# CSE3501-Information Security Analysis and Audit Lab

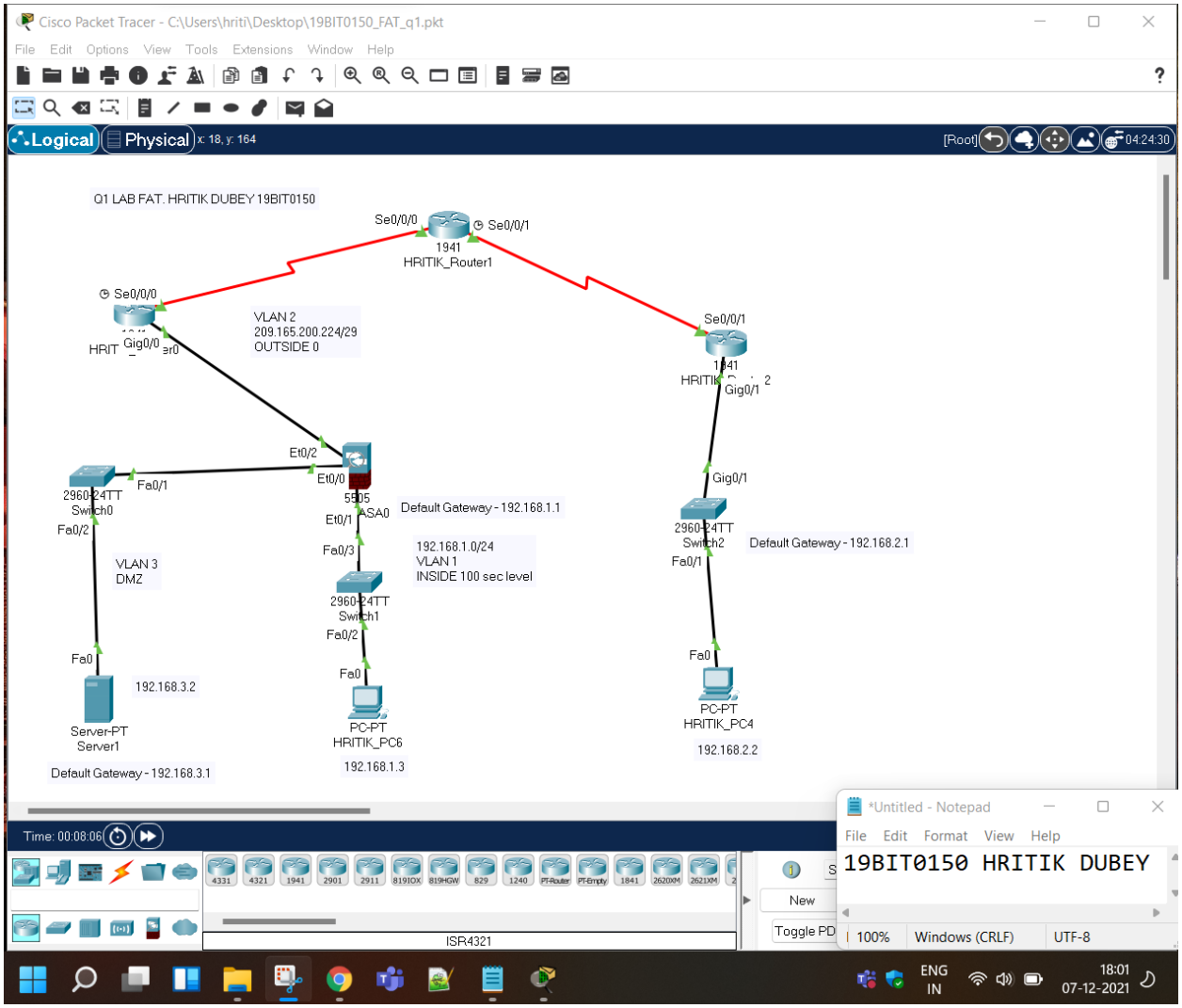
NAME- HRITIK DUBEY  REG NO-19BIT0150  SLOT- L41+L42

---

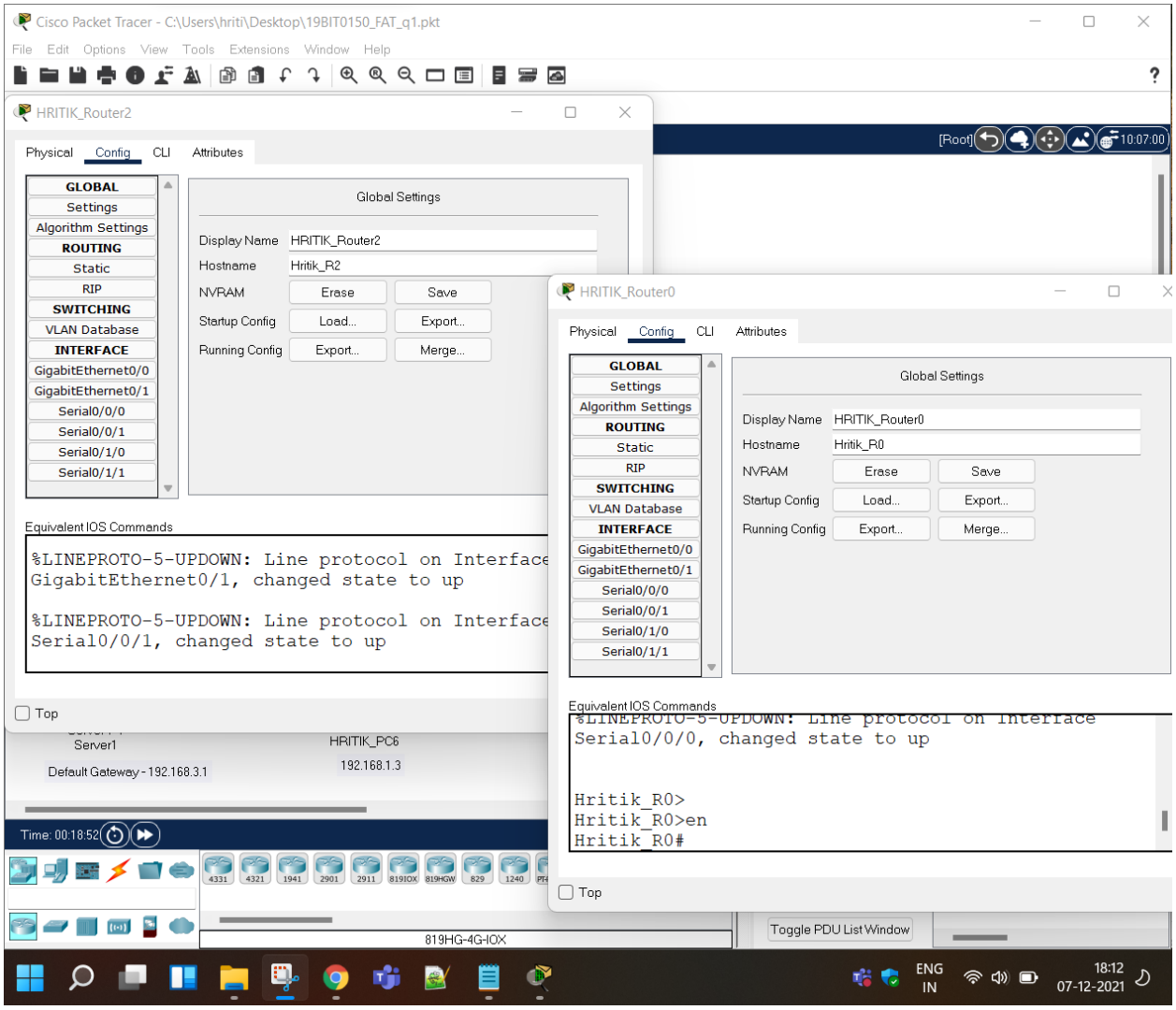
LAB FAT  Faculty : Dr. Priya V

**DRIVE LINK-**
**https://drive.google.com/drive/folders/1wBKGRcglT0AT6lhD0LzvKO6kWQLF_1xL?usp=sharing**

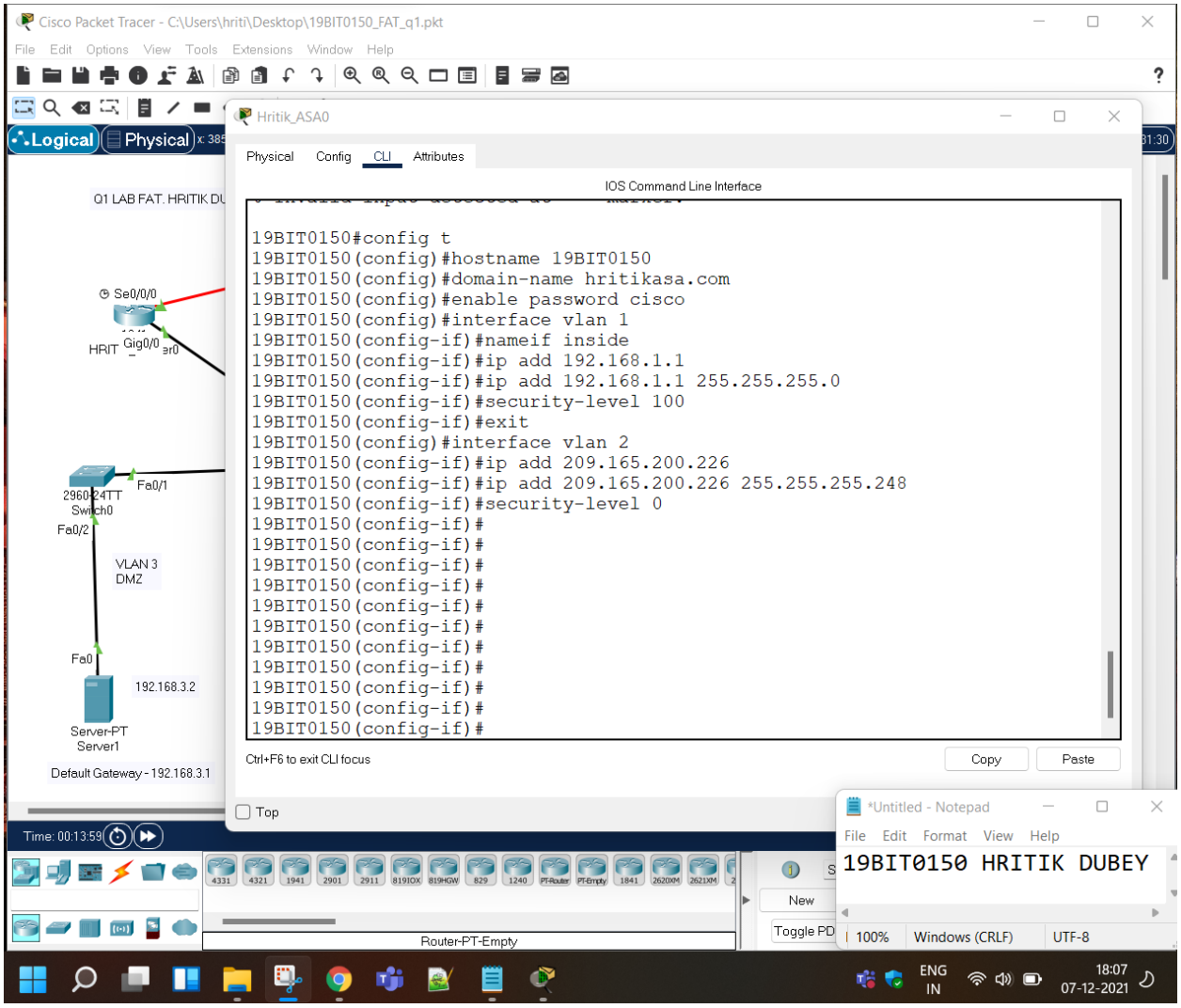
## 1. Question 1: Cisco Packet Tracer [15 Marks]

