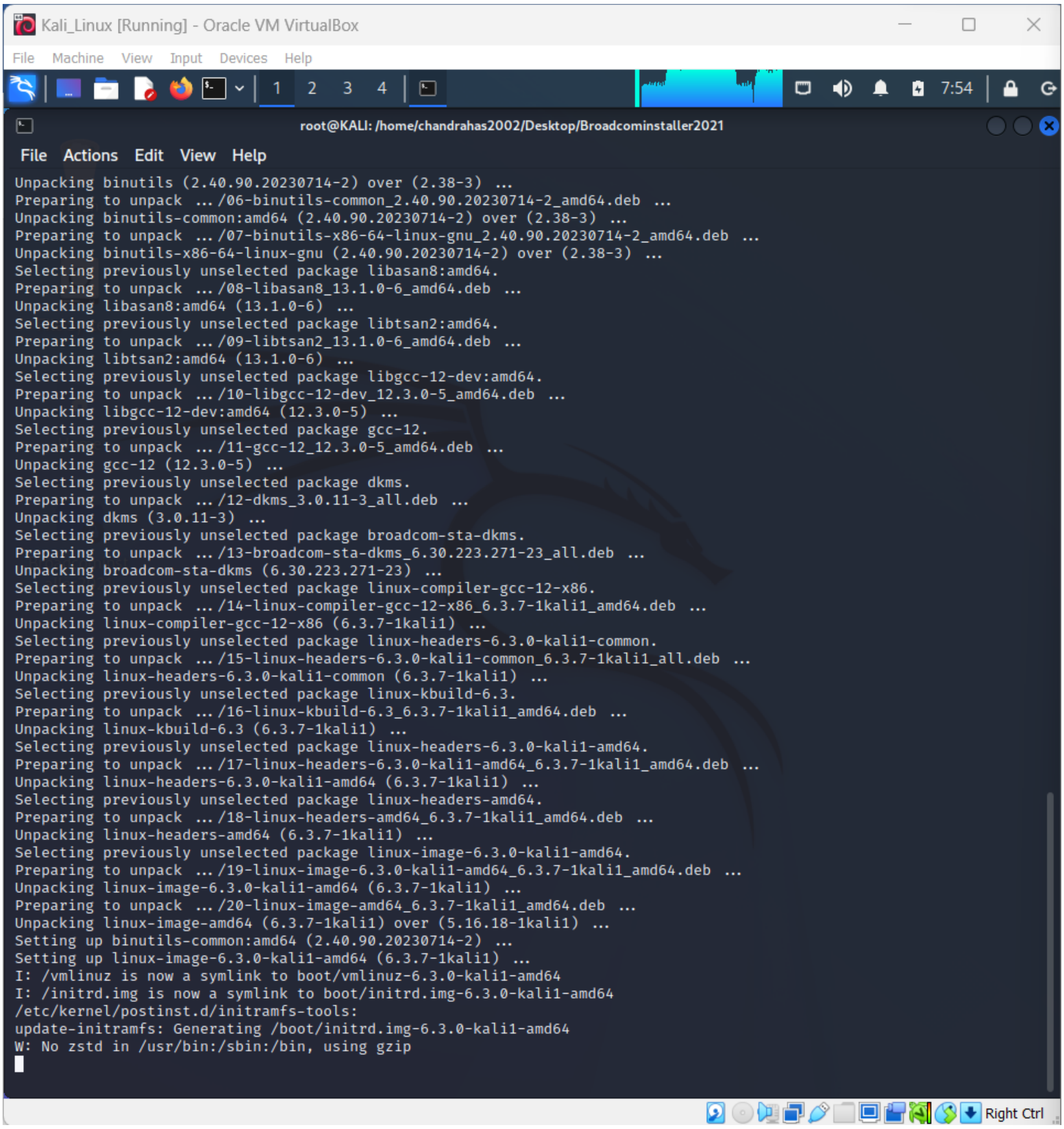
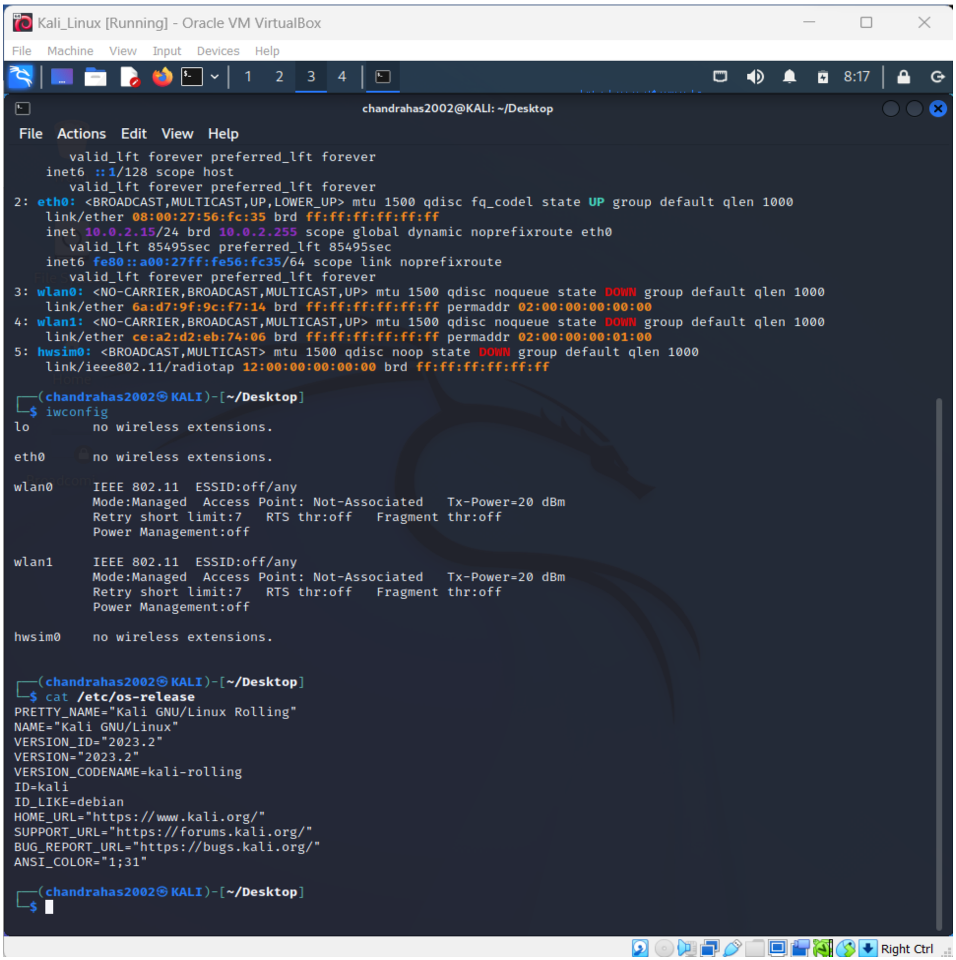
CS-MAJOR-JUNE- CS-06-MLB3

1) WIFI - WPA/2 : Handshake Capturing & Cracking Key


Kali_Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
7:54
root@KALI: /home/chandrahas2002/Desktop/Broadcominstaller2021
File Actions Edit View Help
Right Ctrl

