26131-9000) "MST /vo-contactglogins/single-file-list/w-uning-eques.pp.H194).1" 200 118 "-" "pythone ()200	01-790/4175/2	24.0"				
	Эř	18/01/2021 11:50:38:000	10.8.5.12 [14/18/18/19619619-908] *057 /sc-pas/center files//violater/sem///fieldas/srm*//isedas/srm*/i/ am as/ "http://12.31, class4.4.8, 0205; JRT GR 2.5.59777 JRT GR 3.5.3975; JRT GR 3.6.3975; Bella Center PC 5.6, Tablet PC 2.41"	Weentact-us)	1 196211	1a74.9 (ci	mpatible; M	626 7.0± VS4	dava NT 6.7; T
			Nust - WordThen, Logs - source - or Cess.log - source/pe - access.combined - userspect - Moetha 4.0 (competitive MSR 70; Windows NT 63; Tricest	4.0: SLCC2: NE	CLR.				
	2	14/01/2021 1150:32:000	(4) 49. 59. 212 [14/14/2021-00.28.12 +0000] 'POII hor-juan/contact-form-//si/contact-form//si/faedback HTM21, 1' 200 465 'Unity s/size 21 a signal (1) and (1)	(1/contait-si)	* .7M0213	la/4.0 (ci	mpatible; M	53E (7, 8; ¥)a	does 107 6.1) 7
			torg - WerdFrees_Log1 source - beenstog source/yps - access_combined useregart - Mazita 4 0 (comparison MSIC 70) Wedows NT 6.1, Trobets	4.0; SLOUP; NE	CLR.				
	2	51/01/2021 11:50:32:000	(8):55:55.212 - [14/Tav/2621:06:28:12 +8000] *P077 /ssc-juan/contact-form-7/v1/contact-form/7/feebback #TTP/1, * 200 881 "http://172.28.0 v1/or4/4.4, % 46:22: 387 CLF 2.6.20177; 387 CLF 3.5.30178; 387 CLF 3.6.20179; bolia Centur PC 5.0; Tablet PC 2.6)*	Wontert-us/	* *rozil	la/4.8 (ci	npatible( M	555 7.0, W)A	alovs NT E.1( T
			hoz - WintPress_Logic Locate + access og Locate/pe + access_combined Losenquet + Montal4.0 (compatible MHE 70; Windows NT 61; Tricero	4.0; SLCC2; NE	rcia.				
	2	%01/2021 11/50:32:000	103.65.65.252 [14/18/3021100:18:32 4000] '9051 J0-1568 Contact-form/V/I/Centact-Sone/P/Medidae HTF/L/' 200 661 "Http://U2.314 rident/4.6; SCC21 AET CLR 2.8.58727; AET CLR 3.5.59735; AET CLR 3.5.59735; ACT CLR 3.4.257 Holds Contar FL 8.9; Tablet PC 2.8.1	.3/contact-us/	* "Yozil	ia/4.8 (cs	mpatiol4: H	516 / 0t Win	dows M7 0.11 7

#### 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:



	NOTICE: Changes are coming to <u>CVF List Content Downloads</u> in 2023.
((0)(); \$ (CVF > (CV)(-3)	DI SAMA
	Printer, Frisendiv, Visw
CVE-10	
CVE-2020-35	489 Lobra more at National Vulnerability. Database. (NVD) • CVS5 Seventy, Rating + Fu Information • Vulnerability. Database. (NVD) • CVS5 Seventy, Rating + Fu Information • Vulnerability. CR4 Mappings • CPE Information
Description	
The contact-form-7 (a	ka contact form 7) plugin before 5.3.2 for wordpress allows unrestricted nile upload and remote code execution because a filename may contain special characters.
References	
Note: References are pr	noted for the conversions of the reader to belo distinguish between subscribblies. The first is not intended to be complete.
MISCHING //www     MISCHING://www     Assigning CNA	s, perdeta, com/teo/311/muja-exite/consect-proc./cumentical-re-industry su inconvergese.com/uncetrigted-file-uncodein-contect-proc.7/
MITRE-Corporation	
20201217	Disclament: The <u>recting organization date</u> 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 (Legac	A
Proposed (Legacy	0

