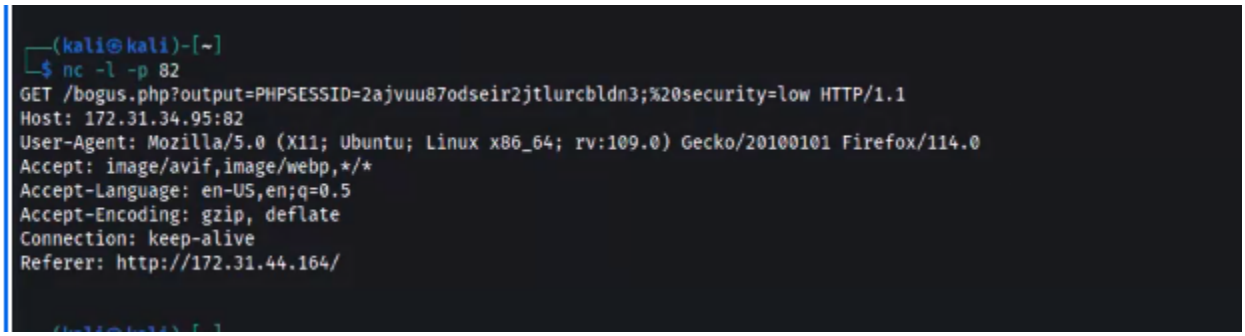
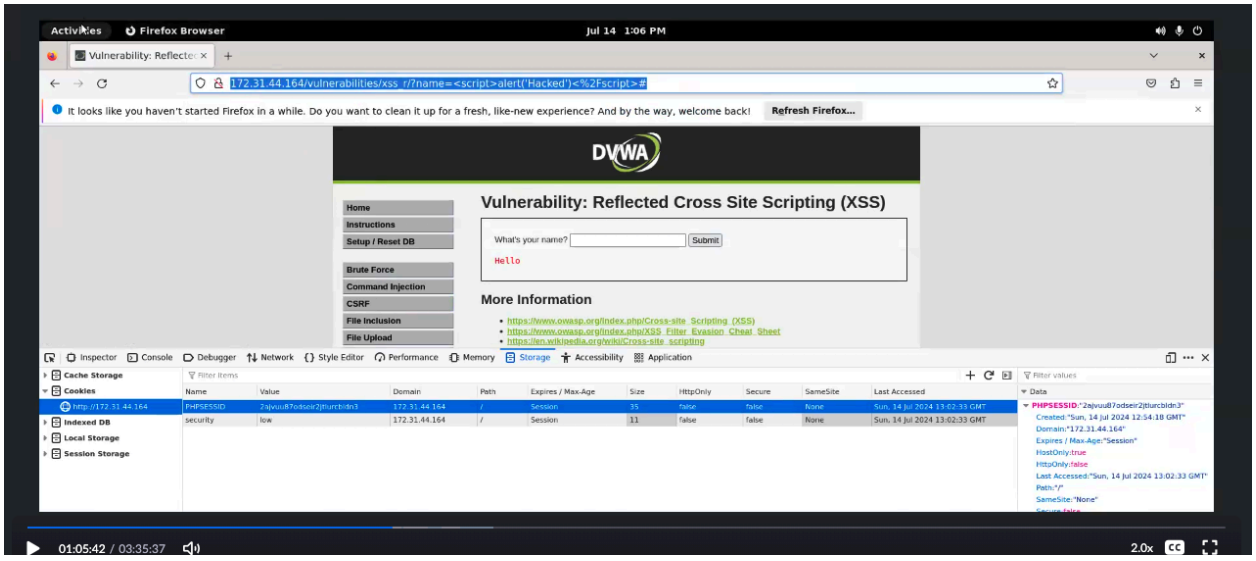
XSS Attack Simulation

Go to KaliLinux and enter the nc command as below to listen for incoming connections on port 82



Prepare the payload inside of the url parameter “name” for application and insert the script as shown below