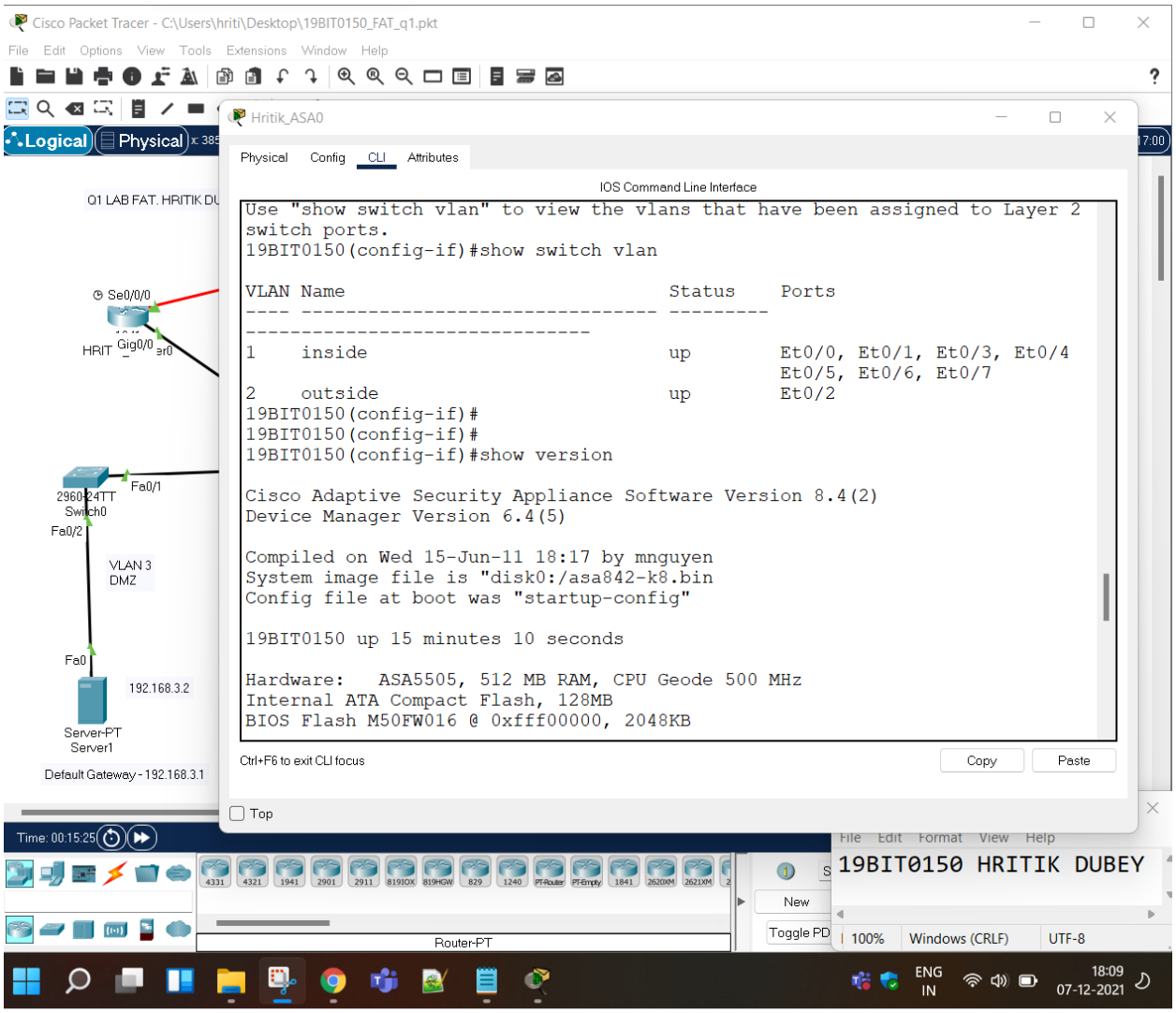


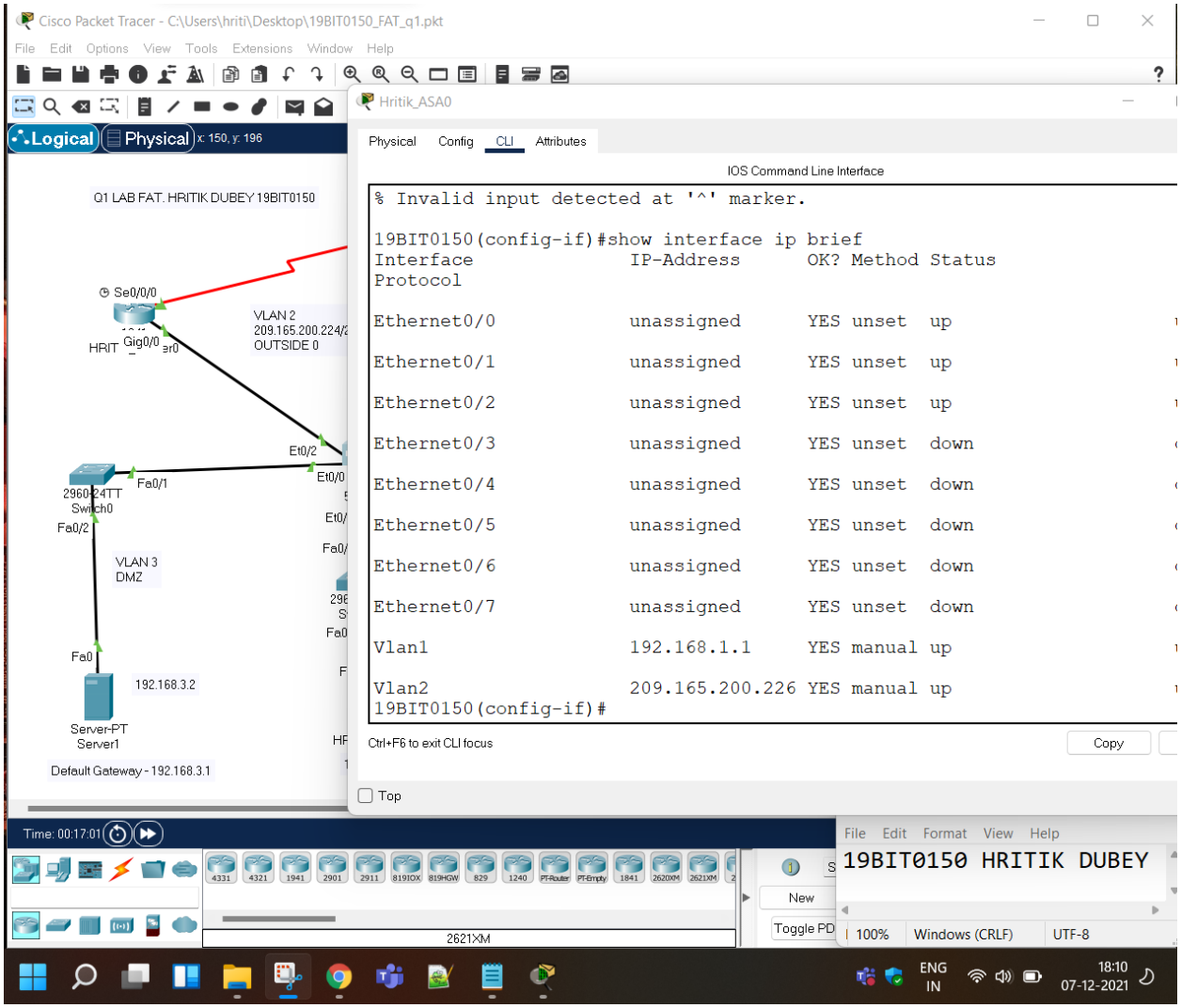
## BASIC ROUTER CONFIGURATION



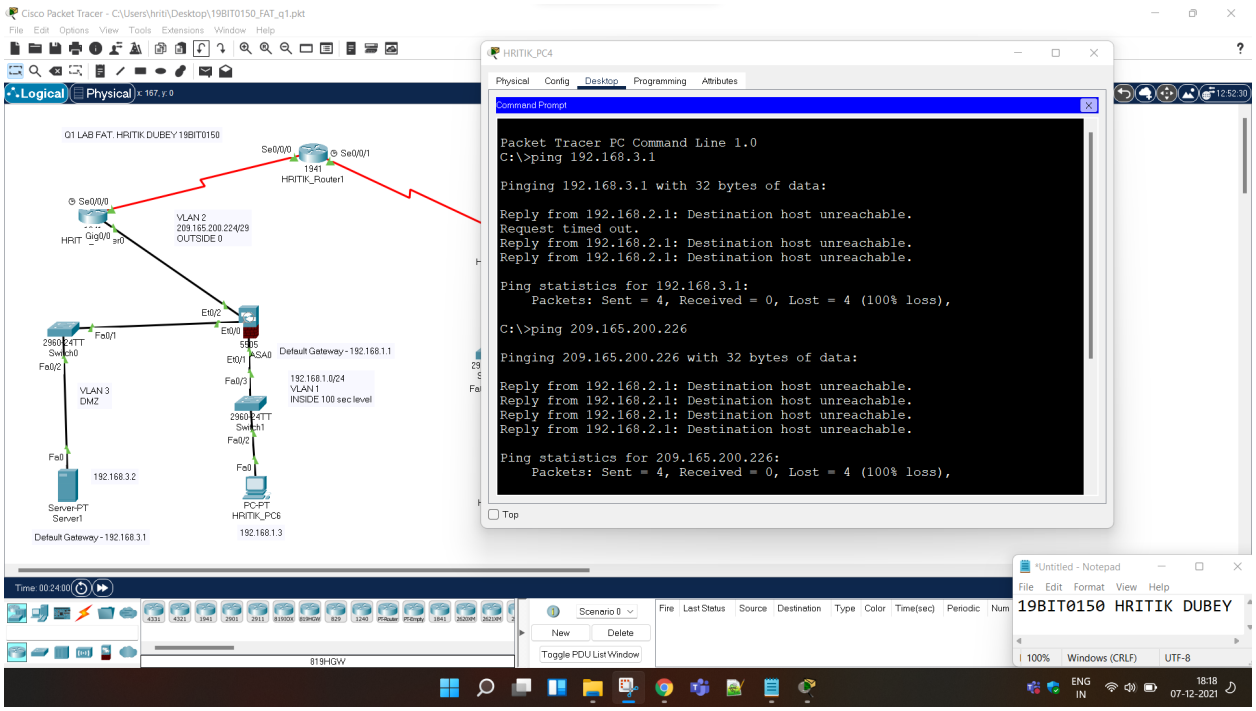
## ASA CONFIGURATION

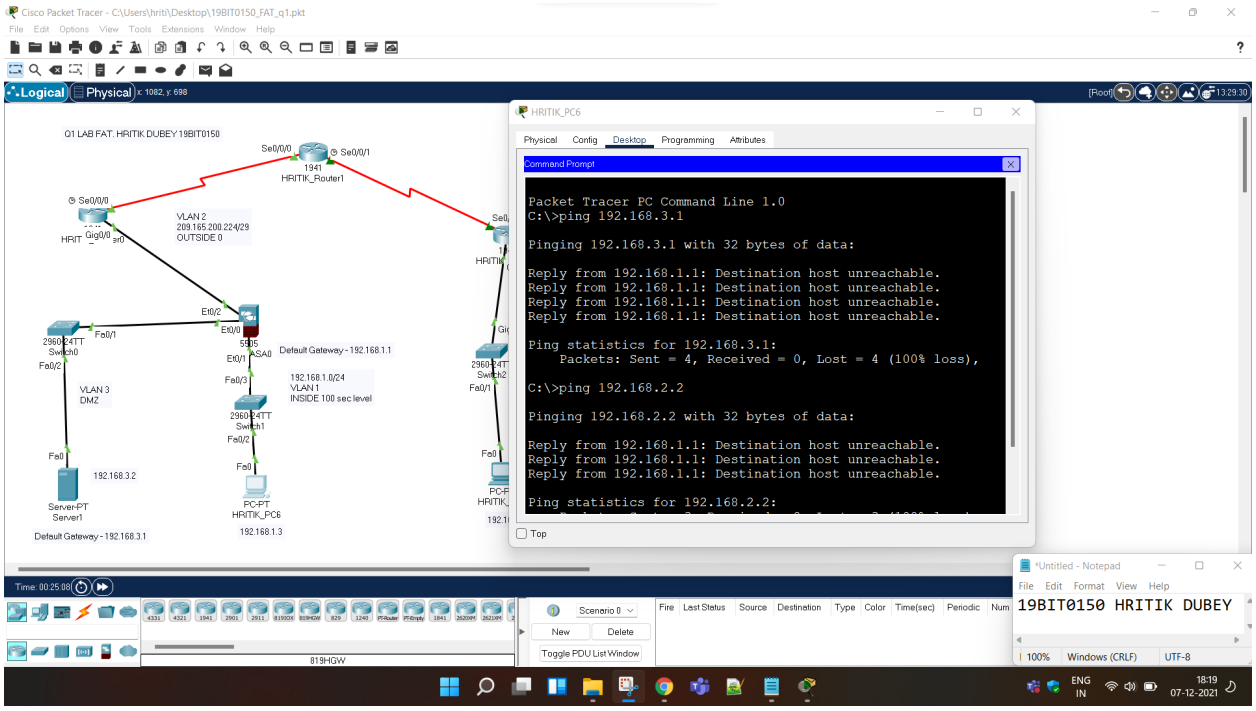



Cisco Packet Tracer - C:\Users\hriti\Desktop\19BIT0150_FAT_q1.pkt
File Edit Options View Tools Extensions Window Help
Logical
Physical
Q1 LAB FAT. HRITIK DU
Se0/0/0
HRIT Gig0/0
Fa0/1
2960-24TT
Switch0
Fa0/2
VLAN 3
DMZ
Fa0
192.168.3.2
Server-PT
Server1
Default Gateway - 192.168.3.1
Hritik_ASA0
Physical Config CLI Attributes
IOS Command Line Interface
Use "show switch vlan" to view the vlans that have been assigned to Layer 2
switch ports.
19BIT0150(config-if)#show switch vlan
VLAN Name Status Ports
1 inside up Et0/0, Et0/1, Et0/3, Et0/4
Et0/5, Et0/6, Et0/7
2 outside up Et0/2
19BIT0150(config-if)#
19BIT0150(config-if)#
19BIT0150(config-if)#show version
Cisco Adaptive Security Appliance Software Version 8.4(2)
Device Manager Version 6.4(5)
Compiled on Wed 15-Jun-11 18:17 by mnguyen
System image file is "disk0:/asa842-k8.bin
Config file at boot was "startup-config"
19BIT0150 up 15 minutes 10 seconds
Hardware: ASA5505, 512 MB RAM, CPU Geode 500 MHz
Internal ATA Compact Flash, 128MB
BIOS Flash M50FW016 @ 0xfff00000, 2048KB
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
Time: 00:15:25
Router-PT
New
Toggle PD
19BIT0150 HRITIK DUBEY
100%
Windows (CRLF)
UTF-8
ENG
IN
18:09
07-12-2021


Cisco Packet Tracer - C:\Users\hriti\Desktop\19BIT0150_FAT_q1.pkt
File Edit Options View Tools Extensions Window Help
Logical
Physical
Q1 LAB FAT. HRITIK DUBEY 19BIT0150
Se0/0/0
HRIT
Gig0/0
VLAN 2
OUTSIDE 0
Et0/2
Et0/0
Fa0/1
Switch0
Fa0/2
VLAN 3
DMZ
Fa0
192.168.3.2
Server-PT
Server1
Default Gateway - 192.168.3.1
Hritik_ASA0
Physical
Config
CLI
Attributes
IOS Command Line Interface
% Invalid input detected at '^' marker.
19BIT0150(config-if)#show interface ip brief
Interface IP-Address OK? Method Status
Protocol
Ethernet0/0 unassigned YES unset up
Ethernet0/1 unassigned YES unset up
Ethernet0/2 unassigned YES unset up
Ethernet0/3 unassigned YES unset down
Ethernet0/4 unassigned YES unset down
Ethernet0/5 unassigned YES unset down
Ethernet0/6 unassigned YES unset down
Ethernet0/7 unassigned YES unset down
Vlan1 192.168.1.1 YES manual up
Vlan2 209.165.200.226 YES manual up
19BIT0150(config-if)#
Ctrl+F6 to exit CLI focus
Copy
Top
Time: 00:17:01
2621XM
New
Toggle PD
File Edit Format View Help
19BIT0150 HRITIK DUBEY
100%
Windows (CRLF)
UTF-8
ENG
IN
18:10
07-12-2021

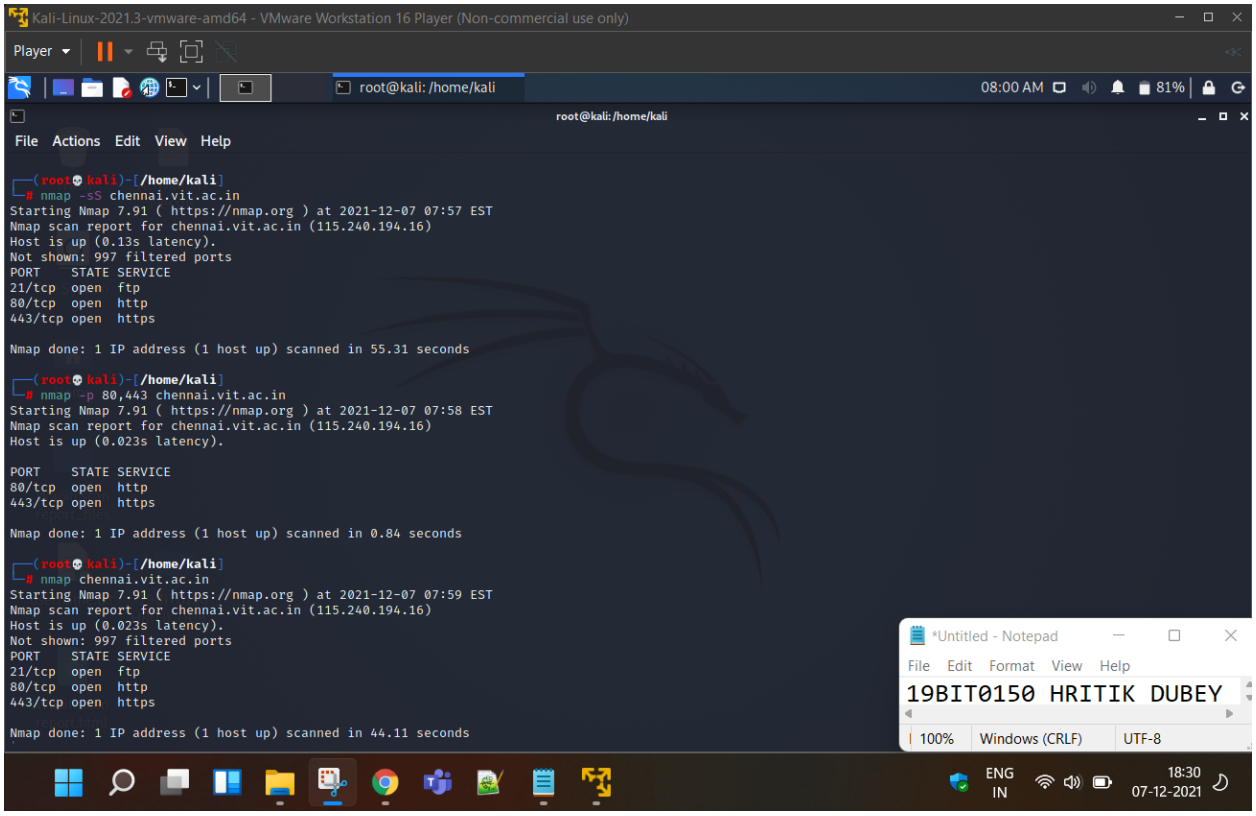
# PING SNAPSHOT



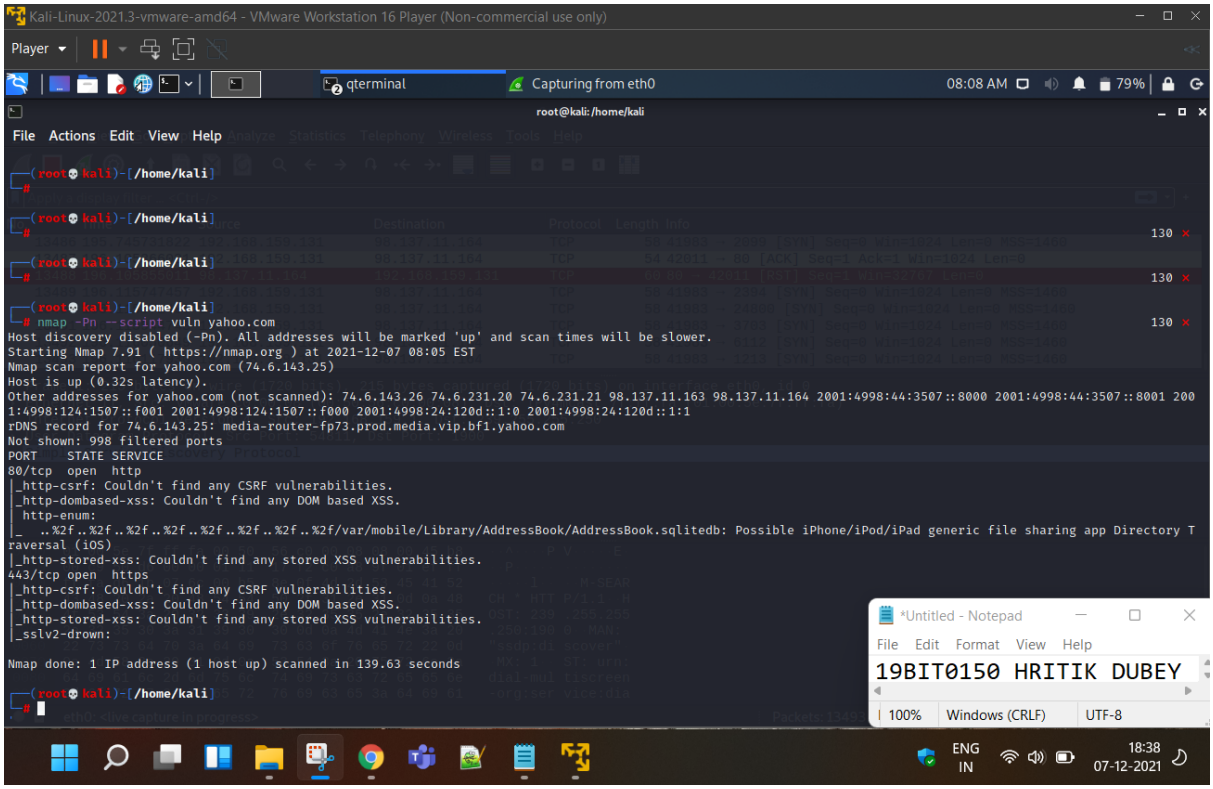
## Question 2 : Cisco Packet Tracer [15 Marks]  NMap Scan