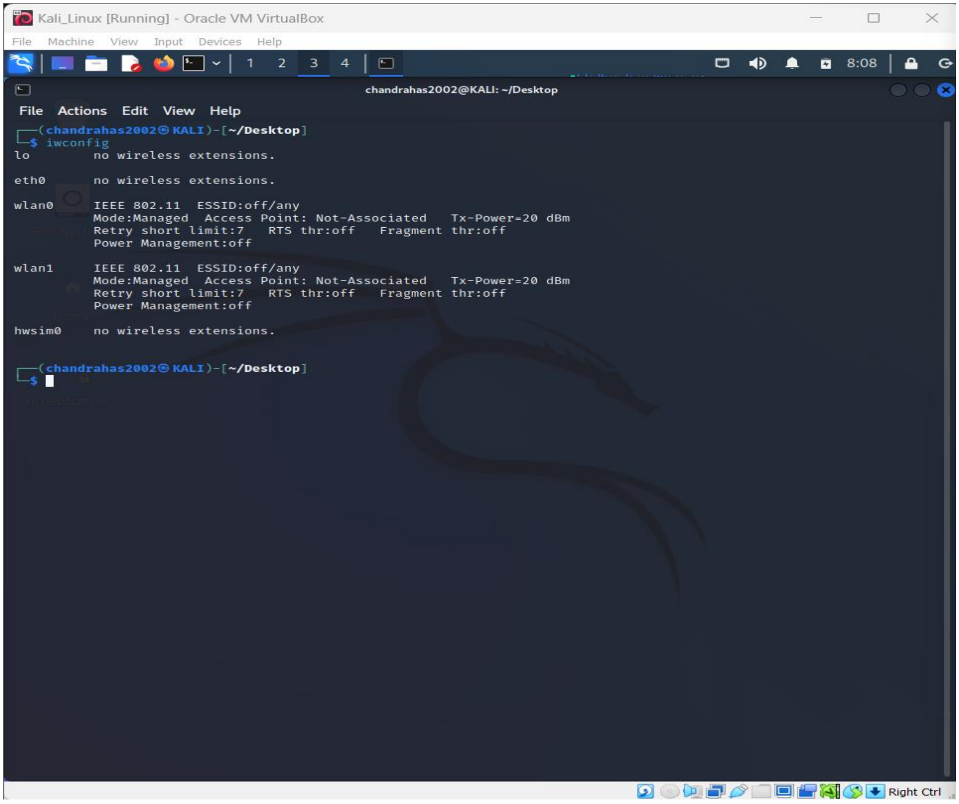
```
Unpacking binutils (2.40.90.20230714-2) over (2.38-3) ...
Preparing to unpack .../06-binutils-common_2.40.90.20230714-2_amd64.deb ...
Unpacking binutils-common:amd64 (2.40.90.20230714-2) over (2.38-3) ...
Preparing to unpack .../07-binutils-x86-64-linux-gnu_2.40.90.20230714-2_amd64.deb ...
Unpacking binutils-x86-64-linux-gnu (2.40.90.20230714-2) over (2.38-3) ...
Selecting previously unselected package libasan8:amd64.
Preparing to unpack .../08-libasan8_13.1.0-6_amd64.deb ...
Unpacking libasan8:amd64 (13.1.0-6) ...
Selecting previously unselected package libtsan2:amd64.
Preparing to unpack .../09-libtsan2_13.1.0-6_amd64.deb ...
Unpacking libtsan2:amd64 (13.1.0-6) ...
Selecting previously unselected package libgcc-12-dev:amd64.
Preparing to unpack .../10-libgcc-12-dev_12.3.0-5_amd64.deb ...
Unpacking libgcc-12-dev:amd64 (12.3.0-5) ...
Selecting previously unselected package gcc-12.
Preparing to unpack .../11-gcc-12_12.3.0-5_amd64.deb ...
Unpacking gcc-12 (12.3.0-5) ...
Selecting previously unselected package dkms.
Preparing to unpack .../12-dkms_3.0.11-3_all.deb ...
Unpacking dkms (3.0.11-3) ...
Selecting previously unselected package broadcom-sta-dkms.
Preparing to unpack .../13-broadcom-sta-dkms_6.30.223.271-23_all.deb ...
Unpacking broadcom-sta-dkms (6.30.223.271-23) ...
Selecting previously unselected package linux-compiler-gcc-12-x86.
Preparing to unpack .../14-linux-compiler-gcc-12-x86_6.3.7-1kali1_amd64.deb ...
Unpacking linux-compiler-gcc-12-x86 (6.3.7-1kali1) ...
Selecting previously unselected package linux-headers-6.3.0-kali1-common.
Preparing to unpack .../15-linux-headers-6.3.0-kali1-common_6.3.7-1kali1_all.deb ...
Unpacking linux-headers-6.3.0-kali1-common (6.3.7-1kali1) ...
Selecting previously unselected package linux-kbuild-6.3.
Preparing to unpack .../16-linux-kbuild-6.3_6.3.7-1kali1_amd64.deb ...
Unpacking linux-kbuild-6.3 (6.3.7-1kali1) ...
Selecting previously unselected package linux-headers-6.3.0-kali1-amd64.
Preparing to unpack .../17-linux-headers-6.3.0-kali1-amd64_6.3.7-1kali1_amd64.deb ...
Unpacking linux-headers-6.3.0-kali1-amd64 (6.3.7-1kali1) ...
Selecting previously unselected package linux-headers-amd64.
Preparing to unpack .../18-linux-headers-amd64_6.3.7-1kali1_amd64.deb ...
Unpacking linux-headers-amd64 (6.3.7-1kali1) ...
Selecting previously unselected package linux-image-6.3.0-kali1-amd64.
Preparing to unpack .../19-linux-image-6.3.0-kali1-amd64_6.3.7-1kali1_amd64.deb ...
Unpacking linux-image-6.3.0-kali1-amd64 (6.3.7-1kali1) ...
Preparing to unpack .../20-linux-image-amd64_6.3.7-1kali1_amd64.deb ...
Unpacking linux-image-amd64 (6.3.7-1kali1) over (5.16.18-1kali1) ...
Setting up binutils-common:amd64 (2.40.90.20230714-2) ...
Setting up linux-image-6.3.0-kali1-amd64 (6.3.7-1kali1) ...
I: /vmlinuz is now a symlink to boot/vmlinuz-6.3.0-kali1-amd64
I: /initrd.img is now a symlink to boot/initrd.img-6.3.0-kali1-amd64
/etc/kernel/postinst.d/initramfs-tools:
update-initramfs: Generating /boot/initrd.img-6.3.0-kali1-amd64
W: No zstd in /usr/bin:/sbin:/bin, using gzip
█
```

Checking the available WIFI near me using (iwconfig)



Kali_Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
8:17
chandrahas2002@KALI: ~/Desktop
File Actions Edit View Help
Right Ctrl

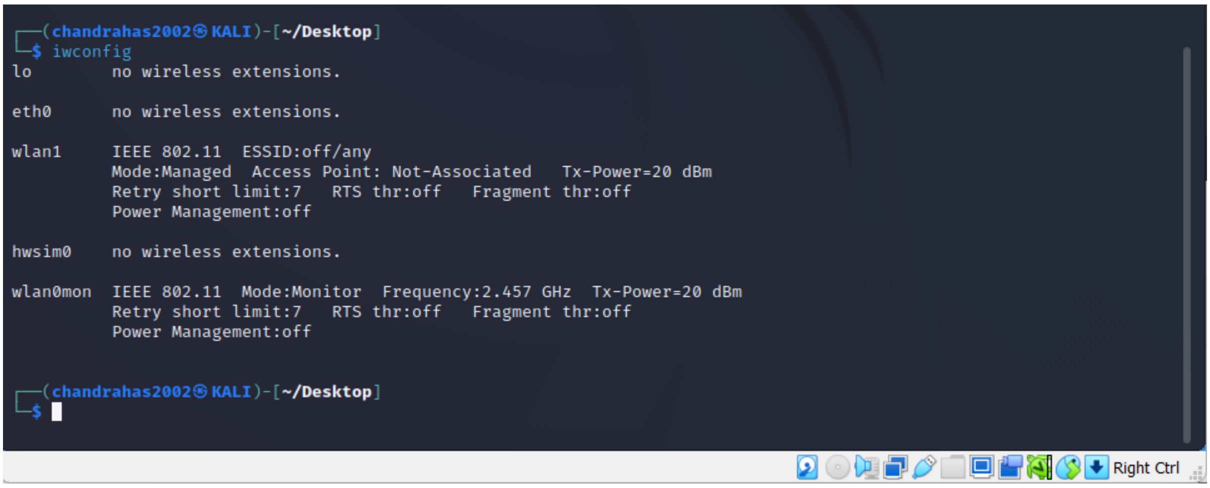
```
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:56:fc:35 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 85495sec preferred_lft 85495sec
    inet6 fe80::a00:27ff:fe56:fc35/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: wlan0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 6a:d7:9f:9c:f7:14 brd ff:ff:ff:ff:ff:ff permaddr 02:00:00:00:00:00
4: wlan1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether ce:a2:d2:eb:74:06 brd ff:ff:ff:ff:ff:ff permaddr 02:00:00:00:01:00
5: hwsim0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ieee802.11/radiotap 12:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff

┌──(chandrahas2002㉿KALI)-[~/Desktop]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

wlan1     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

hwsim0    no wireless extensions.


┌──(chandrahas2002㉿KALI)-[~/Desktop]
└─$ cat /etc/os-release
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
VERSION_ID="2023.2"
VERSION="2023.2"
VERSION_CODENAME=kali-rolling
ID=kali
ID_LIKE=debian
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
ANSI_COLOR="1;31"

┌──(chandrahas2002㉿KALI)-[~/Desktop]
└─$ ▌
```



