

BURP SUITE

ASSIGNMENT-03

Name: Tanishq Kanare

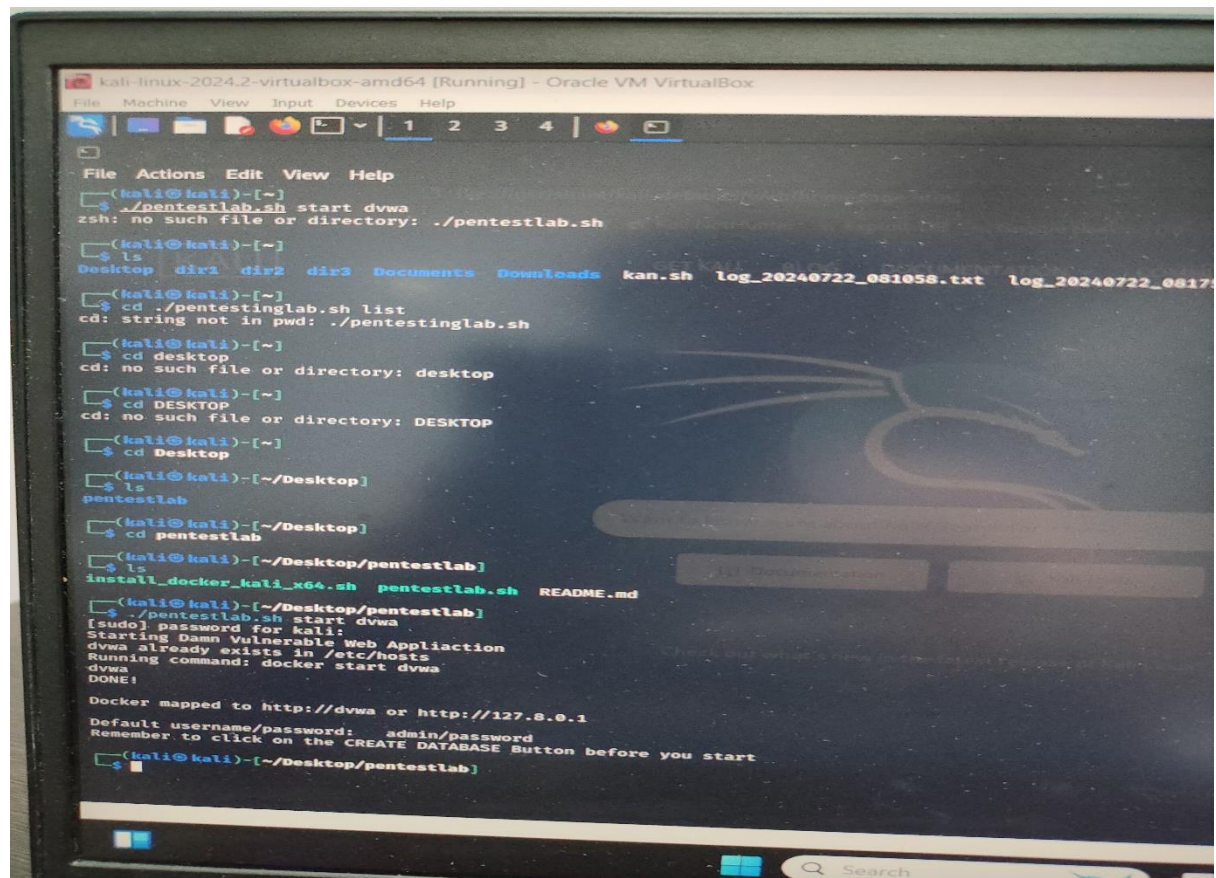
Date: 23/07/24

Q.1) Do DVWA Brute Force Attack – security level is **HIGH**
and share the screen shots of that attack.

Ans. 1)

