BEECTF

QUALIFICATION 2025

Nama Lengkap	:	Muhammad Rayhan Ramadhan
Sekolah	:	SMKN 5 TELKOM BANDA ACEH
Username	:	Rehan23

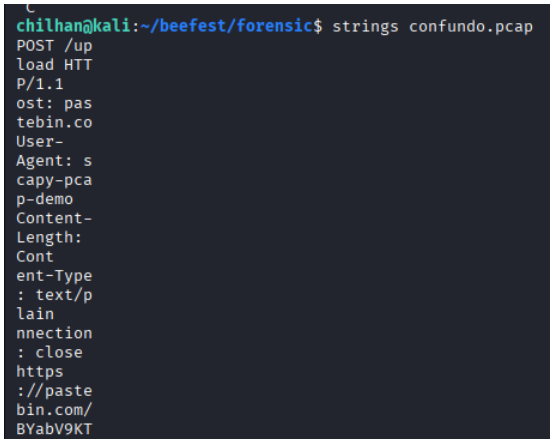
Daftar Isi

Forensics

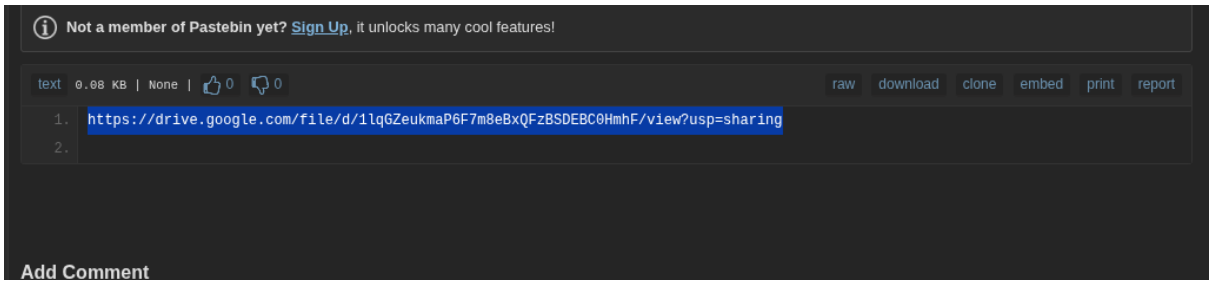
[Nama_Challenge]

Zimzamlabim

Langkahh Penyelesaian:
Pada Challenge ini kita diberikan sebuah file pcap pertama aku buka dengan wireshark dan tidak menemukan apa2 terus karna stuck aku iseng tes menggunakan strings dan dapat sebuah alamat url

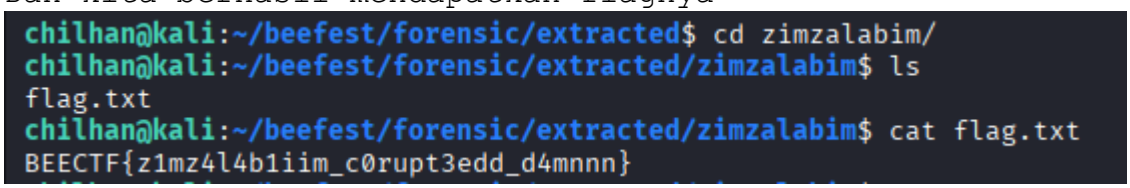


Setelah aku buka alamat URLnya terdapat sebuah link google drive



Saat Aku buka linknya terdapat sebuah file berbentuk zip dengan flag didalamnya langsung saja aku download dan esktrak