Kali_Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
8:08
chandrahas2002@KALI: ~/Desktop
File Actions Edit View Help
Right Ctrl

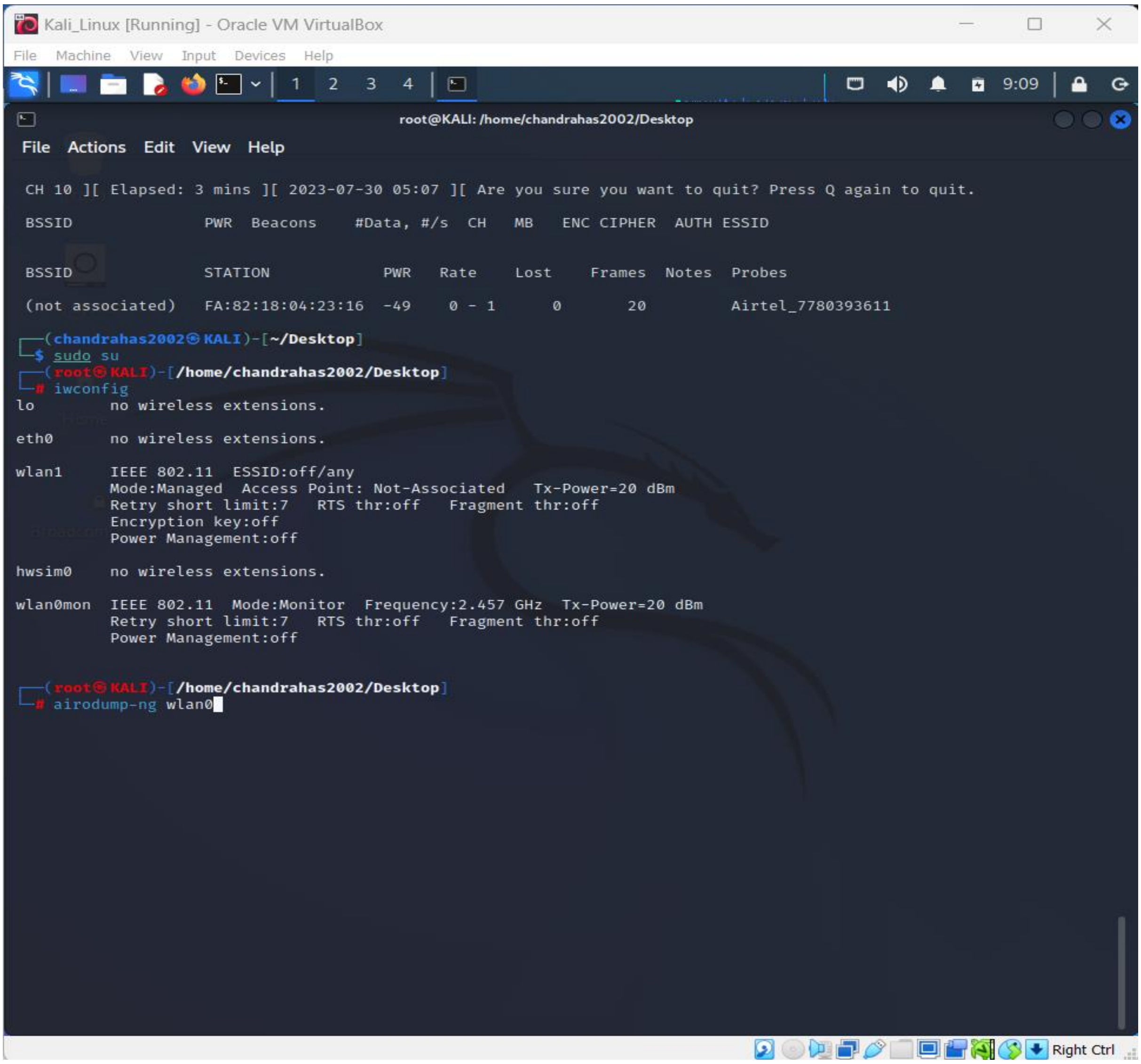
```
┌──(chandrahas2002㉿KALI)-[~/Desktop]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

wlan1     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

hwsim0    no wireless extensions.

┌──(chandrahas2002㉿KALI)-[~/Desktop]
└─$ ▌
```

Successfully changed the Wi-Fi to monitor mode



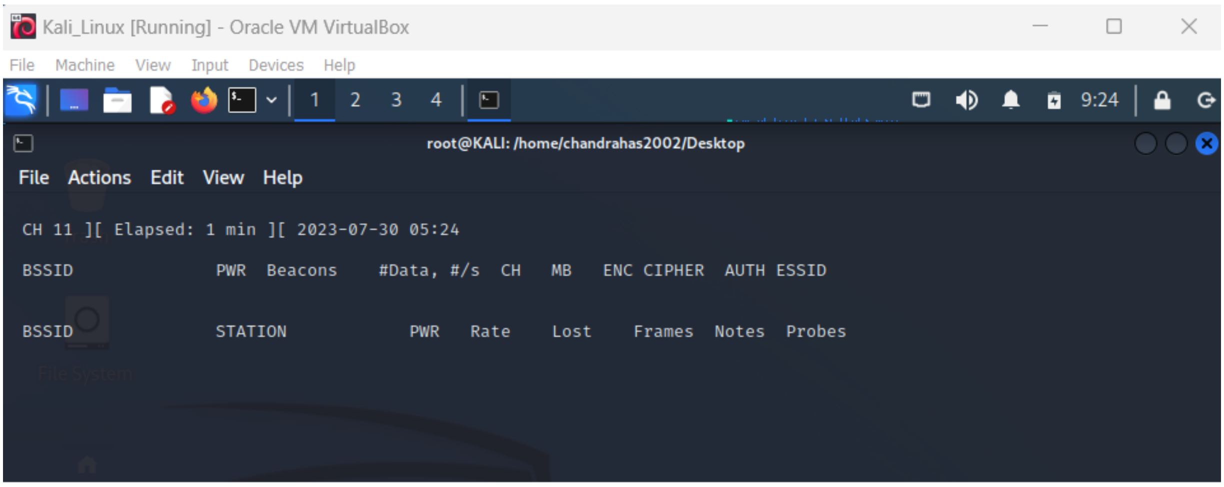
```
┌──(chandrahas2002㉿KALI)-[~/Desktop]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan1     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

hwsim0    no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off


┌──(chandrahas2002㉿KALI)-[~/Desktop]
└─$ 
```

Using (airodump)-ng wlan0 command


Kali_Linux [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
1
2
3
4
9:09
root@KALI: /home/chandrahas2002/Desktop
File
Actions
Edit
View
Help
Right Ctrl

```
 CH 10 ][ Elapsed: 3 mins ][ 2023-07-30 05:07 ][ Are you sure you want to quit? Press Q again to quit.

 BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID


 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 (not associated)   FA:82:18:04:23:16  -49    0 - 1      0       20         Airtel_7780393611

┌──(chandrahas2002㉿KALI)-[~/Desktop]
└─$ sudo su
┌──(root㉿KALI)-[/home/chandrahas2002/Desktop]
└─# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan1     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

hwsim0    no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off


┌──(root㉿KALI)-[/home/chandrahas2002/Desktop]
└─# airodump-ng wlan0
```

Found the BSSID of WIFI and use sudo airomon-ng wlan0mon -d (BSSID)