Now go to browser and run the URL in next tab of application is running

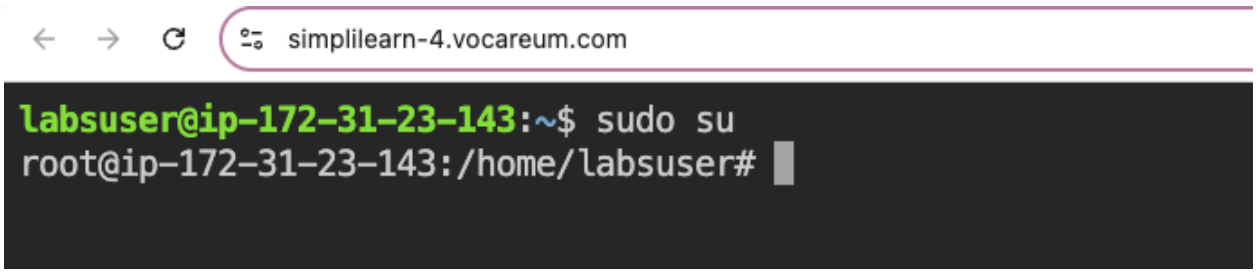


You will be able to see the Request as incoming from User Machine to Kali Linux with Session ID information is present.

Assignment: Now try to perform same in Stored XSS attack

1) Go to Stored XSS Payload in Message Field (Submit the malicious script> and Save
2) Now go to Kali Linux and listen for connections using netcat command
3) Visit the Stored XSS page multiple times
4) Monitor the Kali Linux Console with NC to see every time you visit the page the script should provide the session information

Setup DVWA



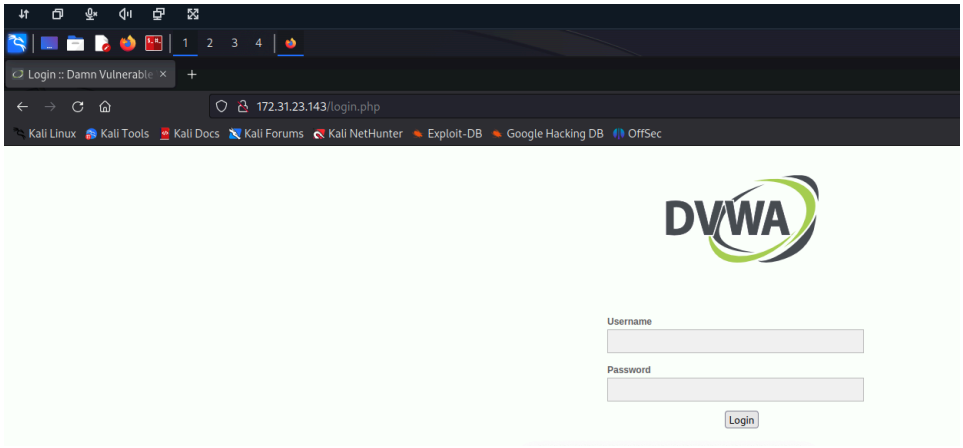

```
root@ip-172-31-23-143:/home/labsuser# docker pull vulnerables/web-dvwa
Using default tag: latest
latest: Pulling from vulnerables/web-dvwa
Digest: sha256:dae203fe11646a86937bf04db0079adef295f426da68a92b40e3b181f337daa7
Status: Image is up to date for vulnerables/web-dvwa:latest
docker.io/vulnerables/web-dvwa:latest
root@ip-172-31-23-143:/home/labsuser#
```

```
root@ip-172-31-23-143:/home/labsuser# docker run --rm -it -p 80:80 vulnerables/web-dvwa
[+] Starting mysql...
[ ok ] Starting MariaDB database server: mysqld.
[+] Starting apache
[....] Starting Apache httpd web server: apache2AH00558: apache2: Could not reliably determine the server's fully qualified domain na
ame' directive globally to suppress this message
. ok
==> /var/log/apache2/access.log <==

==> /var/log/apache2/error.log <==
[Sun Aug 11 03:50:41.495563 2024] [mpm_prefork:notice] [pid 315] AH00163: Apache/2.4.25 (Debian) configured -- resuming normal operat
[Sun Aug 11 03:50:41.495654 2024] [core:notice] [pid 315] AH00094: Command line: '/usr/sbin/apache2'

==> /var/log/apache2/other_vhosts_access.log <==
```

Access the App from Kali Linux



admin/password