#### 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

Crice Fields = Al Pields	Unit - 2 Fairs	ut 20 Mr Page+ c. Triv 1 2 3 4 5 6 7 ft - Heal2
a un 41	k Time	Fait
e un patri 2e e un gaory 23 e user 1	> 14/01/2021 11:58:11:000	103.05.05.212 - (14/14/2021.04/201) The content/ublack/lasis-file-lit/1/104.obs/Th/1/1/200 5555 Thtm://122.01.03/us-sortest/ublack/lasis/imple-file-lit///144.obs/ # 1000 7.8. Window HT 1.1. Trider(A.B. SLC). MT CR 2.5.59757, MT CR 3.5.59757, MT CR 3.5.59757, MT CR 3.5.59757,
# seision 1		hou - Wordhese, Logs source - access to source/yee - access combiner use agent - Multi/AD pompatible, MSE 70, Windows NT 61 Trainer(AD, SLC2: MET CLR.
29 more Relds + Extract New Fields	> 10/01/2021 11:57:57:000	WEI 8155.312 - [W/Jav201.0k12157 NOV0] "WOST App-content/uploads/stmp1=f11e-list/r586.phg =f12f1.17 206.504 "http://172.21.0.1/wp-content/uploads/stmp1e-f11e-list/f740.phg" "Restlia/6.4 (compatial e) MSIE 7.6 Viologe NE 6.1 Tridenck A: SSCC1. HET CLR 2.0.56737. HET CLR 3.5.36735. HET CLR 3.6.30735. Helic Content FE 6.3; Tablet FC 2.0)"
		hmat - WendPrima Lage source - source - sources - source
	> 14/01/2021 11/67/28.000	HEL RE 20: 212 - C14/Tax/2021 RE201738 HERD PROT Op-content/adiade/Claude-F18-List/F184 and F070771 20 1219 "Meta://http http://http://http://http://http://http://http://http://http://http://http://http://http://http://http://http:/ http://http://http://http://http://http://http://http://http://http://http://http://http://http://http://http://http://http
		Noss - WendProse, Logit Source - access log Searcetyce - access, rembined Useragent - Mc2Hs/4.0 (comparting, MSE 2.0, Windows NT 6.1; Trident 4.0; ELCC2, NET CUR.
	# 14/09/2021 11:57:06:000	163 (8):55:372 (14/1a/2021-8):37:65 -00(8) 'POT Aproatest/select
		fmm = WordPress, Loge source = access Log sources; execution of severagem = Mczillai4.0 (compatible: MSE 70, Windows NT 61: Televiti4.0; SLC22; MET 61R.
	> 14/01/2021 11:56:53:000	19-34121 (1) - + [4/38/2411462(3)4-4000] *000] *000 /#-content/slights/supple-file-first/on-file-angles prp #/9/) /* 300 184 *http://11_31./he-andmission.php?ageve-inst.a-file-listian#file_listae.
		hest - WendPress Logs searce - occess log sourcetipe - access combined userspent - pr/hen-requests2340
	> 14/01/2021 11:58:52:000	195 748.22.121 [14/1a/2821.05.20.13 -00042] *0077 /ve-context/http://adami.ed/1/e=1014/ee-adami.ed//or // 200 330 *-* "syther-resents/2.24.0" http://www.book.insci.com//insci.com
	> 19/01/2021 11:50:36:000	(0) 03.55.202 (14/18/321)05.2013 (14/18/321)05.2013 (14/18/100) 0001 0001 0001 0001 0001 0001 0001
		hust - WardPress, Jage: source - access.log: sourcespat - access.combined: userspent - MozBV43 scenarbles: MSE 70. Windows NT 61 Tratest#40: SLCC2: MET CLR.
	> %4/01/2021 11/50:82.000	183,09.25 (12 + 114/1a/2011.01.28;15:96001 99031 Ap-justcontact-form/1/1/contact-form/1/1/seduck.878/1 1* 240 853 *http://17);21.8 Econtact-est** *herita/4.8 (consultible, MSE 7.6) %http:/// 2008.053 *http:////2018.053 *http:///2018.053 *http:///2018.053 *http:////2018.053 *http:////2018.053 *http:////2018.053 *http:///2018.053 *http:///20
		hoss - Wendhoos_Logs severe - accessing severes_excess_combined useragent - Mostbyll (compatible; MSE 20, Windows NT 61, Tream; 10, SLCC2; NET CLR.,
	3 14/09/2021 11:50:32:000	161.65.55.112 - []4/lar/2011/85.20112 -4000] "POT /w-jss/contact-forw-7/i/contact-form/7/i/
		has - WeetProve Logs serverse - actions log serversey - access combined user egent - Mc20164.0 scomparble, MSE 70, Weetprove AT 61 Transch 40, SLCC2, MET C.H.
	> 10/01/2021 11/50:32:000	101.05.05.012104/10/201.061201.001201
		hast - WardPrise Loge source - scients log sourcetype - scients, combined : warrigent - Mosibly40 (compatible, MSE 70, Windows NT 61 Trident 40, SLCC2, NET CLR.,
	> 16/01/2021 11/5/0/0.000	(8): 89:55:112 ++ 114/1ac/001.06.20:04:04001 MOST: Ag-just/contact-form/7/ifcontact-form
		hosr - Word Hass_Logs = source = socressing = source/pe = socress_combined = userspent - Mostlov/L0 (compasting MSE 70, Window NT 6.1, TreamLike SLCC2, MET 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