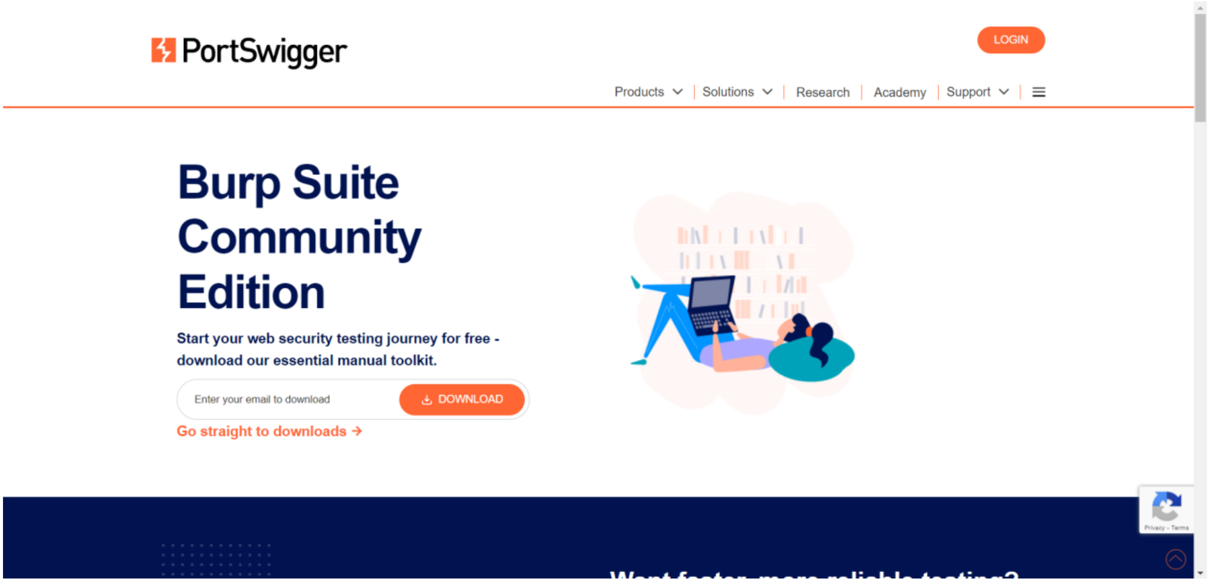


Kali_Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
9:24
root@KALI: /home/chandrahas2002/Desktop
File Actions Edit View Help

```
CH 11 ][ Elapsed: 1 min ][ 2023-07-30 05:24

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes
```

2) Perform Session Hijacking & get Login Access using DVWA

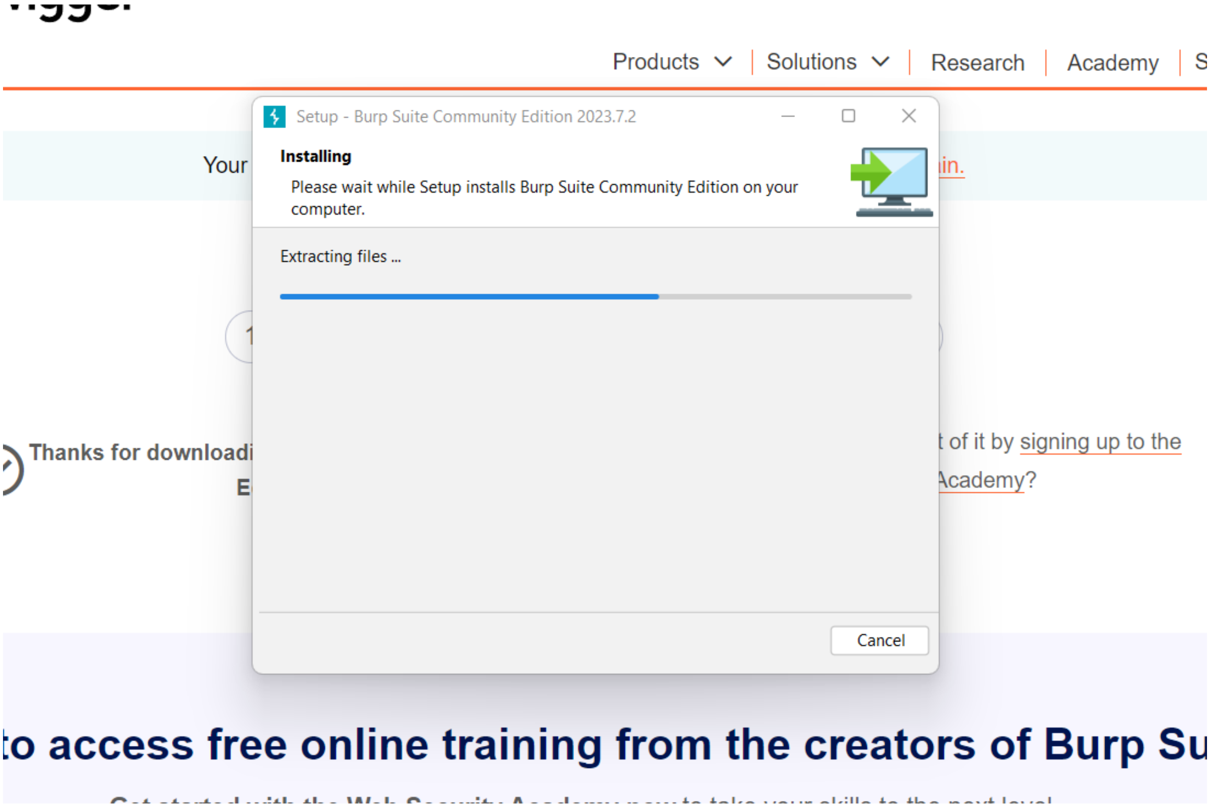
Installing (Burp suit)



Burp Suite Community Edition

Start your web security testing journey for free - download our essential manual toolkit.

Go straight to downloads →



Setup - Burp Suite Community Edition 2023.7.2

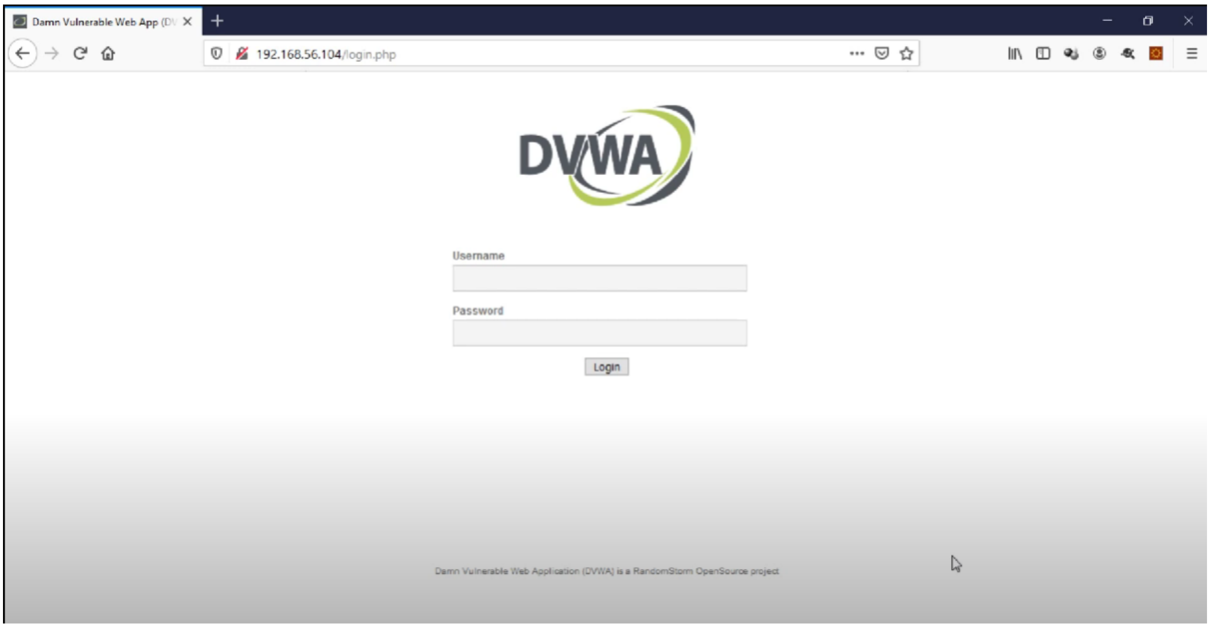
Installing

Please wait while Setup installs Burp Suite Community Edition on your computer.