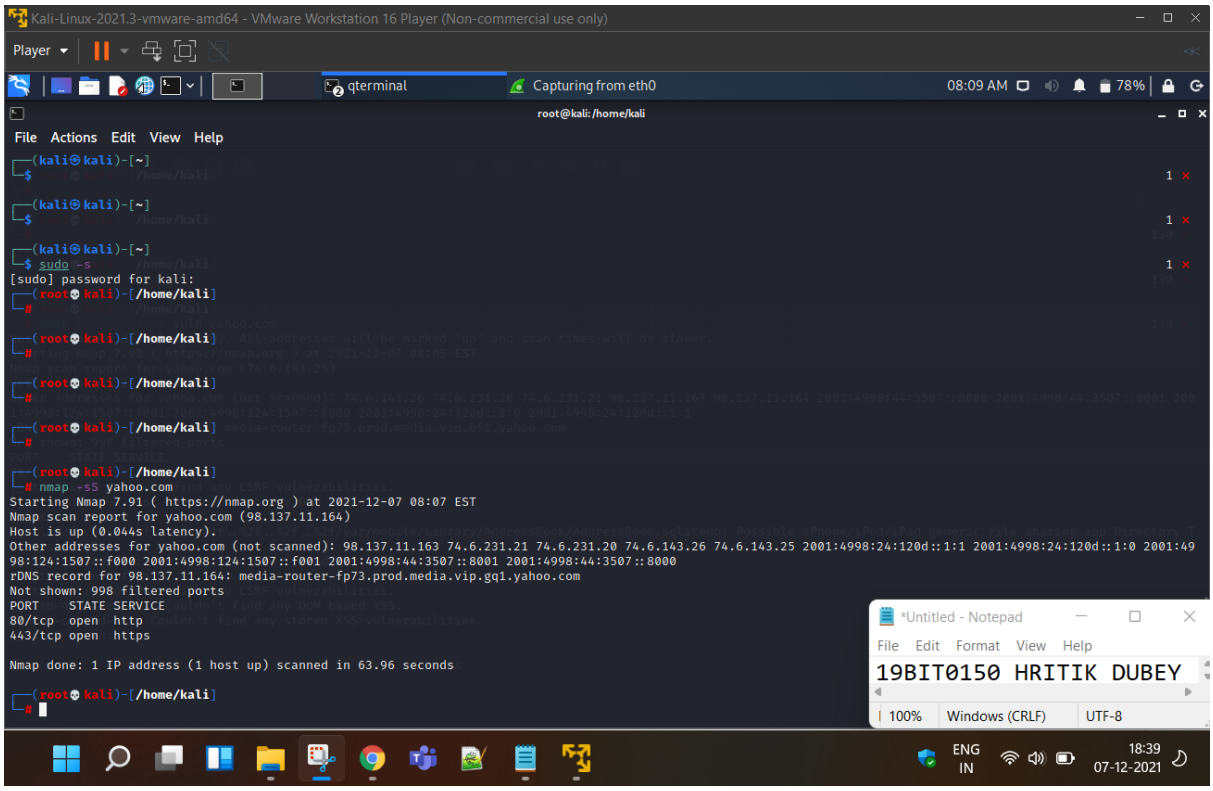
**#nmap -sS chennai.vit.ac.in**
**#nmap -p 80,443 chennai.vit.ac.in**
**#nmap chennai.vit.ac.in**

