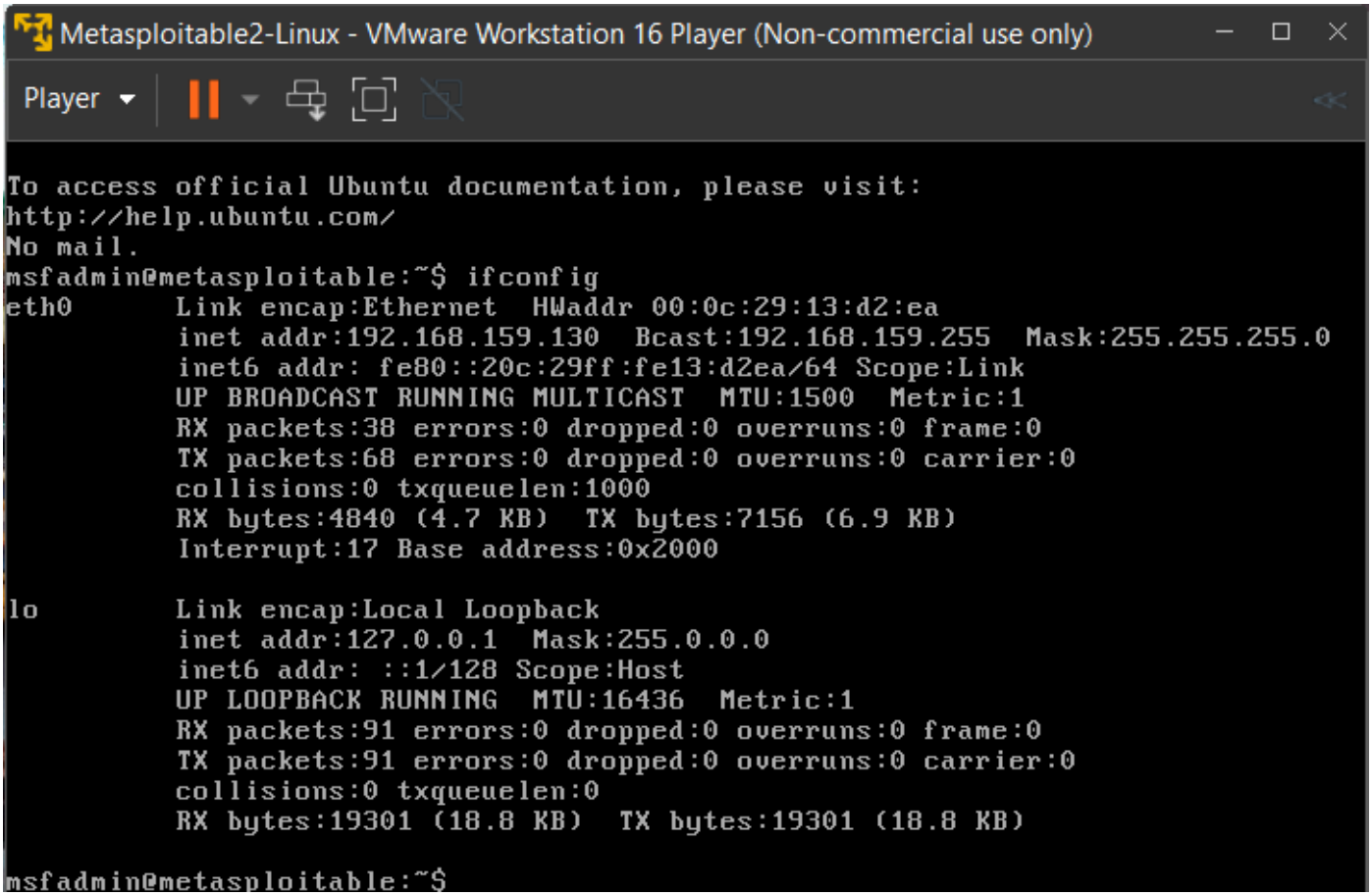
CSE3501-Information Security Analysis and Audit Lab

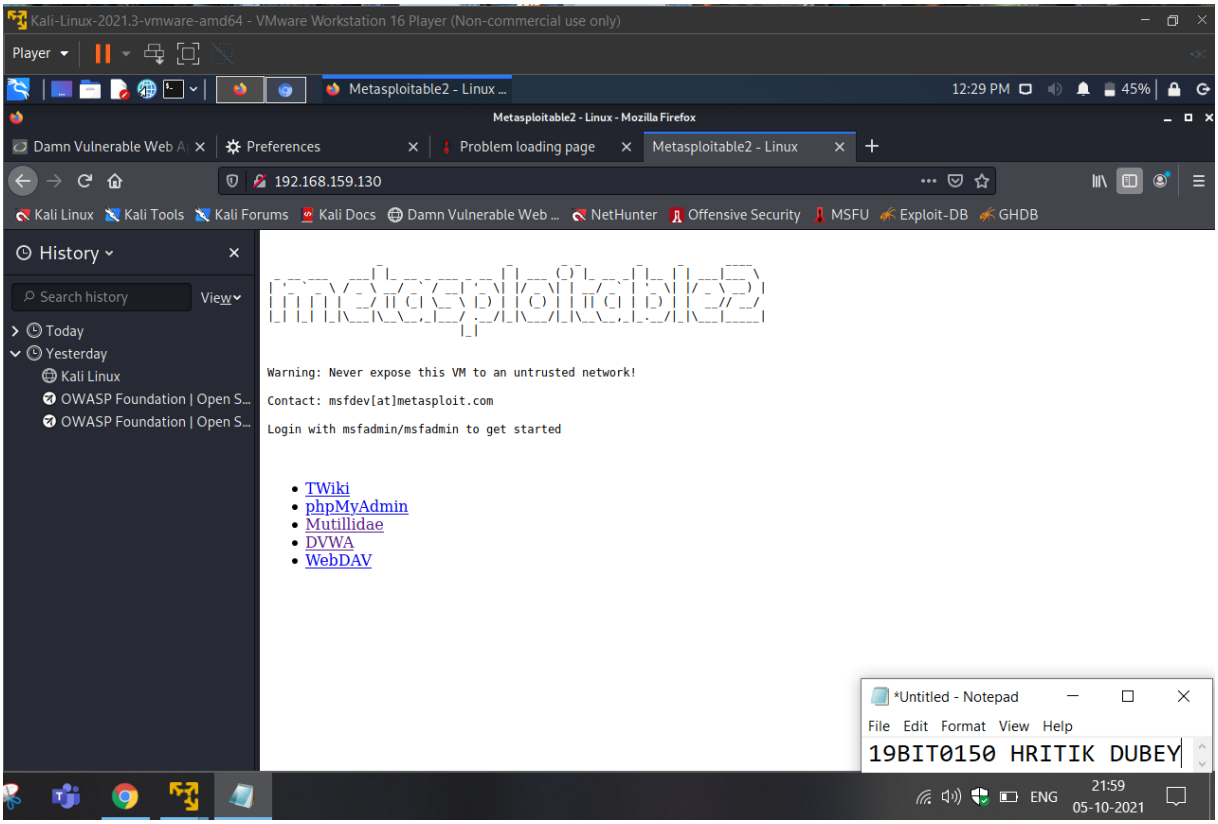
NAME- HRITIK DUBEY REG NO-19BIT0150 SLOT- L41+L42

DIGITAL ASSIGNMENT 3 Faculty : Dr. Priya V

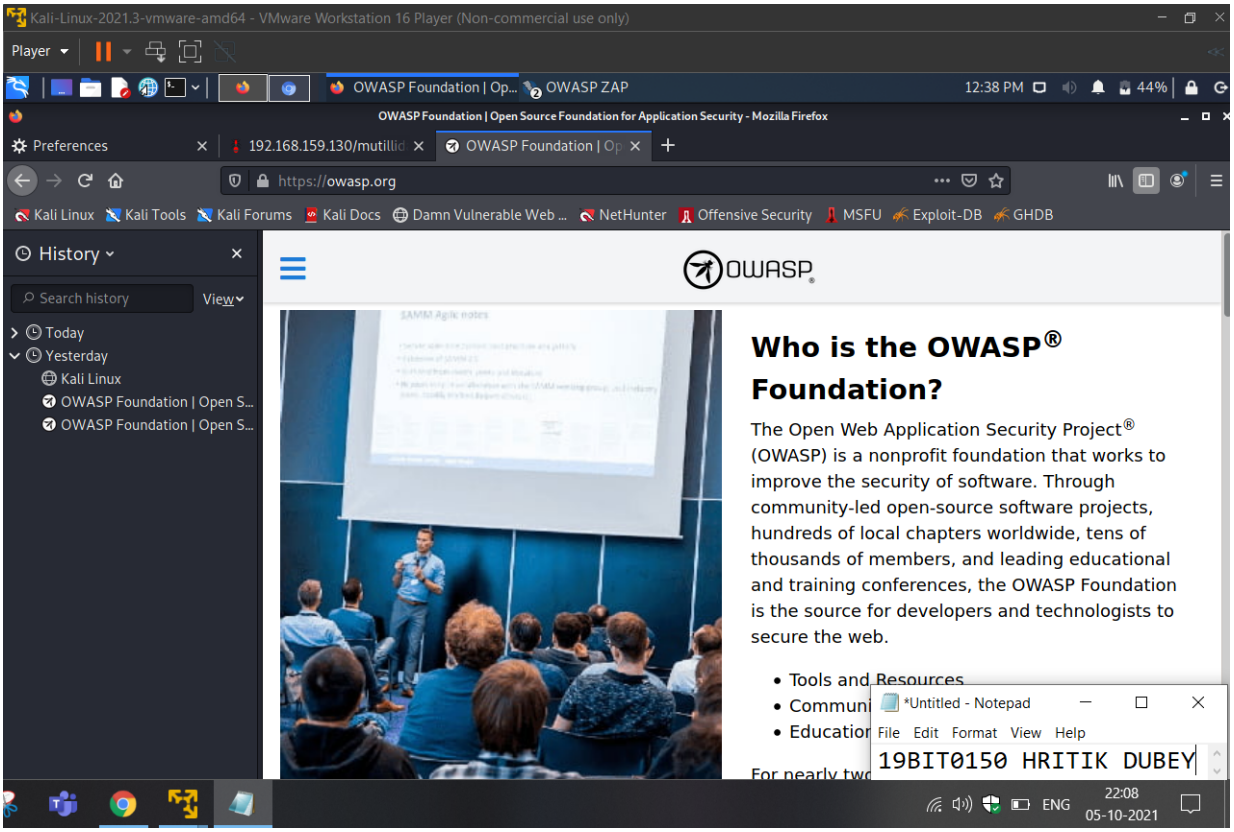
1. In OWASP ZAP do the following:
i. Open Mutillidae through your Metasploitable IP
ii. Perform Spider attack and get the report of no of URI's
iii. Perform Forced browse directory attack and get the report

