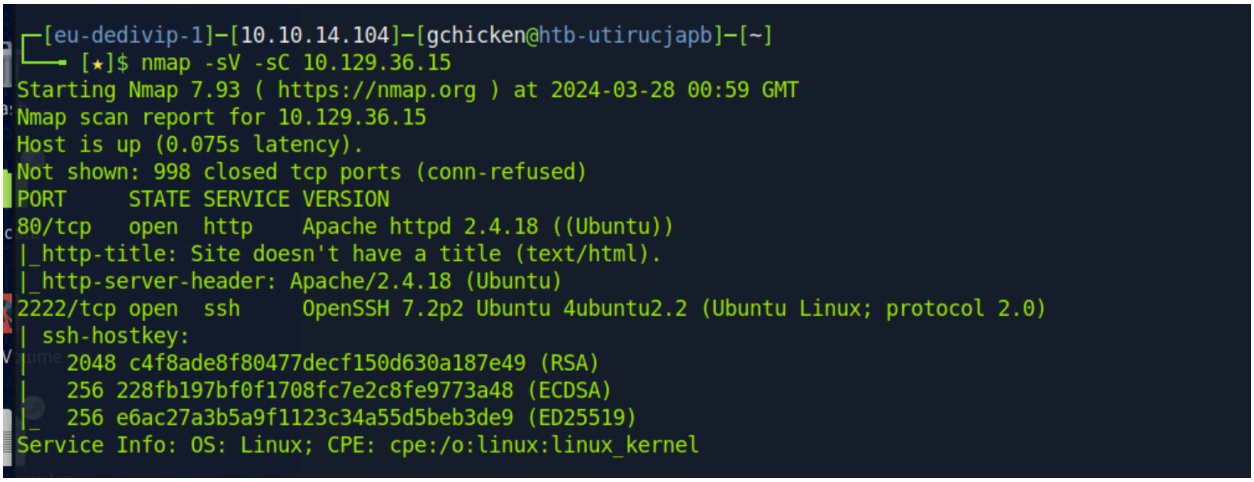
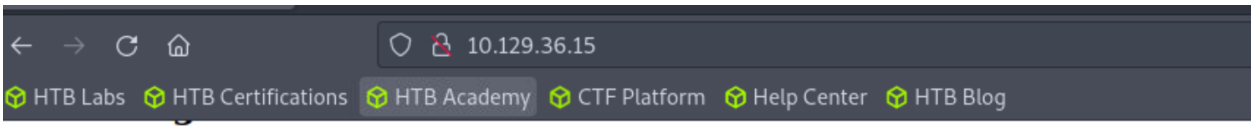
Shocker

~Gavin G

Initial Nmap Scan and Website Discovery

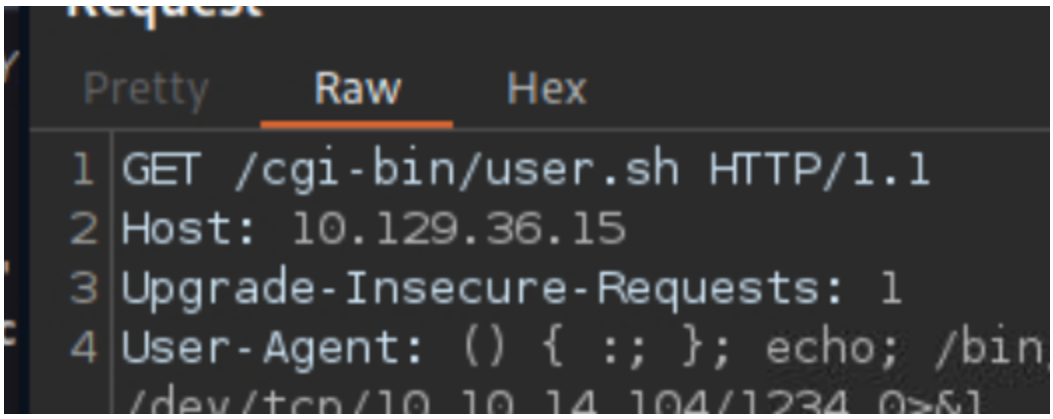
During the initial Nmap scan, ports 2222 and 80 were found to be open, with port 2222 running SSH. We decided to investigate port 80 further and discovered a website hosting a page titled "Don't Bug Me." This finding prompted further exploration to identify any potential vulnerabilities or interesting functionalities within the website.