Dan kita berhasil mendapatkan flagnya



Flag: BEECTF{z1mz4l4b1iim_c0rupt3edd_d4mnnn}

WEB_Exploitation

Message To The Hellow

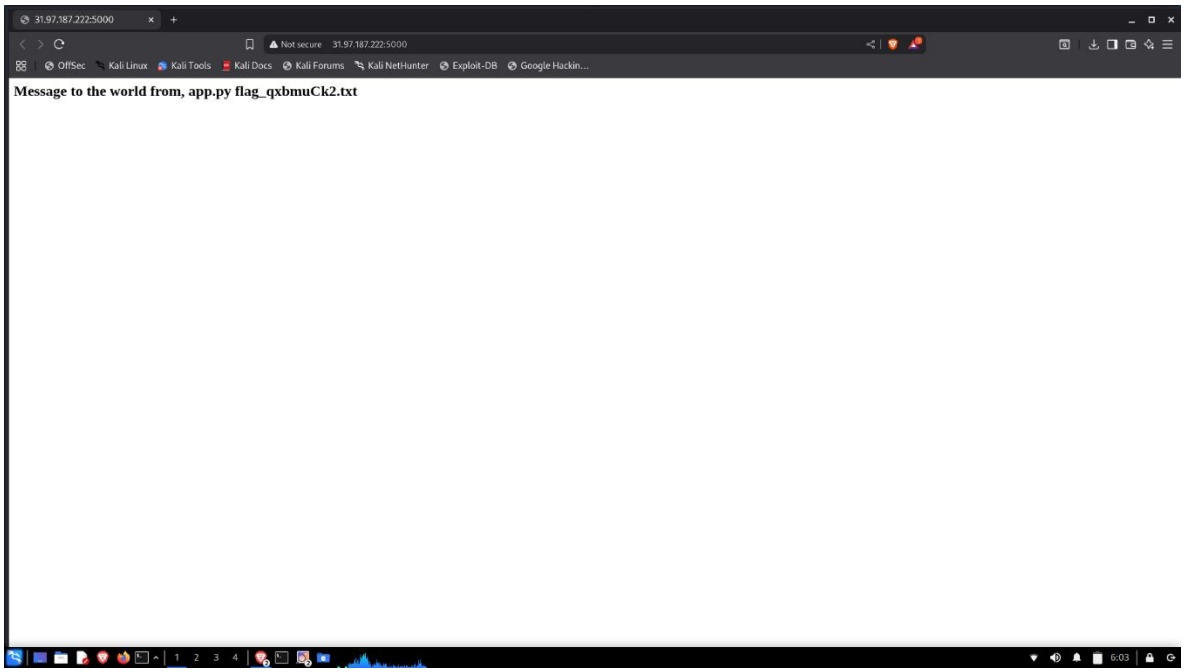
Langkah Penyelesaian:
Pada challenge web kali ini kita berikan web yang dapat menampilkan author dan message yang kita input di halaman web Karena aku pernah menyelesaikan tantangan SSTI di picoctf aku coba {{7*7}} dan web menampilkan mendeteksi input ssti di author dan message kemudian aku coba pakai payload
{{url_for.__globals__['os'].__getattribute__('popen')('cat flag.txt').read()}}

Akan tetapi tetap muncul error yan sama yaitu mendeteksi,disini sesuai kode yang diberikan ada beberapa input yg di ban di challenge ini yang dimana jika character yang ada didalam array banned terdeteksi oleh input dan lebih dari 2(character yang di banned missal BANNED = ["{{",""}}"] dan kita input {{ 7 * 7 }} maka akan terdeteksi sebagai ssti karna menggunakan lebih dari sama dengan 2 character yg dibanned aku gatau cara jelasinnya semoga kalian paham :D) Disitu aku sempat kebingungan kemudian aku searching dan mengetahui bahwa jika kita gunakan seperti ini "p" + "o" + "p" + "e" + "n" maka system tidak mendeteksi itu sebagai character yg dibanned akan tetapi ada masalah yaitu {{}} jika aku memasukan }} pada akhir payload maka akan terdeteksi contoh :
{{url_for.__globals__['o'+'s'].__getattribute__('p'+'o'+'p'+'e'+'n')('cat flag.txt').read()}}