Crice Fields	III Al Pielch	D	e - Z Farma	20 Per Page +	C Fire 1	2 5 4	5 0	7.6	Next.3	
a us #1		36	Time	bet						
a un pain an a un geory 23 a oser 1 a secson 1	a unit, paolin an unit, paologi (23 a usan 1 a sension 1 29 mars Reids + Expect New Fields	×	14/01/2021 11:58:11:000	181.59.55.212	nit/lelvads/sil	mile-file-li	st/fr34k pMg	)" "Hozilia/4.	0 (compatibl	
29 more Reids + Extract New Fields		ż	16/03/2021 11:57:57:090	(B) 88.9.212 - [MADATORIS (MADD) (MADD) (MADD) (MADD) (MADDATORIS (MADDATORIS (MADDATORIS (MADDATOR) (MADDATORIS (MADDATOR) (MADA	int/uploads/sti CC2: NET CLR.	mple-file-li	st/TriA php	/" "Hogijia/4,	0 (compatibl	
			1401/2021 11:57:28:000	101.0.5.713.4.— C.M./ARDID: 00125-31 (1903). Http://doi.org/10.1001/s0104-01004/s0104-0100-1101/1104-400-010701, 101.00110000000000000000000000000000	estégleatsési CC2: NET CUR	nde-file-li	si (fr346in)	/* "Huziila/4.	* (nometibl	
		a.	14/09/2021 11:57:06:000	103.03.03.192 — (M/AAR020.04/2024.04/2024.1920). FEET Approximation (March 2014). The List Yorke, and HTML 19. 2014). The List Yorke (March 2014). The List Yo	Jot/uploads/sir CC2: NET CLR.	mple-file-li	st/fr34k.dhg	/ Morila4.	<pre>4 (compatibl</pre>	
		×	16/01/2021 11:56:53:000	(1): 311.22.121 - 114/Jav/3821-80(201-8): 494093 (NOT Age-content/bilgion/bilgit-bilgit-bilgit/setTilg-ongles.dbp.HTPP1.17.200 234 "http://112.213.4 bill/971" "pathon-recentro/114.4" http://www.marg.dbgsource.ex-contents	//xp-admin/adm	in.php?page*	es-simple-fi	le-listktaö*f	De,listèes,	
		2	14/01/2021 11/58/52:000	195.241.22.121 - 214/Ter/2011.0619/131-06661.19007 /ve-context/http://sigil.ef/lig	ests/2,24.0*					
		×	19/01/2021 11:50:36:000	HEI MAN JUL (MU) AND MAN MAN MAN JUL MAN JUL MAN	LINT-US <sup>ITE</sup> "Not DC2: MET CLR.	ills/A.W.(ce	epotible: HS	.16 7.0 <u>1</u> Windo	NE NE L'IT	
			3	94/09/2021 19:50:82,000	181.9.55.112 Elw22a/2801.81.28.15.146441 74517 Aur-juszkontact-fors-7/1/ Contact-forw/7/14edack.wT#7/1.1*244.851 *http://17.21.8.16on 7588624481 50000 (Art Data 2.6.9000)) (Art Data 3.6.8025) (Art Dat	ract-es/" "Nor	11a/4.8 (co	oputifile; MS	(E.T.O) Windo	wh 40 0.1; 7
		<u>.</u>	14/07/2021 11:50:32:000	161. (5), 55. 312 (34/)3a/3601196/2013 - 4049) ************************************	Lact-va/" "Not	illa/4.9 (co	nootibie: HS	IIE 7.0; Windo	NS HT €.1. T	
		ŝ	10/09/20/21 11:50:32:000	01.65.81.212 (14/120/2021.65.2013.4600) *001 (-0-100/00121-59-1/0/1200121-5000/0121-5000/0120-5000/0100-5000/0100-5000/0100-5000/0100-5000/0000/0	tact-vel" "Nez	1132/4 # (03	mpatihie, Mi	(1€ 7,0) Mindo	NS NE B. (), 7	
			3	160V2021 115006.000	(4). 60, 51, 713 — - Elevizar/2021. 60, 56, 44 +9646]. *FOIT Am-juri/onitati-form-Trivitati-form/Trivitations, MTPJ, 14, 3446 881 *Foitsc/172.21.4 Mice rainetal-49, \$5022, APE Car 2, 6 MPZJ, 1457 Car 8, 5, 19223, 1457 Car 8, 5 MPZJ, 1457 Car 8, 5 MPZ, 15 Car 8, 5 MPZJ, 1457 Car 8, 5 M	LICE-IN/* "Hou	illa/4 # (co	ountible: PS	ite T.Q. Winds	ws WF 6 11 T

