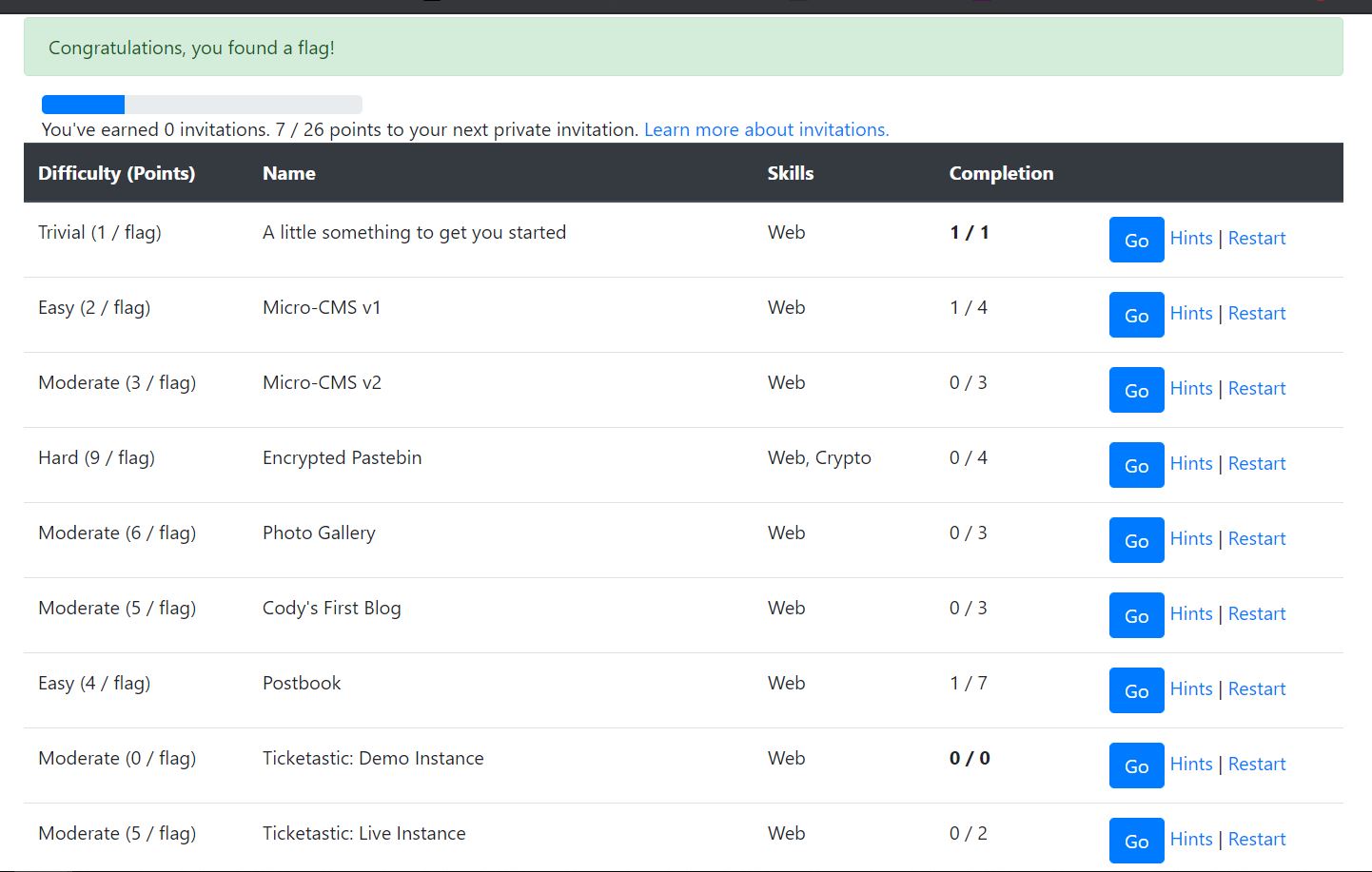
**Current Progress of Bug Bounty**

