CYBER JAWARA

NAMA TIM : [Pengen Solved Soal PWN]

Sabtu, 03 Desember 2022

MEMBER	
1	Muh Fani Akbar
2	Muhammad Ichwan
3	Paska Parahita

Daftar Isi

WEB

Wordpress Enjoyer

Soal:

I just installed wordpress to host my epic hacking course. Please let me know if there is a vuln.

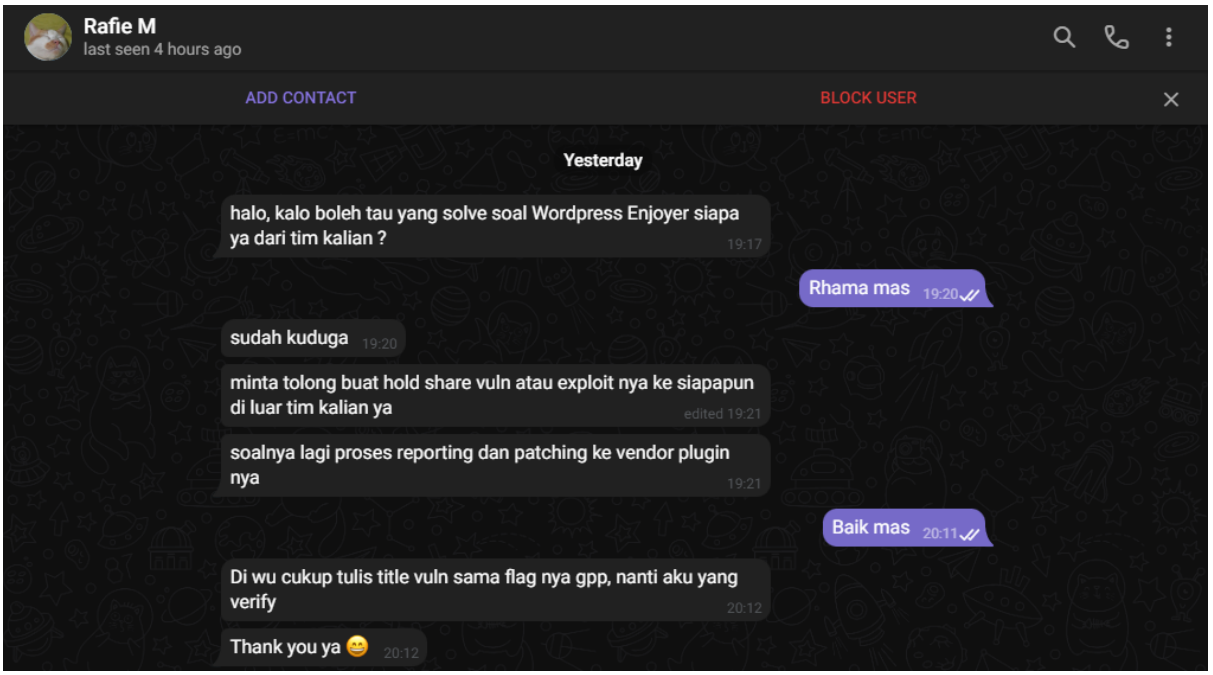
NOTE: this is a fully whitebox challenge, no need to bruteforce anything (login, endpoint, etc). The team that associated with the IP that detected try to do a heavy bruteforce will be given a penalty point.

http://167.172.80.90:8686/

Author: Yeraisci

Solving Scenario:

Terdapat bug LFI di plugin learnpress



FLAG : CJ2022{just_classic_vuln_nothing_spectacular_here_98287b9a}

Fetch Your Way

Soal:

I make this simple fetch app. Not so sure if it's good or not :/

NOTE: this is a fully whitebox challenge, no need to bruteforce anything (login, endpoint, etc). The team that associated with the IP that detected try to do a heavy bruteforce will be given a penalty point.