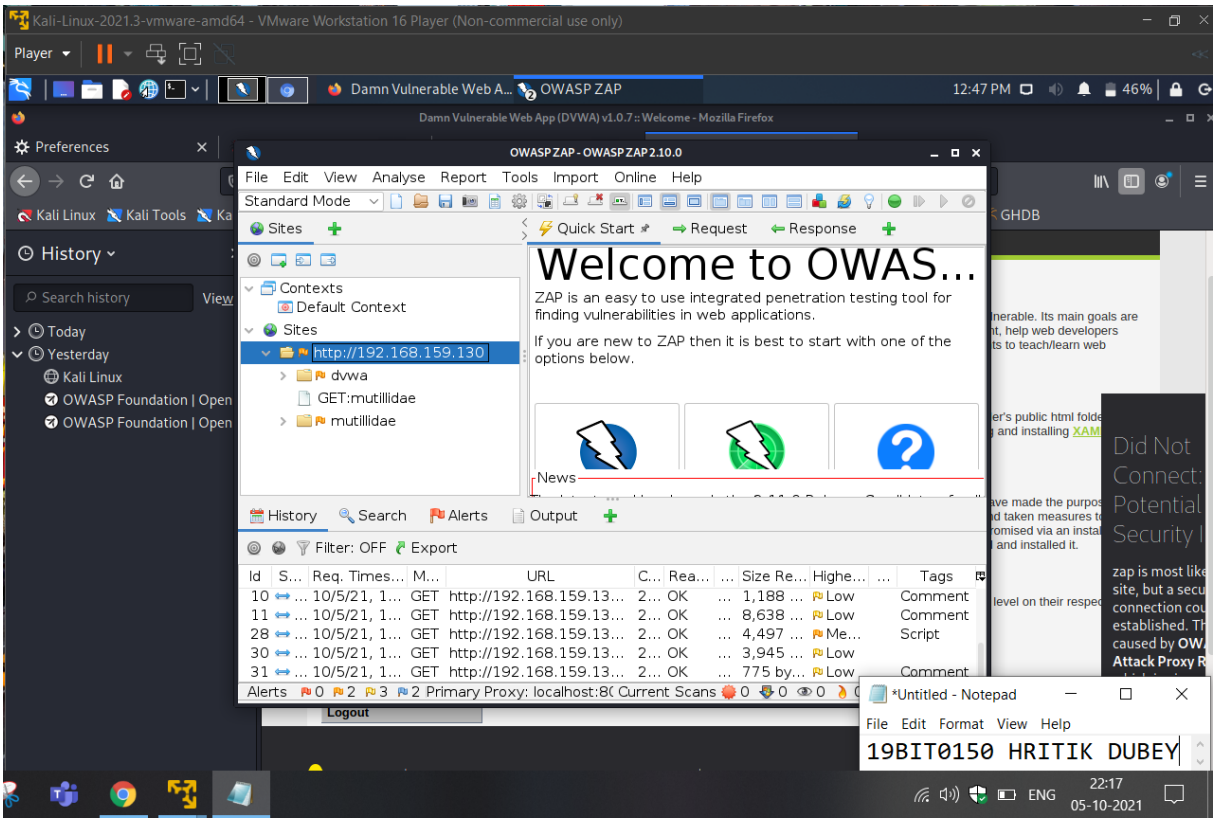


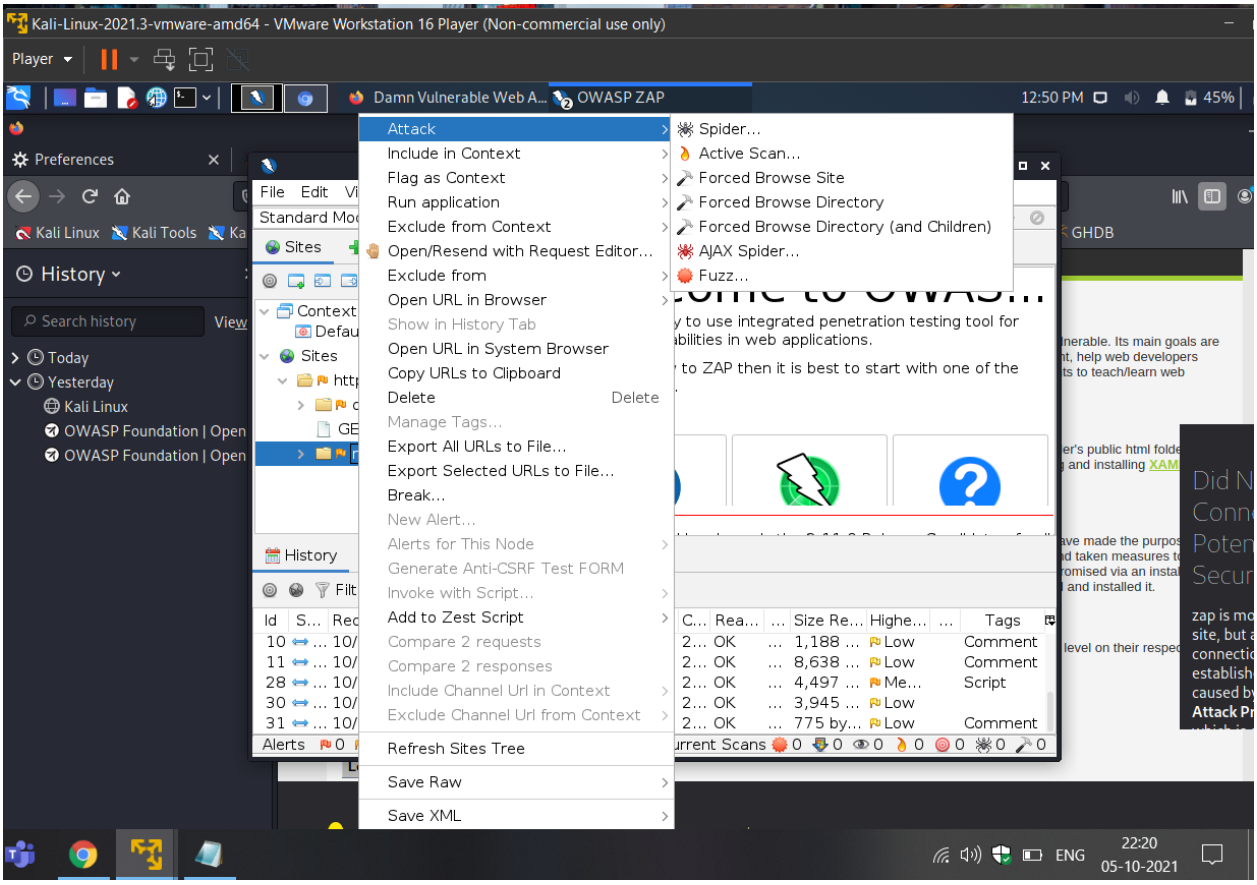
My metasploit Inet address- 192.168.159.130

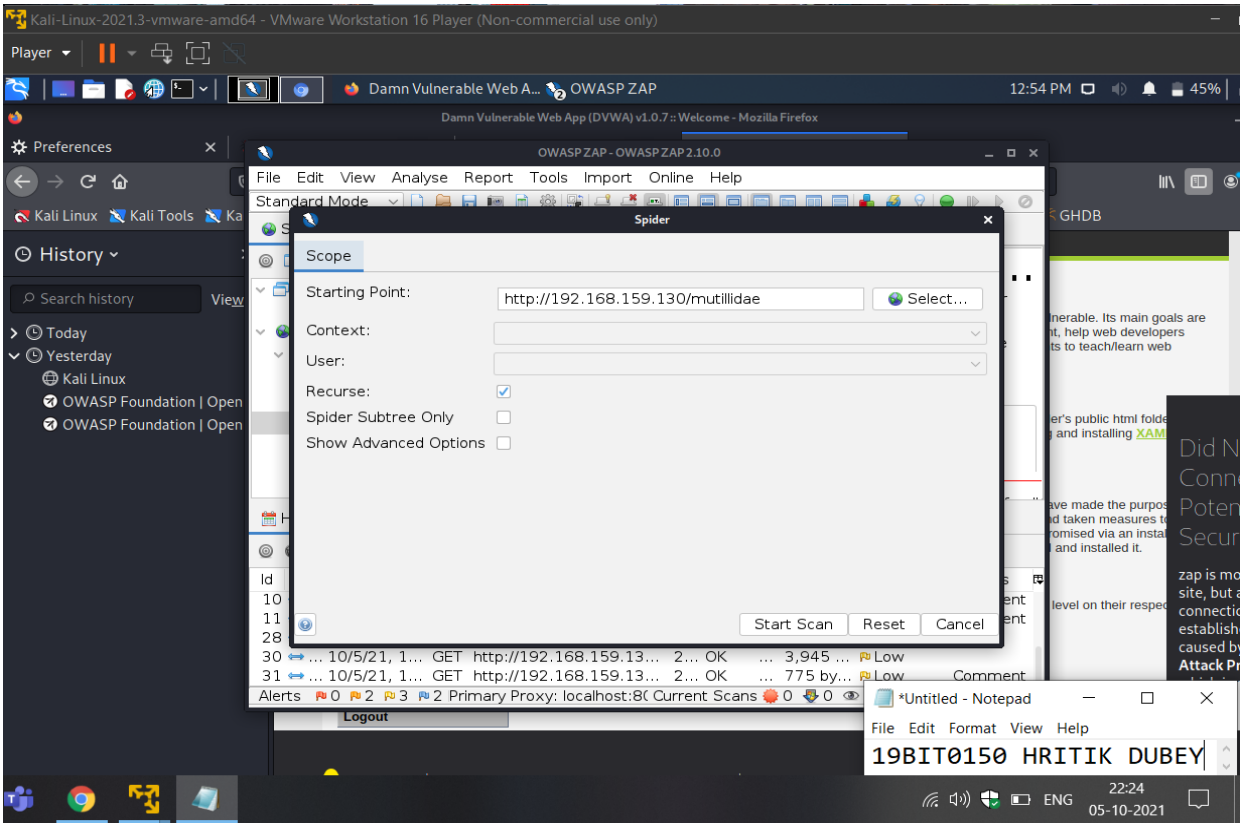

Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Metasploitable2 - Linux ...
12:29 PM
45%
Metasploitable2 - Linux - Mozilla Firefox
Damn Vulnerable Web A
Preferences
Problem loading page
Metasploitable2 - Linux
192.168.159.130
Kali Linux
Kali Tools
Kali Forums
Kali Docs
Damn Vulnerable Web ...
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
History
Search history
View
Today
Yesterday
Kali Linux
OWASP Foundation | Open S...
OWASP Foundation | Open S...
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
TWiki
phpMyAdmin
Mutillidae
DVWA
WebDAV
*Untitled - Notepad
File Edit Format View Help
19BIT0150 HRITIK DUBEY
ENG
21:59
05-10-2021

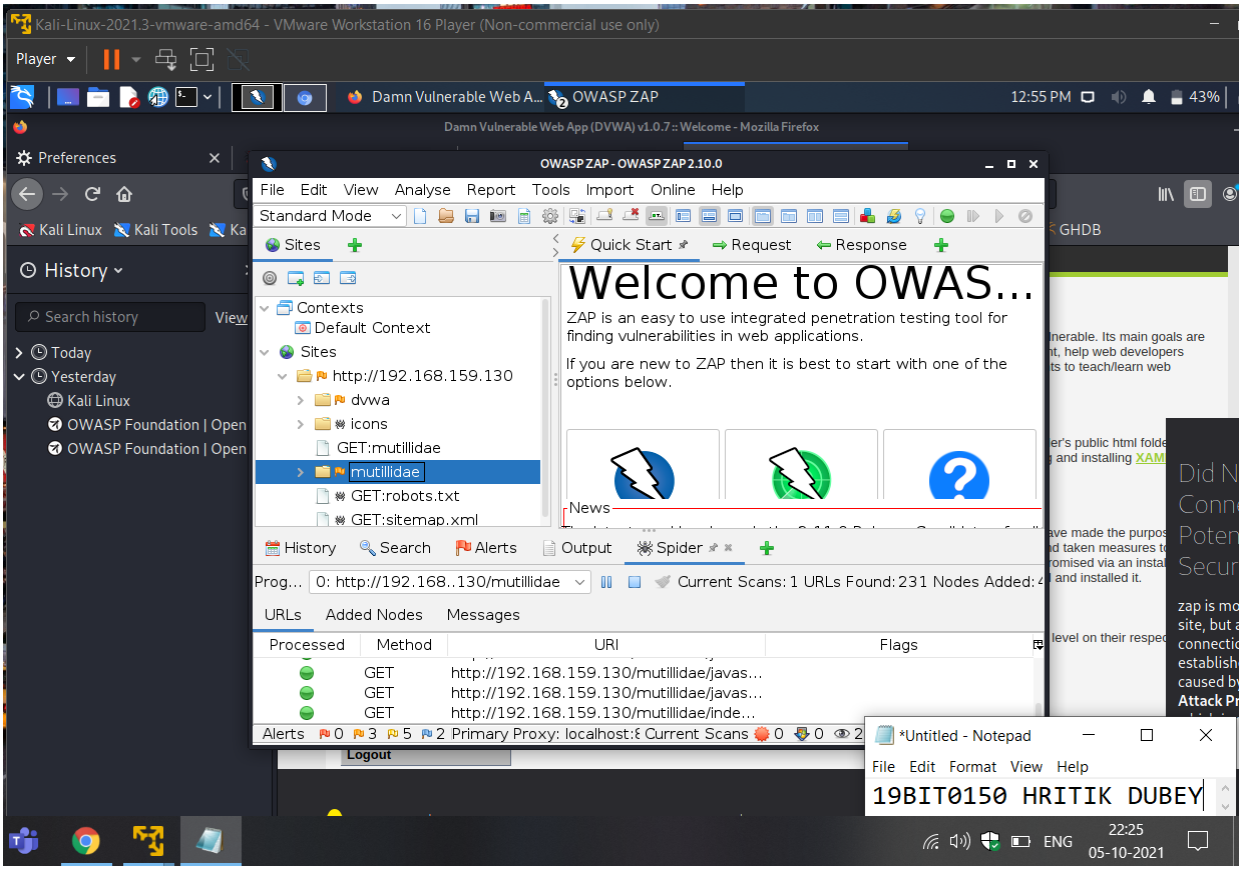

Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Problem loading page - ...
12:23 PM
46%
Problem loading page - Mozilla Firefox
Damn Vulnerable Web A
Preferences
Problem loading page
192.168.159.130/mutillidae/
Kali Linux
Kali Tools
Kali Forums
Kali Docs
Damn Vulnerable Web ...
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
History
Search history
View
Today
Yesterday
Kali Linux
OWASP Foundation | Open S...
OWASP Foundation | Open S...
Mutillidae: Born to be Hacked
Version: 2.1.19
Security Level: 0 (Hosed)
Hints: Disabled (0 - I try harder)
Not Logged In
Home
Login/Register
Toggle Hints
Toggle Security
Reset DB
View Log
View Captured Data
Core Controls
OWASP Top 10
Others
Documentation
Resources
Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons
Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10
Latest Version / Installation
Latest Version
Installation Instructions
Usage Instructions
Get rid of those pesky PHP errors
Change Log
Notes
Samurai WTF and Backtrack contains all the tools needed or you may build your own collection
backtrack
*Untitled - Notepad
File Edit Format View Help
19BIT0150 HRITIK DUBEY
ENG
21:53
05-10-2021