Performing the DVWA Brute force attack: -

1.) Opening the DVWA page from the kali-Linux terminal



```
kali - linux-2024.2 - virtualbox - amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

(kali@kali)~$ ./pentestlab.sh start dvwa
zsh: no such file or directory: ./pentestlab.sh

(kali@kali)~$ ls
Desktop  dir1  dir2  dir3  Documents  Downloads  kan.sh  log_20240722_081058.txt  log_20240722_0817...

(kali@kali)~$ cd ./pentestinglab.sh list
cd: string not in pwd: ./pentestinglab.sh

(kali@kali)~$ cd desktop
cd: no such file or directory: desktop

(kali@kali)~$ cd DESKTOP
cd: no such file or directory: DESKTOP

(kali@kali)~$ cd Desktop
(kali@kali)~$ ls
pentestlab

(kali@kali)~$ cd Desktop
(kali@kali)~$ cd pentestlab

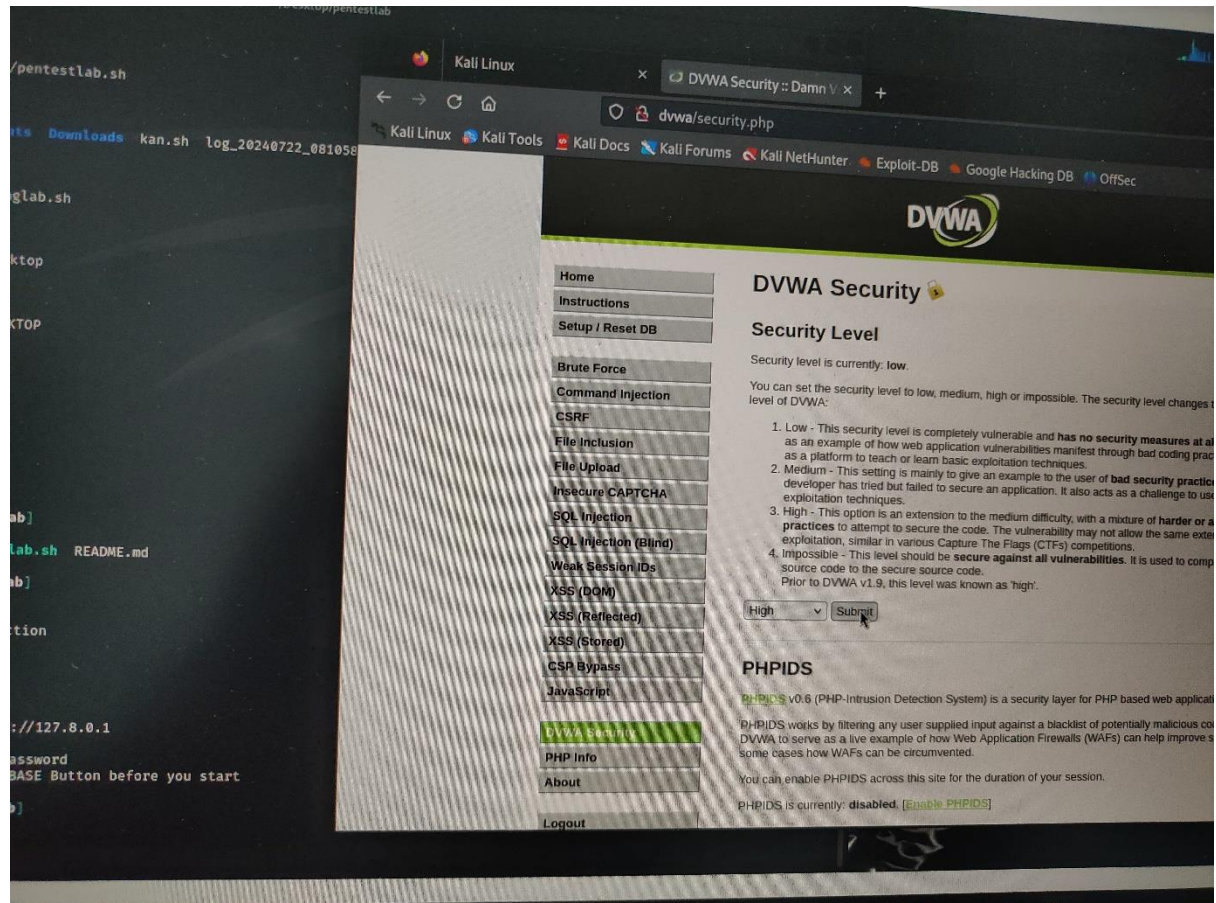
(kali@kali)~$ ls
install_docker_kali_x64.sh  pentestlab.sh  README.md

(kali@kali)~$ ./pentestlab.sh start dvwa
[sudo] password for kali:
Starting Damn Vulnerable Web Application
dvwa already exists in /etc/hosts
Running command: docker start dvwa
dvwa
DONE!

Docker mapped to http://dvwa or http://127.8.0.1
Default username/password: admin/password
Remember to click on the CREATE DATABASE Button before you start

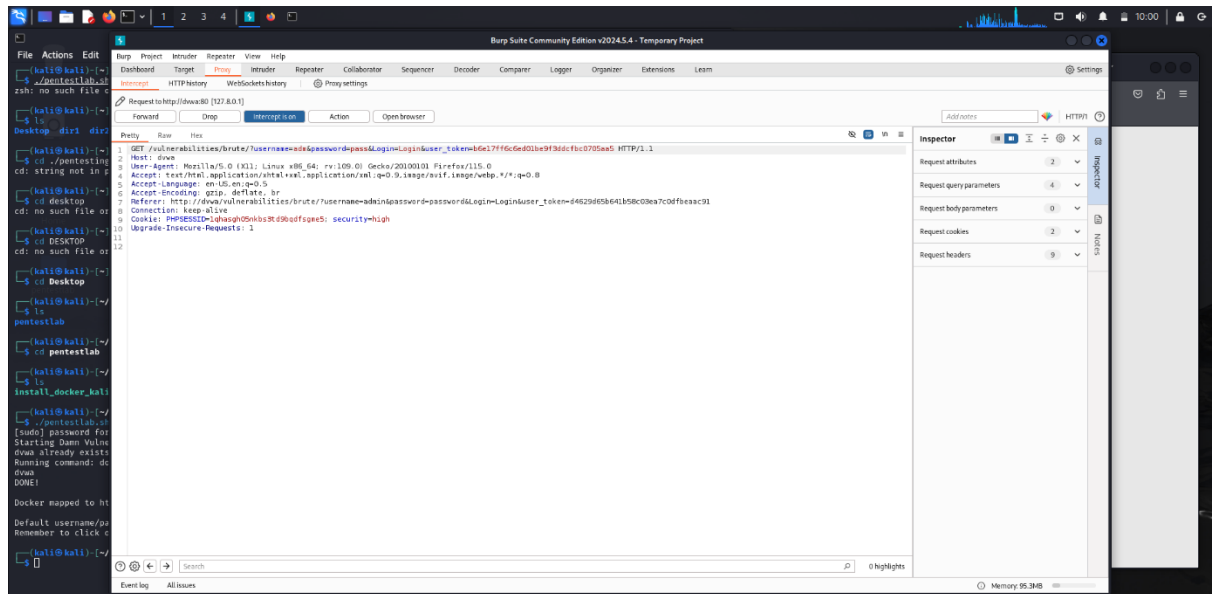
(kali@kali)~$
```