Discovery: CGI-Bin Directory and User Script

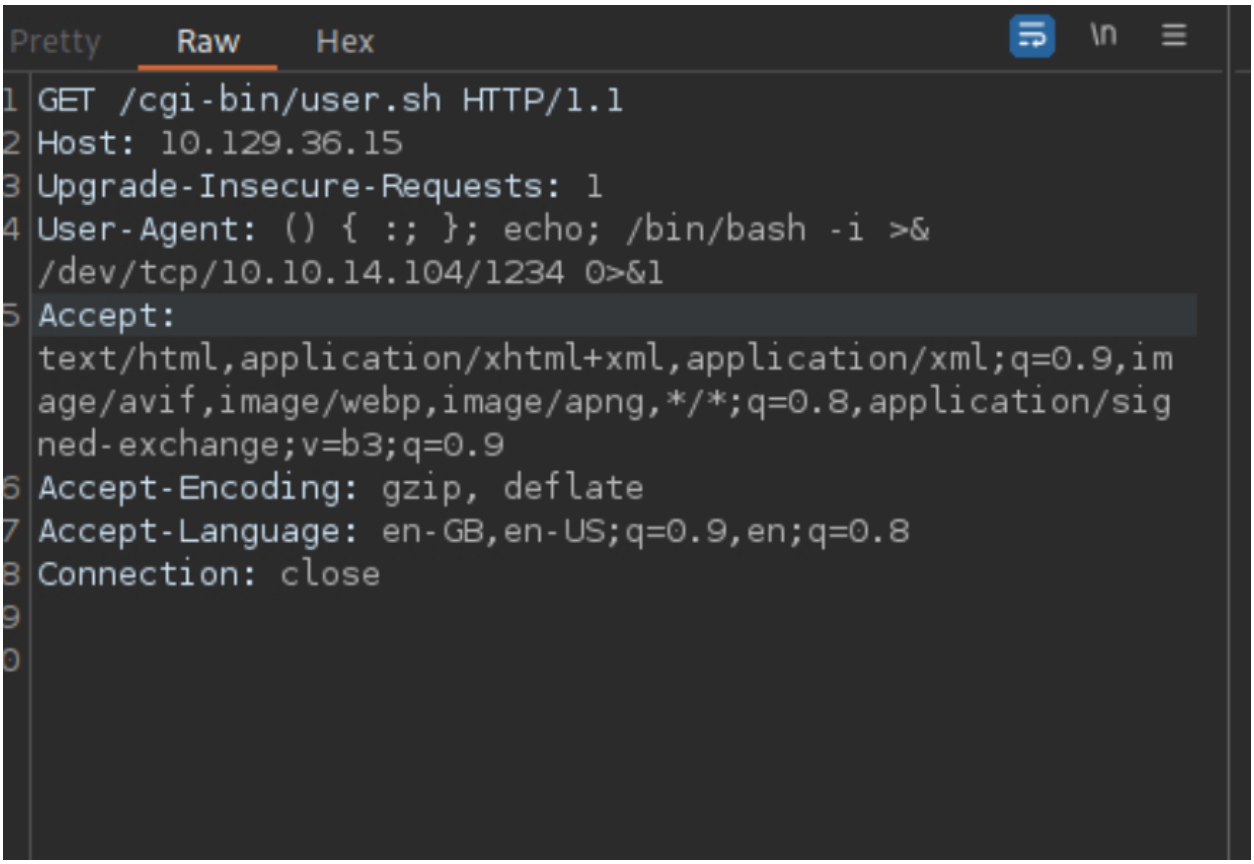
During enumeration using tools such as Gobuster and Dirbuster, a CGI-Bin directory was uncovered on the Apache server. Within this directory, a script named "user.sh" was discovered. Further analysis of this script revealed potential functionalities or vulnerabilities that could be explored during the penetration testing process.

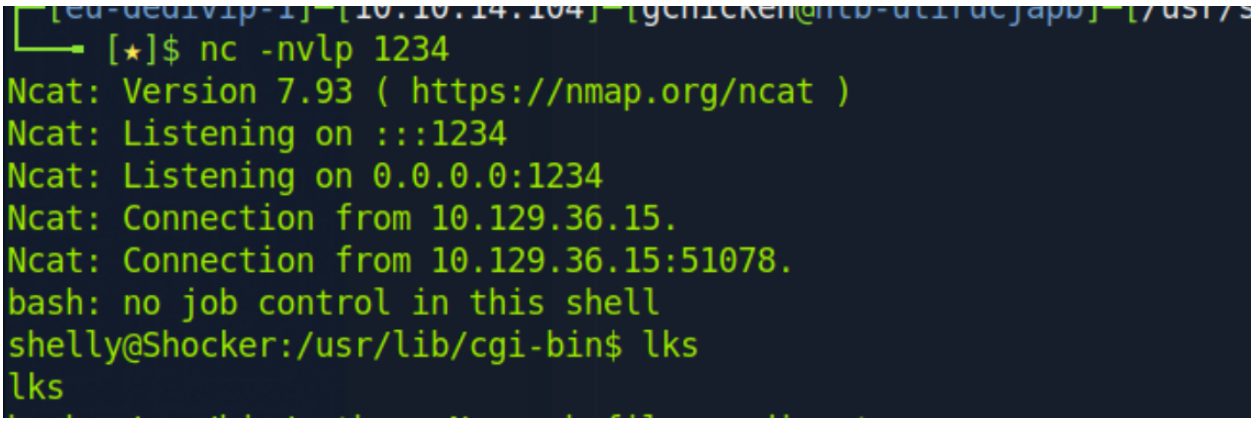


Exploiting Shellshock Vulnerability to Obtain Shell Access

Given that the target system is named "Shocker," it's prudent to test for the Shellshock vulnerability, which affects the Bash shell. We plan to exploit this

vulnerability to gain unauthorized shell access to the target system. By crafting specific HTTP requests that exploit the vulnerability, we aim to execute arbitrary commands on the server and establish a reverse shell connection, thereby gaining control over the target system's command line interface.





Post-Shell Access Actions

After obtaining shell access, we navigated to the home directory ('cd ~') and retrieved the user flag by using the 'cat' command. With the user flag obtained, we proceeded to investigate potential privilege escalation opportunities. By executing 'sudo -l' on the 'shelly' account, it was discovered that she possesses sudo privileges to run Perl commands without requiring a password, offering a straightforward path for privilege escalation.

Exploitation and Root Shell Achievement

In our pursuit of privilege escalation, we visited revshells.com to explore potential options. Opting for a Perl reverse shell, we input our IP address and executed the shell on the compromised account. After setting up a listener, the exploit succeeded, granting us a root shell. HAZZAH, root access achieved!