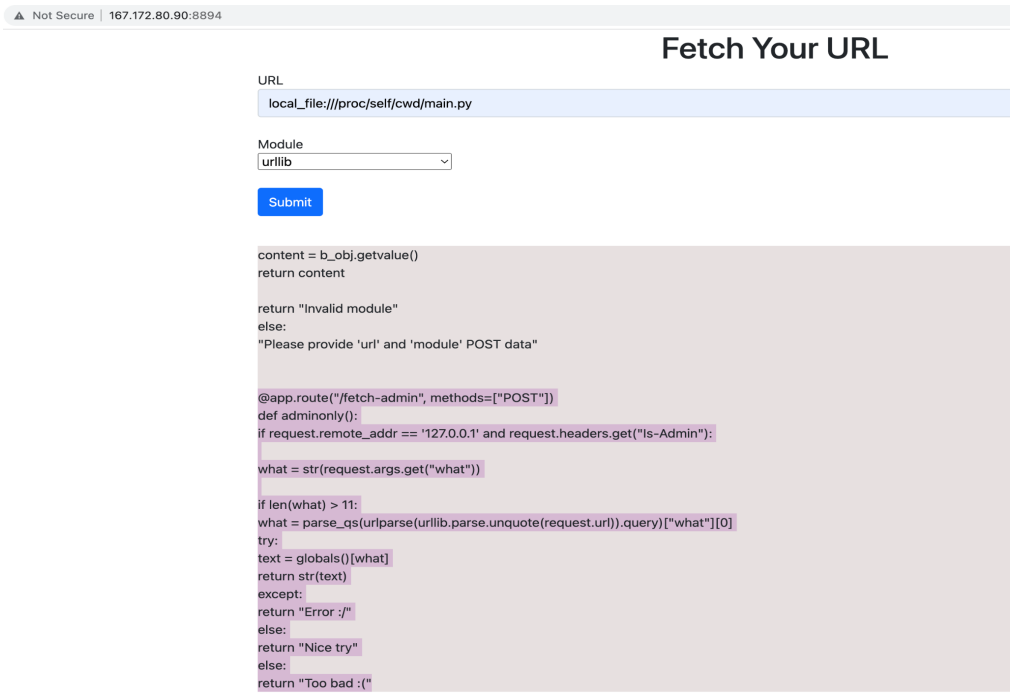
http://167.172.80.90:8894/

Author: Yeraisci

Solving Scenario:

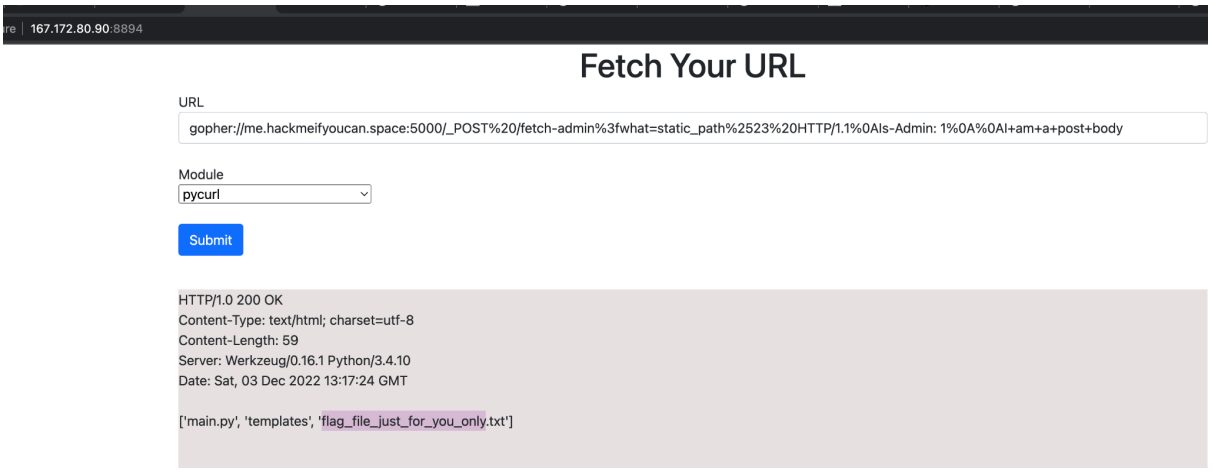
Terdapat 2 module yang bisa digunakan untuk fetch remote resource yaitu urllib dan pycurl.
urllib : kami gunakan untuk local file read
pycurl : kami gunakan untuk SSRF protocol gopher untuk mengirimkan packet HTTP ke /fetch_admin

Pertama, untuk mendapatkan full source dan melihat fungsi yang hilang pada main.py dari source code yang diberikan, kami melakukan local file read main.py untuk mendapatkan source code asli nya.