- 2.) In the DVWA page, setting the DVWA security to “HIGH”

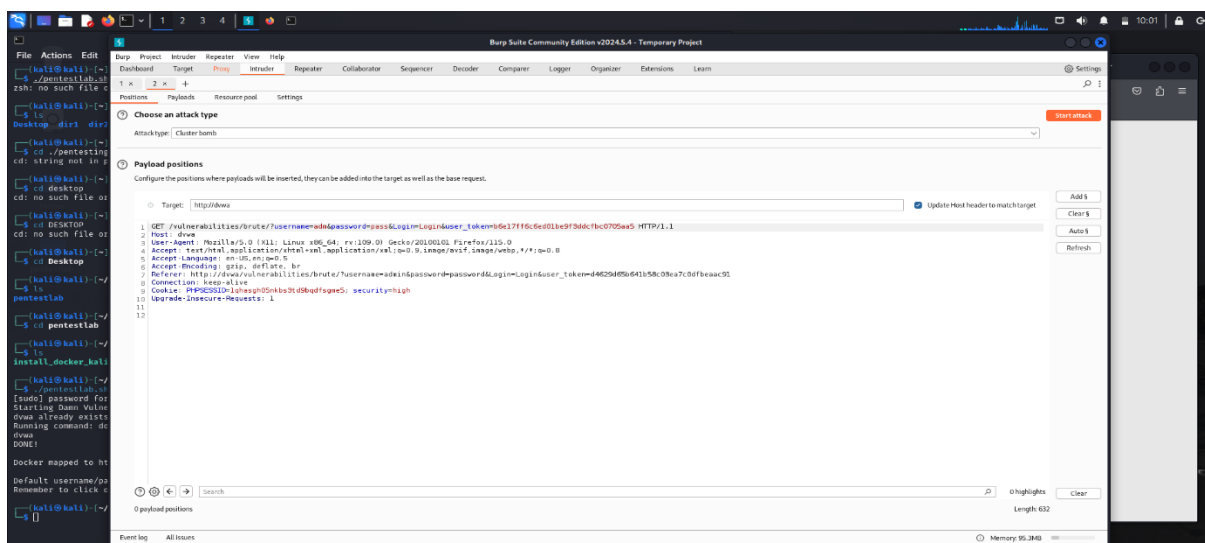


- 3.) Now, I have logged into Brute Force with the correct username and password.
- 4.) Then I again logged into the Brute Force page by different username and password.
- 5.) I enabled the foxy-proxy extension in the browser