Extracting files ...

to access free online training from the creators of Burp Su

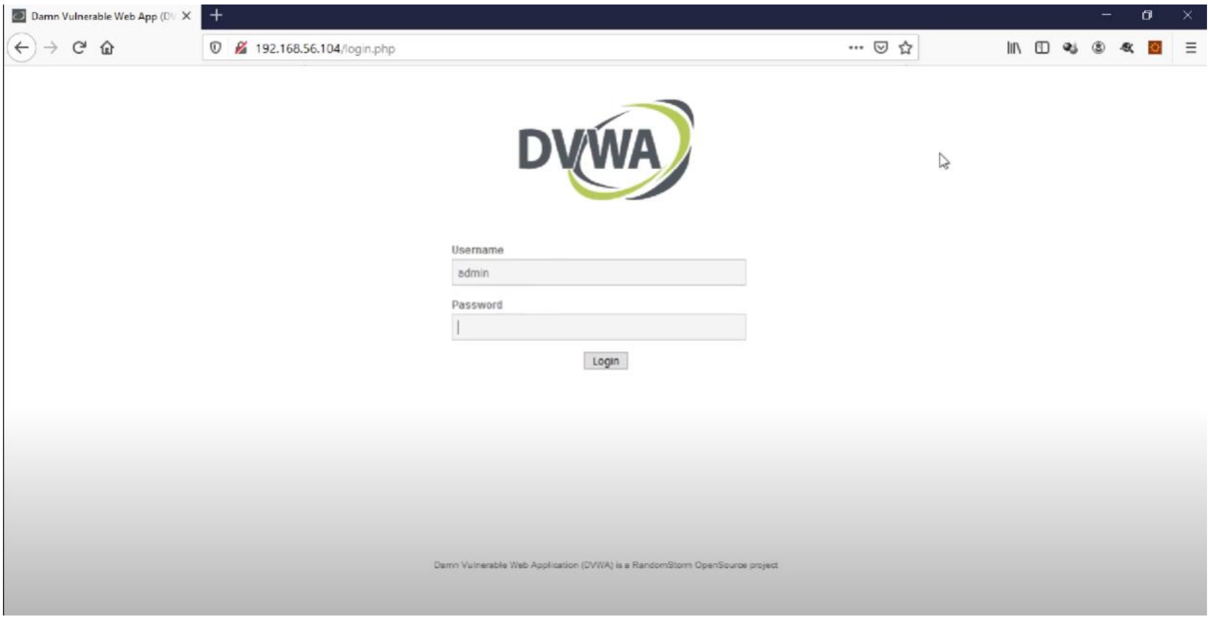
Login in DVWA



192.168.56.104/login.php

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Gave credentials but login failed

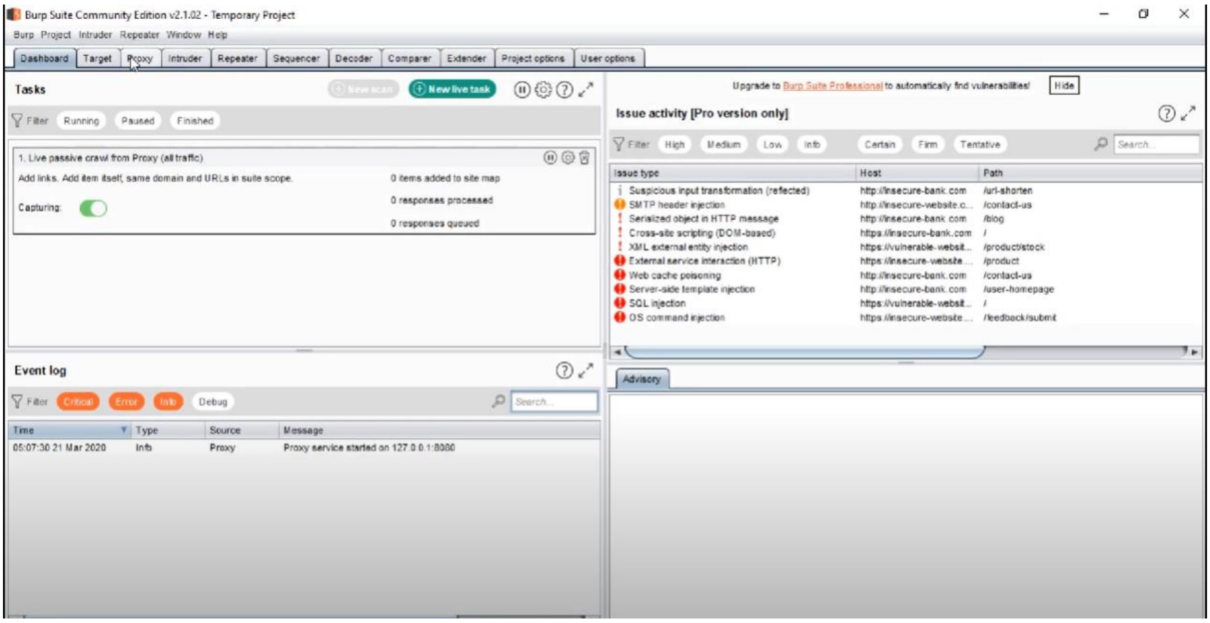


192.168.56.104/login.php

Username: admin

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Opening the Burp suite and checking the proxy



Burp Suite Community Edition v2.1.02 - Temporary Project

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Tasks
New scan
New live task
Filter Running Paused Finished
Event log
Filter Critical Error Info Debug
Search...
Upgrade to Burp Suite Professional to automatically find vulnerabilities!
Hide
Issue activity [Pro version only]
Filter High Medium Low Info Certain Firm Tentative
Advisory

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope.

Capturing:

0 items added to site map

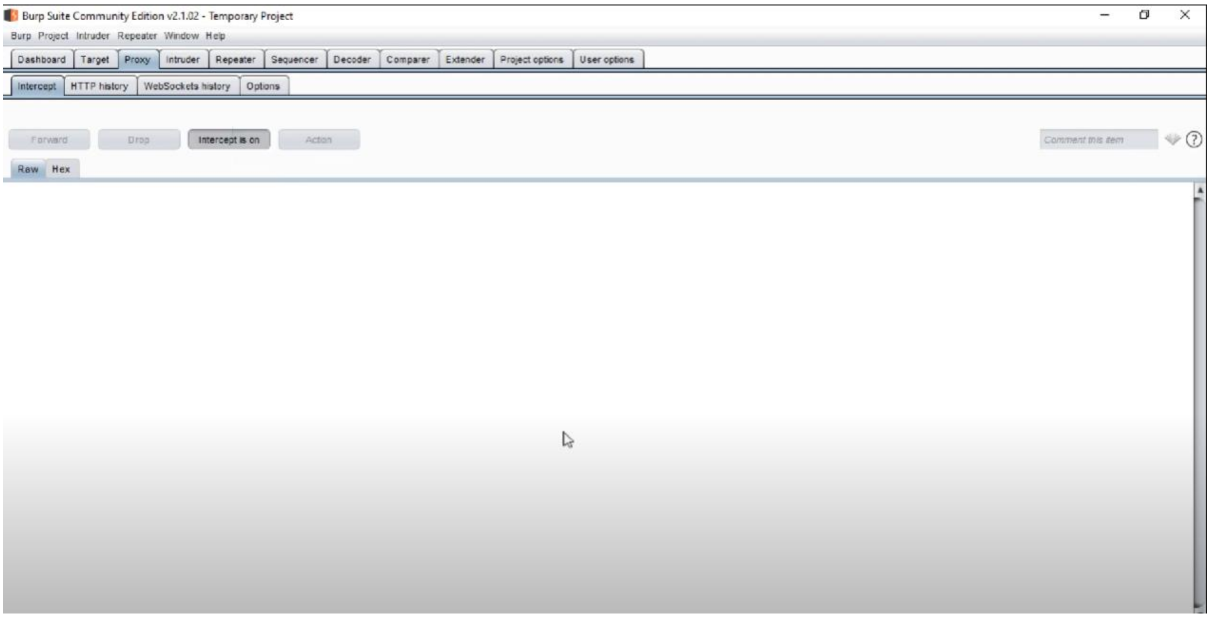
0 responses processed

0 responses queued

Time	Type	Source	Message
05:07:30 21 Mar 2020	Info	Proxy	Proxy service started on 127.0.0.1:8080