#### 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+"MP_bo	gs" cow cotype+"access_torbi(ed"			/At the • Q
2.054 events (netcer 07/01/2023 10/1/22.000) As Event Sampling *				John - 10 in 🔥 🛓 🕈 Smart Mode +
Events (2,054) Potterns Sorticia	ce Maunization			
Format Timeline • - Zoom Dut	Altown Entertor Altowheth			This per palarie
	List = 2 Format 20 Ptt Pt	90c.*		1 Prov 1 2 3 4 5 6 7 8 - 1683
K Hole Frame III Al Taklos struktoren akusta e kont i a struktoren i a struktoren i a struktoren strukt a struktoren strukt a struktoren strukt a struktoren i a strukto	file >100 Values, BE 358% of events Reports Too values. Too values	by time	Selected yes	a bit (1017).1" 208.48         "tetra/171,2,71.8.44"         "tetra/171,8"         Beda/28198191         Trefox/78.4"           Mo         de ubsogent = Motified UCL Law, HSL 64.11/25 (Globor 2000000 Fedbo/280         Fedbo/281         Trefox/78.8"           Mo         de ubsogent = Motified UCL Law, HSL 64.11/25 (Globor 2000000 Fedbo/280         Fedbo/281         Trefox/78.8"           Mo         de ubsogent = Motified UCL Law, HSL 64.11/25 (Globor 2000000 Fedbo/280         Fedbo/281         Trefox/78.8"           Mo         ubsogent = Motified UCL Law, HSL 64.11/25 (Globor 20000000 Fedbo/280         Fedbo/281         Trefox/78.8"
	Events with this field	Court		Torizantiet=file-file/list/jace-bea.jctver+9-WT#7.1* 484-488. http://fiz.if.au// Hezilla/5.9 (Kit), Linux, s85,64; N/78,9) Secon/2010101 / Inne ad usangen - Mosta/5.6 (Kit, Linux s86,64; N/78.6) Geoko/20100081 (Fieldw78.6
	sp-Lugin php administration, php	154	1.6815 I	estimaterizations/factor dis confuser1.8.11 4110/1.11 444 400 "http://112.31.8.4/" "Metrillaris.8 (011) Linux VIB.84; nv:31.83 Generalizations/
	unsin-notices	30	3.1425	useragent - Mozifa@6 (X1; Linux x86_64, nv;78/0) Secke/20100101 Fixe/ov;78/0
# oute_percent 61 a date_witex 2	Gevicon.tes	31	1.4476	es/Waderice/assets/cos/content.min.cos?ver=1.0.11 wTP/1.1* 404 406 "http://102.21.0.4/* "Modille/3.0 (KT1) Linux X00_84, Http://02.01001
# 0388_9408 1	phogtes.php	25	1.40%	11 useragent = Mozifia-5 0 (Ktt. Linux x88, 64, rv:78 0) Gecke/20100401 FileNov/78 0
# GBB_2000-2	(25-07-5)	10	r. etts	us/hadanca/assocs/cos/header.mbn.cos/hea/er.0.11 #779/1.11 004 488 /http://112.21.0.0/1 /h0s211a/5.0 (X11: Linux +86_64: 17:74.0) Gecke/2010010
a kount 1 a molect 1	fr34kainir 🔸	17	0.9505	ed Schootnt = MotRes-0 00111/nor x05-64: nv75 0r Secko/2010001 Fredox/78-0