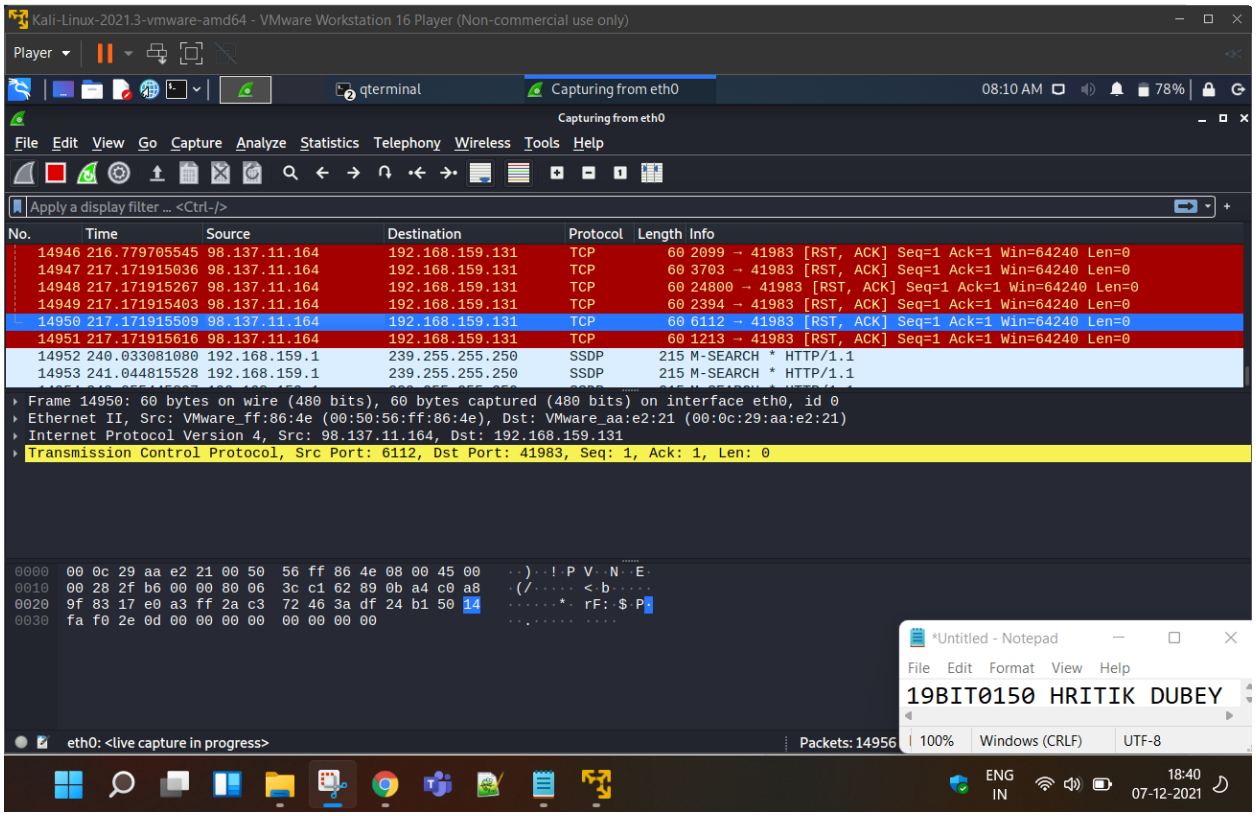


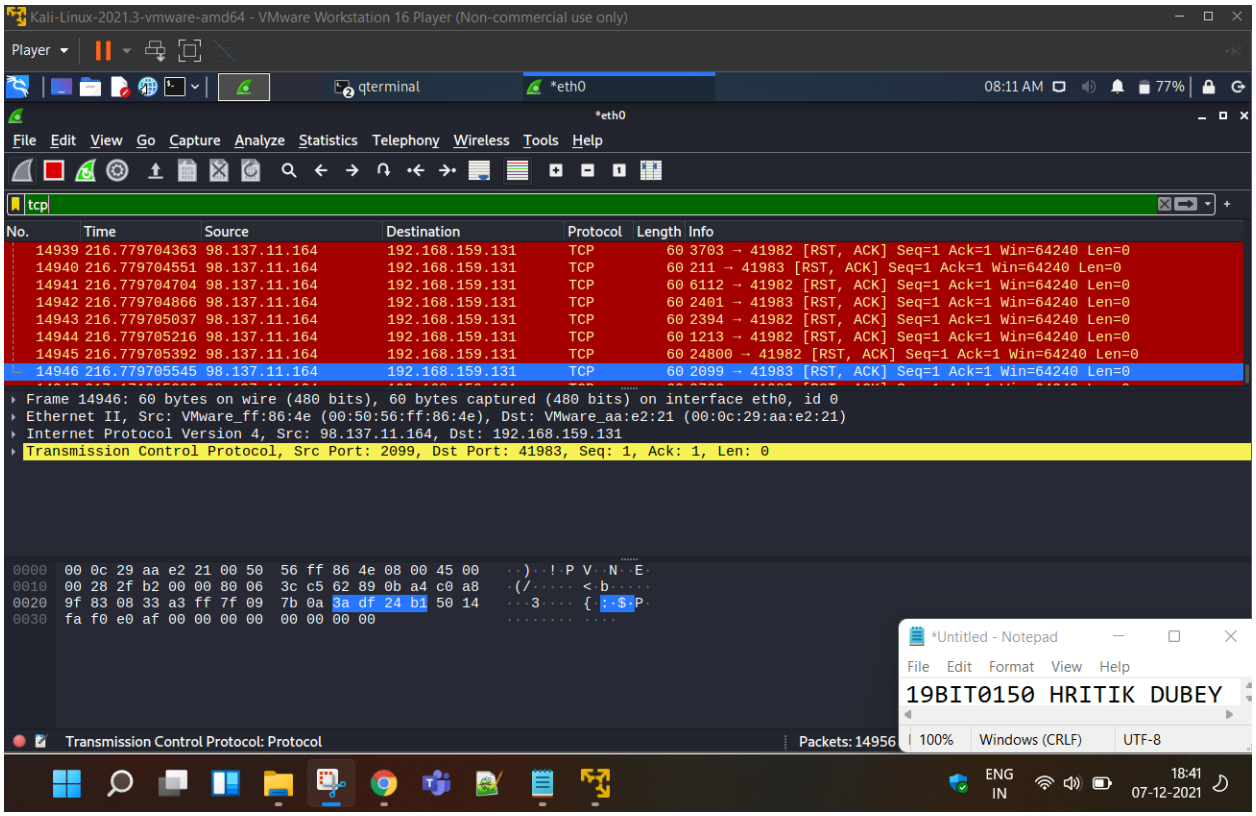

PORT  STATE SERVICE
21/tcp  open  ftp
80/tcp  open  http
443/tcp open  https

## Question 2 : Yahoo.com". Which NMAP switch would the hacker use? In

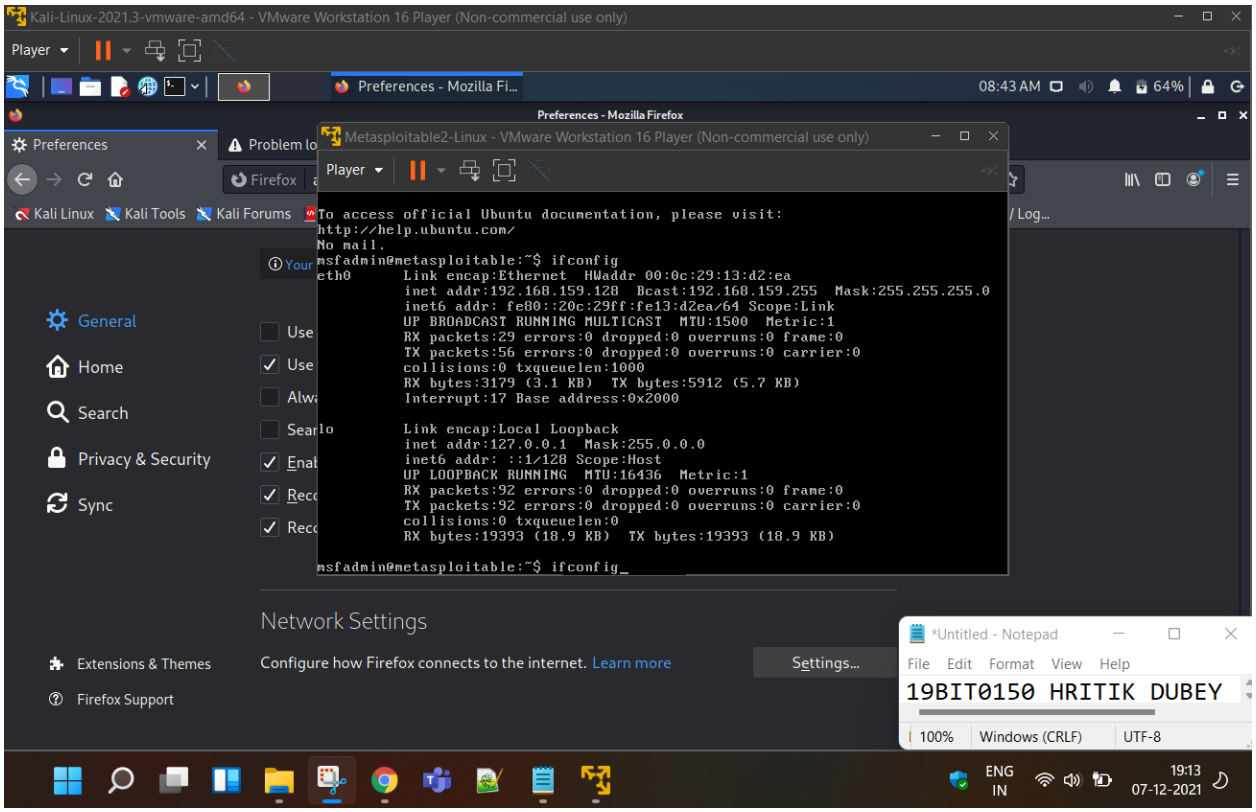


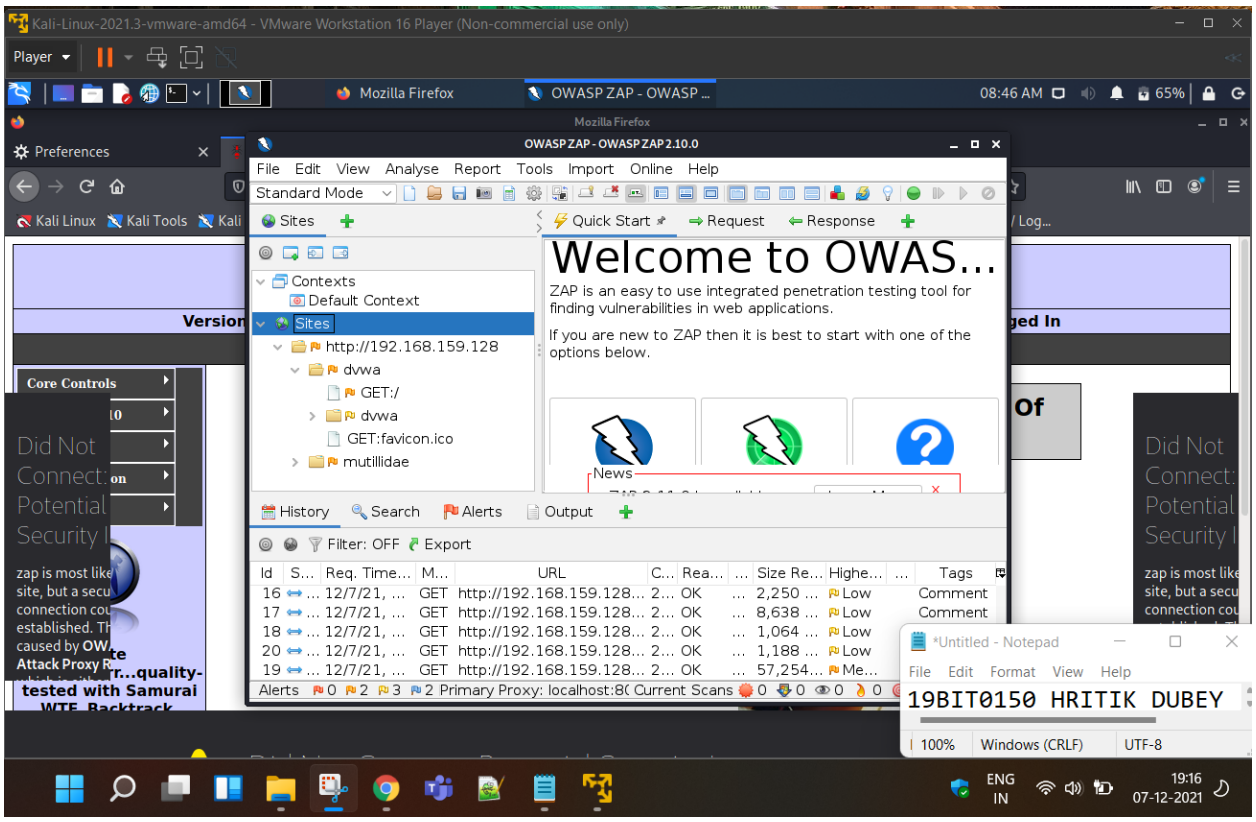



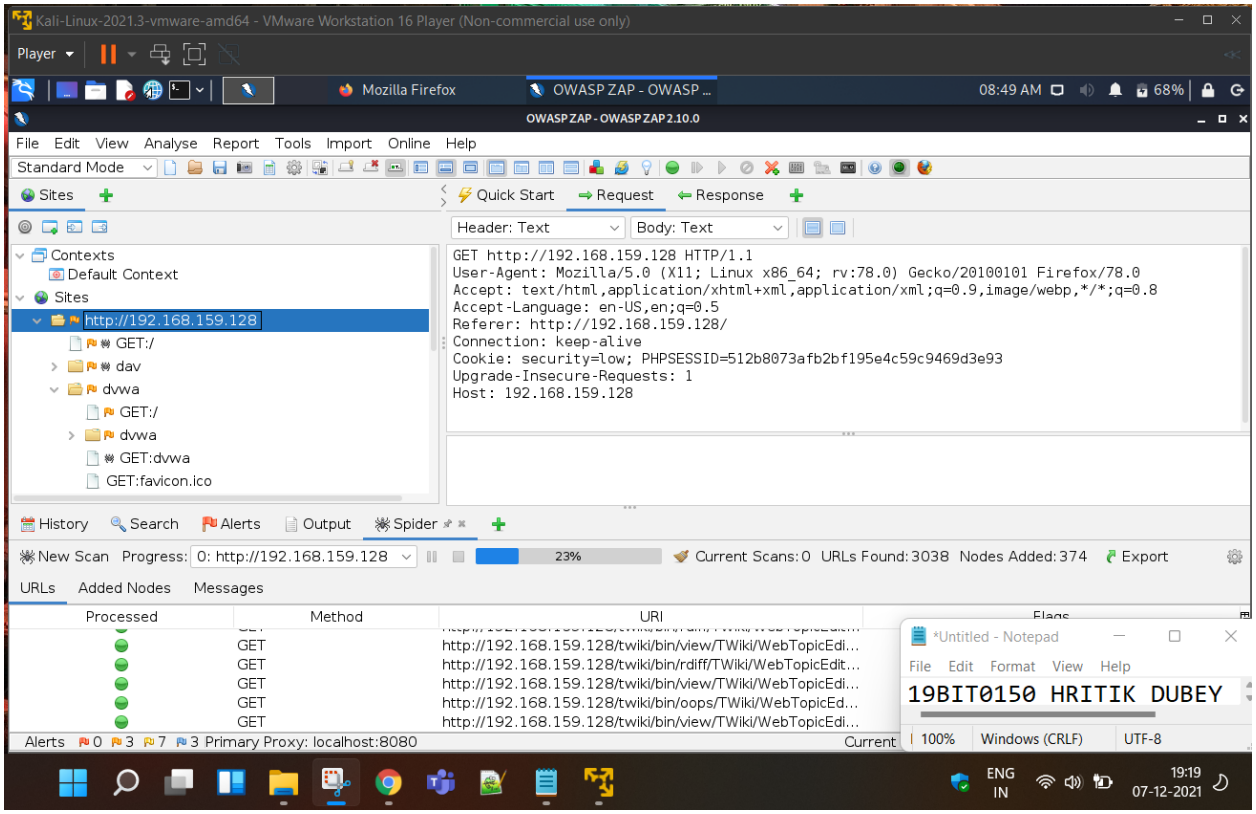

Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
qterminal
Capturing from eth0
08:10 AM
78%
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
14946 216.779705545 98.137.11.164 192.168.159.131 TCP 60 2099 → 41983 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
14947 217.171915036 98.137.11.164 192.168.159.131 TCP 60 3703 → 41983 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
14948 217.171915267 98.137.11.164 192.168.159.131 TCP 60 24800 → 41983 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
14949 217.171915403 98.137.11.164 192.168.159.131 TCP 60 2394 → 41983 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
14950 217.171915509 98.137.11.164 192.168.159.131 TCP 60 6112 → 41983 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
14951 217.171915616 98.137.11.164 192.168.159.131 TCP 60 1213 → 41983 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
14952 240.033081080 192.168.159.1 239.255.255.250 SSDP 215 M-SEARCH * HTTP/1.1
14953 241.044815528 192.168.159.1 239.255.255.250 SSDP 215 M-SEARCH * HTTP/1.1
Frame 14950: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
Ethernet II, Src: VMware_ff:86:4e (00:50:56:ff:86:4e), Dst: VMware_aa:e2:21 (00:0c:29:aa:e2:21)
Internet Protocol Version 4, Src: 98.137.11.164, Dst: 192.168.159.131
Transmission Control Protocol, Src Port: 6112, Dst Port: 41983, Seq: 1, Ack: 1, Len: 0
0000 00 0c 29 aa e2 21 00 50 56 ff 86 4e 08 00 45 00
0010 00 28 2f b6 00 00 80 06 3c c1 62 89 0b a4 c0 a8
0020 9f 83 17 e0 a3 ff 2a c3 72 46 3a df 24 b1 50 14
0030 fa f0 2e 0d 00 00 00 00 00 00 00 00
eth0: <live capture in progress>
Packets: 14956
*Untitled - Notepad
File Edit Format View Help
19BIT0150 HRITIK DUBEY
100%
Windows (CRLF)
UTF-8
ENG
IN
18:40
07-12-2021

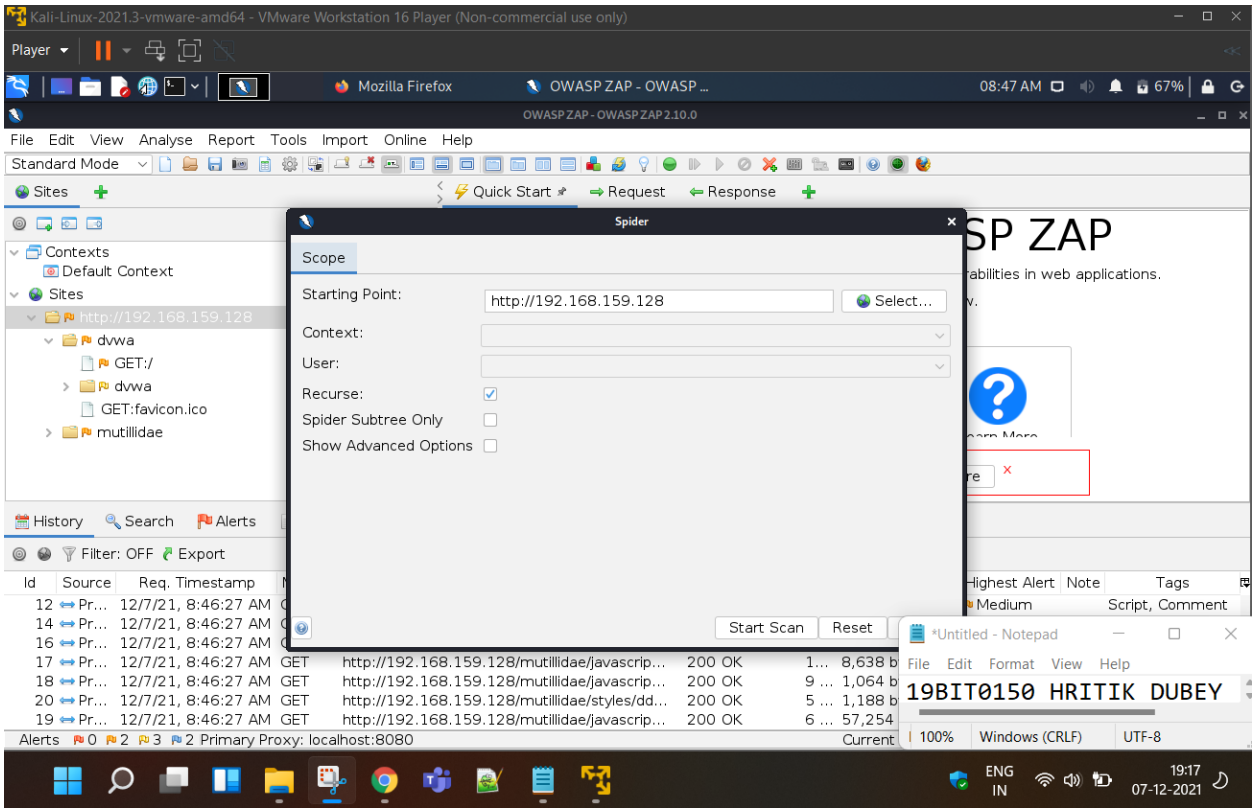

Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
qterminal
*eth0
08:11 AM
77%
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
14939 216.779704363 98.137.11.164 192.168.159.131 TCP 60 3703 → 41982 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
14940 216.779704551 98.137.11.164 192.168.159.131 TCP 60 211 → 41983 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
14941 216.779704704 98.137.11.164 192.168.159.131 TCP 60 6112 → 41982 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
14942 216.779704866 98.137.11.164 192.168.159.131 TCP 60 2401 → 41983 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
14943 216.779705037 98.137.11.164 192.168.159.131 TCP 60 2394 → 41982 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
14944 216.779705216 98.137.11.164 192.168.159.131 TCP 60 1213 → 41982 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
14945 216.779705392 98.137.11.164 192.168.159.131 TCP 60 24800 → 41982 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
14946 216.779705545 98.137.11.164 192.168.159.131 TCP 60 2099 → 41983 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
Frame 14946: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
Ethernet II, Src: VMware_ff:86:4e (00:50:56:ff:86:4e), Dst: VMware_aa:e2:21 (00:0c:29:aa:e2:21)
Internet Protocol Version 4, Src: 98.137.11.164, Dst: 192.168.159.131
Transmission Control Protocol, Src Port: 2099, Dst Port: 41983, Seq: 1, Ack: 1, Len: 0
0000 00 0c 29 aa e2 21 00 50 56 ff 86 4e 08 00 45 00
0010 00 28 2f b2 00 00 80 06 3c c5 62 89 0b a4 c0 a8
0020 9f 83 08 33 a3 ff 7f 09 7b 0a 3a df 24 b1 50 14
0030 fa f0 e0 af 00 00 00 00 00 00 00 00
Transmission Control Protocol: Protocol
Packets: 14956
*Untitled - Notepad
File Edit Format View Help
19BIT0150 HRITIK DUBEY
100%
Windows (CRLF)
UTF-8
ENG
IN
18:41
07-12-2021