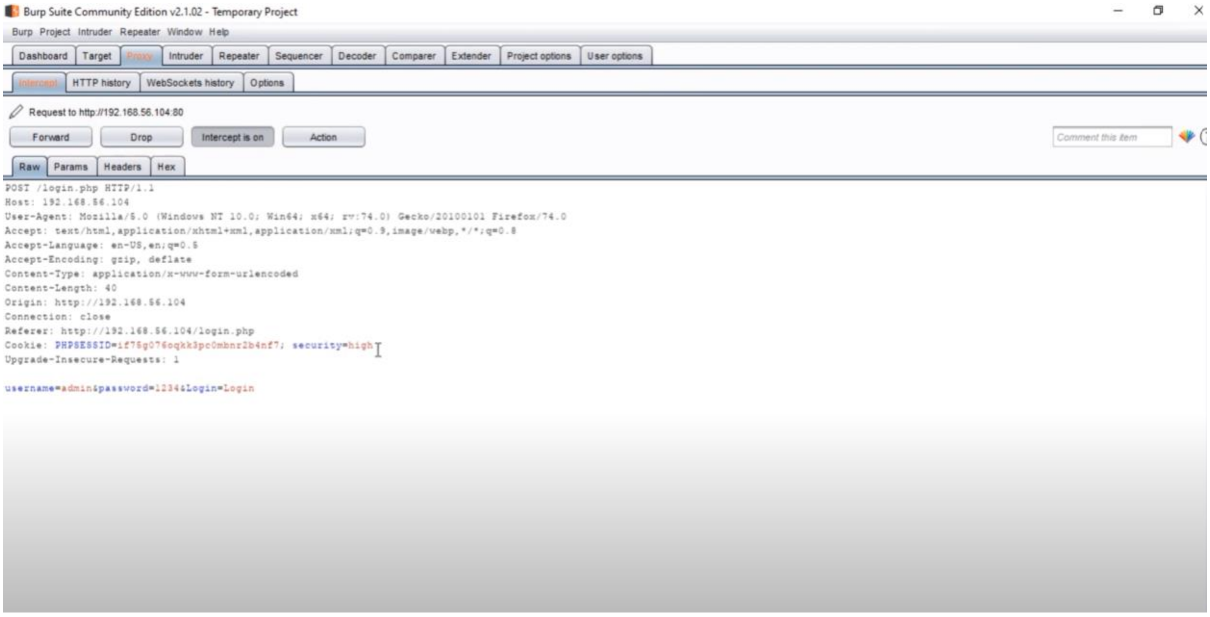
Issue type	Host	Path
Suspicious input transformation (reflected)	http://insecure-bank.com	/url-shorten
SMTP header injection	http://insecure-website.c...	/contact-us
Serialized object in HTTP message	http://insecure-bank.com	/blog
Cross-site scripting (DOM-based)	https://insecure-bank.com	/
XML external entity injection	https://vulnerable-websit...	/product/stock
External service interaction (HTTP)	https://insecure-website....	/product
Web cache poisoning	http://insecure-bank.com	/contact-us
Server-side template injection	http://insecure-bank.com	/user-homepage
SQL injection	https://vulnerable-websit...	/
OS command injection	https://insecure-website....	/feedback/submit

Turn on the intercept



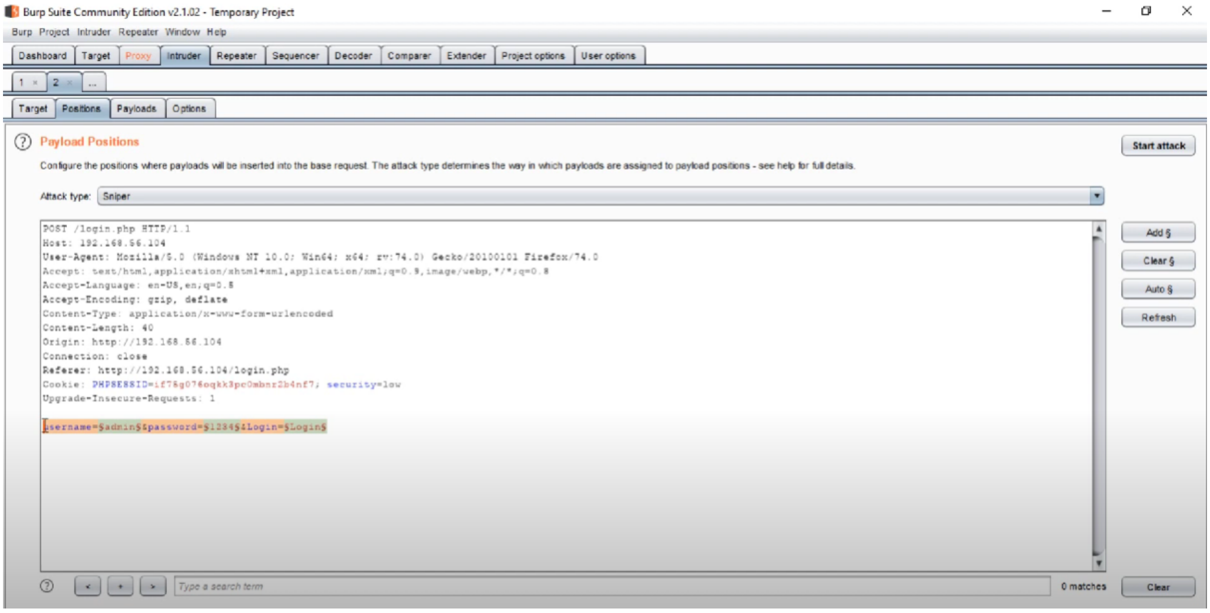
Burp Suite Community Edition v2.1.02 - Temporary Project

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Comment this item
Raw Hex


Burp Suite Community Edition v2.1.02 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://192.168.56.104:80
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex

```
POST /login.php HTTP/1.1
Host: 192.168.56.104
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0
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: 40
Origin: http://192.168.56.104
Connection: close
Referer: http://192.168.56.104/login.php
Cookie: PHPSESSID=if76g076oqkk3pc0mbnr2b4nf7; security=high
Upgrade-Insecure-Requests: 1

username=admin&password=1234&Login=Login
```

Setting the payload positions

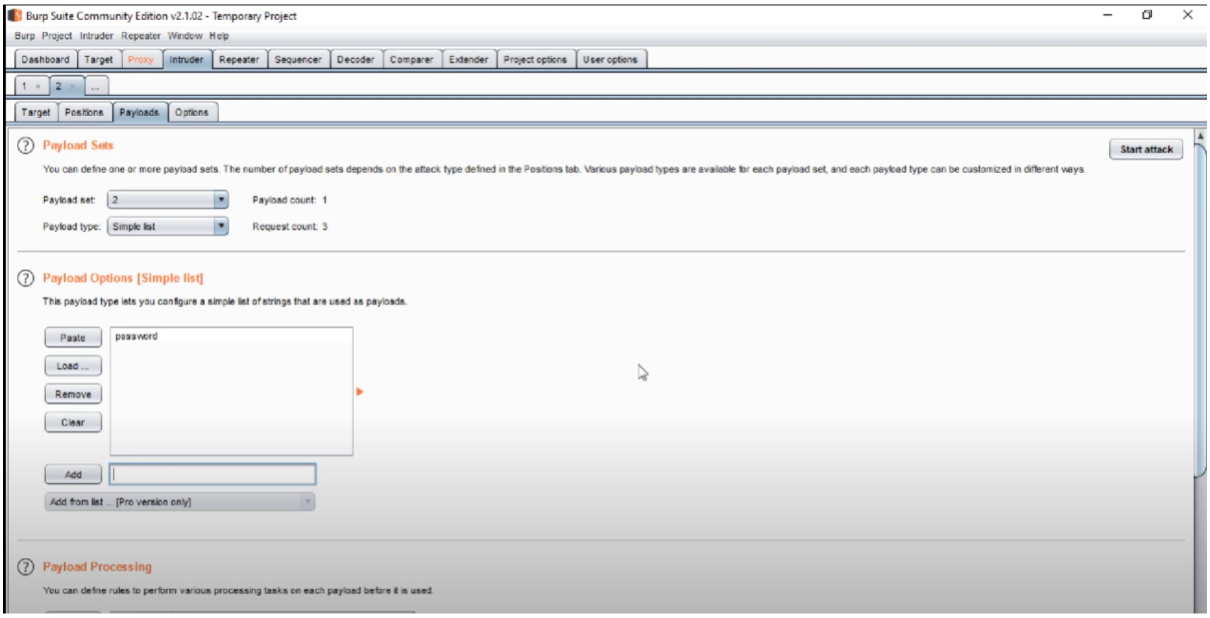

Burp Suite Community Edition v2.1.02 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 × 2 × ...
Target Positions Payloads Options
Payload Positions
Start attack
Add §
Clear §
Auto §
Refresh
Type a search term
0 matches
Clear

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

```
POST /login.php HTTP/1.1
Host: 192.168.56.104
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0
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: 40
Origin: http://192.168.56.104
Connection: close
Referer: http://192.168.56.104/login.php
Cookie: PHPSESSID=if76g076oqkk3pc0mbnr2b4nf7; security=low
Upgrade-Insecure-Requests: 1

username=§admin§&password=§1234§&Login=§Login§
```