1. Studied basic concepts about bug bounty
2. Hackone.com account created and studied hacktivity activities.
3. Studied Hacker101 basic hacker tools.
4. Learning videos and materials mainly about Burpsuite , OWASP ZAP , Metasploit.
5. Configured Docker setup for sample vulnerable web site (DVWA).
6. Hack the Box started.
7. Further studying CTF.
8. Further studying different tools and vulnerability identification methods.
9. Further studying Hack the box different challenges.
10. Next step is to attack web sites published in hackerone.com.

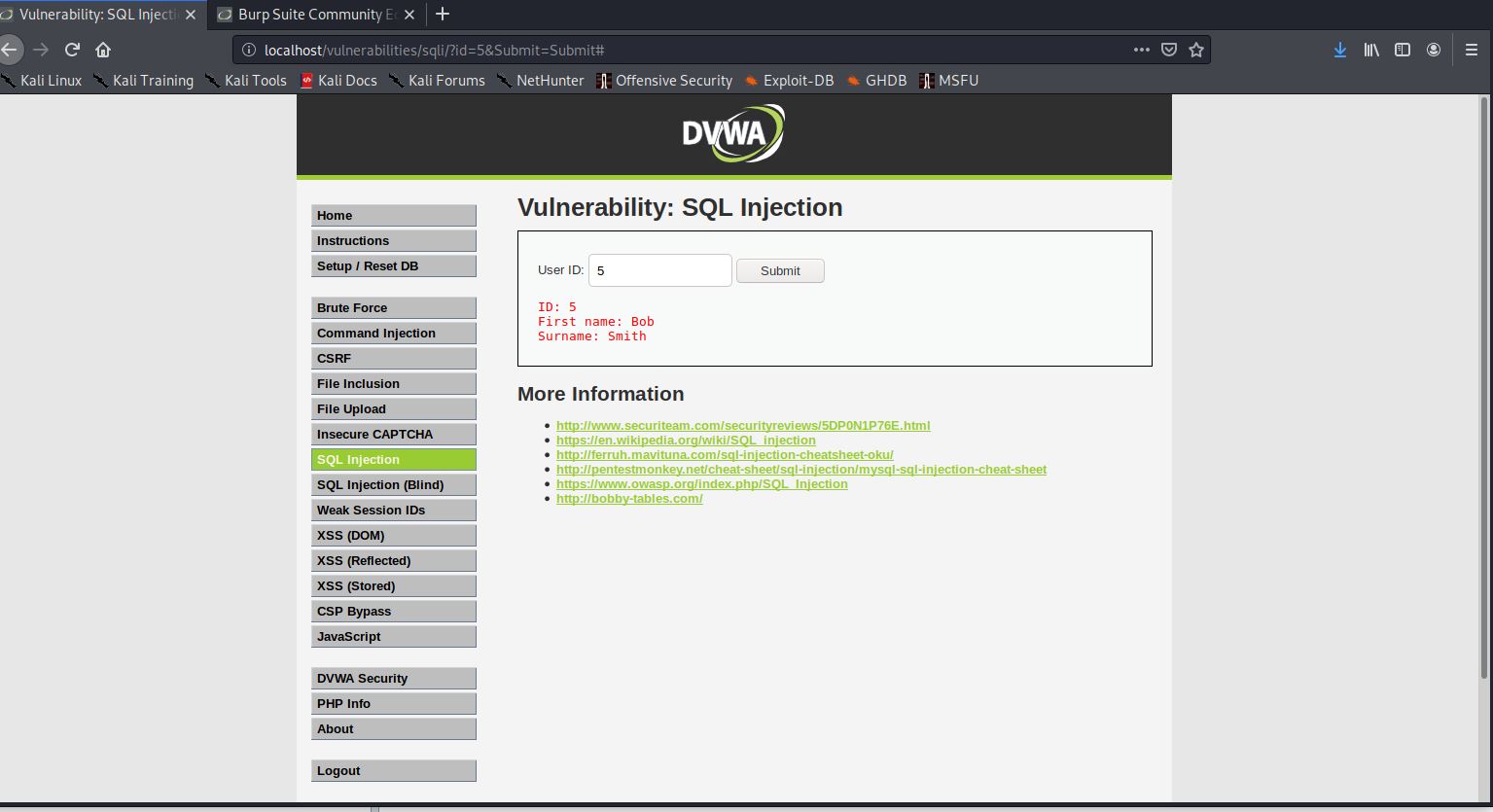
**One Drive URL:**

<https://mysliit-my.sharepoint.com/:f:/g/personal/ms19814520_my_sliit_lk/Eshpv499g-JNssyp6Fe_vNQBmVl1EDlzr_fFfuMUlMb-5g?e=CW9v6V>