Diketahui bahwa fungsi yang hilang tersebut melakukan route ke /fetch-admin dengan beberapa kondisi didalamnya yang harus terpenuhi seperti request.remote_addr dan request.headers.get. Namun, terdapat filter untuk ipaddress localhost. Kami melakukan dns

binding untuk membypass nya. Langsung saja untuk solver nya kami menggunakan gopher untuk melakukan SSRF dan mengirimkan paket HTTP ke /fetch-admin dengan menyesuaikan kondisinya.



Karena nama file flag nya sudah didapatkan, tinggal read flag tersebut menggunakan module urllib.

FLAG : CJ2022{understanding_and_chaining_cve_are_an_art_itself_8b2a3090}

Flag Ceker

Soal:

Huh ASCII??? Yowai Mo!!!

http://167.172.80.90:10971/index.php

15 jam enak turu daripada ctf

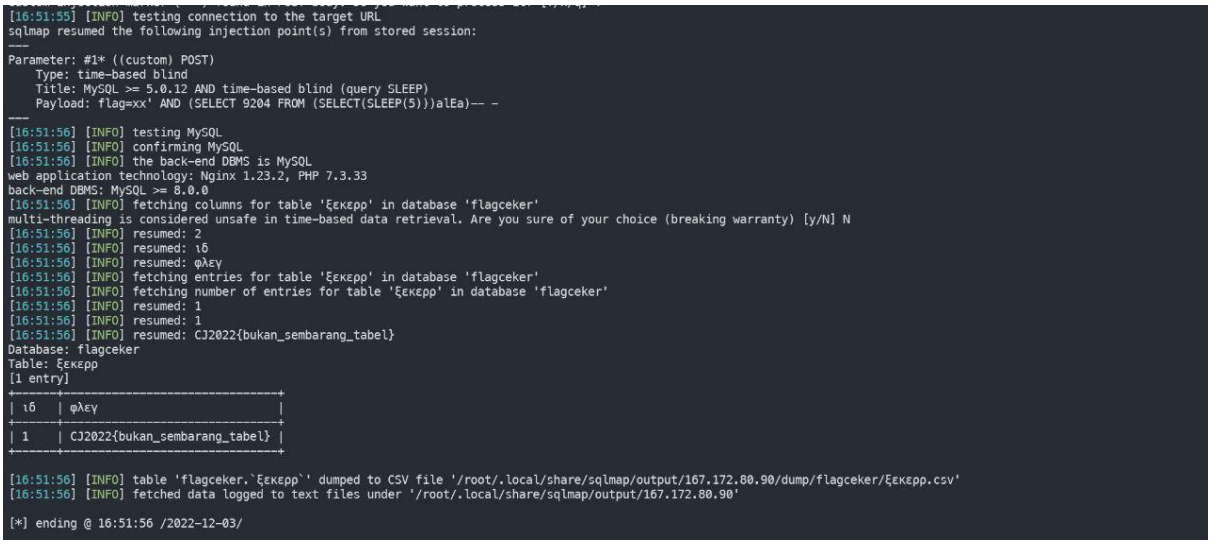
Author: cacadosman

Solving Scenario:

Disini kami menggunakan sqlmap untuk penyelesaiannya karena tidak mengetahui bahwa SQLmap dilarang (tidak baca discord :(). Diketahui bahwa website vuln terhadap time-based sql injection. Untuk payload yang kami gunakan adalah :

python3 sqlmap.py -u http://167.172.80.90:10971/index.php --data 'flag=x*' --threads 3 --batch --dbms MySQL --delay=0.7 --prefix "x'" --suffix "-- -" --level 2 --risk 2 --random-agent --technique BT -D flagceker -T 'ξεκερρ' --dump --hex

Pada payload tersebut kami setting delay selama 0.7, ya tentu saja tetap dilarang menggunakan sqlmap karena baru membaca discord 30 menit sebelum submit writeup selesai jadi tidak bisa bikin scripting :(. Setelah dijalankan, didapatkan flag pada output sqlmap tersebut.