Setting up the payload


Burp Suite Community Edition v2.1.02 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 × 2 × ...
Target Positions Payloads Options
Start attack
Paste
Load ...
Remove
Clear
Add
Add from list ... [Pro version only]

Payload Sets

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: 2

Payload count: 1

Payload type: Simple list

Request count: 3

Payload Options [Simple list]

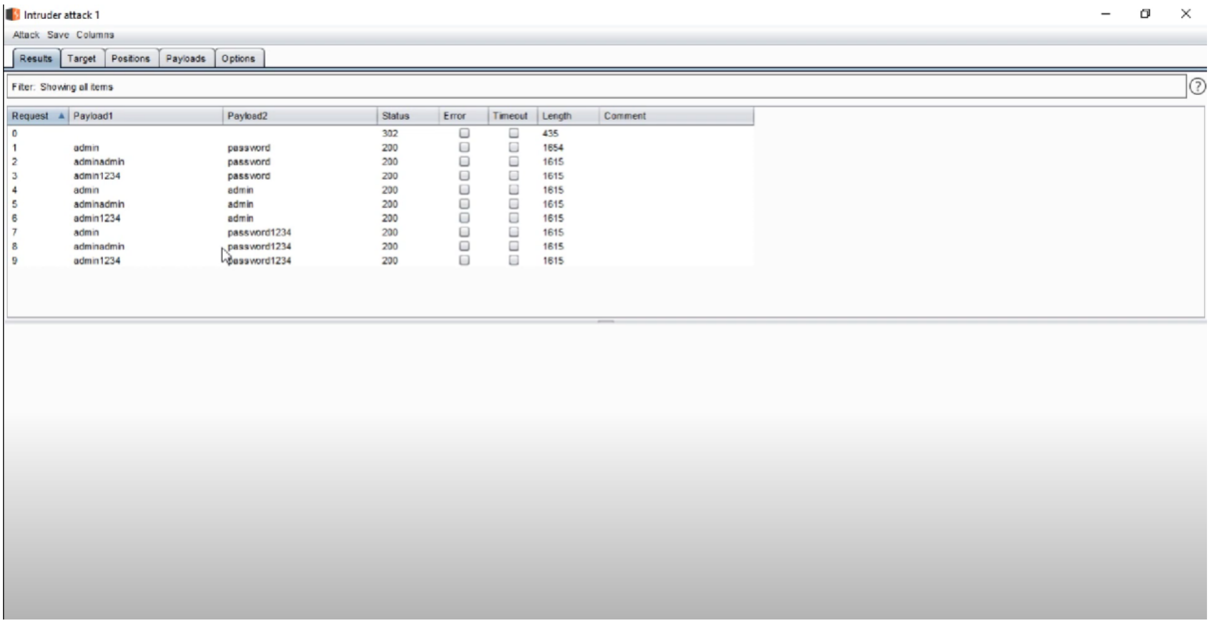
This payload type lets you configure a simple list of strings that are used as payloads.

password

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

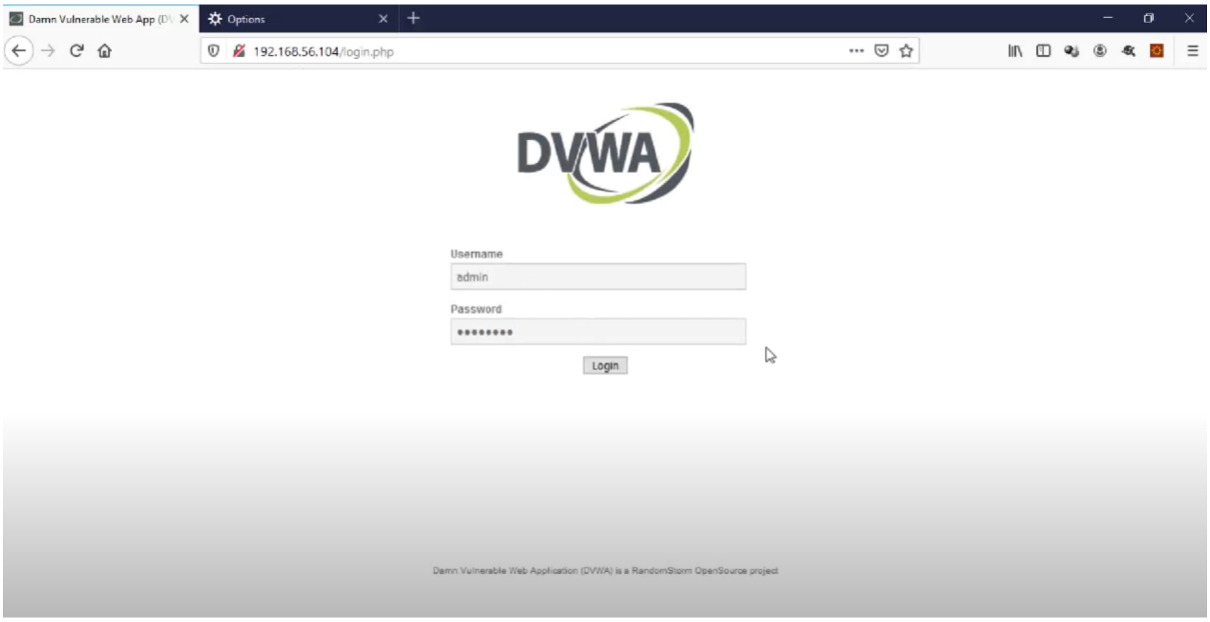
Results



Filter: Showing all items

Request ▲	Payload1	Payload2	Status	Error	Timeout	Length	Comment
0			302	□	□	435	
1	admin	password	200	□	□	1654	
2	adminadmin	password	200	□	□	1615	
3	admin1234	password	200	□	□	1615	
4	admin	admin	200	□	□	1615	
5	adminadmin	admin	200	□	□	1615	
6	admin1234	admin	200	□	□	1615	
7	admin	password1234	200	□	□	1615	
8	adminadmin	password1234	200	□	□	1615	
9	admin1234	password1234	200	□	□	1615	

Login in to DVWA

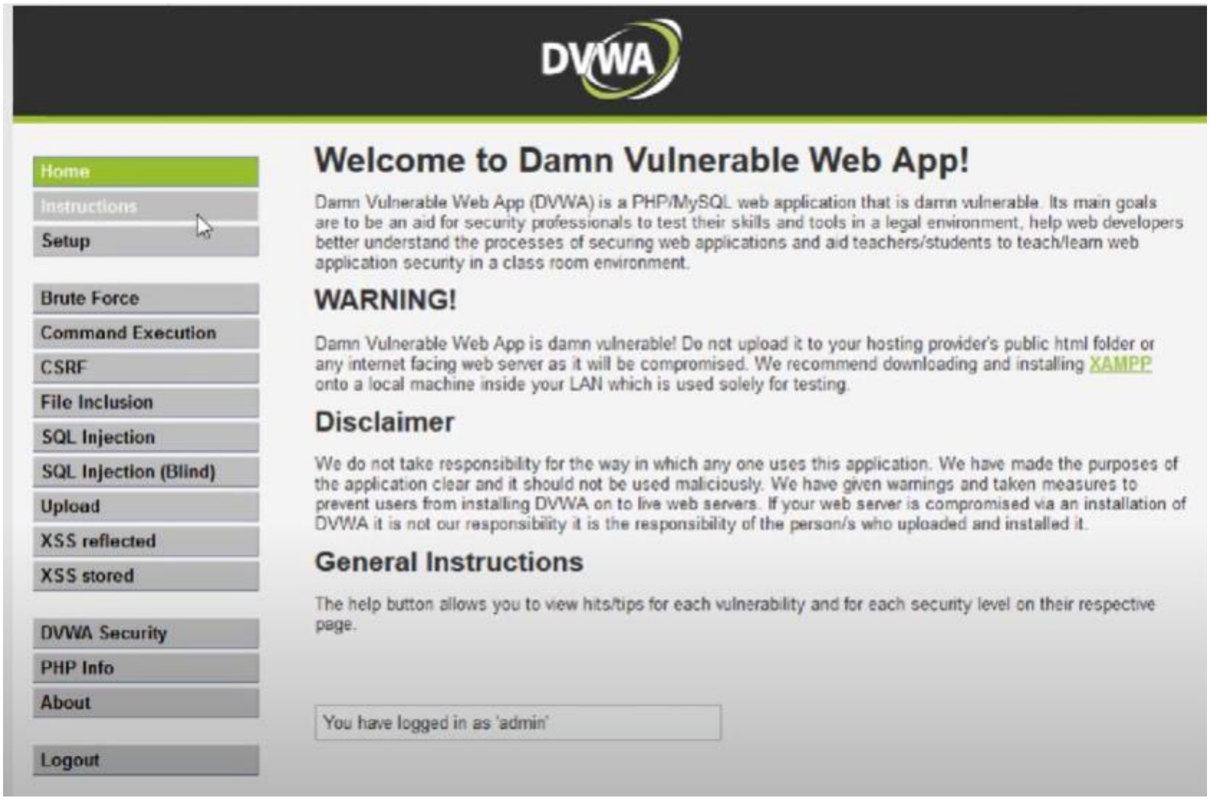


Username
admin

Password
••••••••

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Login successful



Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

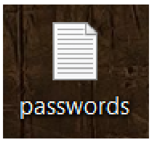
You have logged in as 'admin'