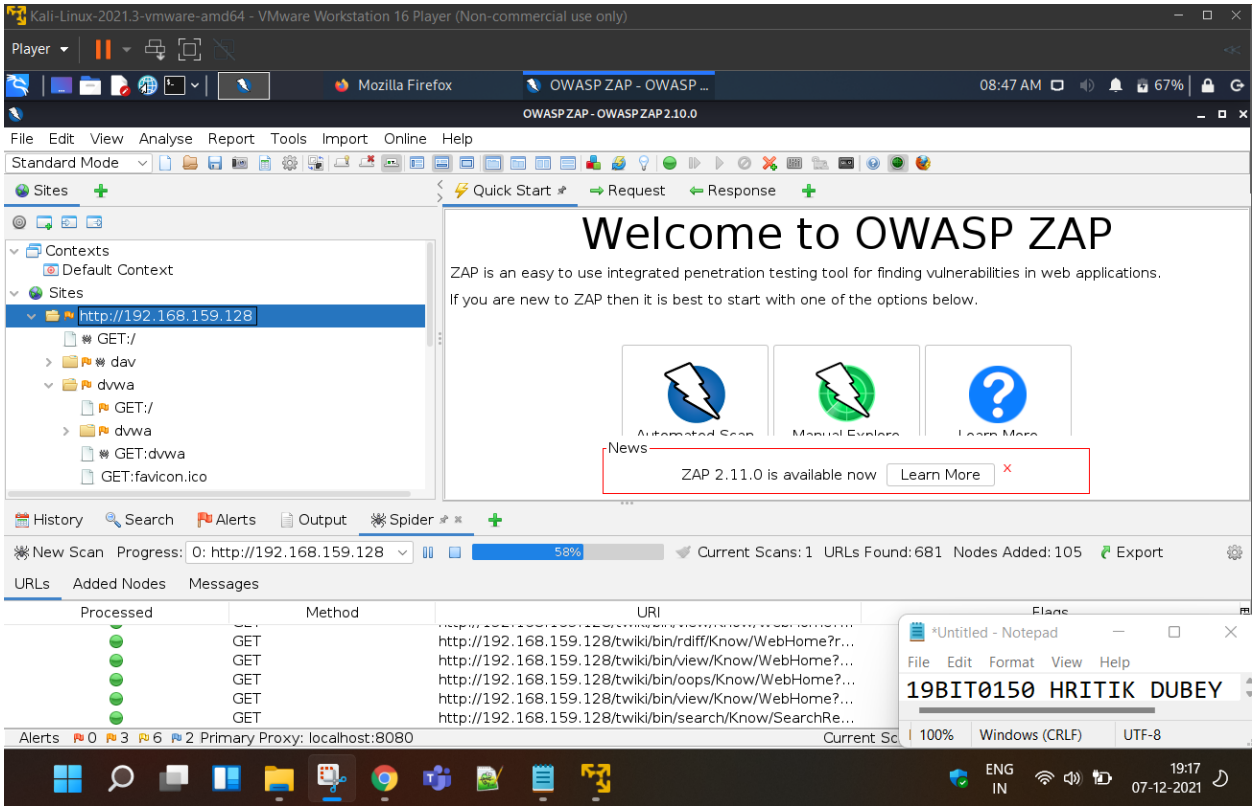
## Question 3: Nessus Scan / OWASP ZAP

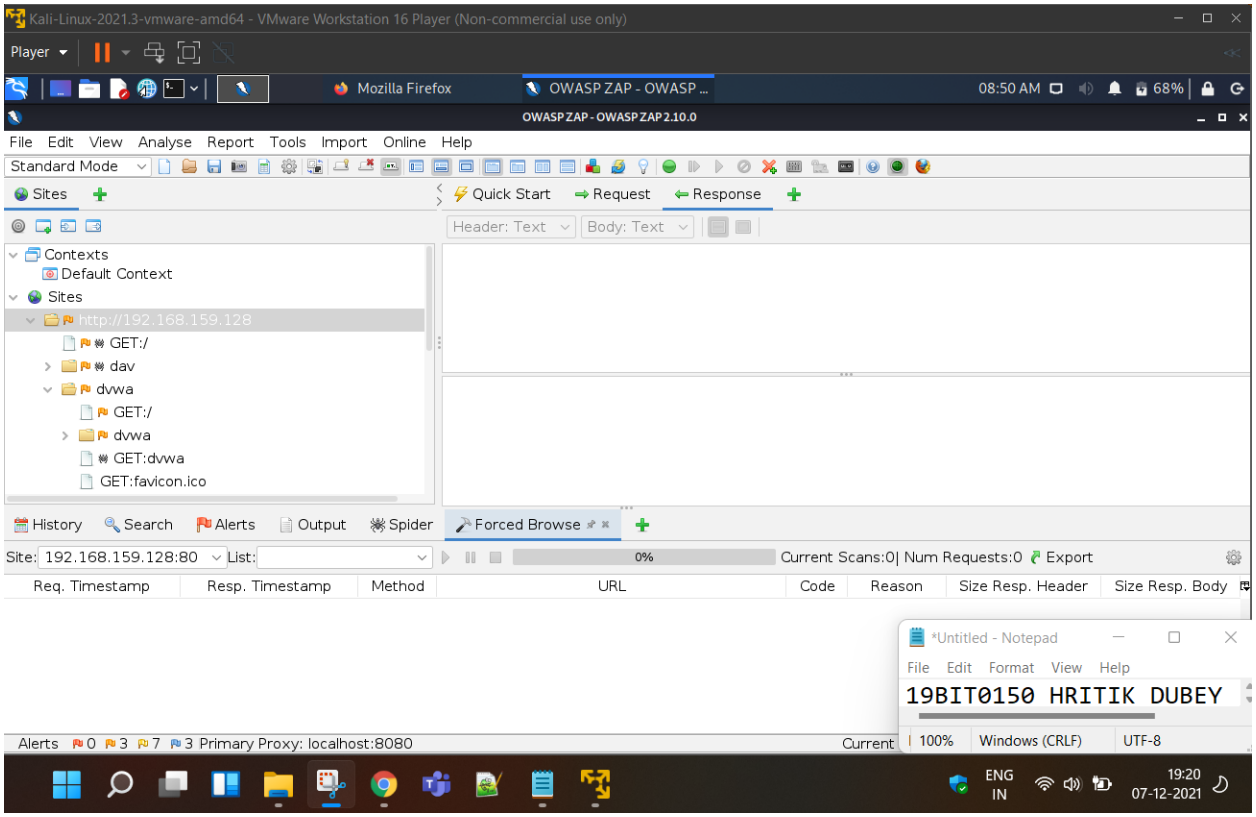


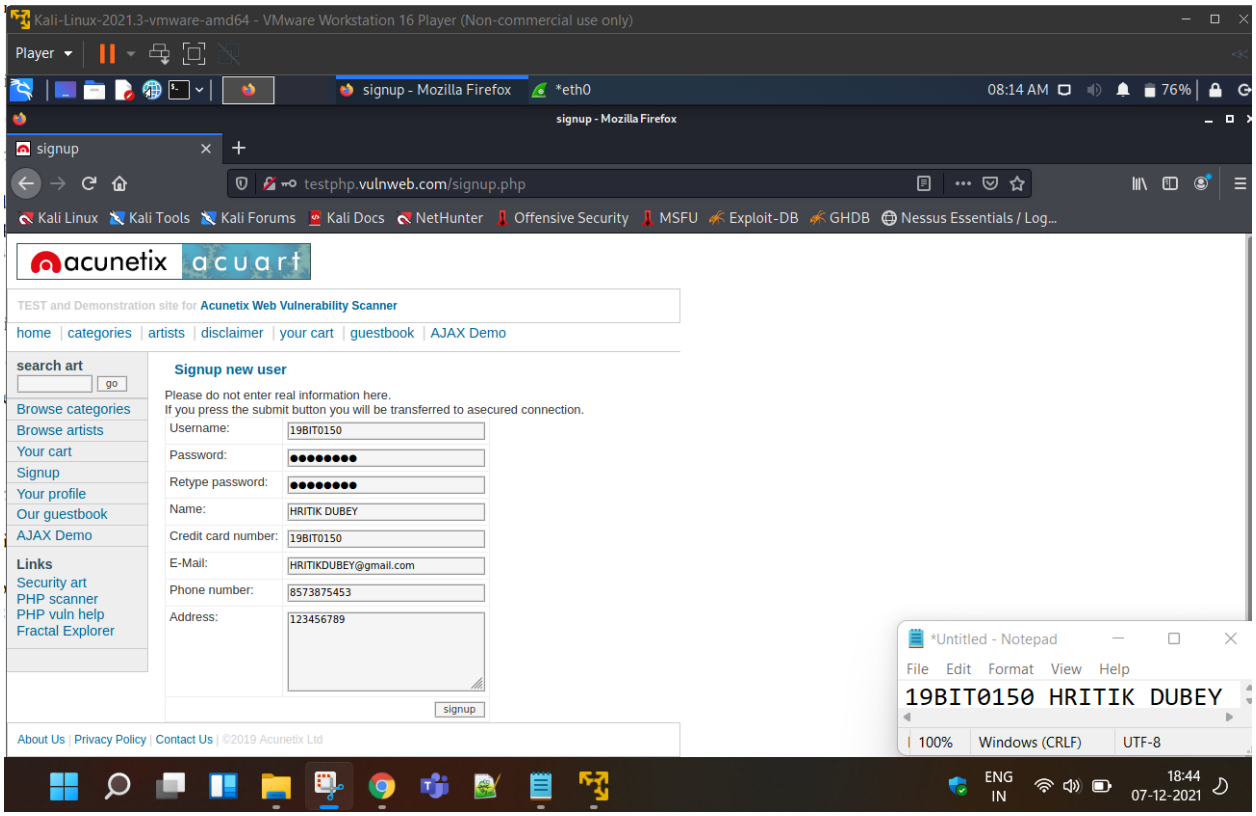

Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Mozilla Firefox
OWASP ZAP - OWASP ...
08:49 AM
68%
OWASP ZAP - OWASP ZAP 2.10.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Header: Text
Body: Text
Contexts
Default Context
Sites
http://192.168.159.128
GET:/
dav
dvwa
GET:/
dvwa
GET:dvwa
GET:favicon.ico
GET http://192.168.159.128 HTTP/1.1
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
Referer: http://192.168.159.128/
Connection: keep-alive
Cookie: security=low; PHPSESSID=512b8073afb2bf195e4c59c9469d3e93
Upgrade-Insecure-Requests: 1
Host: 192.168.159.128
History
Search
Alerts
Output
Spider
New Scan
Progress: 0: http://192.168.159.128
23%
Current Scans: 0
URLs Found: 3038
Nodes Added: 374
Export
URLs
Added Nodes
Messages
Processed
Method
URI
GET http://192.168.159.128/twiki/bin/view/TWiki/WebTopicEdi...
GET http://192.168.159.128/twiki/bin/rdiff/TWiki/WebTopicEdit...
GET http://192.168.159.128/twiki/bin/view/TWiki/WebTopicEdi...
GET http://192.168.159.128/twiki/bin/oops/TWiki/WebTopicEd...
GET http://192.168.159.128/twiki/bin/view/TWiki/WebTopicEdi...
Alerts 0 3 7 3 Primary Proxy: localhost:8080
*Untitled - Notepad
File Edit Format View Help
19BIT0150 HRITIK DUBEY
100%
Windows (CRLF)
UTF-8
ENG
IN
19:19
07-12-2021

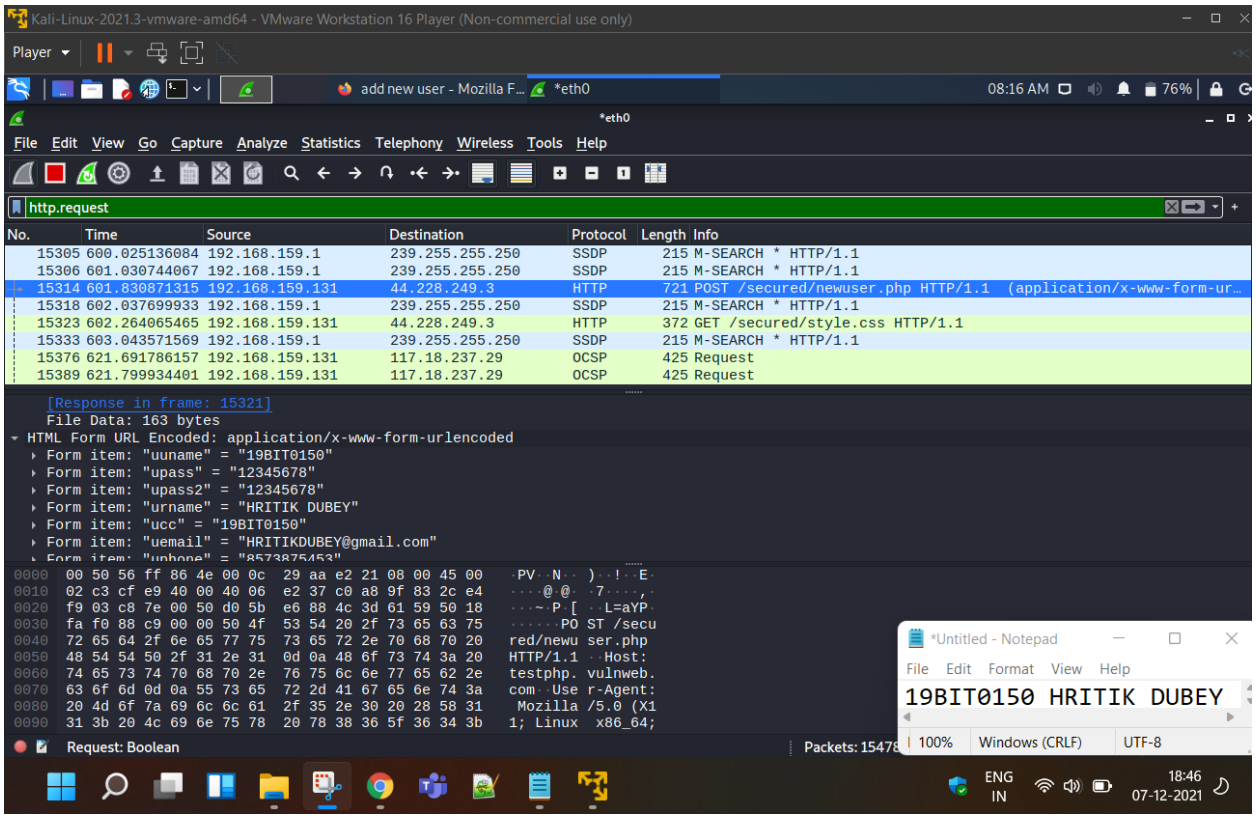

Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Mozilla Firefox
OWASP ZAP - OWASP ...
08:47 AM
67%
OWASP ZAP - OWASP ZAP 2.10.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Spider
Scope
Starting Point:
http://192.168.159.128
Select...
Context:
User:
Recurse:
Spider Subtree Only
Show Advanced Options
Start Scan
Reset
Contexts
Default Context
Sites
http://192.168.159.128
dvwa
GET:/
dvwa
GET:favicon.ico
mutillidae
SP ZAP
abilities in web applications.
History
Search
Alerts
Filter: OFF
Export
Id
Source
Req. Timestamp
Highest Alert
Note
Tags
Medium
Script, Comment
12 Pr... 12/7/21, 8:46:27 AM
14 Pr... 12/7/21, 8:46:27 AM
16 Pr... 12/7/21, 8:46:27 AM
17 Pr... 12/7/21, 8:46:27 AM GET http://192.168.159.128/mutillidae/javascrip... 200 OK
18 Pr... 12/7/21, 8:46:27 AM GET http://192.168.159.128/mutillidae/javascrip... 200 OK
20 Pr... 12/7/21, 8:46:27 AM GET http://192.168.159.128/mutillidae/styles/dd... 200 OK
19 Pr... 12/7/21, 8:46:27 AM GET http://192.168.159.128/mutillidae/javascrip... 200 OK
Alerts 0 2 3 2 Primary Proxy: localhost:8080
*Untitled - Notepad
File Edit Format View Help
19BIT0150 HRITIK DUBEY
100%
Windows (CRLF)
UTF-8
ENG
IN
19:17
07-12-2021

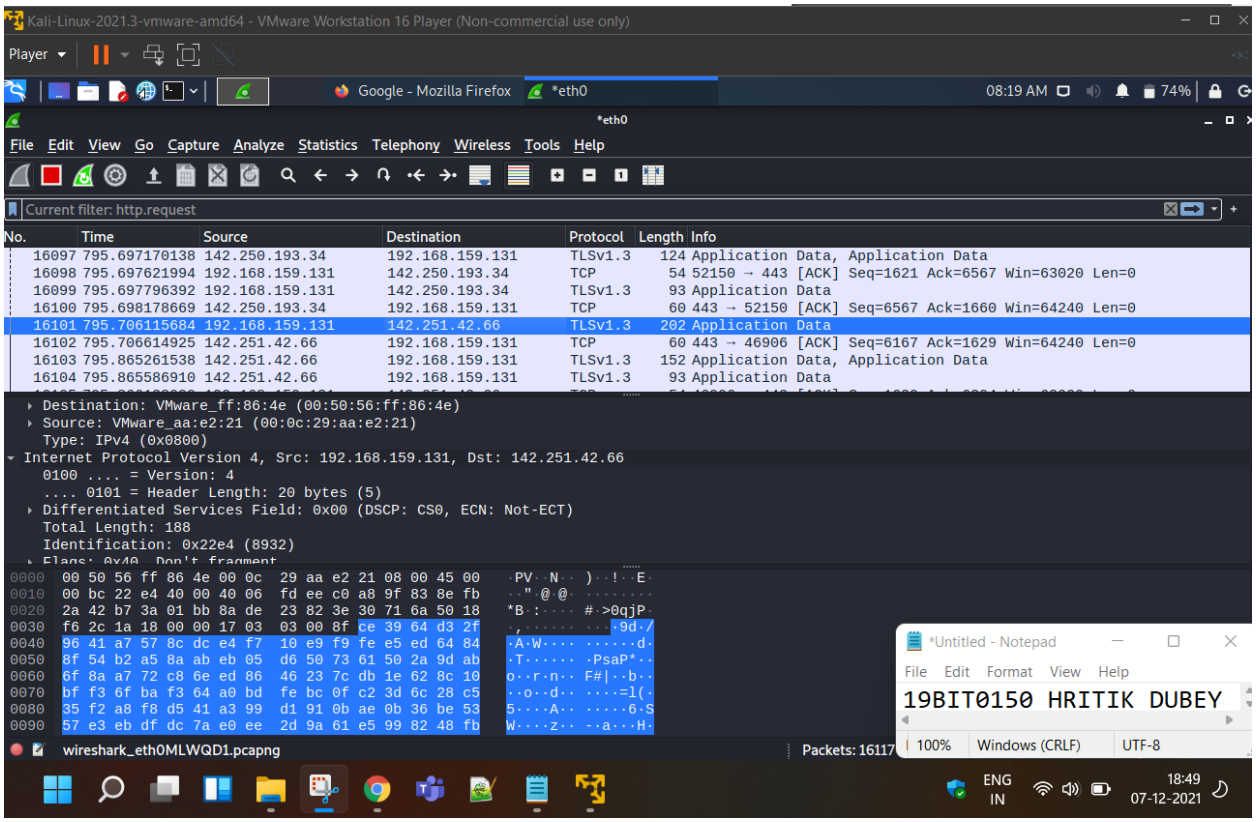

Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Mozilla Firefox
OWASP ZAP - OWASP ...
08:47 AM
67%
OWASP ZAP - OWASP ZAP 2.10.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Welcome to OWASP ZAP
ZAP 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.
Automated Scan
Manual Explore
Learn More
News
ZAP 2.11.0 is available now
Learn More
Contexts
Default Context
Sites
http://192.168.159.128
GET:/
dav
dvwa
GET:/
dvwa
GET:dvwa
GET:favicon.ico
History
Search
Alerts
Output
Spider
New Scan
Progress: 0: http://192.168.159.128
58%
Current Scans: 1
URLs Found: 681
Nodes Added: 105
Export
URLs
Added Nodes
Messages
Processed
Method
URI
GET http://192.168.159.128/twiki/bin/rdiff/Know/WebHome?r...
GET http://192.168.159.128/twiki/bin/view/Know/WebHome?...
GET http://192.168.159.128/twiki/bin/oops/Know/WebHome?...
GET http://192.168.159.128/twiki/bin/view/Know/WebHome?...
GET http://192.168.159.128/twiki/bin/search/Know/SearchRe...
Alerts 0 3 6 2 Primary Proxy: localhost:8080
*Untitled - Notepad
File Edit Format View Help
19BIT0150 HRITIK DUBEY
100%
Windows (CRLF)
UTF-8
ENG
IN
19:17
07-12-2021


Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Mozilla Firefox
OWASP ZAP - OWASP ...
08:50 AM
68%
OWASP ZAP - OWASP ZAP 2.10.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Header: Text
Body: Text
Contexts
Default Context
Sites
http://192.168.159.128
GET:/
dav
dvwa
GET:/
dvwa
GET:dvwa
GET:favicon.ico
History
Search
Alerts
Output
Spider
Forced Browse
Site: 192.168.159.128:80
List:
0%
Current Scans:0| Num Requests:0
Export
Req. Timestamp
Resp. Timestamp
Method
URL
Code
Reason
Size Resp. Header
Size Resp. Body
Alerts 0 3 7 3 Primary Proxy: localhost:8080
*Untitled - Notepad
File Edit Format View Help
19BIT0150 HRITIK DUBEY
100%
Windows (CRLF)
UTF-8
ENG
IN
19:20
07-12-2021

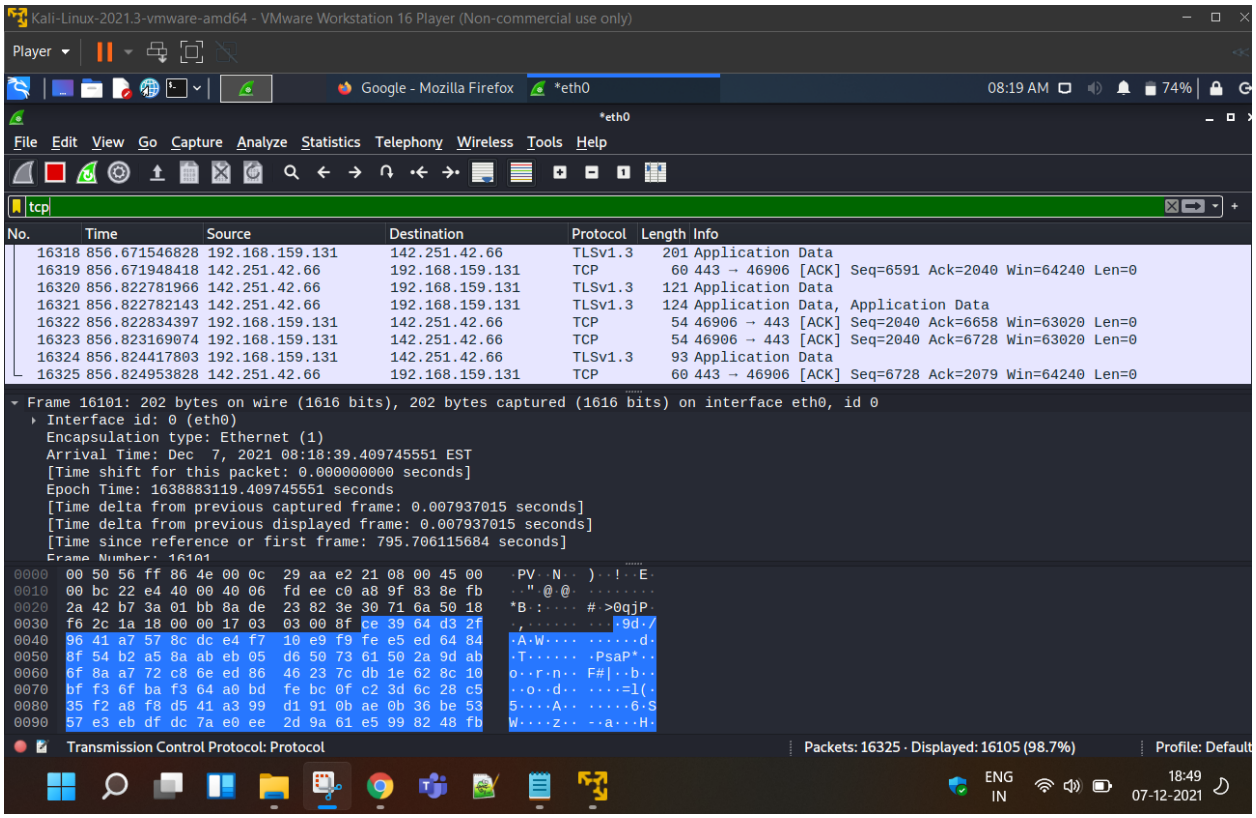
Question 4: Wireshark [6 Marks]