FLAG : CJ2022{bukan_sembarang_tabel}

Reverse Engineering

BabyRev

Soal:

Intro Bois Author: lunashci

Solving Scenario:

Lakukan decompile binary babyrev untuk mempermudah melakukan static analisis flow code nya.

```
1  int __fastcall main(int a1, char **a2, char **a3)
2  {
3    int result; // eax
4    char s2[32]; // [rsp+0h] [rbp-50h] BYREF
5    char s1[43]; // [rsp+20h] [rbp-30h] BYREF
6    char v6; // [rsp+4Bh] [rbp-5h]
7    int i; // [rsp+4Ch] [rbp-4h]
8
9    for ( i = 0; i <= 29; ++i )
10   {
11     v6 = off_6360[i] ^ *((_BYTE *)off_6368 + i);
12     s2[i] = v6;
13   }
14   puts("Whats the flag?");
15   __isoc99_scanf("%s", s1);
16   if ( !strcmp(s1, s2) )
17     result = puts("Correct!");
18   else
19     result = puts("Wrong!");
20   return result;
21 }
```

Diketahui bahwa inputan kita (s1) akan dilakukan komparasi/perbandingan dengan s2, dimana s2 tersebut sebelumnya adalah hasil dari XOR dari off_6360 dan 0ff_6368. Setelah dilakukan perbandingan maka akan masuk kedalam if condition apabila inputan kita (s1) dan s2 sama maka akan menampilkan “Correct!”, namun apabila salah maka akan menampilkan “Wrong!”. Langsung saja untuk mempermudah kita mengetahui output dari s2 tersebut atau nilai yang di compare dengan inputan kita, kami menggunakan ltrace untuk penyelesaiannya.

```
Shell-$ ltrace ./babyrev
puts("Whats the flag?"Whats the flag?
)                           = 16
__isoc99_scanf(0x56417ca1f665, 0x7ffda183d7a0, 1, 0x7f4dc8caaa37Pengen Solved So
al PWN
) = 1
strcmp("Pengen", "CJ2022{no_strings_just_ltrace}") = 13
puts("Wrong!"Wrong!
)                                   = 7
+++ exited (status 7) +++
```

Diketahui bahwa inputan kita “Pengen Solved Soal PWN” dilakukan compare dengan CJ2022{no_strings_just_ltrace}. Langsung saja kami validasi apakah CJ2022 tersebut benar dengan menjalankan binary babyrev nya dan CJ2022 tersebut sebagai inputan.

```
Shell-$ ./babyrev
Whats the flag?
CJ2022{no_strings_just_ltrace}
Correct!
```

FLAG : CJ2022{no_strings_just_ltrace}

Sekr3T Message

Soal:

Slamet mendapatkan file yang berisi pesan dari Joko, tetapi sebelum membaca pesan tersebut si Slamet harus mendapatkan Kode terlebih dahulu.

Bantu si Slamet mendapatkan isi pesan dari Joko ya kawan2.

Author: KangGorengan

Solving Scenario:

Lakukan decompile binary Sekr3T untuk mempermudah melakukan static analisis flow code nya.

```
{
  int v0; // edi
  int v1; // esi
  int v2; // edx
  int v3; // ecx
  __int64 v4; // r8
  __int64 v5; // r9
  int v6; // edx
  int v7; // er8
  int v8; // er9
  _QWORD *v9; // [rsp+8h] [rbp-98h]
  __int64 v10[3]; // [rsp+80h] [rbp-20h] BYREF

  if ( (unsigned __int64)v10 <= *(_QWORD *)(__readfsqword(0xFFFFFFF8) + 16) )
    runtime_morestack_noctxt();
  v10[1] = (__int64)&unk_4AB9C0;
  v10[2] = (__int64)&off_4E9260;
  v9 = (_QWORD *)os_Stdout;
  fmt_Fprintln();
  runtime_newobject(v0, v1, v2, v3, v4, v5);
  v10[0] = (__int64)v9;
  fmt_Fscanln();
  if ( *v9 == 666640444133377LL )
    runtime_convTstring(v0, v1, v6, (_DWORD)v9, v7, v8, (__int64)&unk_4D5E77, 43LL);
  fmt_Fprintln();
  fmt_Fscanln();
}
```

Diketahui bahwa pada binary hanya terdapat satu kondisi dimana inputan kita akan dilakukan compare atau perbandingan dengan 666640444133377. Apabila inputan kita bernilai sama, maka akan menjalankan fungsi runtime_convTstring. Karena nilai perbandingan sudah diketahui, maka untuk penyelesaiannya langsung saja kita masukkan 666640444133377 sebagai inputan.

```
Shell-$ ./Sekr3T
Masukan Kode Dulu Kang~
666640444133377
Q0oyMDIye1MxbjR1X0Jlbl82YV9LM3QxbmdnNGw0Tn0
```

Didapatkan output berupa Q0oyMDIye1MxbjR1X0Jlbl82YV9LM3QxbmdnNGw0Tn0 yang kemungkinan adalah base64. Disini kami melakukan decode menggunakan magic Cyberchef dan mendapatkan flagnya.