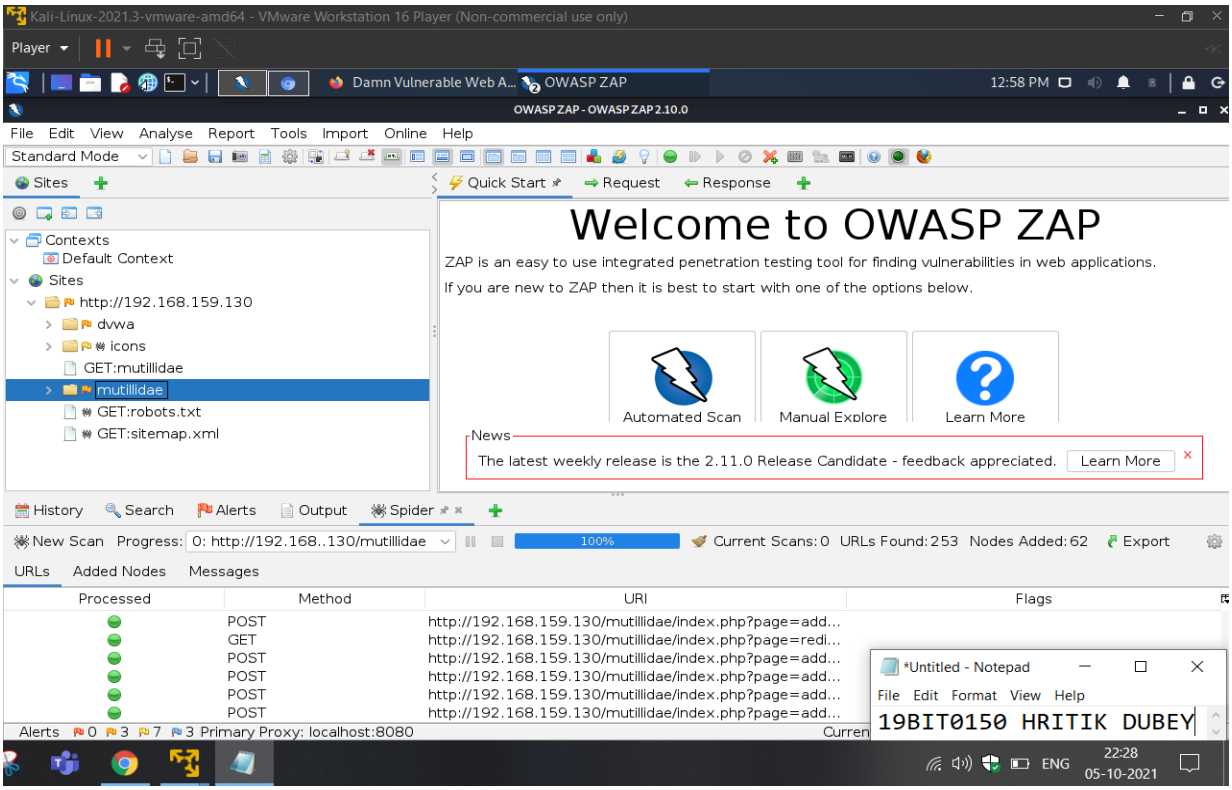

Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
OWASP Foundation | Op...
OWASP ZAP
12:38 PM
44%
OWASP Foundation | Open Source Foundation for Application Security - Mozilla Firefox
Preferences
192.168.159.130/mutillid
OWASP Foundation | Op
https://owasp.org
Kali Linux
Kali Tools
Kali Forums
Kali Docs
Damn Vulnerable Web ...
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
History
Search history
View
Today
Yesterday
Kali Linux
OWASP Foundation | Open S...
OWASP Foundation | Open S...
OWASP
Who is the OWASP® Foundation?
The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.
Tools and Resources
Communi
Educatior
For nearly two
*Untitled - Notepad
File Edit Format View Help
19BIT0150 HRITIK DUBEY
ENG
22:08
05-10-2021


Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Damn Vulnerable Web A...
OWASP ZAP
12:47 PM
46%
Damn Vulnerable Web App (DVWA) v1.0.7 :: Welcome - Mozilla Firefox
Preferences
OWASP ZAP - OWASP ZAP 2.10.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Welcome to OWAS...
ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
If you are new to ZAP then it is best to start with one of the options below.
Contexts
Default Context
Sites
http://192.168.159.130
dvwa
GET:mutillidae
mutillidae
News
History
Search
Alerts
Output
Filter: OFF
Export
Id S... Req. Times... M... URL C... Rea... ... Size Re... Highe... ... Tags
10 ... 10/5/21, 1... GET http://192.168.159.13... 2... OK ... 1,188 ... Low Comment
11 ... 10/5/21, 1... GET http://192.168.159.13... 2... OK ... 8,638 ... Low Comment
28 ... 10/5/21, 1... GET http://192.168.159.13... 2... OK ... 4,497 ... Me... Script
30 ... 10/5/21, 1... GET http://192.168.159.13... 2... OK ... 3,945 ... Low
31 ... 10/5/21, 1... GET http://192.168.159.13... 2... OK ... 775 by... Low Comment
Alerts 0 2 3 2 Primary Proxy: localhost:8(Current Scans 0 0 0 0
Logout
Did Not Connect: Potential Security I
*Untitled - Notepad
File Edit Format View Help
19BIT0150 HRITIK DUBEY
ENG
22:17
05-10-2021

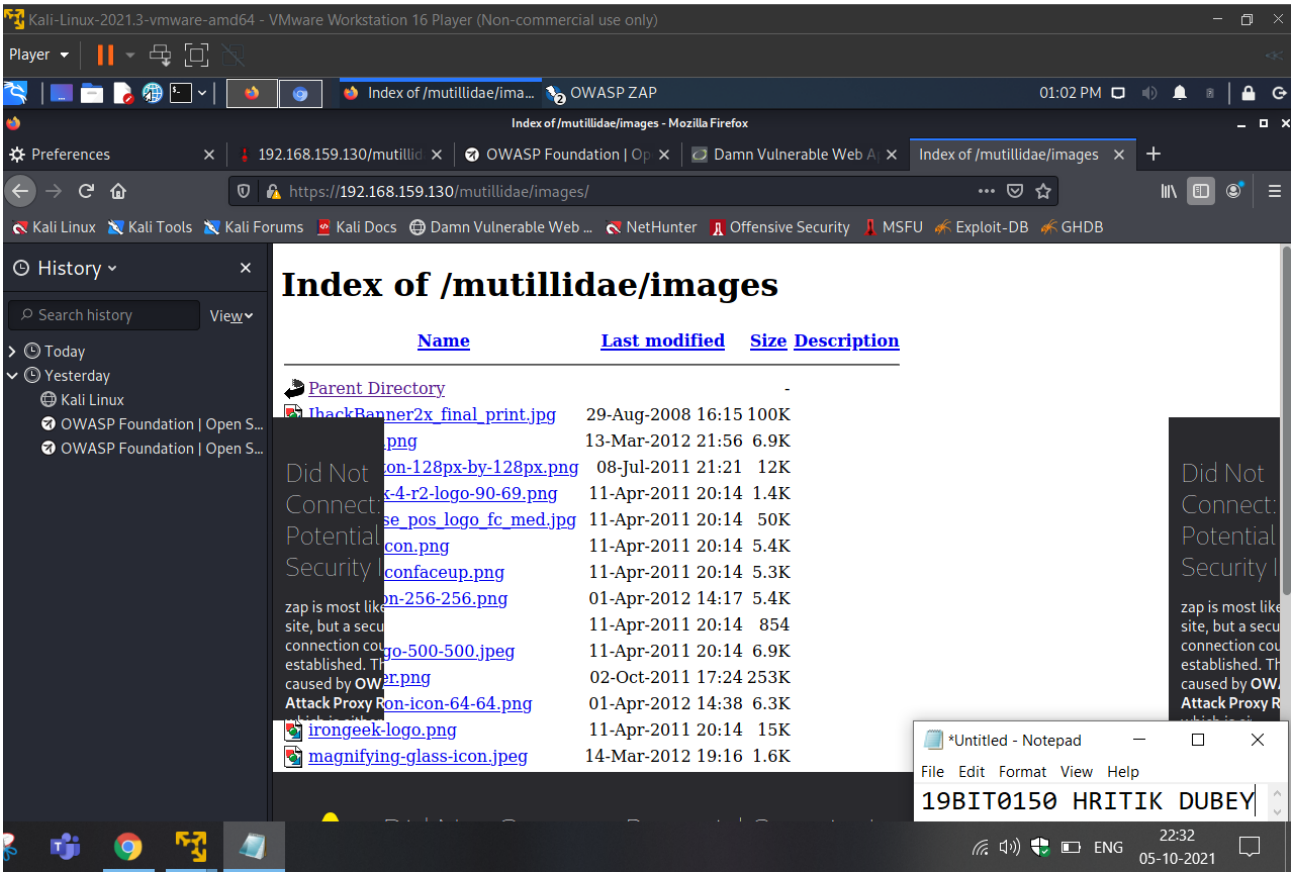

Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Damn Vulnerable Web A...
OWASP ZAP
12:50 PM
45%
Attack
Include in Context
Flag as Context
Run application
Exclude from Context
Open/Resend with Request Editor...
Exclude from
Open URL in Browser
Show in History Tab
Open URL in System Browser
Copy URLs to Clipboard
Delete
Delete
Manage Tags...
Export All URLs to File...
Export Selected URLs to File...
Break...
New Alert...
Alerts for This Node
Generate Anti-CSRF Test FORM
Invoke with Script...
Add to Zest Script
Compare 2 requests
Compare 2 responses
Include Channel Url in Context
Exclude Channel Url from Context
Refresh Sites Tree
Save Raw
Save XML
Spider...
Active Scan...
Forced Browse Site
Forced Browse Directory
Forced Browse Directory (and Children)
AJAX Spider...
Fuzz...
ENG
22:20
05-10-2021


Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Damn Vulnerable Web A...
OWASP ZAP
12:54 PM
45%
Damn Vulnerable Web App (DVWA) v1.0.7 :: Welcome - Mozilla Firefox
OWASP ZAP - OWASP ZAP 2.10.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Spider
Scope
Starting Point:
http://192.168.159.130/mutillidae
Select...
Context:
User:
Recurse:
Spider Subtree Only
Show Advanced Options
Start Scan
Reset
Cancel
*Untitled - Notepad
File Edit Format View Help
19BIT0150 HRITIK DUBEY
ENG
22:24
05-10-2021