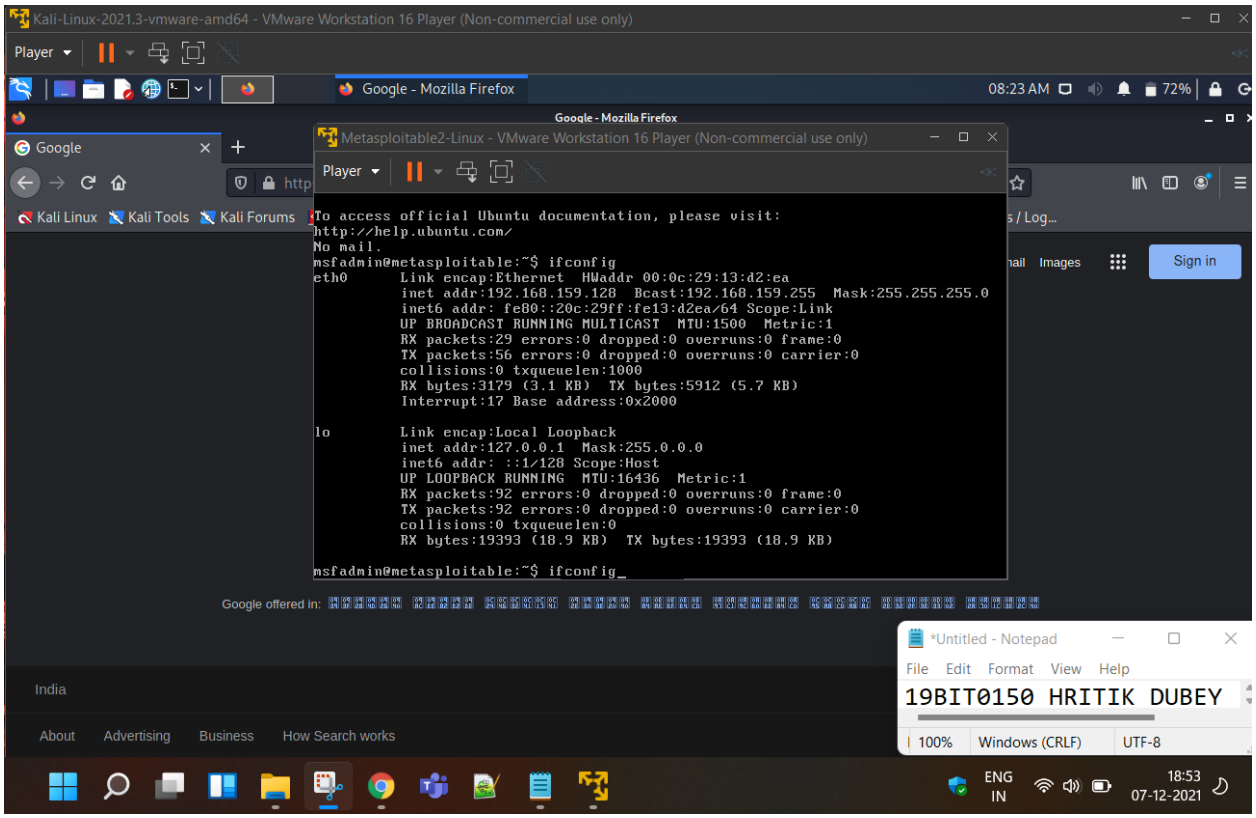



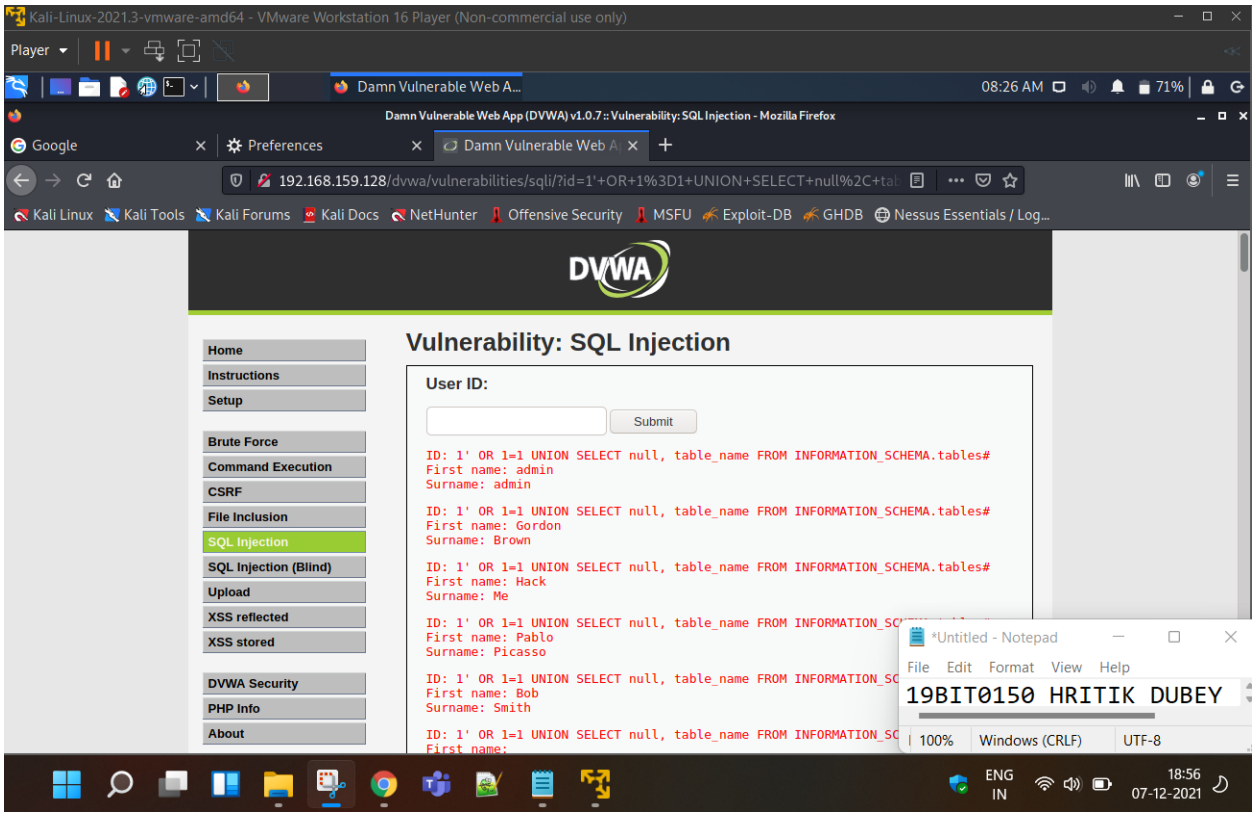



FOR GOOGLE.COM tcp packets were filtered.. 142.251.42.66



## Question 5: DVWA [12 Marks]

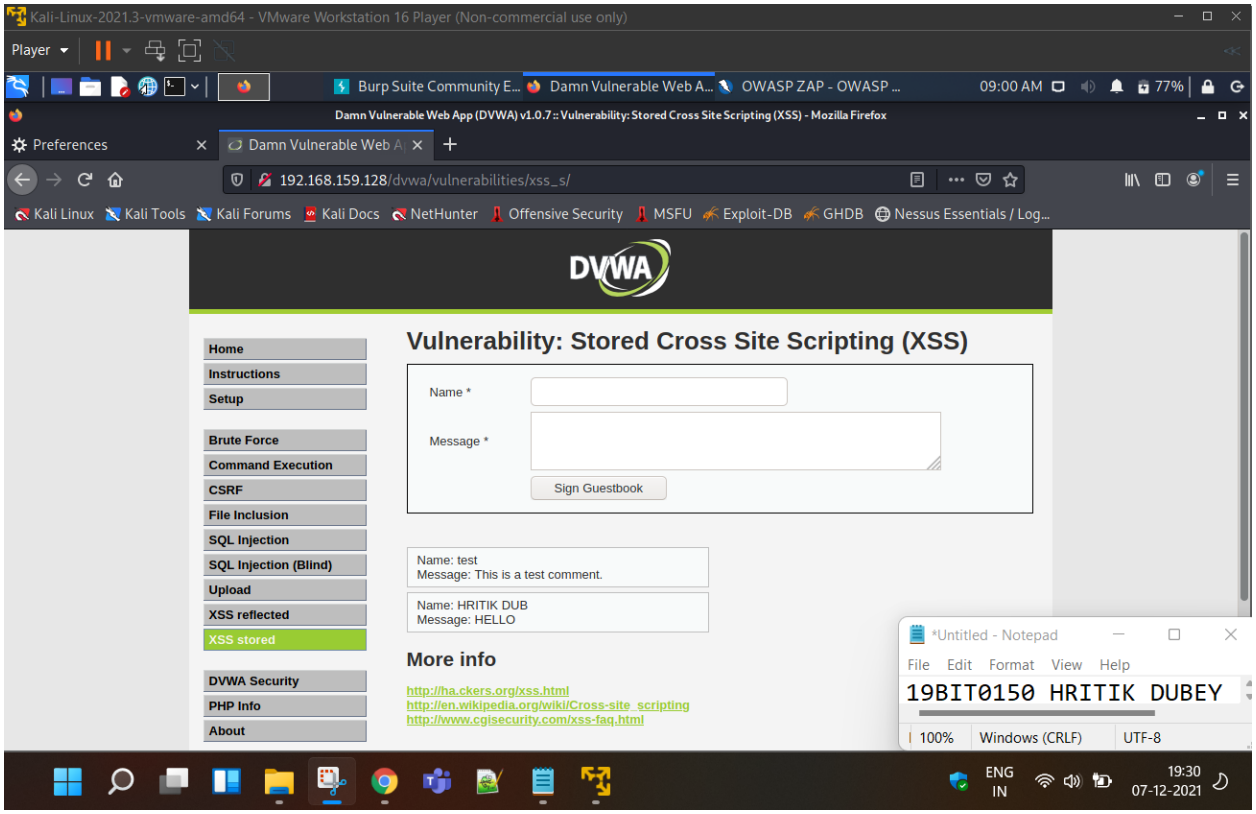


**CREATING PAYLOAD FOR XSS ON r**

```
<form action="http://192.168.159.128/dvwa/vulnerabilities/xss_s/?"
method="GET"><br><br><br>
                    <h2>CLICK HERE- {ISAA LAB HRITIK DUBEY 19BIT0150 }:<br
/></h2>
                    <input type="hidden" AUTOCOMPLETE="off" name="name" value
="HRITIK DUBEY"><br />
<input type="hidden" AUTOCOMPLETE="off" name="name" value ="hello 19BIT0150"><br
/>
                    <br />
                    <input type="submit" value="Change" name="Change">

                </form>
```



**CREATING PAYLOAD FOR XSS ON s**

<form action="http://192.168.159.128/dvwa/vulnerabilities/xss_s/?" method="GET"><br><br><br>

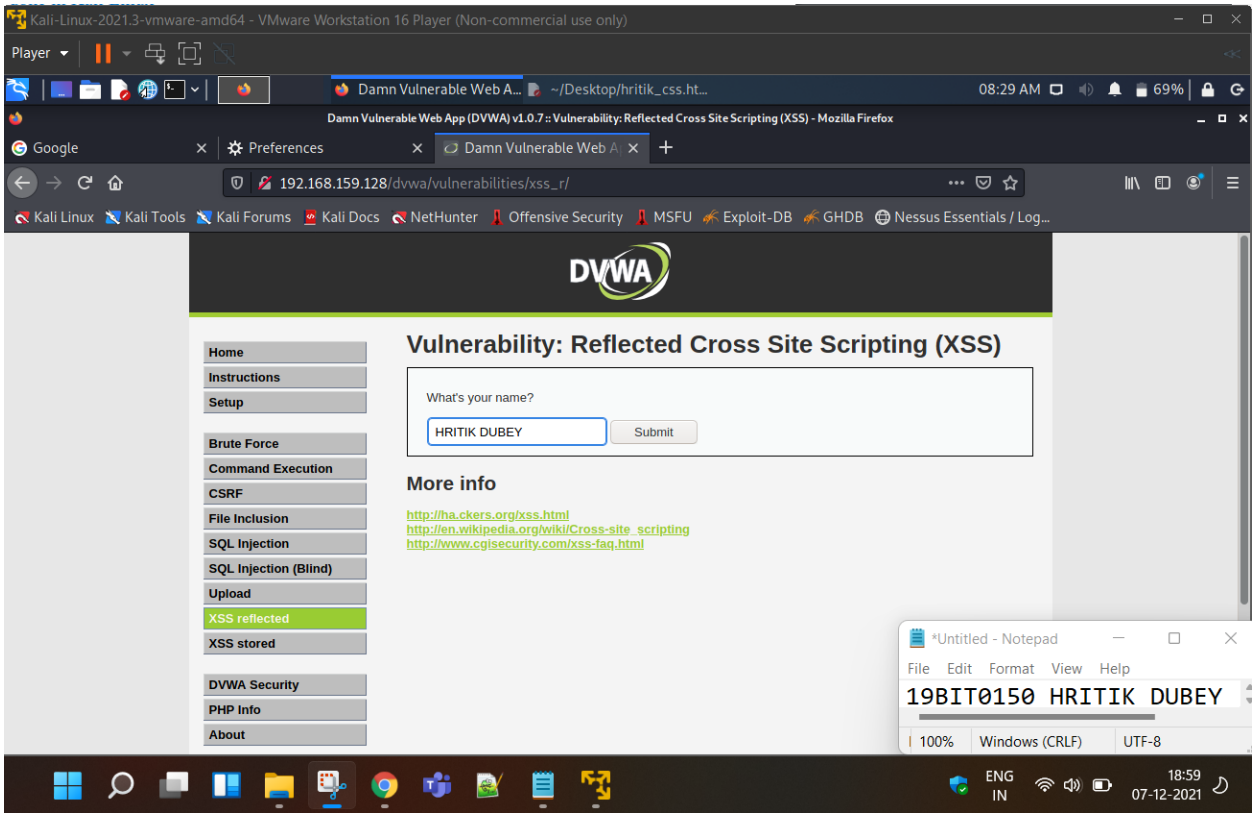
<h2>CLICK HERE- {ISAA LAB HRITIK DUBEY 19BIT0150 }:<br /></h2>

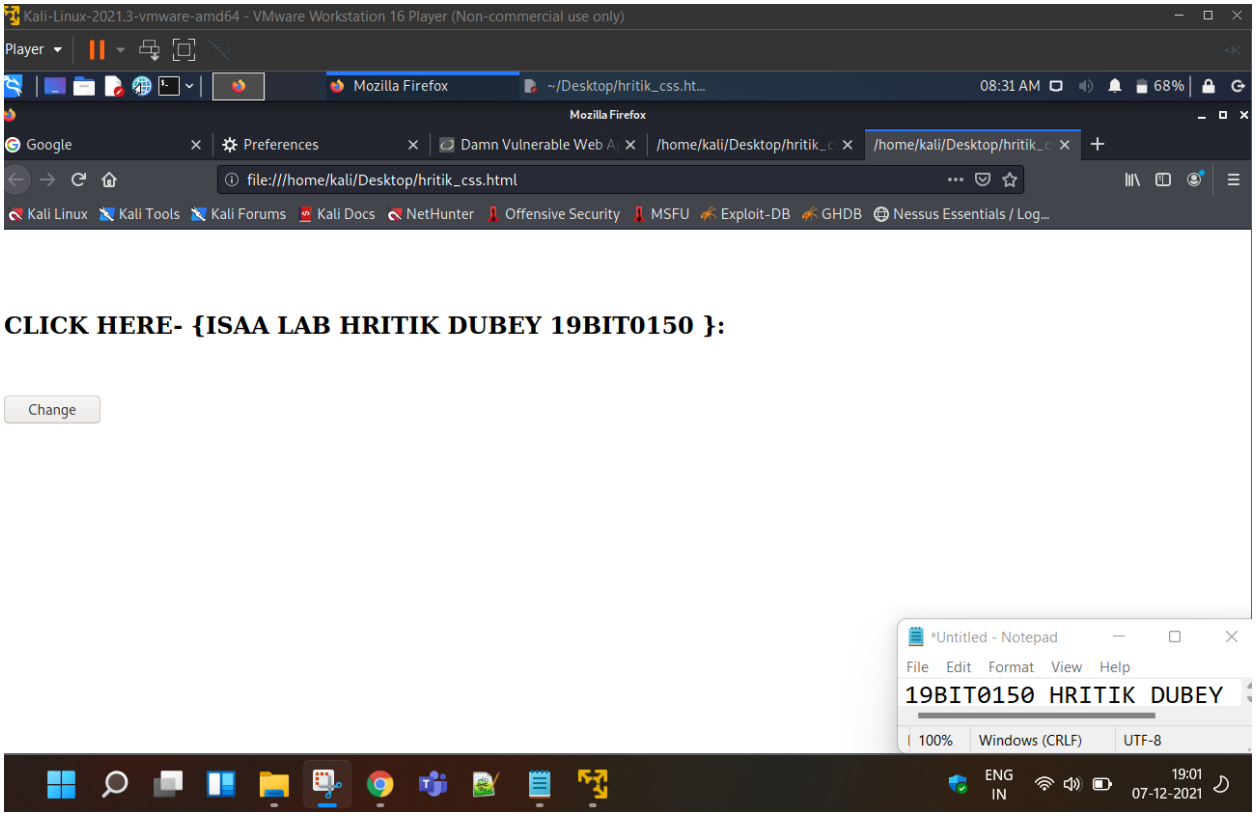
<input type="hidden" AUTOCOMPLETE="off" name="name" value ="HRITIK DUBEY"><br />