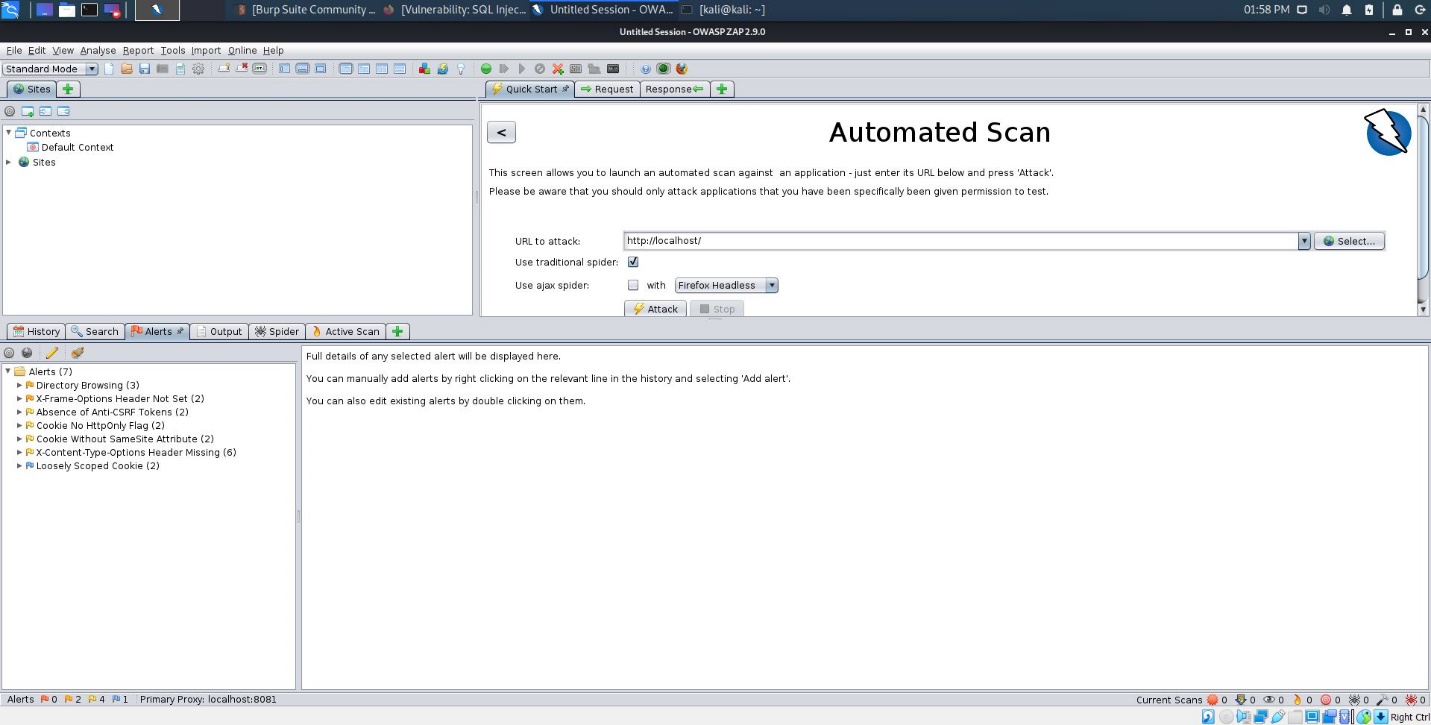
**Hacker101CTF**



**DVWA Vulnerable Web portal**

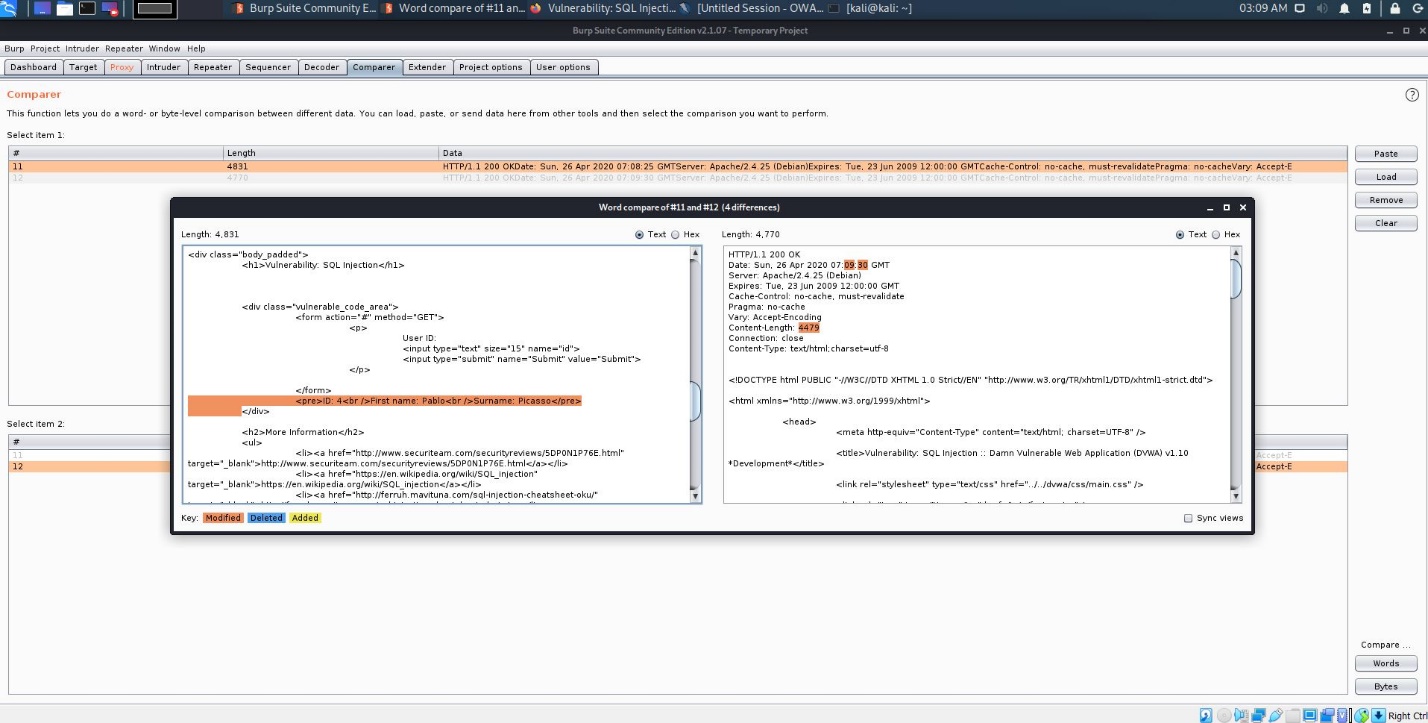
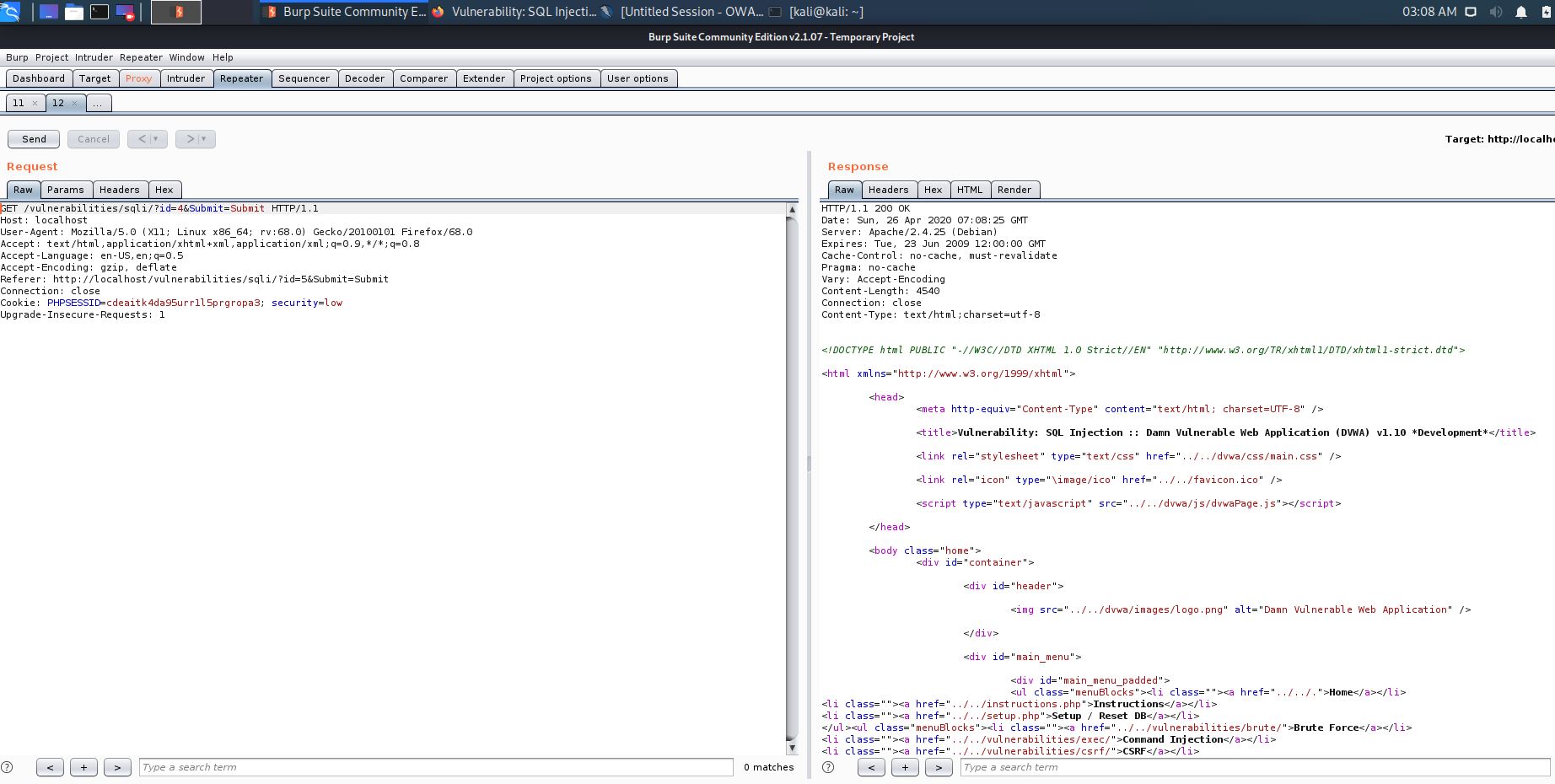