Recipe (click to load)	Result snippet	Properties
From_Base64('A-Za-z0-9-_',true,false)	CJ2022{S1n4u_Ben_6a_K3t1ngg4l4N}	Matching ops: Decode NetBIOS Name, From Base85 Valid UTF8 Entropy: 4.28

FLAG : CJ2022{S1n4u_Ben_6a_K3t1ngg4l4N}.

Misc

Your ImageNation

Soal:

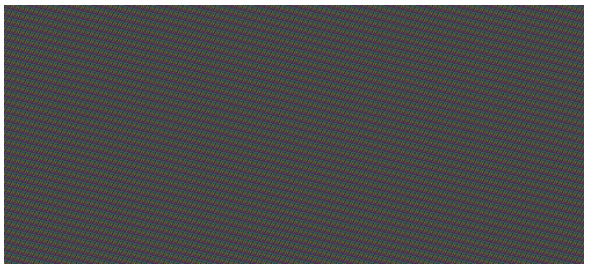
Siti mendapatkan file gambar yang ternyata berupa gambar garis bergaris menjadi satu.

Kawan2 dapat membantu siti apakah terdapat pesan tersembunyi di balik gambar tersebut.

Author: KangGorengan

Solving Scenario:

Diberikan file png ketika dibuka berupa gambar garis



Kita diminta untuk mencari pesan tersembunyi. Kami menduga pesan disembunyikan dengan metode lsb, ketika dicoba dengan zsteg ditemukan flagnya pada b8. rgb, lsb, xy.

```
root@ExpectoPatronum:~# zsteg -a ImageNation.png
b8,r,lsb,xy         .. text: "C0{5_0_SH}223!00eH!J2WHy0WHiC0{5_0_SH}223!00eH!J2WHy0WH
iC0{5_0_SH}223!00eH!J2WHy0WHiC0{5_0_SH}223!00eH!J2WHy0WHiC0{5_0_SH}223!00eH!J2WHy0WHi
C0{5_0_SH}223!00eH!J2WHy0WHiC0{5_0_SH}223!00eH!J2WHy0WHiC0{5_0_SH}223!00eH!J2WHy0WHiC
0{5_0_SH}223!00eH!J2WHy0WHiC0{5"
b8,g,lsb,xy         .. text: "J2WHy0WHiC0{5_0_SH}223!00eH!J2WHy0WHiC0{5_0_SH}223!00eH
!J2WHy0WHiC0{5_0_SH}223!00eH!J2WHy0WHiC0{5_0_SH}223!00eH!J2WHy0WHiC0{5_0_SH}223!00eH!
J2WHy0WHiC0{5_0_SH}223!00eH!J2WHy0WHiC0{5_0_SH}223!00eH!J2WHy0WHiC0{5_0_SH}223!00eH!J
2WHy0WHiC0{5_0_SH}223!00eH!J2WH"
b8,b,lsb,xy         .. text: "223!00eH!J2WHy0WHiC0{5_0_SH}223!00eH!J2WHy0WHiC0{5_0_SH
}223!00eH!J2WHy0WHiC0{5_0_SH}223!00eH!J2WHy0WHiC0{5_0_SH}223!00eH!J2WHy0WHiC0{5_0_SH}
223!00eH!J2WHy0WHiC0{5_0_SH}223!00eH!J2WHy0WHiC0{5_0_SH}223!00eH!J2WHy0WHiC0{5_0_SH}2
23!00eH!J2WHy0WHiC0{5_0_SH}223!"
b8,rgb,lsb,xy       .. text: "CJ2022{W35H!_y0000_WeSHHHi!}CJ2022{W35H!_y0000_WeSHHHi!
}CJ2022{W35H!_y0000_WeSHHHi!}CJ2022{W35H!_y0000_WeSHHHi!}CJ2022{W35H!_y0000_WeSHHHi!}
CJ2022{W35H!_y0000_WeSHHHi!}CJ2022{W35H!_y0000_WeSHHHi!}CJ2022{W35H!_y0000_WeSHHHi!}C
J2022{W35H!_y0000_WeSHHHi!}CJ20"
```

FLAG : CJ2022{W35H!_y0000_WeSHHHi!}