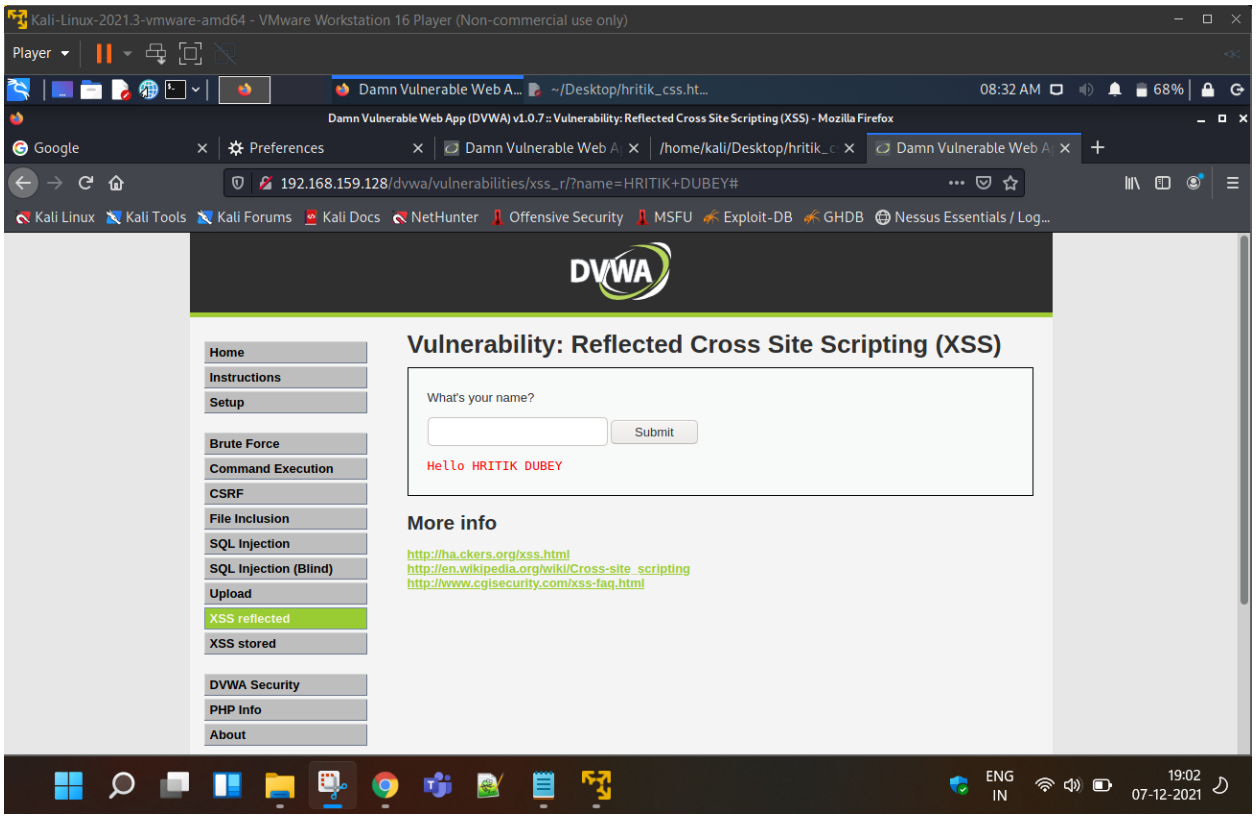
<br />

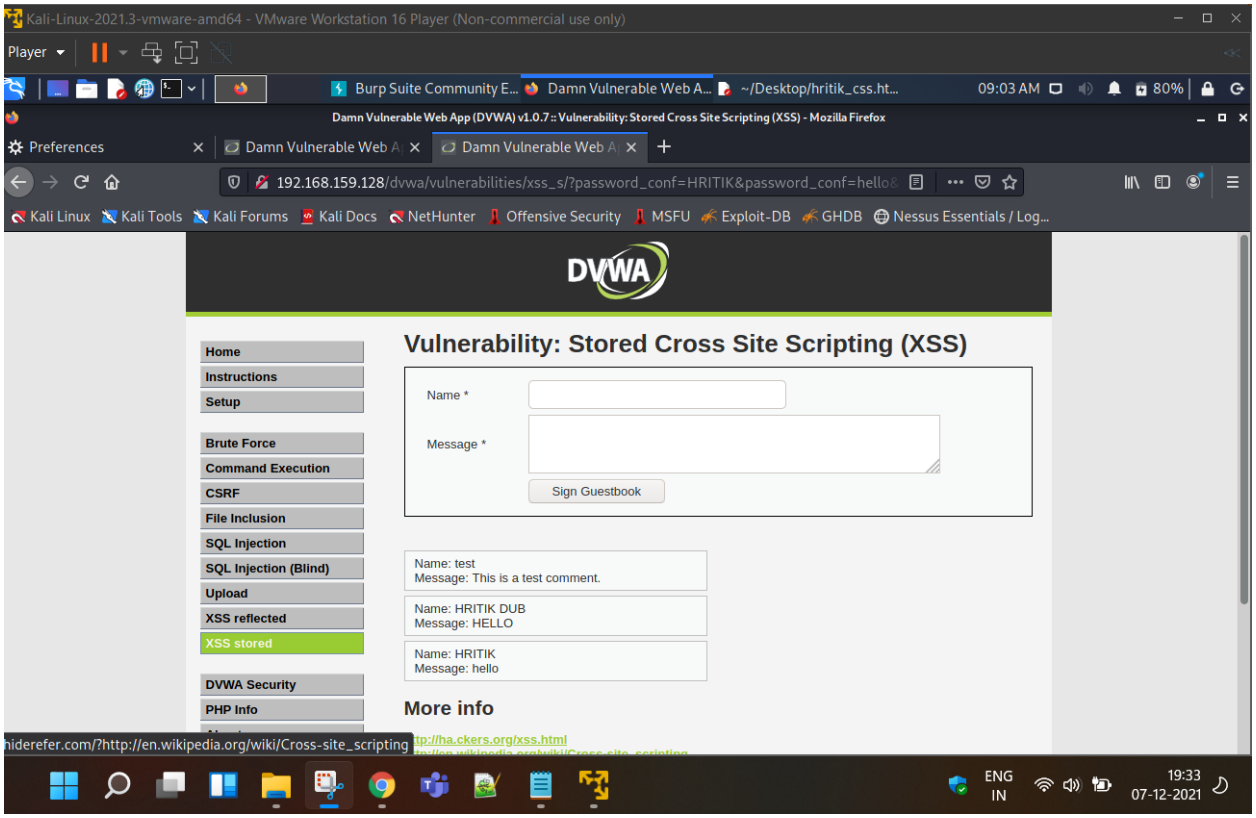
<input type="submit" value="Change" name="Change">

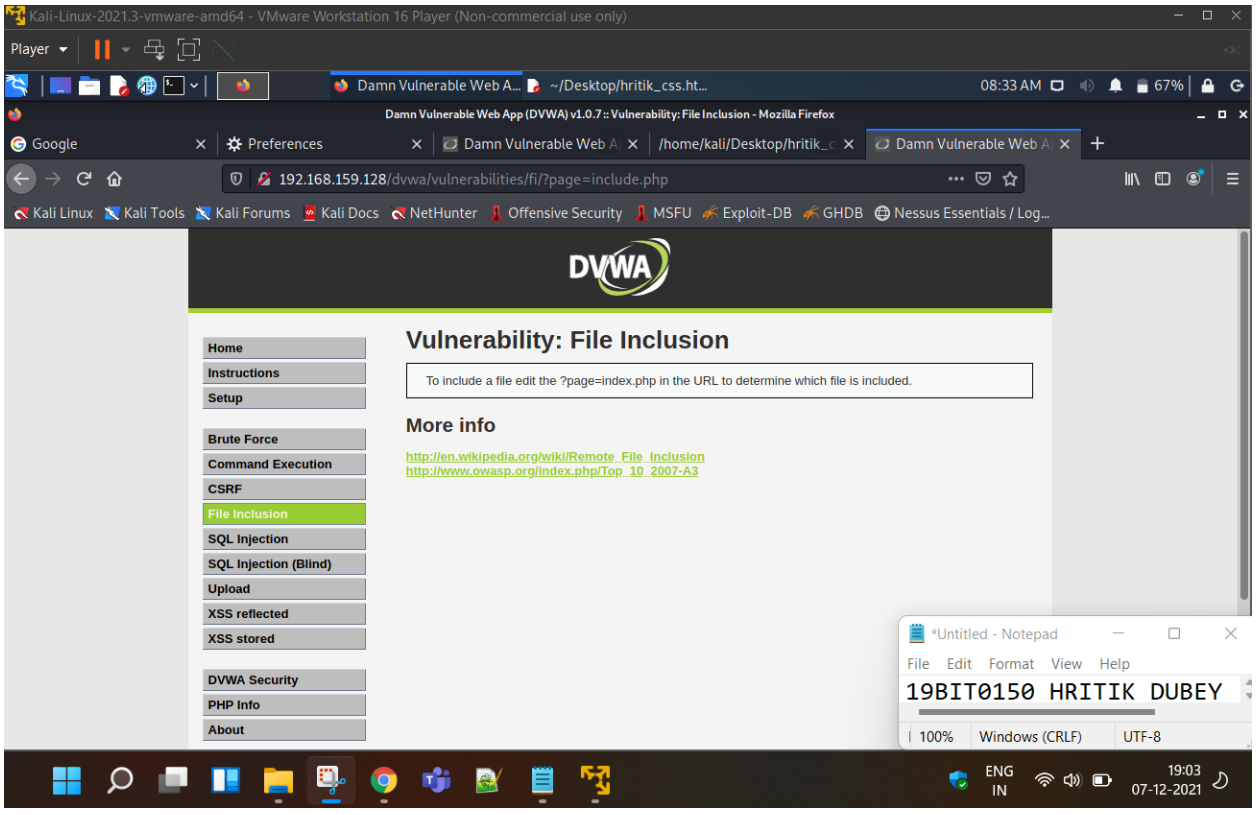
</form>



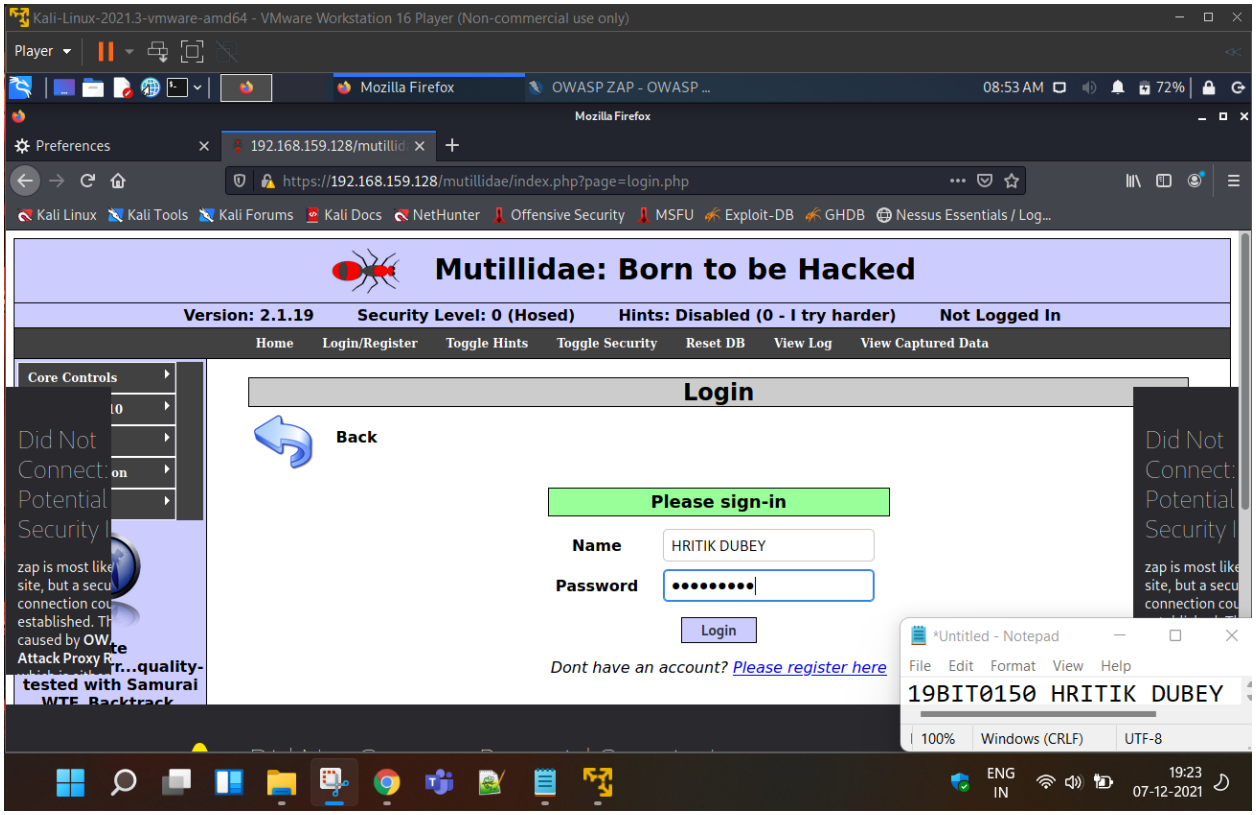

Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Mozilla Firefox
~/Desktop/hritik_css.ht...
08:31 AM
68%
Mozilla Firefox
Google
Preferences
Damn Vulnerable Web A
/home/kali/Desktop/hritik_c
/home/kali/Desktop/hritik_c
file:///home/kali/Desktop/hritik_css.html
Kali Linux
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
Nessus Essentials / Log...
CLICK HERE- {ISAA LAB HRITIK DUBEY 19BIT0150 }:
Change
*Untitled - Notepad
File Edit Format View Help
19BIT0150 HRITIK DUBEY
100%
Windows (CRLF)
UTF-8
ENG
IN
19:01
07-12-2021

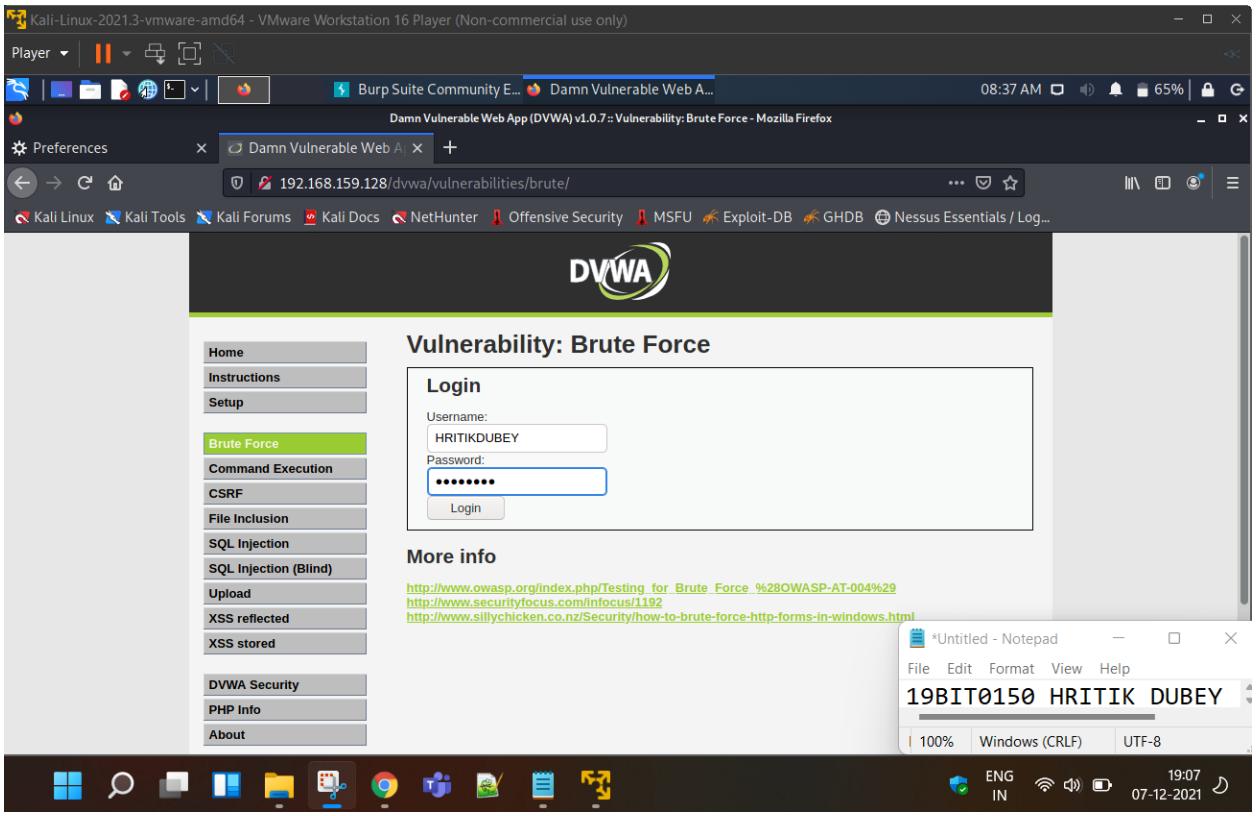

Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Damn Vulnerable Web A...
~/Desktop/hritik_css.ht...
08:32 AM
68%
Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Reflected Cross Site Scripting (XSS) - Mozilla Firefox
Google
Preferences
Damn Vulnerable Web A
/home/kali/Desktop/hritik_c
Damn Vulnerable Web A
192.168.159.128/dvwa/vulnerabilities/xss_r/?name=HRITIK+DUBEY#
Kali Linux
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
Nessus Essentials / Log...
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
Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
Submit
Hello HRITIK DUBEY
More info
http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html
ENG
IN
19:02
07-12-2021