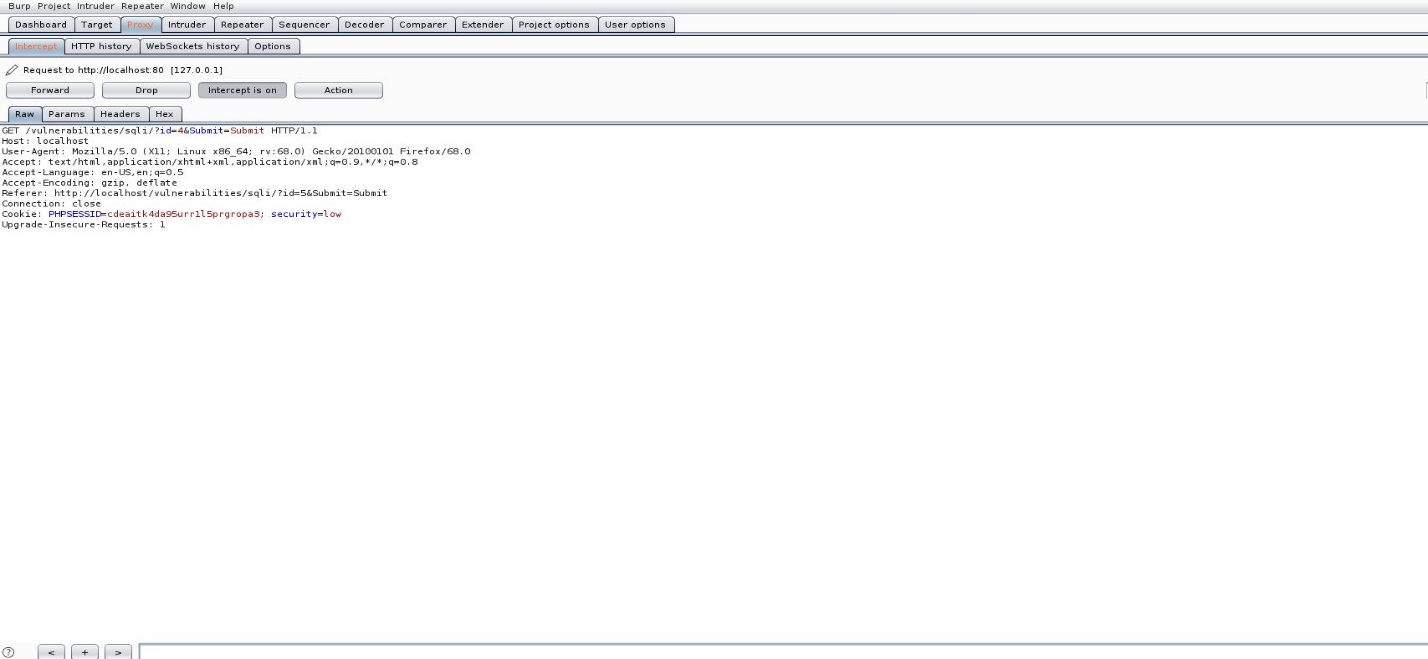
****

**OWASP ZAP**

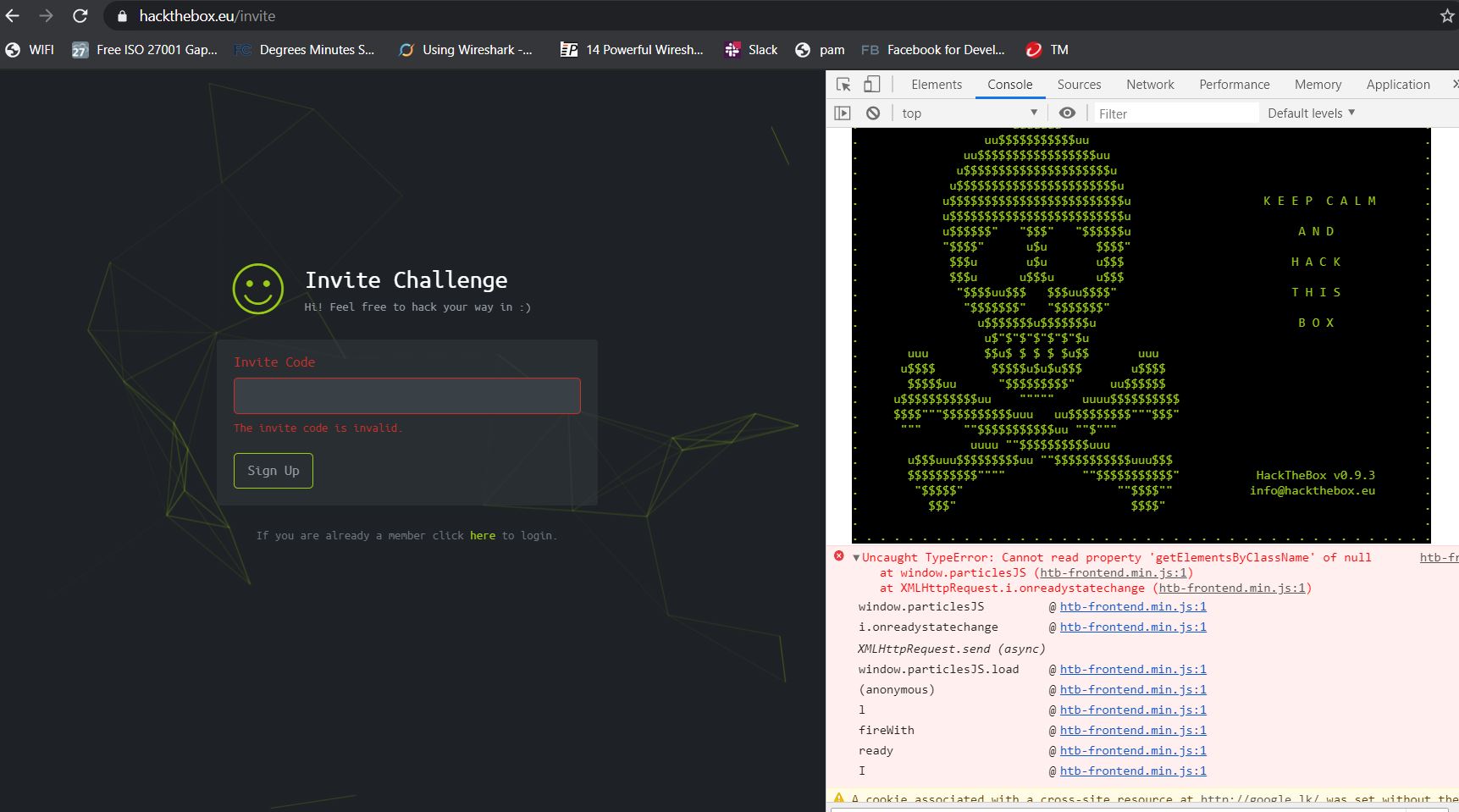
****

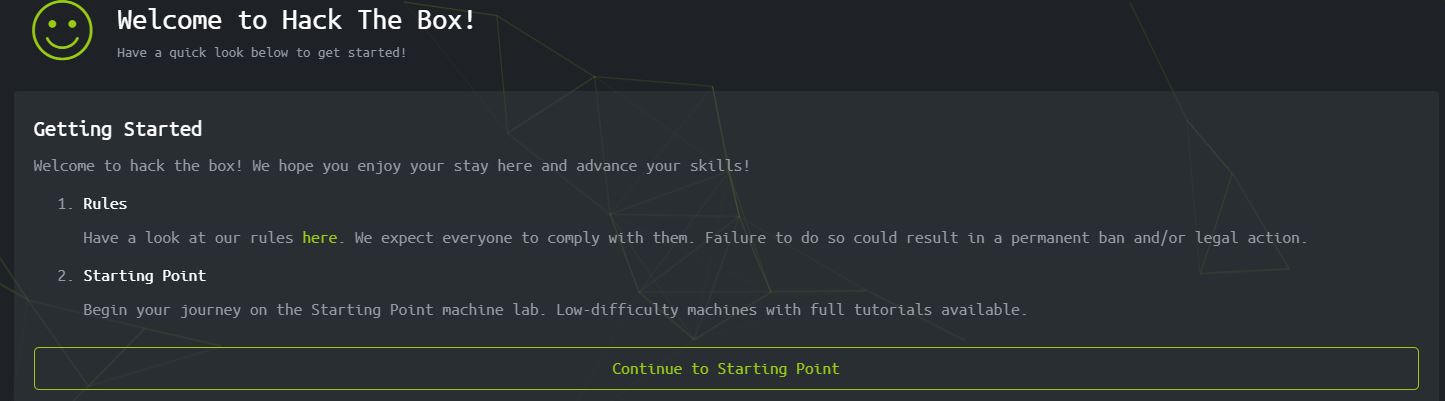
**BurpSuite**

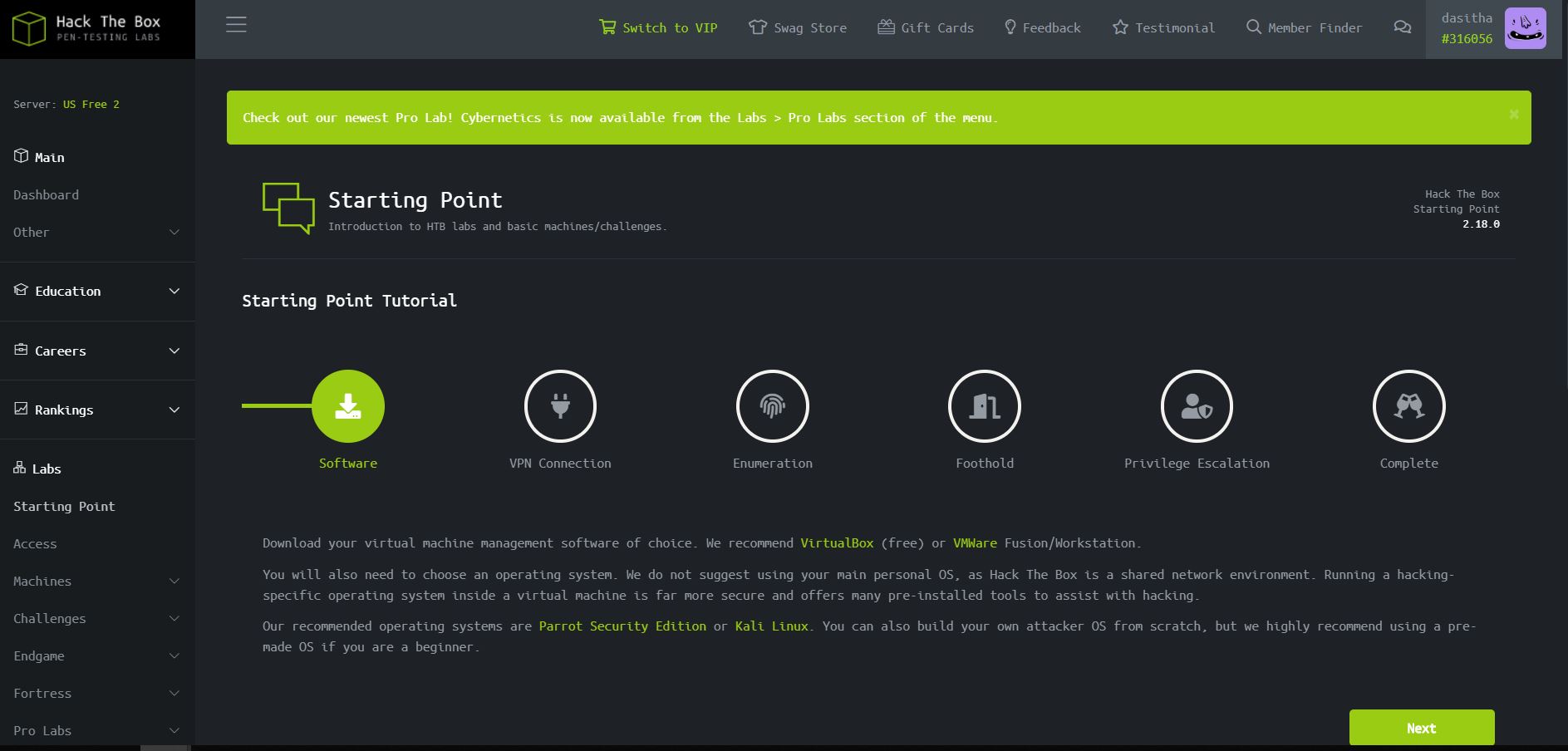
I could be able to understand many things in the BurpSuite. Specially how we traffic capture, how repeater, comparer, decoder, scope change works …etc.



**HackTheBox**

****

****

****