CyberCube2020 - k3yz4 Writeup

ერთ-ერთ სამთავრობო სერვერზე აღმოჩენილი იქნა საეჭვო სკრიპის ფაილი, რომელიც გაშვებისას ითხოვს პაროლს. თქვენი მიზანია გააანალიზოთ აღნიშნული სკრიპის ფაილი, დაადგინოთ საჭირო პაროლი და მოიპოვოთ ე.წ. "Flag"-ი.

k3yz4.bat

გვაქვს .bat ფაილი თუ შევხედავთ მის შიგთავსს დავინახავთ რომ ის Base64-ში არის დაშიფრული

```
powershell.exe -enc JABVAHMAZQByAFAAYQBzAHMAdwBvAHIAZAAgAD0AIABSAGUAYQBkAC0ASABvAHMAdAAgAC0AUABy
AEEARABJAEEATQBBAEIAbQBBAEQAawBBAE8AQQBBADIAQQBEAEEAQQBaAFEAQgBsAEEARABFAEEAWgBBAEEAdwBBAEQARQBBAE
ACQAQgBTAFQAUgAgAD0AIABbAFMAeQBzAHQAZQBtAC4AUgB1AG4AdABpAG0AZQAuAEkAbgB0AGUAcgBvAHAAUwBlAHIAdgBpAG
ADAAQQBHAE0AQQBZAGcAQgBqAEEARABnAEEAWgBRAEIAawBBAEcATQBBAE4AQQBBADUAQQBHAFEAQQBZAGcAQQAxAEEARwBFAE
ACQAZgBsAGEAZwBfAGsAZQB5AF8AYgB5AHQAZQBzACAAPQAgAFsAUwB5AHMAdABlAG0ALgBUAGUAeAB0AC4ARQBuAGMAbwBkAG
ACAAcABhAHMAcwB3AG8AcgBkAC4AJwA7ACAAfQA=
```

□ირველ რიგში, გავშიფრავთ ფაილს. □მისათვის შეგვიძლია გამოვიყენოთ https://www.base64decode.org

DECODE > Decodes your data into the textarea below.

```
$UserPassword = Read-Host -Prompt 'Enter your password'; $AESKey = [byte] 220, 22, 83, 174, 203, 44, 204, 117, 115, 154,
222, 39, 11, 56, 76, 254, 34, 89, 128, 71, 32, 229, 121, 173, 65, 102, 169, 33, 136, 115, 36, 132; $RealPassword = '76492d111
6743f0423413b16050a5345MgB8AFkASQAvAEUAbgB6AEsAZgBHAHAAdwBlAGMAdgBnAHoAMQBXAGlAaQBsAFEAPQA9
AHwAZgA2ADEAYwAyAGEAMQBiAGUAYwBhADAAOAA5ADlAMABmADkAOAA2ADAAZQBlADEAZAAwADEAMABjAGQAY
wA2AGQAYwA0AGYAZQBkADQAOQA0ADYAYQBiADQAYQAzADQAZQBmAGQAYwA3ADcANQBmADMANABmADkAYQA
wADAAYwAwAGYAOAA1AGMAYgBkAGQAYgBjAGlAYgA2ADgAMABlADlAMwBmAGQAMABjAGYAMwAzAGMAZQBiADYAY
wBlADYAZAA5ADYAYQA2ADQAYgAxADgANAAzAGUAZQAwAGlANQAzADkAZgAwAGMAMAA0ADcANgAzAGMANgBhAGE
AZABjAA==''; $SecurePass = ConvertTo-SecureString -String $RealPassword -Key $AESKey; $BSTR = [System.Runtime.Inter
opServices.Marshal]::SecureStringToBSTR($SecurePass); $UnsecurePassword = [System.Runtime.InteropServices.Marshal]::
PtrToStringAuto($BSTR); if ($UserPassword.equals($UnsecurePassword)) {     $flag = '76492d1116743f0423413b16050a5345
MgB8AFQATAB6AEEAVwB3AGUAcQA0AFkAdgB6ACsASgAvAFAARABuADkATgByAEEAPQA9AHwAMQBmADMAOAA2AD
YAMwBlADEAOQAxADUAZAAyAGYANwAzAGMAMgA0AGMAYgBjADgAZQBkAGMANAA5AGQAYgA1AGEAMwA2AGEAOQ
AzADEAZQAwAGYAYgA2ADUAZAA5ADgAMwA4ADkANAAyAGMAYgBjAGYAYgBlAGQAZQA5AGMAZQAyAGEANgBlAGQA
ZgA1ADAAZgAzADQANgBjADlANgAyAGMAMQAwADYAMwA0AGUAZgAzADkAMwBiADMAMQAyADAAZAAxADcAMAAwA
```

□მისათვის რომ უკეთ გავიცნოთ კოდი, შეგვიძლია ის გადავიტანოთ PowerShell ISE-ში

```powershell
$UserPassword = Read-Host -Prompt 'Enter your password';
$AESKey = [byte] 220, 22, 83, 174, 203, 44, 204, 117, 115, 154, 222, 39, 11, 56, 76, 254, 34, 89, 128, 71, 32, 229, 121, 173, 65, 102, 169, 33, 136, 115, 36, 132;
$RealPassword = '76492d1116743f0423413b16050a5345MgB8AFkASQAvAEUAbgB6AEsAZgBHAHAAdwBIAGMAdgBnAHoAMQBXAGIAaQBsAFEAPQA9AHwAZgA2ADEAYwAyAGEAMQBiAGUAYwBhADAAOAA5ADIAMABmADk
$SecurePass = ConvertTo-SecureString -String $RealPassword -Key $AESKey;
$BSTR = [System.Runtime.InteropServices.Marshal]::SecureStringToBSTR($SecurePass);
$UnsecurePassword = [System.Runtime.InteropServices.Marshal]::PtrToStringAuto($BSTR);
if ($UserPassword.equals($UnsecurePassword)) {     $flag = '76492d1116743f0423413b16050a5345MgB8AFQATAB6AEEAVwB3AGUAcQA0AFkAdgB6ACsASgAvAFAARABuADkATgByAEEAPQA9AHwAMQBm
    $flag_key_bytes = [System.Text.Encoding]::UTF8.GetBytes($UnsecurePassword);
    $SecureString = ConvertTo-SecureString $flag -Key $flag_key_bytes;
    $BSTR = [System.Runtime.InteropServices.Marshal]::SecureStringToBSTR($SecureString);
    $Unsecureflag = [System.Runtime.InteropServices.Marshal]::PtrToStringAuto($BSTR);
    Write-Host $Unsecureflag; } else {     Write-Host 'Invalid password.'; }
```

იმისათვის რომ ეს ამოცანა ამოვხსანათ, უნდა გავიგოთ თუ რა უნდა მოხდეს იმისათვის რომ ეკრანზე ამოიბეჭდოს $Unsecureflag.

□ირველ რიგში იმისათვის რომ ეს მოხდეს, უნდა დაკმაყოფილდეს if ($UserPassword.equals($UnsecurePassword)) დებულება, ანუ ჩვენი შეყვანილი პაროლი უნდა ემთხვეოდეს ნამდვილ პაროლს. □უმცა სისტემა ამას ამ დებულებების შემდეგ არსად ამოწმებს. □ესაბამისად შეგვიძლია დებულება მარტივად შევცვალოთ ასე: if (1). □ა მივიღოთ შედეგი