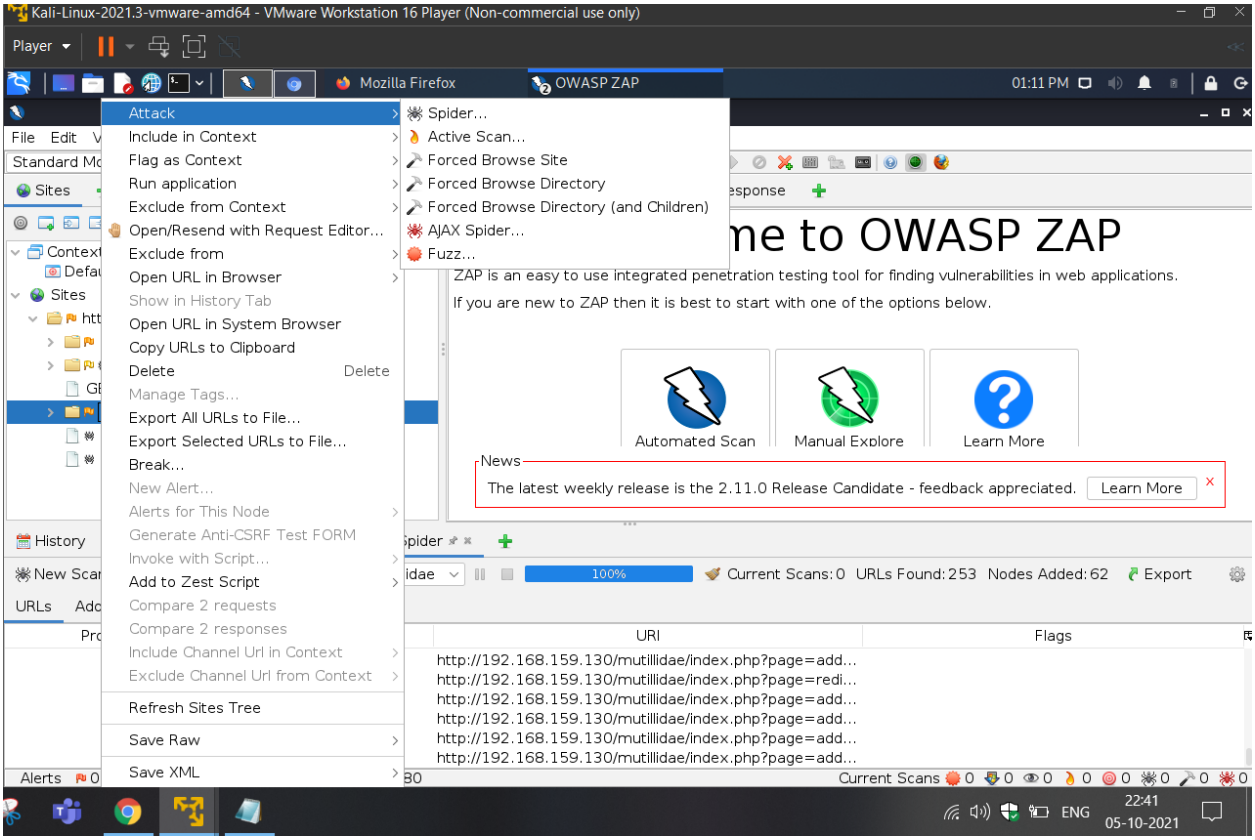




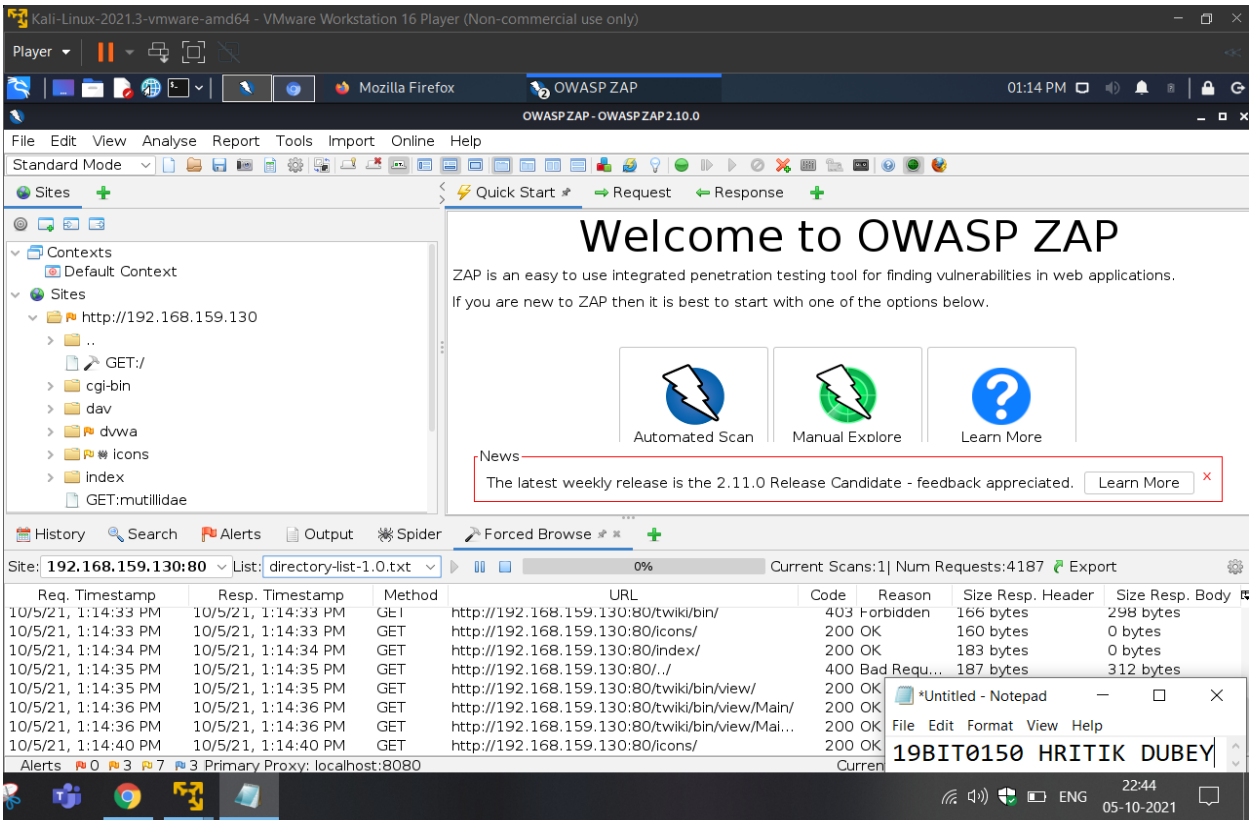
253 URI REPORTED


Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Index of /mutillidae/ima...
OWASP ZAP
01:02 PM
Index of /mutillidae/images - Mozilla Firefox
Preferences
192.168.159.130/mutilli
OWASP Foundation | Op
Damn Vulnerable Web A
Index of /mutillidae/images
https://192.168.159.130/mutillidae/images/
Kali Linux
Kali Tools
Kali Forums
Kali Docs
Damn Vulnerable Web ...
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
History
Search history
View
Today
Yesterday
Kali Linux
OWASP Foundation | Open S...
OWASP Foundation | Open S...
Index of /mutillidae/images
Name
Last modified
Size
Description
Parent Directory -
IhackBanner2x_final_print.jpg 29-Aug-2008 16:15 100K
.png 13-Mar-2012 21:56 6.9K
on-128px-by-128px.png 08-Jul-2011 21:21 12K
-4-r2-logo-90-69.png 11-Apr-2011 20:14 1.4K
se_pos_logo_fc_med.jpg 11-Apr-2011 20:14 50K
con.png 11-Apr-2011 20:14 5.4K
confaceup.png 11-Apr-2011 20:14 5.3K
n-256-256.png 01-Apr-2012 14:17 5.4K
11-Apr-2011 20:14 854
go-500-500.jpeg 11-Apr-2011 20:14 6.9K
r.png 02-Oct-2011 17:24 253K
on-icon-64-64.png 01-Apr-2012 14:38 6.3K
irongeek-logo.png 11-Apr-2011 20:14 15K
magnifying-glass-icon.jpeg 14-Mar-2012 19:16 1.6K
Did Not Connect: Potential Security I
zap is most like site, but a secu connection cou established. Th caused by OW Attack Proxy R
*Untitled - Notepad
File Edit Format View Help
19BIT0150 HRITIK DUBEY
ENG
22:32
05-10-2021


Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
IhackBanner2x_final_pri...
OWASP ZAP
01:04 PM
IhackBanner2x_final_print.jpg (JPEG Image, 1024 × 403 pixels) - Mozilla Firefox
Preferences
192.168.159.130/mutilli
OWASP Foundation | Op
Damn Vulnerable Web A
IhackBanner2x_final_print.jp
https://192.168.159.130/mutillidae/images/IhackBanner2x_final_print.jpg
Kali Linux
Kali Tools
Kali Forums
Kali Docs
Damn Vulnerable Web ...
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
HACKERS FOR CHARITY
www.hackersforcharity.org
*Untitled - Notepad
File Edit Format View Help
19BIT0150 HRITIK DUBEY
ENG
22:34
05-10-2021