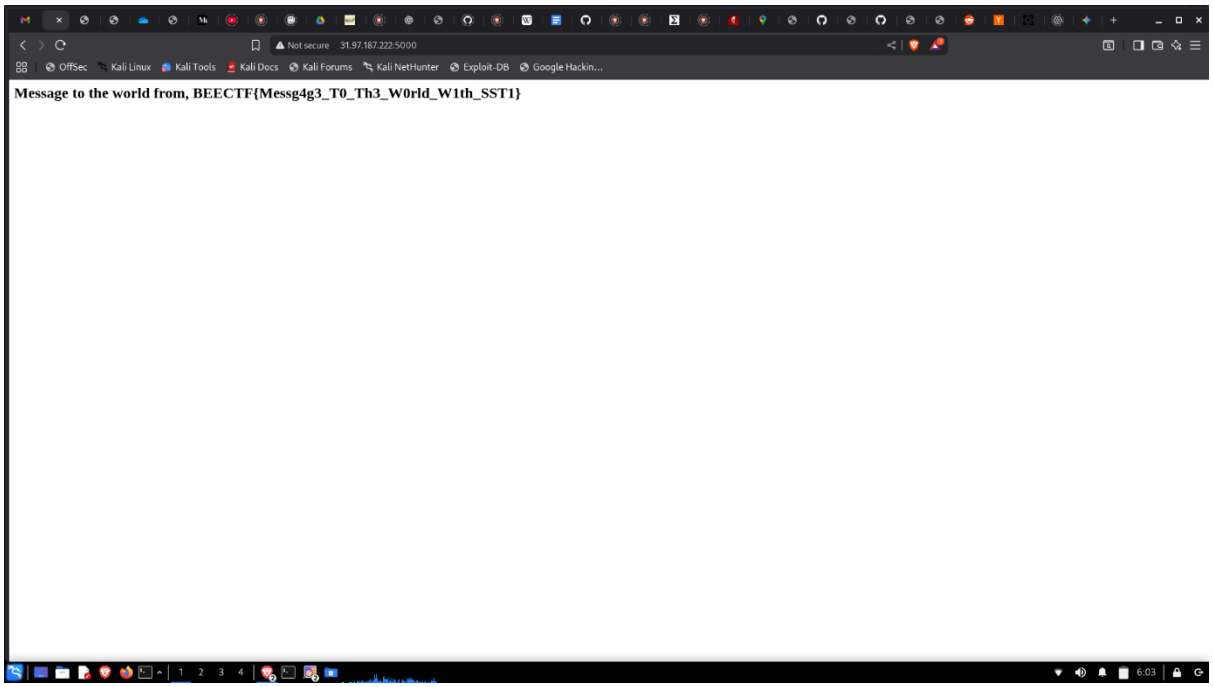
Maka aku memikirkan lagi gimana car aga terdeteksi oleh system dan setelah aku baca lagi source code nya aku liat ada sebuah variable yang menampung input dari author dan message menjadi satu yg dimana jika aku input ke
author {{url_for.__globals__['o'+'s'].__getattribute__('p'+'o'+'p'+'e'+'n')('cat flag.txt').read()
Dan di message }} maka input tidak akan mendeteksi itu ssti karna string yg dibanned yg kumasukan hanya {{ di author dan message }} (tidak lebih dari sama dengan 2)

Aku masukan payload ini di author
{{url_for.__globals__['o'+'s'].__getattribute__('p'+'o'+'p'+'e'+'n')('cat flag.txt').read()
Dan ini di message }} dan berhasill cuman kosong yang berarti flag tidak ada disitu
Aku kemudian baca lagi isi file yg diberikan di challenge dan mendapati sesuatu di dockerfile y aitu adalah lokasi flag yaitu di /app

Kemudian aku gunakan {{url_for.__globals__['o'+'s'].__getattribute__('p'+'o'+'p'+'e'+'n')('ls /app/').read()}}



Dan kita dapat nama file flagnya tinggal kita cat {{url_for.__globals__['o'+'s'].__getattribute__('p'+'o'+'p'+'e'+'n')('cat /app/flag.txtt').read()}} (malas ngetik nama filenya cik:v)
Dan kita dapat flagnya



Flag: BeeCTF{Messg4g3_To_Th3_World_Wih_SSTI}

Sekian Terimakasih