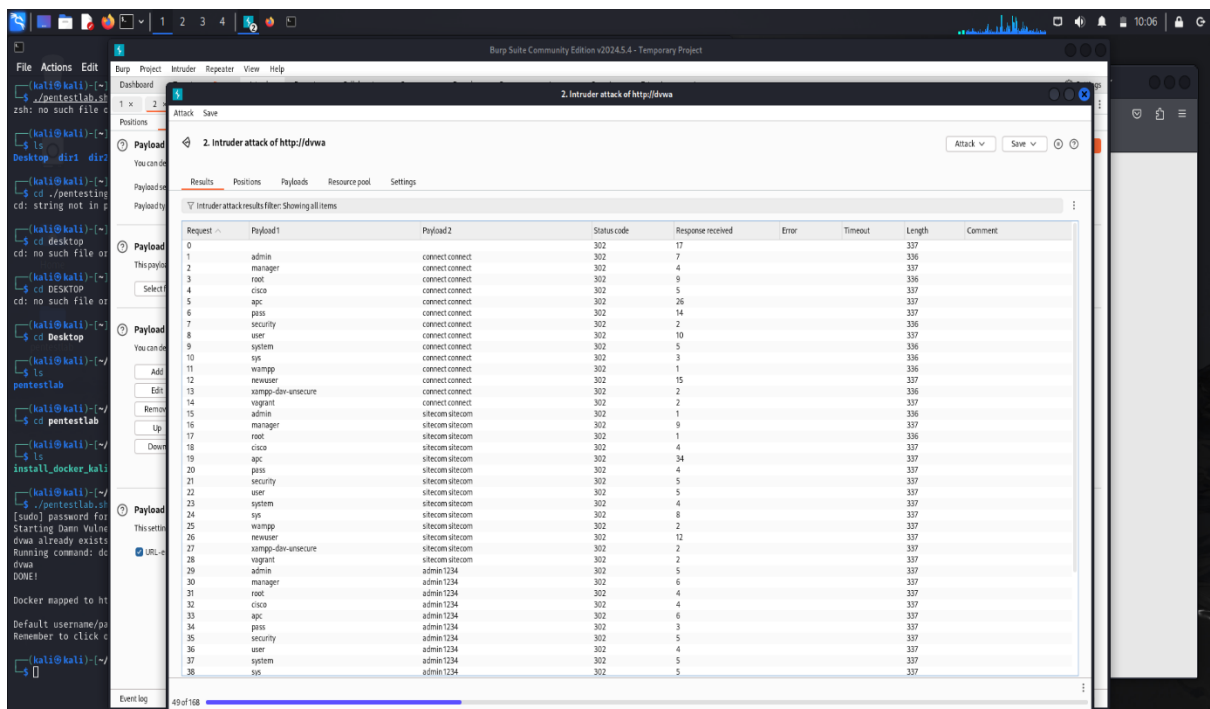
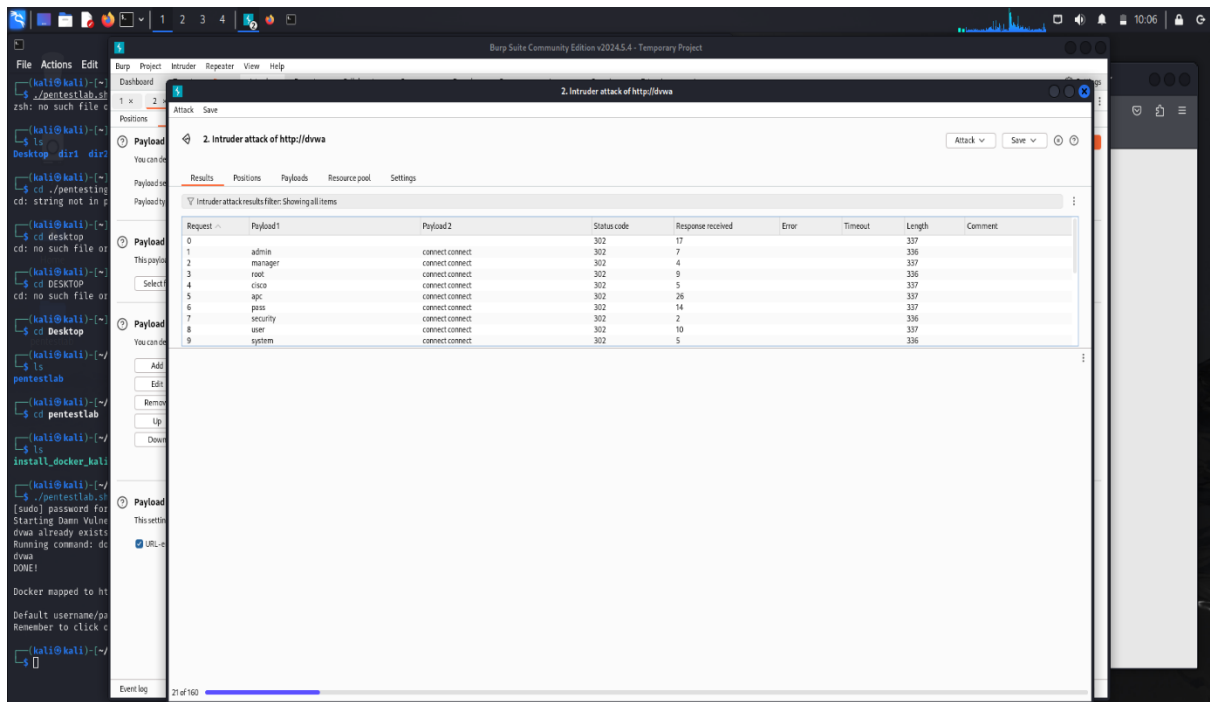
- 6.) Then, I opened BurpSuite in Kali
- 7.) Turned on the interception.
- 8.) I got the intercepted content there.