Forced browse directory attack

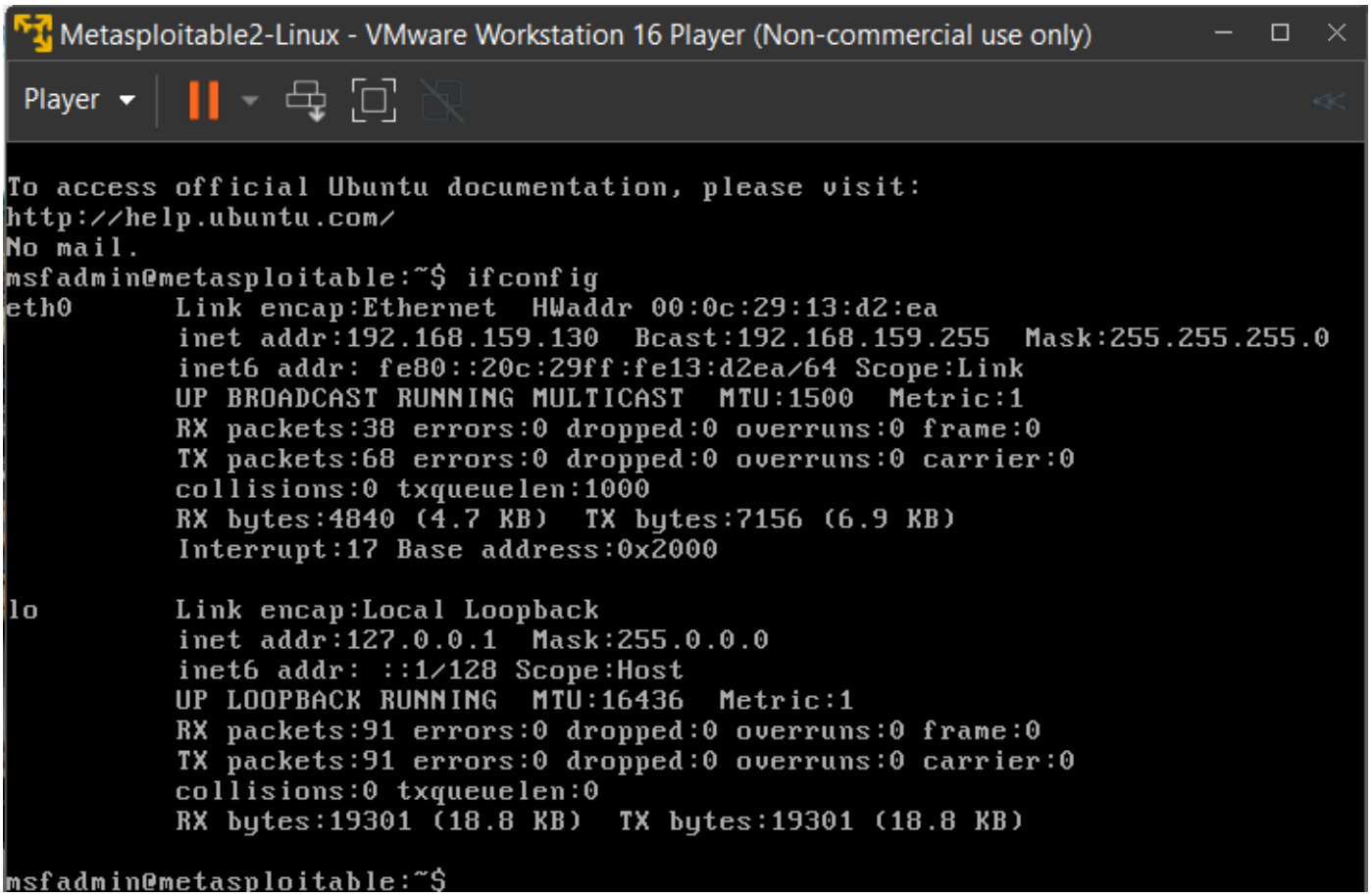


So far we have,

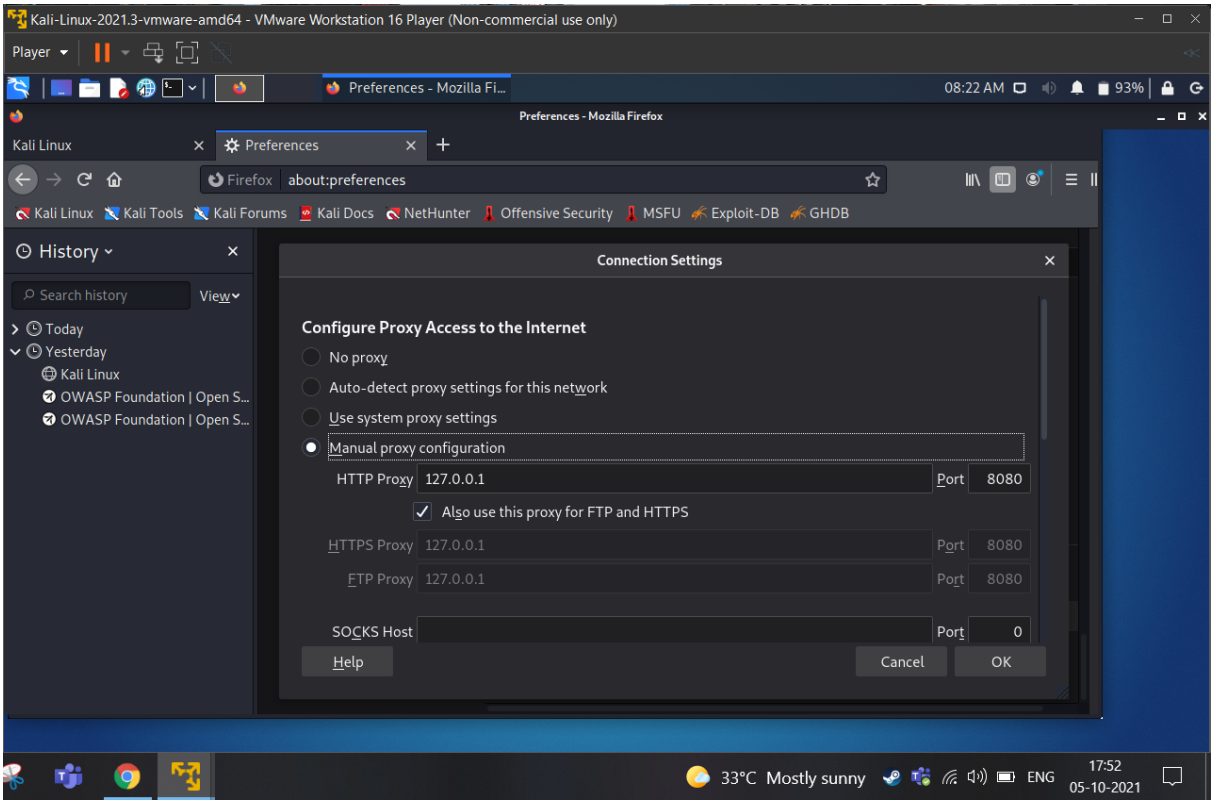
1. Opened Mutillidae using our metasploit IP address.
2. Opened OWASP ZAP and changed the local proxy to 8080.
3. After connecting, Mutillidae and DVMA will be visible on site.
4. Perform spider attack & reported 253 URI
5. Obtained image from get images.
6. Performed Forced browse directory attack and obtained results.

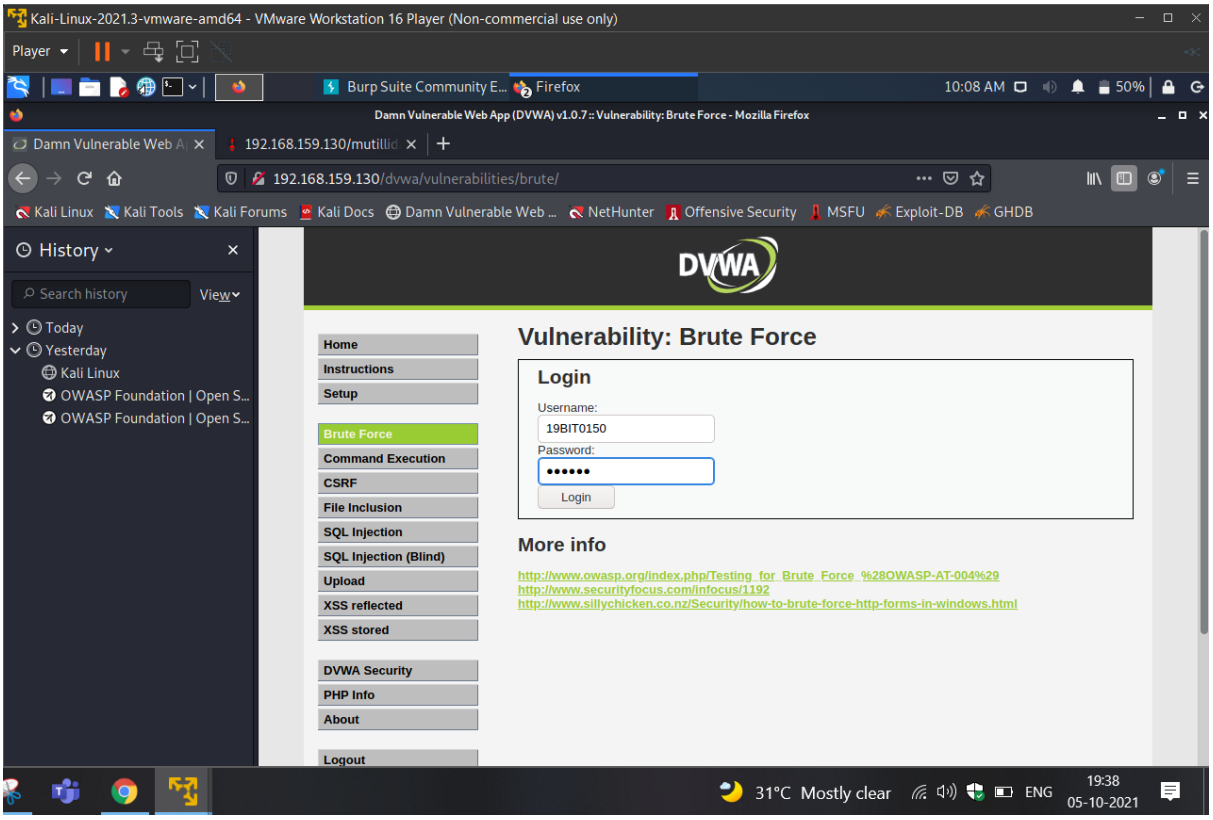
-----x----------x----------x----------x----------x----------x----------x----------x----------x----------x----------x

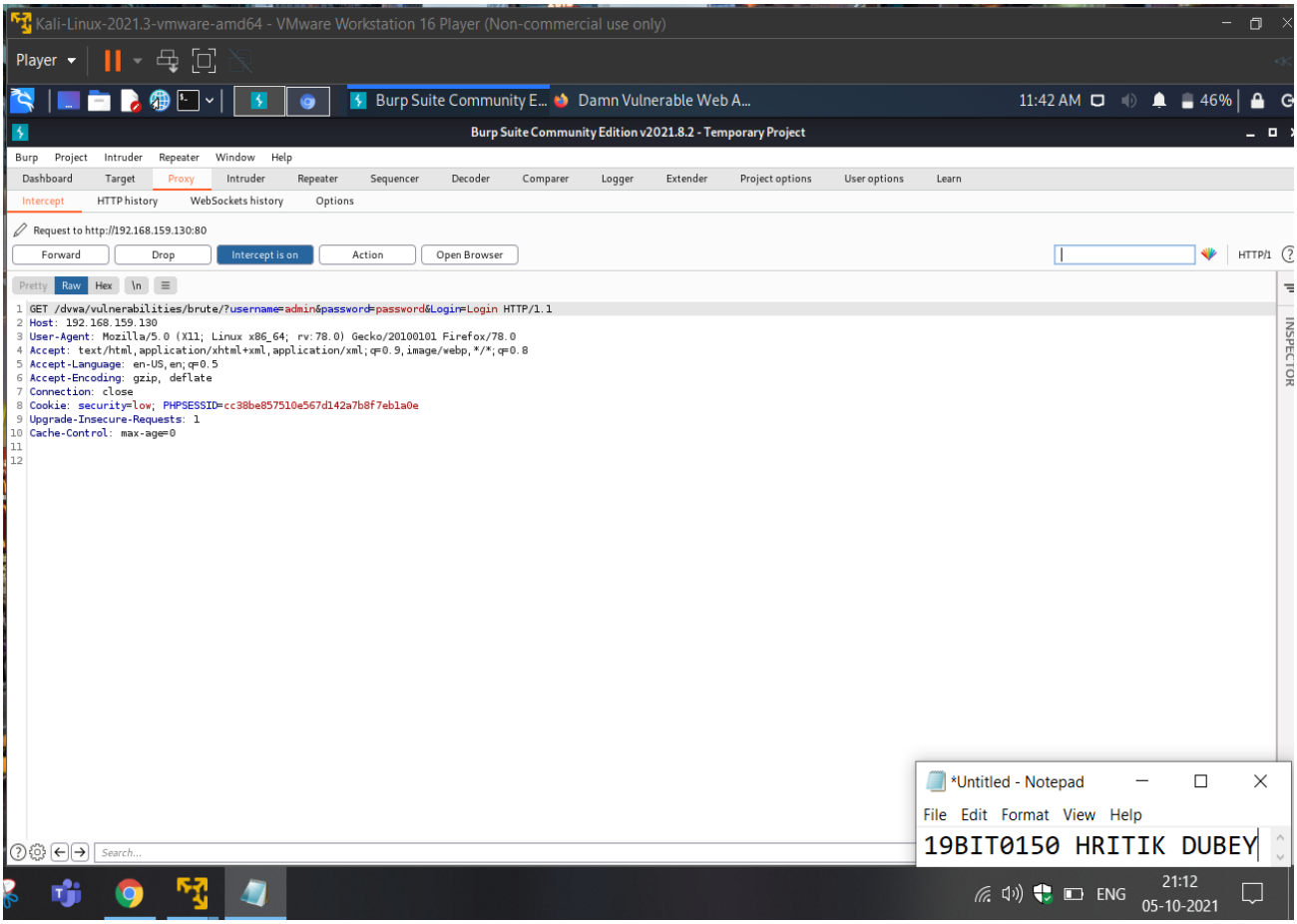
2. Open DVWA through your Metasploitable IP and perform the following:
A. Perform a brute force attack through Burp Suite
i. Show the snapshots of proxy, positions, payloads, intercept, intruder
ii. Get the report of intruder attack



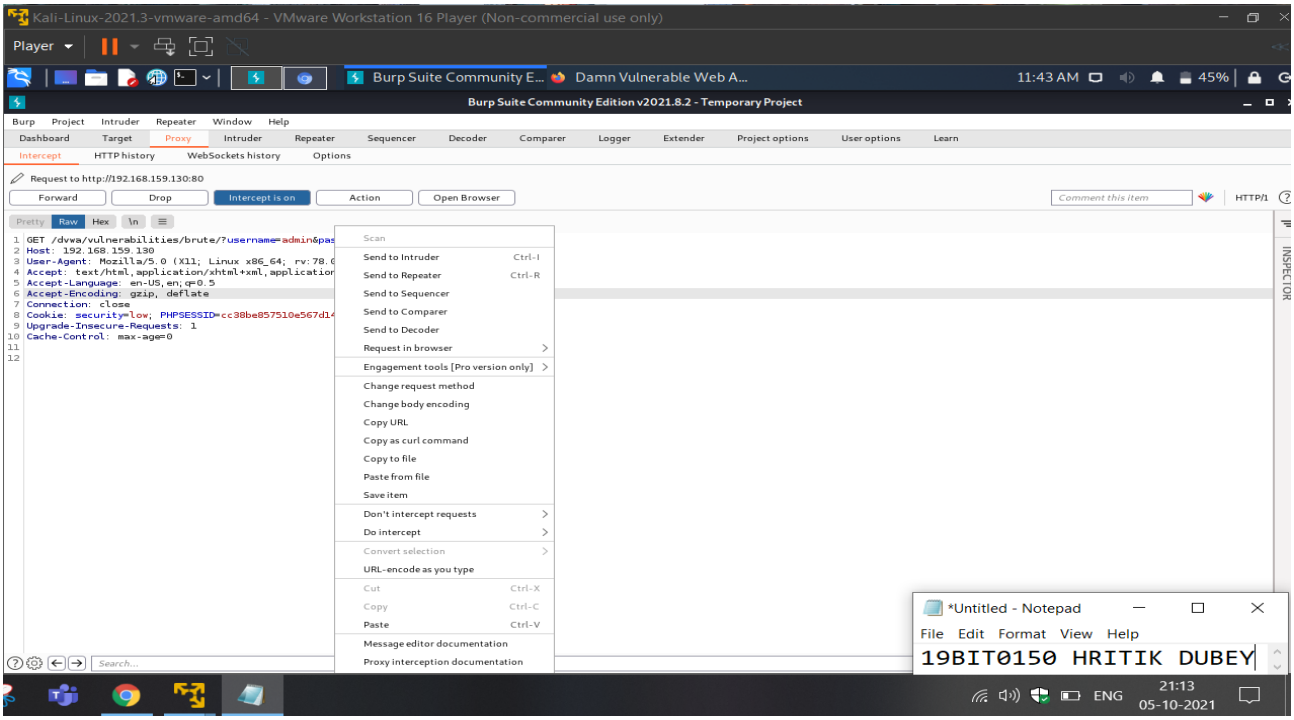
My metasploit Inet address- 192.168.159.130


Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Preferences - Mozilla Fi...
08:22 AM
93%
Preferences - Mozilla Firefox
Kali Linux
Preferences
Firefox
about:preferences
Kali Linux
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
History
Search history
View
Today
Yesterday
Kali Linux
OWASP Foundation | Open S...
OWASP Foundation | Open S...
Connection Settings
Configure Proxy Access to the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration
HTTP Proxy
127.0.0.1
Port
8080
Also use this proxy for FTP and HTTPS
HTTPS Proxy
127.0.0.1
Port
8080
FTP Proxy
127.0.0.1
Port
8080
SOCKS Host
Port
0
Help
Cancel
OK
33°C
Mostly sunny
ENG
17:52
05-10-2021


Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Burp Suite Community E...
Firefox
10:08 AM
50%
Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Brute Force - Mozilla Firefox
Damn Vulnerable Web A
192.168.159.130/mutillid
192.168.159.130/dvwa/vulnerabilities/brute/
Kali Linux
Kali Tools
Kali Forums
Kali Docs
Damn Vulnerable Web ...
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
History
Search history
View
Today
Yesterday
Kali Linux
OWASP Foundation | Open S...
OWASP Foundation | Open S...
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: Brute Force
Login
Username:
19BIT0150
Password:
Login
More info
http://www.owasp.org/index.php/Testing_for_Brute_Force_%28OWASP-AT-004%29
http://www.securityfocus.com/infocus/1192
http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html
31°C
Mostly clear
ENG
19:38
05-10-2021

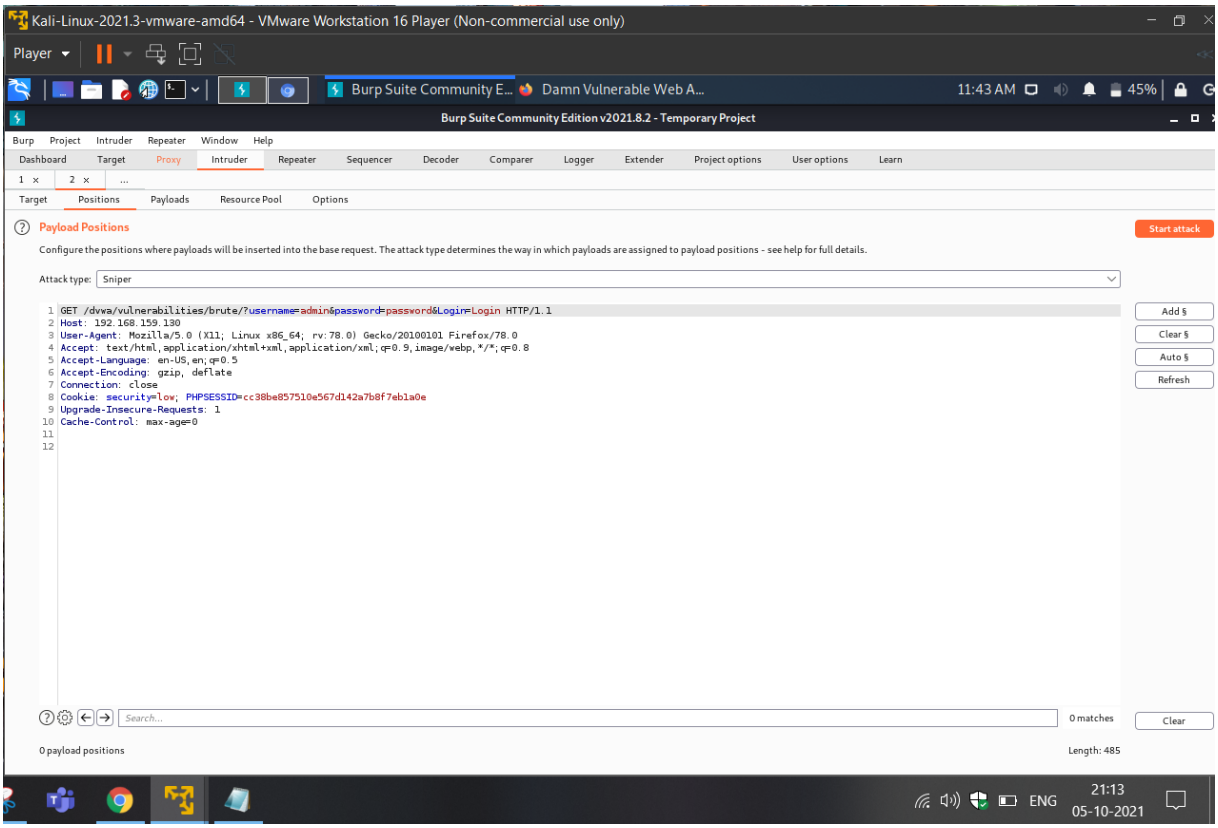


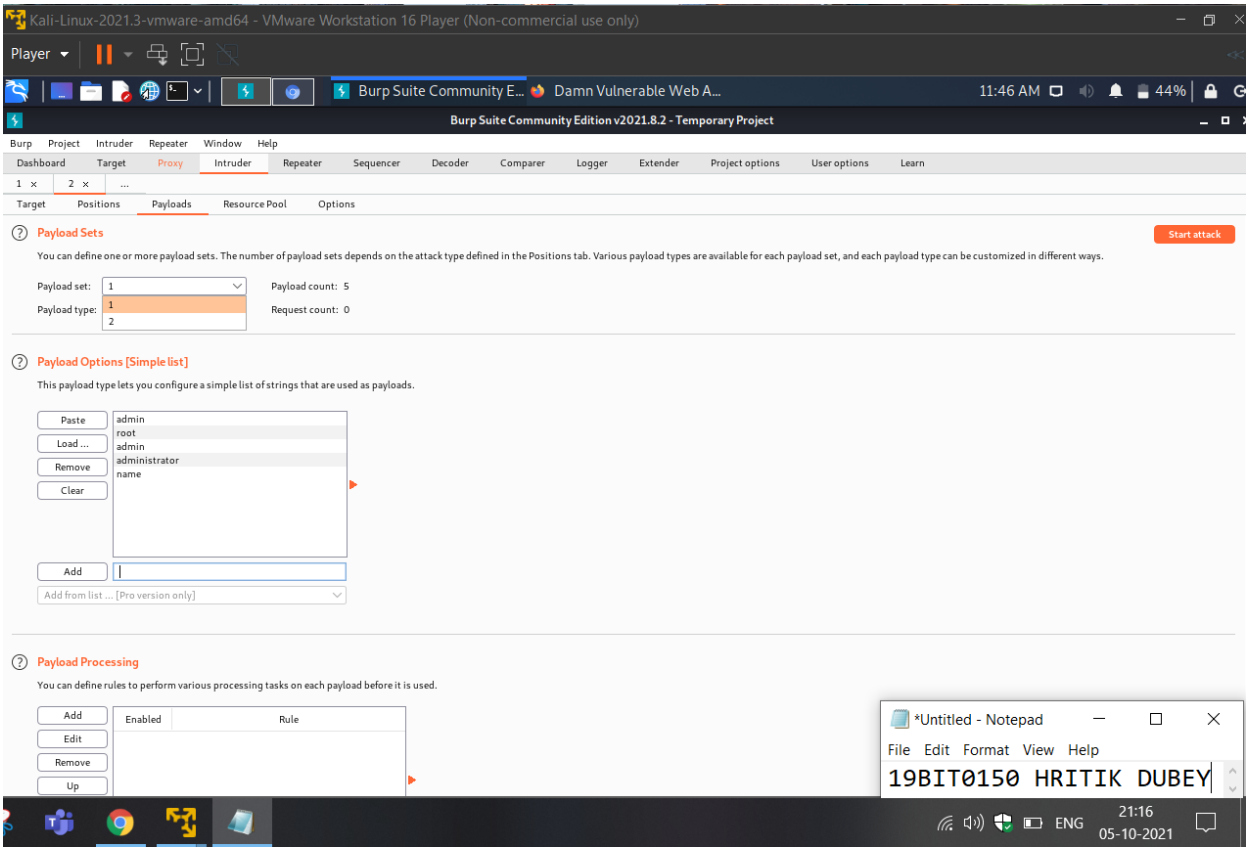

```
1  GET /dvwa/vulnerabilities/brute/?username=admin+&password=password&Login=Login HTTP/1.1
2  Host: 192.168.159.130
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Connection: close
8  Referer: http://192.168.159.130/dvwa/vulnerabilities/brute/
9  Cookie: security=low; PHPSESSID=cc38be857510e567d142a7b8f7eb1a0e
10 Upgrade-Insecure-Requests: 1
11
```

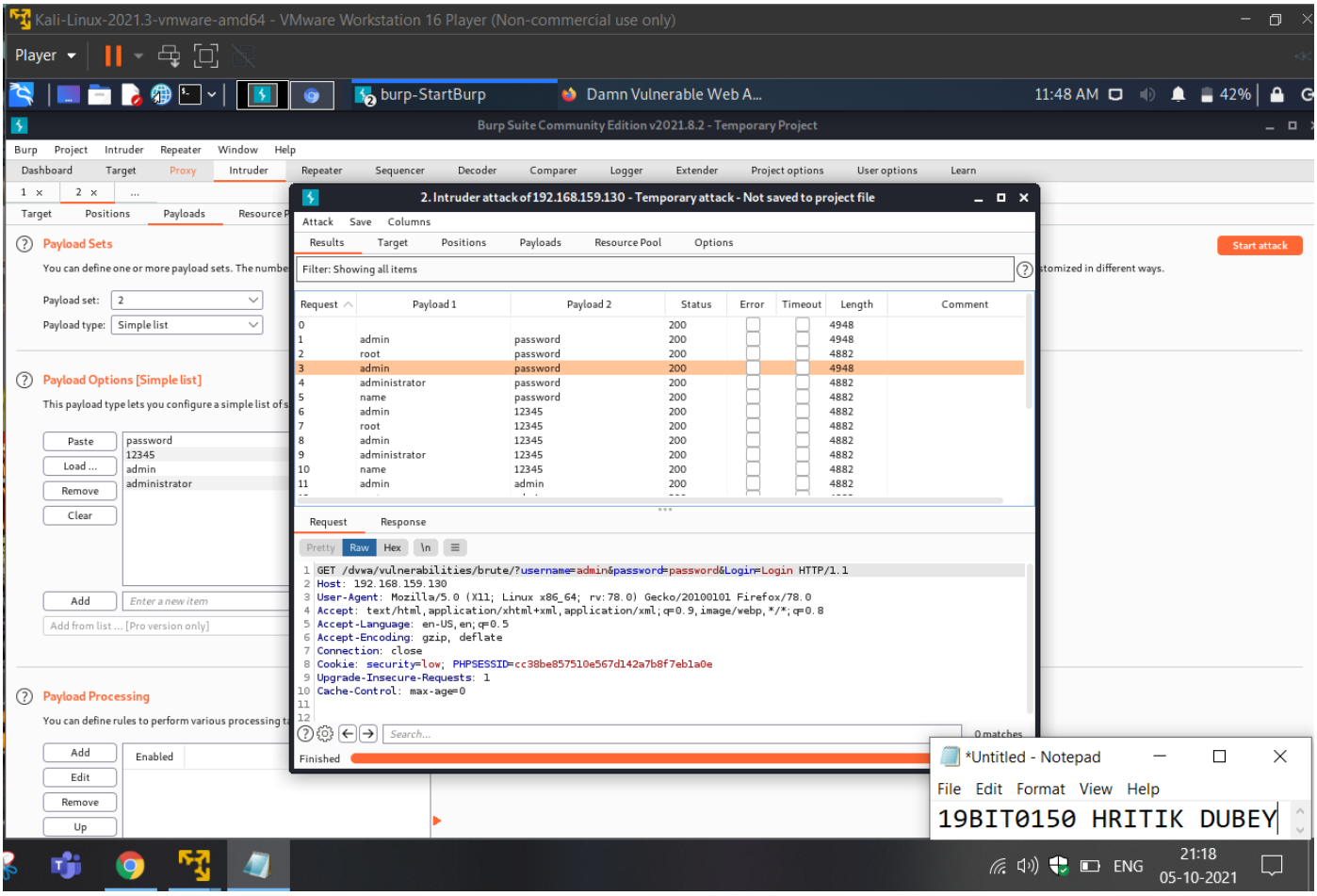


We have changed the network setting and performed following operation-

1. Open Dvwa with metasploit inet address
2. Enter login ID admin and password password
3. Burp suite Intercept
4. Send to intruder
5. Clear the highlighted text
6. Select admin and password
7. Add admin and password
8. Add payload 1 & 2
9. Start Attack


Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Burp Suite Community E...
Damn Vulnerable Web A...
11:43 AM
45%
Burp Suite Community Edition v2021.8.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 × ...
Target Positions Payloads Resource Pool Options
Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
GET /dvwa/vulnerabilities/brute/?username=admin&password=password&Login=Login HTTP/1.1
Host: 192.168.159.130
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
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
Connection: close
Cookie: security=low; PHPSESSID=cc38be857510e567d142a7b8f7eb1a0e
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Add §
Clear §
Auto §
Refresh
Search...
0 matches
Clear
0 payload positions
Length: 485
ENG
21:13
05-10-2021

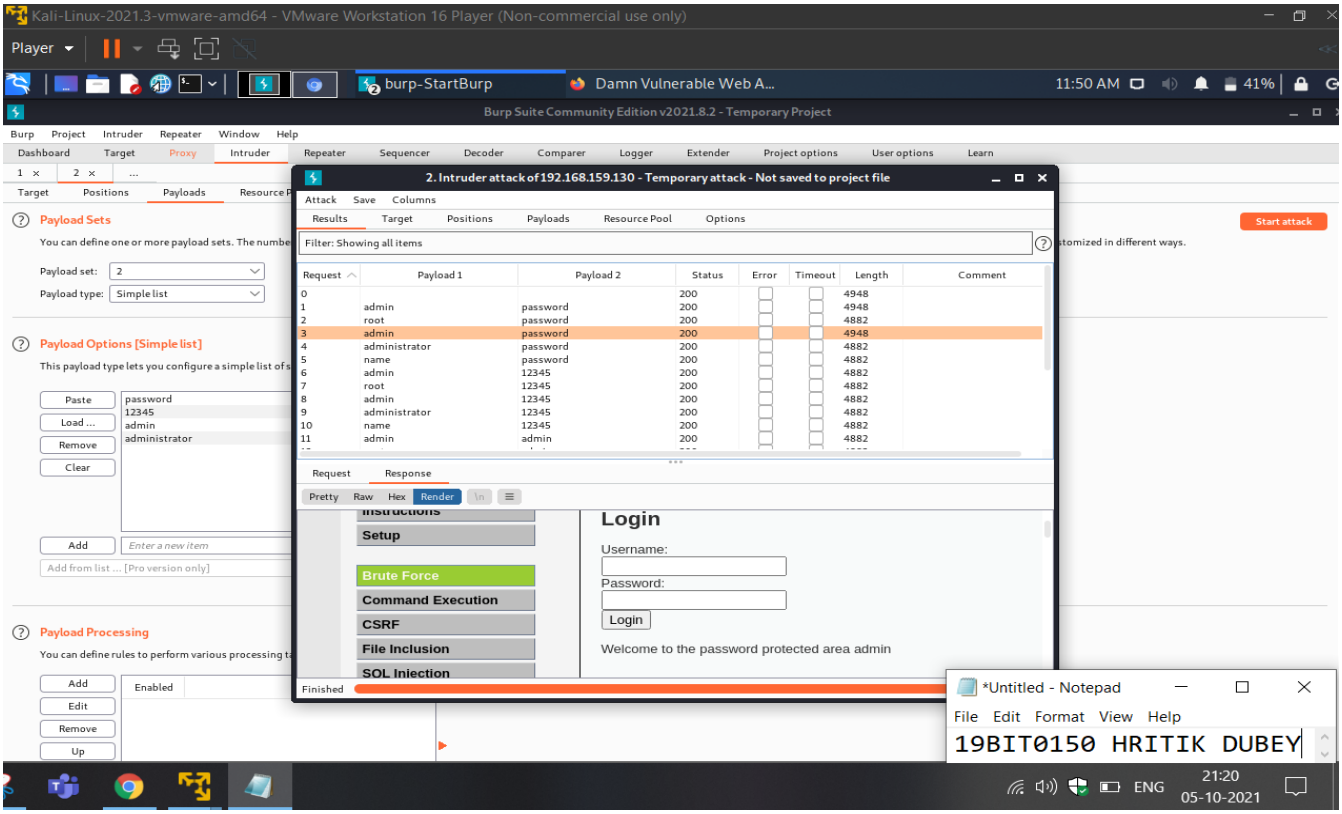

Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Burp Suite Community E...
Damn Vulnerable Web A...
11:46 AM
44%
Burp Suite Community Edition v2021.8.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 × ...
Target Positions Payloads Resource Pool Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 5
Payload type: 1 2
Request count: 0
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
admin
root
admin
administrator
name
Add
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Enabled
Rule
*Untitled - Notepad
File Edit Format View Help
19BIT0150 HRITIK DUBEY
ENG
21:16
05-10-2021



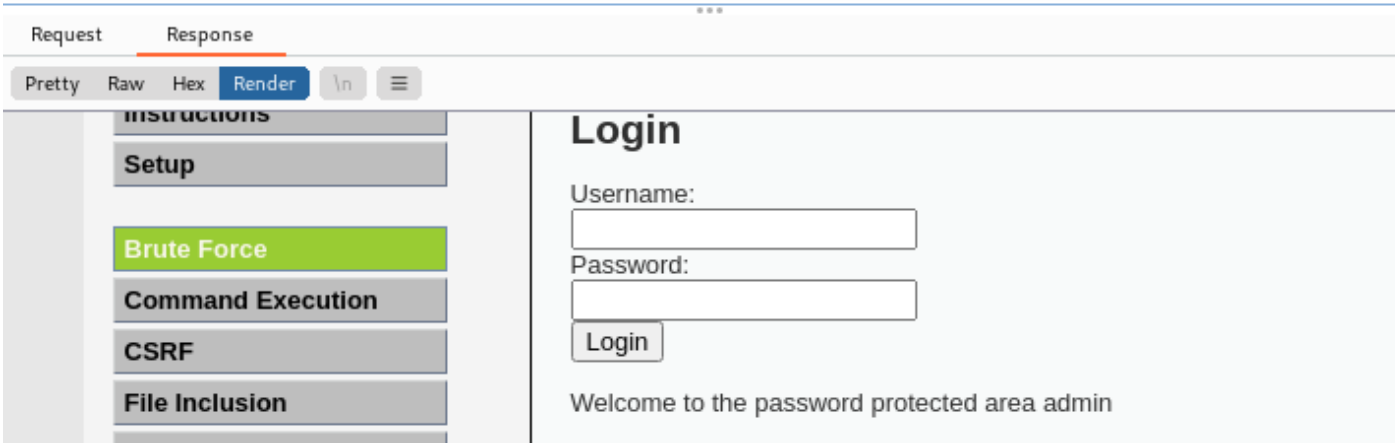
After performing attack, check for length