#### Figure 19

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

New Search	Since As + Creater Table View Case
1 sources accessing foots of source toes accession the file of the	At true + 🔍
✓ 17 veents Dictors 17/07/2029 18:82:25.005) No.Event Sangung +	Job + 11 II ->
Boands (17) Performs Statistics Visualization	
Format Treaders + +Zoom Out + Source to Section - Committee	1 www.no.ber.cok.ave
Life - of Francist 20 Per Plage -	
(Hde Fields # All Fields # Trive Exemit	
142.007207 HEIDE 14.0.0072021 142.0.0.07719 - 114/14/20/20114518.05 100001 7027 Ac-content/uplast/sign=f18+114/7:54.pho HTF/ 1* 444 408 *** Mer21114/4.0 ( 17200-05.000 0727; 342 114 1.5 10727; 342 114 1.5 10727; Merz A. 0. 07719; Merz Achter M. 6. 07710; Merz Achter M. 6. 07719; Merz Achter M. 6	commetible; MS1E 7.0; wirdness WF 0.1; $Tr/devt/4.4;$ SLCC2; .NET CLE 2.0.5
A TAN I 4 Source 1	3; SECC2; . MET CLR
# SourceNpe 1 >> Mc0/2021 103.05.55.212 (M/Sov/2021/163.06.97 4606) 17657 Apr-content/inicide/source-file-list/Fride.php.34719/1.17 200.215 17610 (//12.21.4) # seeingent 1 1200.01000 e: HSIT 7.8 mindeen MT 6.1. Tristen 4.6.5 SCC2, MET DX 2.6.50721, MET DX 3.6.30725, Bett DX 3.6.30725, Betts Censer AC 5.6, Table	l/so-context/upipeds/simple-file-list/fr34k.stg* "Mozills/4.0 (compatibl et 70 2.0)"
armanine wates nor we logs source + accounting source + accounting contineed usersageer + Monitor&D (compatible, MSE 20, Westers V & C & Tribert 4	E SLCC2. NET CLR.

#### Figure 20

#### C. When we expand we get the status code



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

#### BTLO

https://blueteamlabs.online/home/challenge/log-analysis-compromised-wordpressce000f5b59

CVE:

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