- 9.) Onto the last line, I right clicked and selected the option 'Send To Intruder'



- 10.) The content was sent to intruder, as shown in the above image.
- 11.) Then, I clicked on the payload option.
- 12.) There, I selected payload 1 as a run-time file and selected a certain username.txt file from the system, which would serve for providing the content of usernames
- 13.) Payload -2 was selected as a run-time file and selected a certain username_pass.txtx file from the system, which would serve for providing the content of passwords
- 14.) I selected the attack type as 'Cluster-Bomb' attack
- 15.) And then started the attack.
- 16.) Following below screenshots shows the output for the given configuration-



2. Intruder attack of http://dwwa

Attack Save

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload1	Payload2	Status code	Response received	Error	Timeout	Length	Comment
22	user	sitecom sitecom	302	5			337	
23	system	sitecom sitecom	302	4			337	
24	sys	sitecom sitecom	302	8			337	
25	wampwp	sitecom sitecom	302	2			337	
26	newuser	sitecom sitecom	302	12			337	
27	xampp-dav-unsecure	sitecom sitecom	302	2			337	
28	vagrant	sitecom sitecom	302	2			337	
29	admin	admin 1234	302	5			337	
30	manager	admin 1234	302	6			337	
31	root	admin 1234	302	4			337	
32	cisco	admin 1234	302	4			337	
33	apc	admin 1234	302	6			337	
34	pass	admin 1234	302	3			337	
35	security	admin 1234	302	5			337	
36	user	admin 1234	302	4			337	
37	system	admin 1234	302	5			337	
38	sys	admin 1234	302	5			337	
39	wampwp	admin 1234	302	12			337	
40	newuser	admin 1234	302	7			337	
41	xampp-dav-unsecure	admin 1234	302	6			337	
42	vagrant	admin 1234	302	4			337	
43	admin	cisco cisco	302	5			337	
44	manager	cisco cisco	302	8			337	
45	root	cisco cisco	302	4			337	
46	cisco	cisco cisco	302	6			337	
47	apc	cisco cisco	302	5			337	
48	pass	cisco cisco	302	5			337	
49	security	cisco cisco	302	2			337	
50	user	cisco cisco	302	3			337	
51	system	cisco cisco	302	5			337	
52	sys	cisco cisco	302	3			337	
53	wampwp	cisco cisco	302	2			337	
54	newuser	cisco cisco	302	7			337	
55	xampp-dav-unsecure	cisco cisco	302	4			337	
56	vagrant	cisco cisco	302	4			337	
57	admin	cisco sanfran	302	2			337	
58	manager	cisco sanfran	302	2			337	
59	root	cisco sanfran	302	10			337	
60	cisco	cisco sanfran	302	3			337	

Event log 63 of 188