Select different length

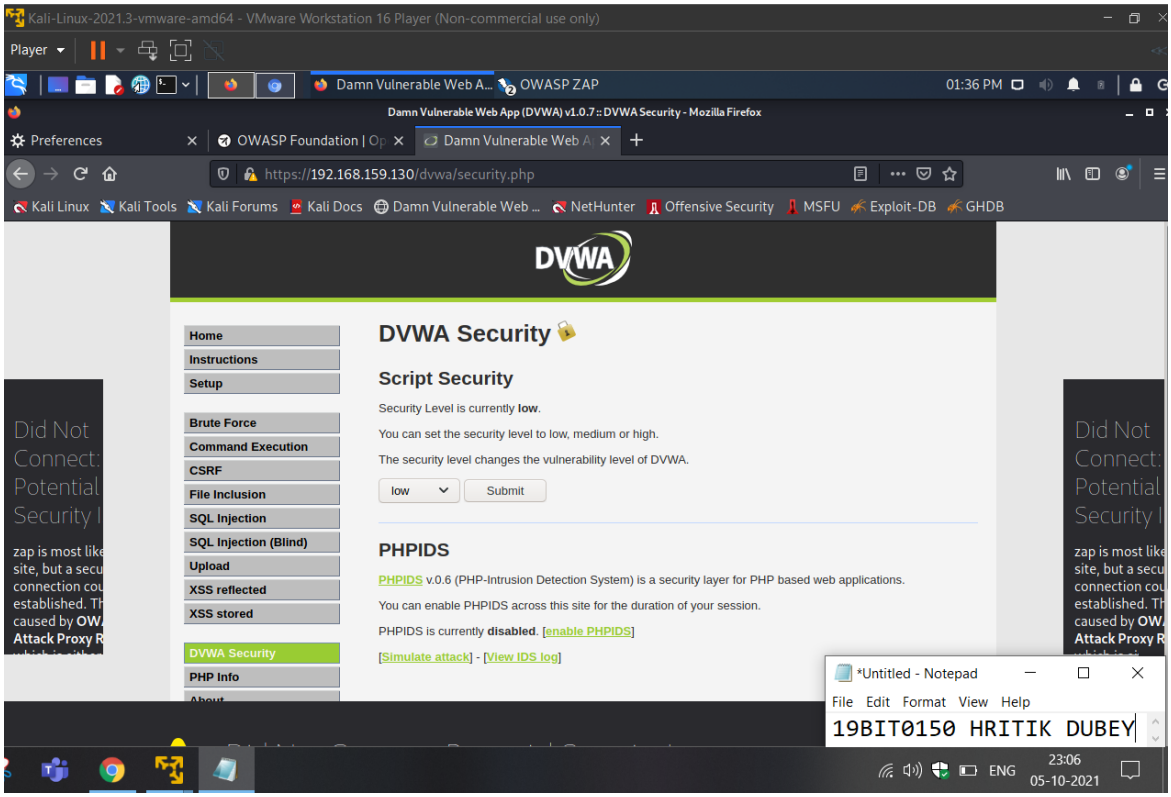
Click on response -> render

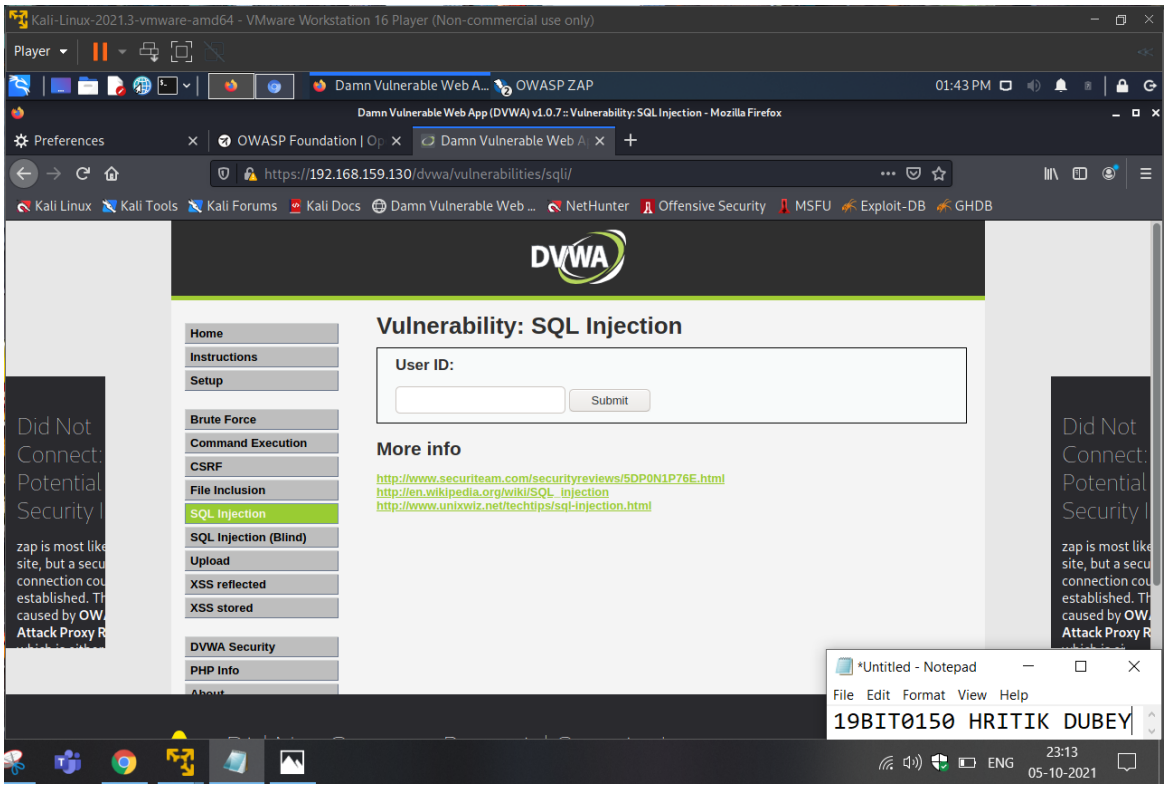


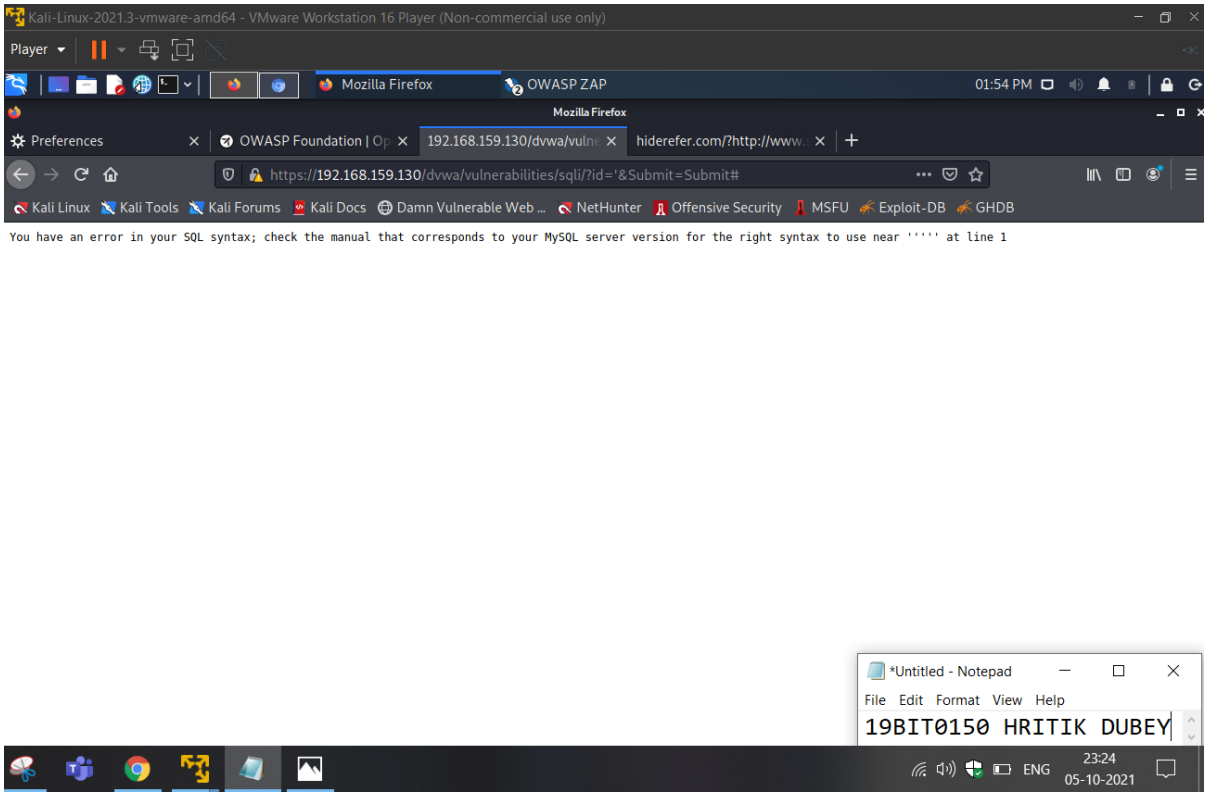
2	root	password	200			4882
3	admin	password	200			4948
4	administrator	password	200			4882
5	name	password	200			4882
6	admin	12345	200			4882
7	root	12345	200			4882
8	admin	12345	200			4882
9	administrator	12345	200			4882
10	name	12345	200			4882
11	admin	admin	200			4882



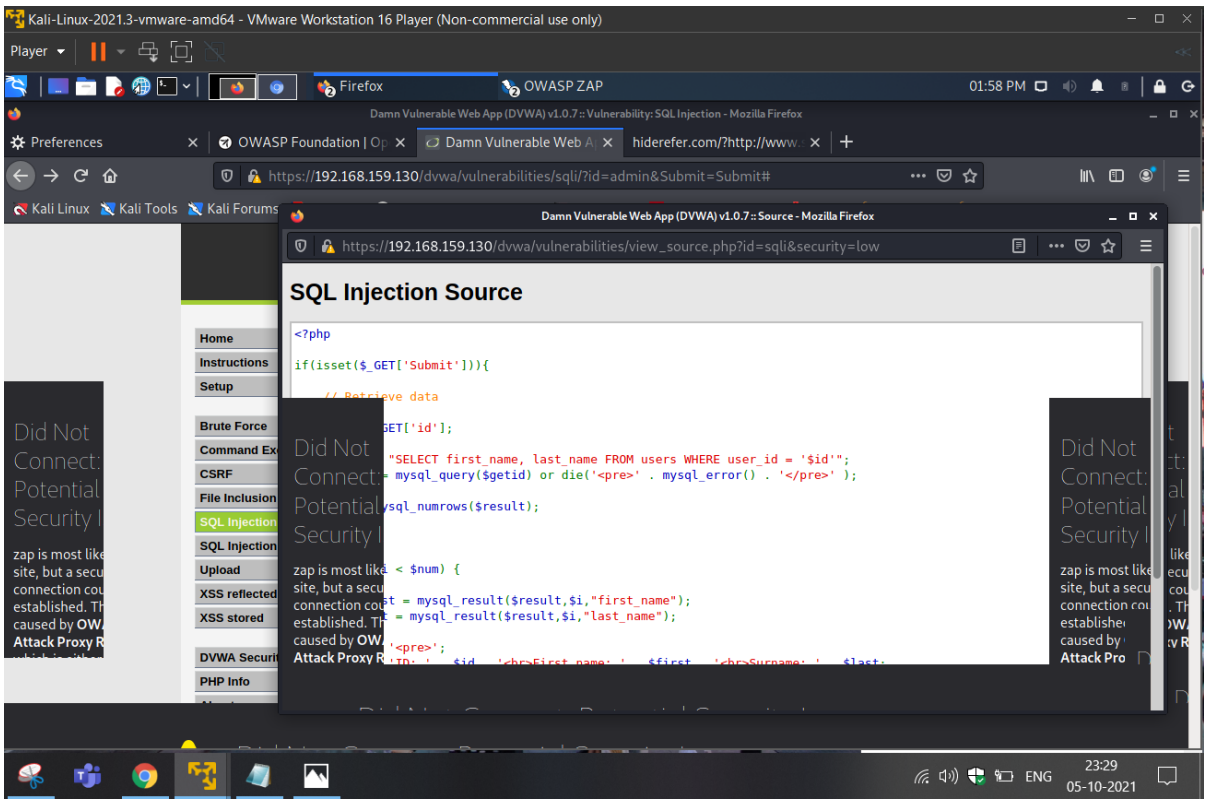
B. Perform a SQL injection to retrieve the hashed passwords of the users database





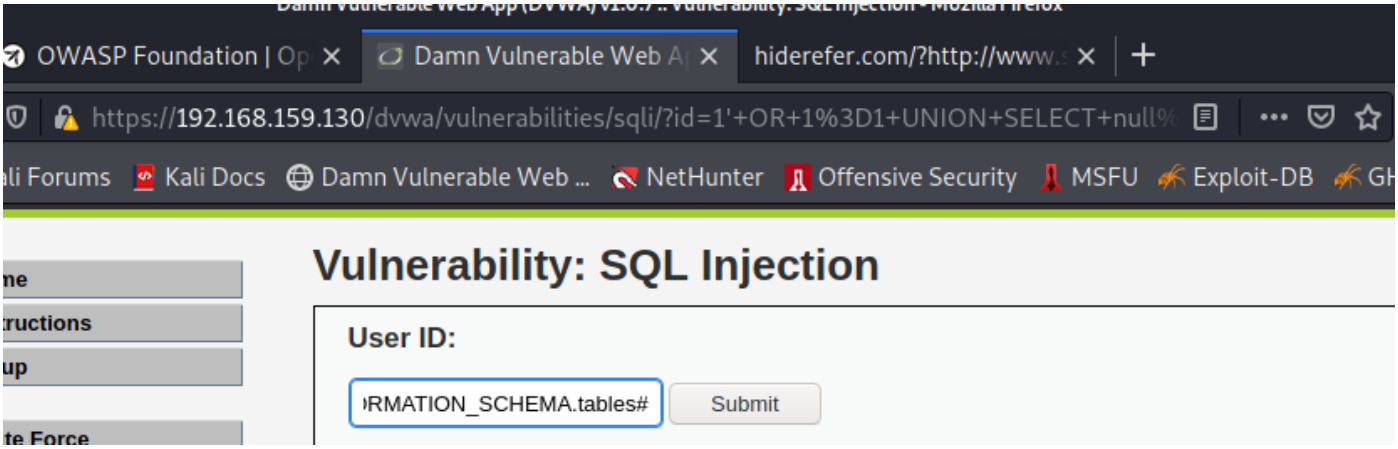


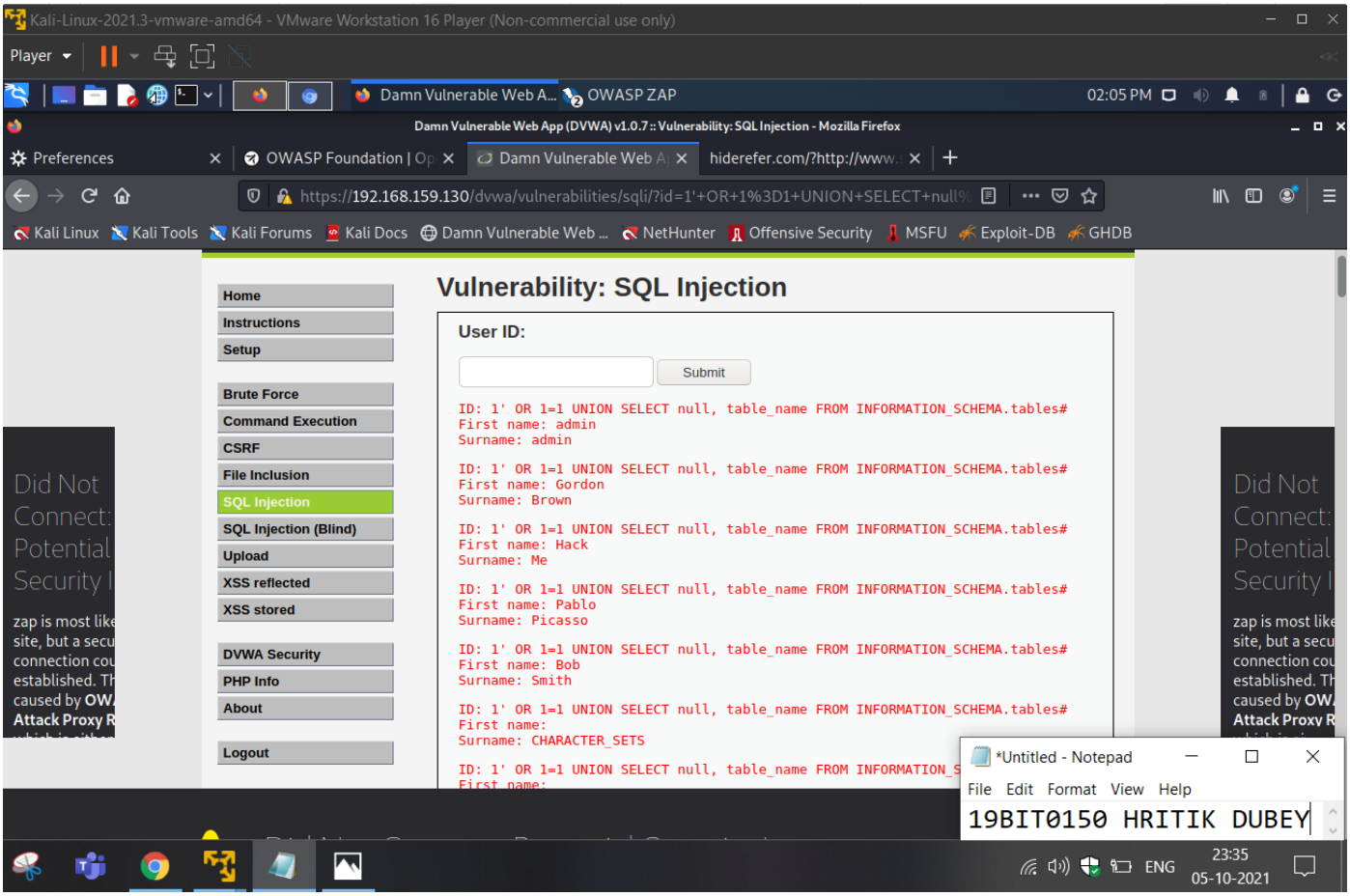
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '''' at line 1



$getid = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";

USING COMMAND
1' OR 1=1 UNION SELECT null, table_name FROM INFORMATION_SCHEMA.tables#





GOOGLE DRIVE LINK WITH ALL THE SNAPSHOTS -

https://drive.google.com/drive/folders/1F2pemZ9uwrIh47EgtuSlpFswbyQwXoCF?usp=sharing