-- Write Up Pico CTF --

by dzzlr..

# Web Exploitation

## GET aHEAD

**Lorem Ipsum** is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.

# Cryptography

## Mod 26

**Encode Flag: cvpbPGS{arkg\_gvzr\_V'yy\_gel\_2\_ebhaqf\_bs\_ebg13\_MAZyqFQj}**

**Buka pada website** <https://cryptii.com/pipes/rot13-decoder>**, lalu *copy-paste* encode flag pada website tersebut. Sehingga akan muncul sebuah flag yang membentuk kata.**

**Flag: picoCTF{next\_time\_I'll\_try\_2\_rounds\_of\_rot13\_ZNMldSDw}**

# General Skills

## Obedient Cat

**Gunakan command pada wsl atau linux yaitu**

$cat [filename]

**Command itu membantu membaca data dari file dan memberikan kontennya sebagai output. Ini membantu kita untuk membuat, melihat, menggabungkan file.**

**Command pada terminal wsl**

|  |
| --- |
| **$cat flag** |

Maka, akan langsung muncul sebuah flag.

Flag: **picoCTF{s4n1ty\_v3r1f13d\_b5aeb3dd}**

## Python Wrangling

**Dalam soal tersebut terdapat sebuah hint yaitu berupa command**

**$man python**

**Terdapat 3 file dalam soal tersebut ‘ende.py’ sebagai source code untuk melakukan encode atau decode****, ‘pw.txt’ yang dicurigai berisi flag, ‘flag.txt.en’ sebagai encoder atau decodernya. Karena dalam soal tersebut terdapt hint, saya curiga ‘flag.txt.en’ tersebut sebagai decodernya dan ‘pw.txt’ sebagai input untuk password.**

**Command pada terminal wsl**

|  |
| --- |
| **$python3 ende.py -d flag.txt.en** |

Lalu, inputkan pw.txt maka akan langsung muncul sebuah flag.

Flag: **picoCTF{4p0110\_1n\_7h3\_h0us3\_aa821c16}**

## Wave a Flag

**Gunakan command pada wsl atau linux yaitu**

**$chmod [OPTION]... MODE[,MODE]... FILE....**

**Untuk memberikan permission pada file tersebut agar bisa di run lakukan command.**

**$chmod +x warm**

**Lalu jalankan file executable tersebut dengan command** $sudo ./warm**. Kemudian file tersebut akan mengeluarkan sebuah output berupa.**

**Hello user! Pass me a -h to learn what I can do!**

**Pada soal tersebut tedapat sebuah hint di outputnya yaitu** -h**.**

**Command pada terminal wsl**

|  |
| --- |
| **$sudo ./warm -h** |

Maka, akan langsung muncul sebuah outputnya.

Oh, help? I actually don't do much, but I do have this flag here: picoCTF{b1scu1ts\_4nd\_gr4vy\_755f3544}

Flag: **picoCTF{b1scu1ts\_4nd\_gr4vy\_755f3544}**

## Nice netcat...

**Gunakan command pada wsl atau linux yaitu**

**$nc [options] host port**

**Netcat adalah utilitas baris perintah yang membaca dan menulis data melalui koneksi jaringan, menggunakan protokol TCP atau UDP. Untuk mendapatkan soalnya masukkan command** $nc mercury.picoctf.net 43239 Setelah itu akan muncul beberapa bilangan yang dicurigai merupakan karakter pada ASCII table. Kemudian, saya membuat sebuah algoritma menggunakan python3 untuk mengetahui output yang sebenarnya.

**Source code python3.**

|  |
| --- |
| **unsolve = [112,105,99,111,67,84,70,123,103,48,48,100,95,107,49,116,116,121,**  **33,95,110,49,99,51,95,107,49,116,116,121,33,95,55,99,48,56,50,**  **49,102,53,125,10]**  **for word\_decode in unsolve:**  **print(chr(word\_decode), end="")** |

Maka, akan langsung muncul sebuah outputnya.

Flag: **picoCTF{g00d\_k1tty!\_n1c3\_k1tty!\_7c0821f5}**

## Static ain't always noise

**Gunakan command pada wsl atau linux yaitu**

**$chmod [OPTION]... MODE[,MODE]... FILE....**

**Untuk memberikan permission pada file tersebut agar bisa di run lakukan command.**

**$chmod +x ltdis.sh**

**Lalu jalankan file executable tersebut dengan command** $sudo ./ltdis.sh **Kemudian file tersebut akan mengeluarkan output namun terdeteksi failed. Maka lakukanlah lagi command** $sudo ./ltdis.sh static agar file ‘static’ bisa dijalankan oleh script bash. Akhirnya terdapat beberapa file yang terekstrak (decompile) menjadi beberapa bagian. Lalu, mencoba command $cat satu per satu file dan menemukan sebuah flag dalam file ‘static.ltdis.strings.txt’.

**Command pada terminal wsl**

|  |
| --- |
| **$cat static.ltdis.strings.txt** |

Maka, dalam file tersebut terdapat sebuah string dalam satu baris yang mencirikan sebuah flag.

Flag: **picoCTF{d15a5m\_t34s3r\_1e6a7731}**

## Tab, Tab, Attack

**Gunakan command pada wsl atau linux yaitu**

**$unzip [FILE]**

**Untuk ektrak file ‘Addadshashanammu.zip’ gunakan zip.**

**$unzip Addadshashanammu.zip**

**Lalu akan muncul sebuah folder, dalam folder tersebut terdapat folder lagi. Sesuai dengan nama soal dalam terminal kita mesti memasuki inti dari folder tersebut. Akhir dari folder-folder tersebut terdapat file ‘fang-of-haynekhtnamet’. Kemudian saya melakukan** $cat namun terbaca seperti executable menggunakan gcc. Akhirnya saya menjalankan file tersebut.

**Command pada terminal wsl**

|  |
| --- |
| **$./fang-of-haynekhtnamet** |

Maka, dalam file tersebut terdapat sebuah string dalam satu baris yang mencirikan sebuah flag.

Flag: **picoCTF{l3v3l\_up!\_t4k3\_4\_r35t!\_524e3dc4}**

## Magikarp Ground Mission

**Gunakan command pada wsl atau linux yaitu**

**$ssh your\_username@host\_ip\_address [MODE] [VALUE]**

**Untuk masuk ke dalam server yang telah dibuatkan oleh picoCTF.**

**$ssh** [ctf-palyer@venus.picoctf.net](mailto:ctf-palyer@venus.picoctf.net) **-p 57767 6d448c9c**

**Lalu akan masuk dalam sistem tersebut dan terdapat beberapa folder serta clue. Saya mesti mengumpulkan semua clue yang dapat dilihat dari folder file ‘instructions-to-2of3.txt’ dan mesti juga untuk melakukan $cat pada file ‘1of3.flag.txt’. Untuk setiap nama file pada flag dan instructions memiliki pola yang sama sehingga kita hanya mesti mencari file tersebut berada dimana.**

**Command pada terminal wsl**

|  |
| --- |
| **$cat 1of3.flag.txt, 2of3.flag.txt, 3of3.flag.txt** |

Sehingga hasil dari pengumpulan flag tersebut akan membentuk outputnya.

Flag: **picoCTF{xxsh\_0ut\_0f\_//4t3r\_5190b070}**