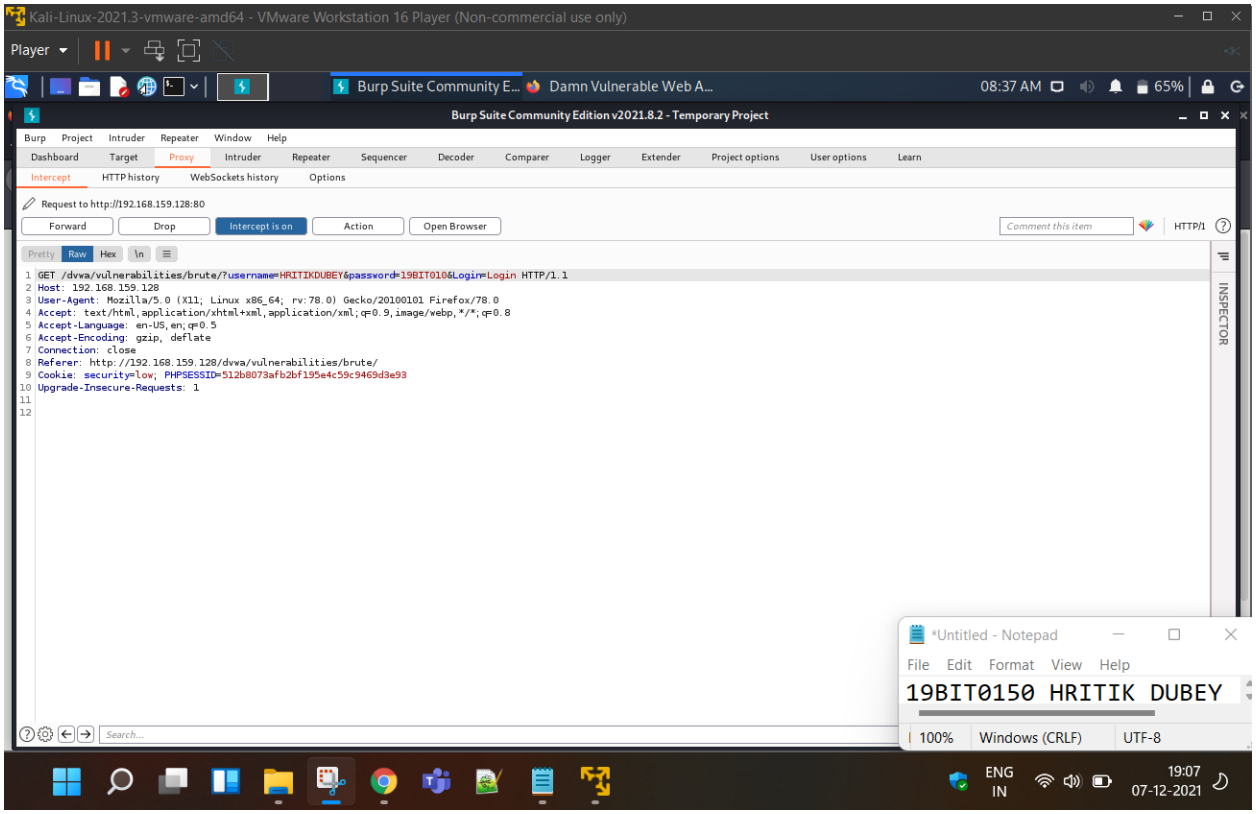

Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Stored Cross Site Scripting (XSS) - Mozilla Firefox
192.168.159.128/dvwa/vulnerabilities/xss_s/?password_conf=HRITIK&password_conf=hello
DVWA
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
Message *
Sign Guestbook
Name: test
Message: This is a test comment.
Name: HRITIK DUB
Message: HELLO
Name: HRITIK
Message: hello
More info
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
hiderefer.com/?http://en.wikipedia.org/wiki/Cross-site_scripting


Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: File Inclusion - Mozilla Firefox
192.168.159.128/dvwa/vulnerabilities/fi/?page=include.php
DVWA
Vulnerability: File Inclusion
To include a file edit the ?page=index.php in the URL to determine which file is included.
More info
http://en.wikipedia.org/wiki/Remote_File_Inclusion
http://www.owasp.org/index.php/Top_10_2007-A3
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
*Untitled - Notepad
File Edit Format View Help
19BIT0150 HRITIK DUBEY
100% Windows (CRLF) UTF-8

## Question 6: Burpsite [6 Marks] Perform the brute force attack through Burpsite.

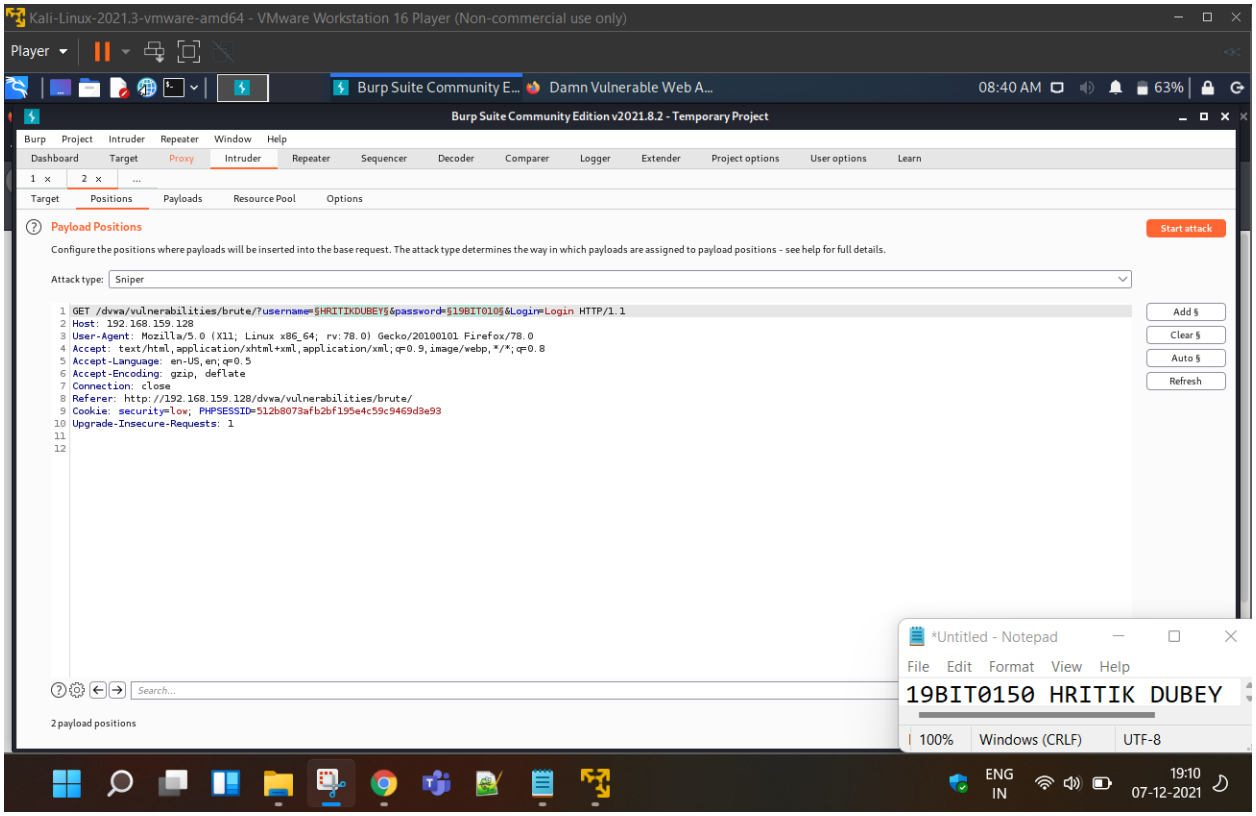


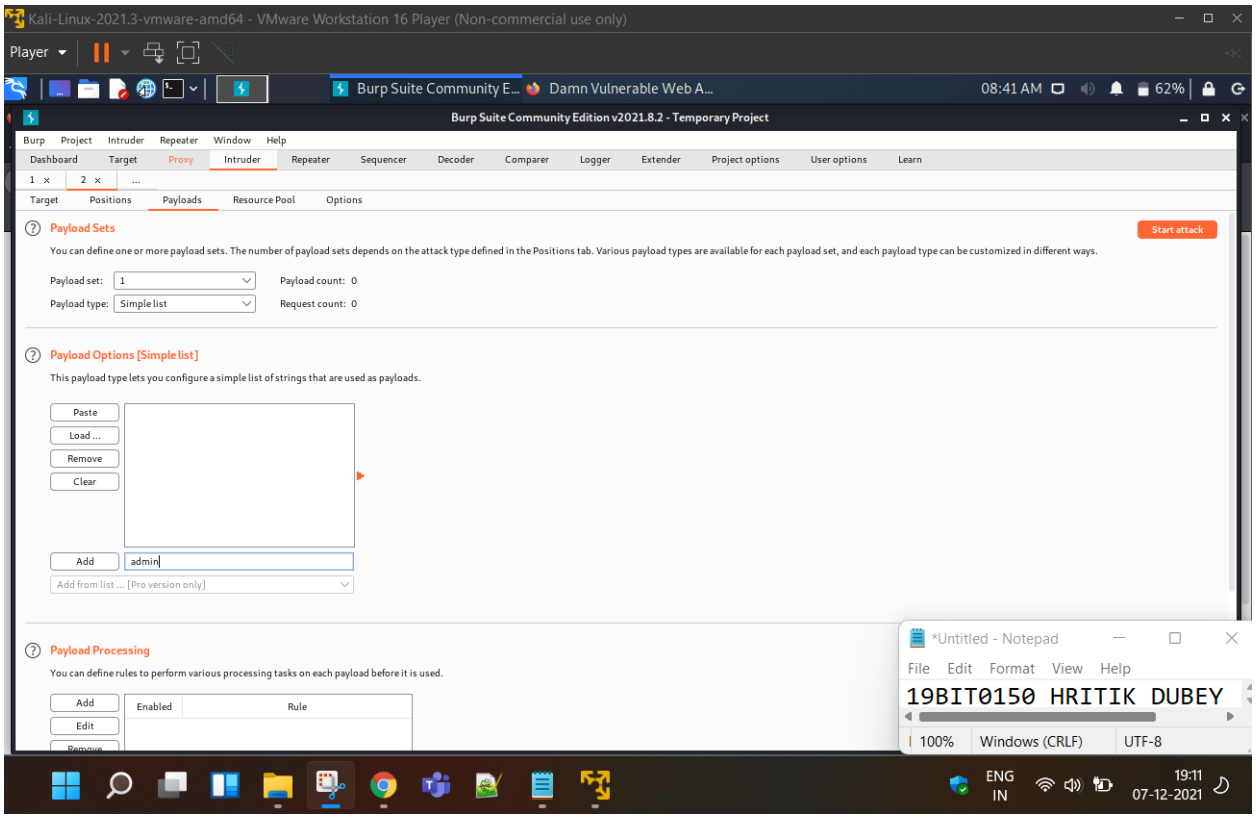



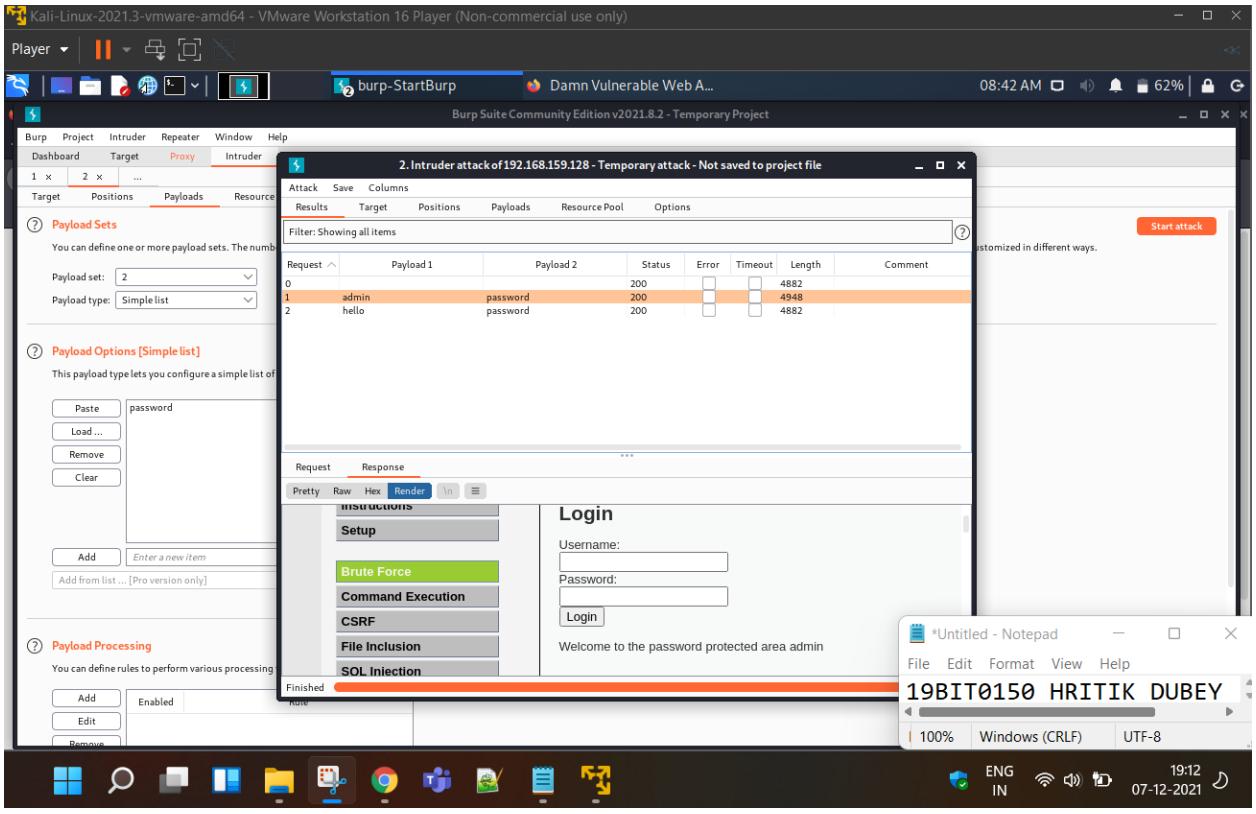



Pretty Raw Hex \n

```
1 GET /dvwa/vulnerabilities/brute/?username=HRITIKDUBEY&password=19BIT010&Login=Login HTTP/1.1
2 Host: 192.168.159.128
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://192.168.159.128/dvwa/vulnerabilities/brute/
9 Cookie: security=low; PHPSESSID=512b8073afb2bf195e4c59c9469d3e93
10 Upgrade-Insecure-Requests: 1
11
12
```


Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Burp Suite Community E...
Damn Vulnerable Web A...
08:40 AM
63%
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=§HRITIKDUBEY§&password=§19BIT010§&Login=Login HTTP/1.1
Host: 192.168.159.128
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
Referer: http://192.168.159.128/dvwa/vulnerabilities/brute/
Cookie: security=low; PHPSESSID=512b8073afb2bf195e4c59c9469d3e93
Upgrade-Insecure-Requests: 1
Add §
Clear §
Auto §
Refresh
Search...
2 payload positions
*Untitled - Notepad
File Edit Format View Help
19BIT0150 HRITIK DUBEY
100% Windows (CRLF) UTF-8
ENG IN
19:10
07-12-2021


Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Burp Suite Community E...
Damn Vulnerable Web A...
08:41 AM
62%
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: 0
Payload type: Simple list
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
Add
admin
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
Enabled
Rule
*Untitled - Notepad
File Edit Format View Help
19BIT0150 HRITIK DUBEY
100% Windows (CRLF) UTF-8
ENG IN
19:11
07-12-2021


Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
burp-StartBurp
Damn Vulnerable Web A...
08:42 AM
62%
Burp Suite Community Edition v2021.8.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder
Target Positions Payloads Resource
Payload Sets
You can define one or more payload sets. The numb
Payload set: 2
Payload type: Simple list
Payload Options [Simple list]
This payload type lets you configure a simple list of
Paste
Load ...
Remove
Clear
password
Add
Enter a new item
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing
Add
Edit
Enabled
2. Intruder attack of 192.168.159.128 - Temporary attack - Not saved to project file
Attack Save Columns
Results Target Positions Payloads Resource Pool Options
Filter: Showing all items
Request Payload 1 Payload 2 Status Error Timeout Length Comment
0 200 4882
1 admin password 200 4948
2 hello password 200 4882
Request Response
Pretty Raw Hex Render
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
Login
Username:
Password:
Login
Welcome to the password protected area admin
Finished
Start attack
*Untitled - Notepad
File Edit Format View Help
19BIT0150 HRITIK DUBEY
100% Windows (CRLF) UTF-8
ENG
IN
19:12
07-12-2021