3) Generate cipher.txt which includes Encrypted value of your “Name” using the RSA public

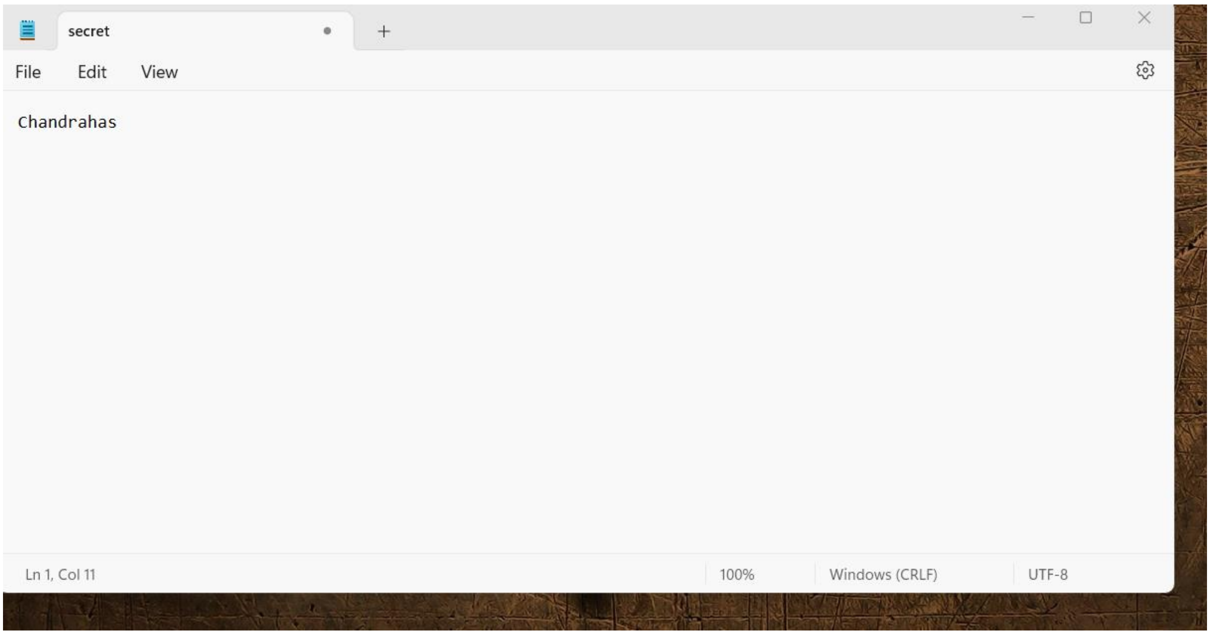
key & Hide cipher.txt behind Image using Steganography. Also showcase decryption

using RSA Private Key

created a new TXT file



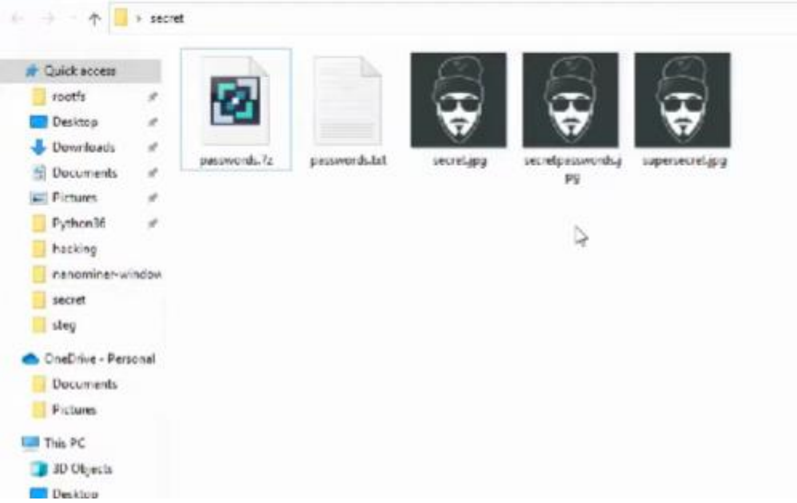
Entered my name in the text file



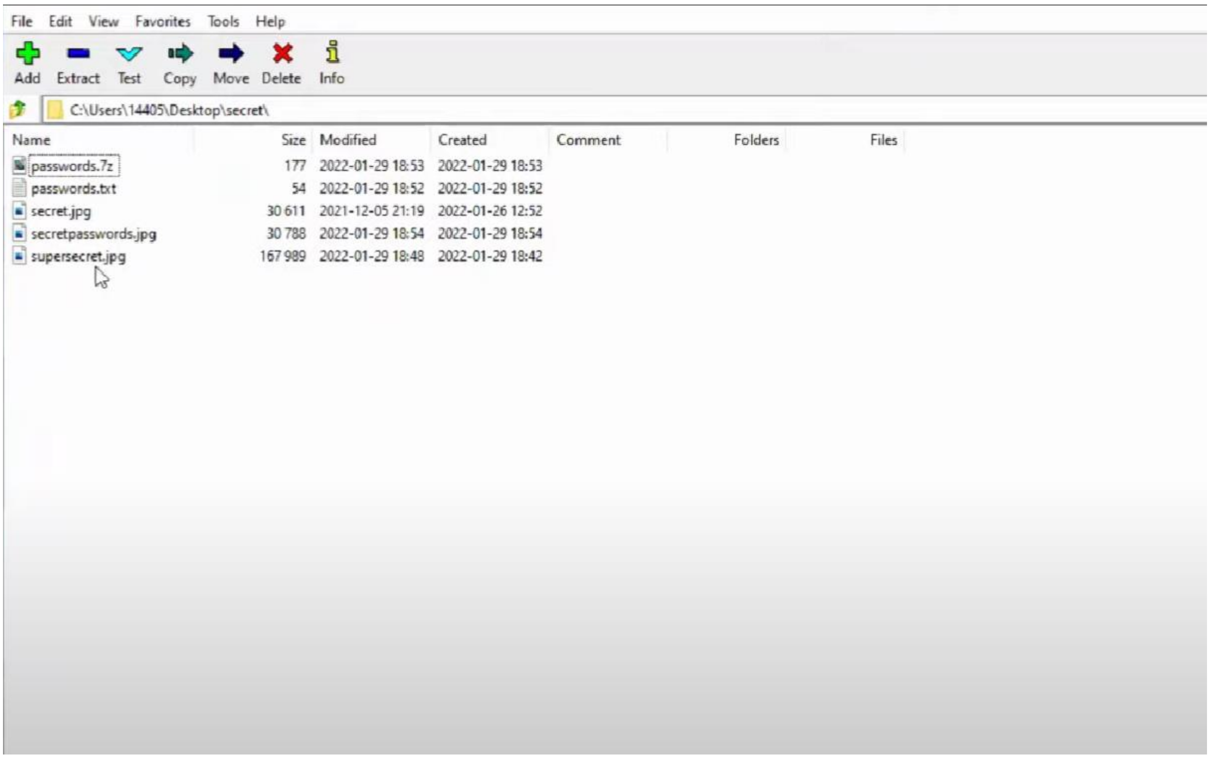
Chandrahas

compressed to a Zip file

Used 7 Zip to make a password file and encrypted the txt into image



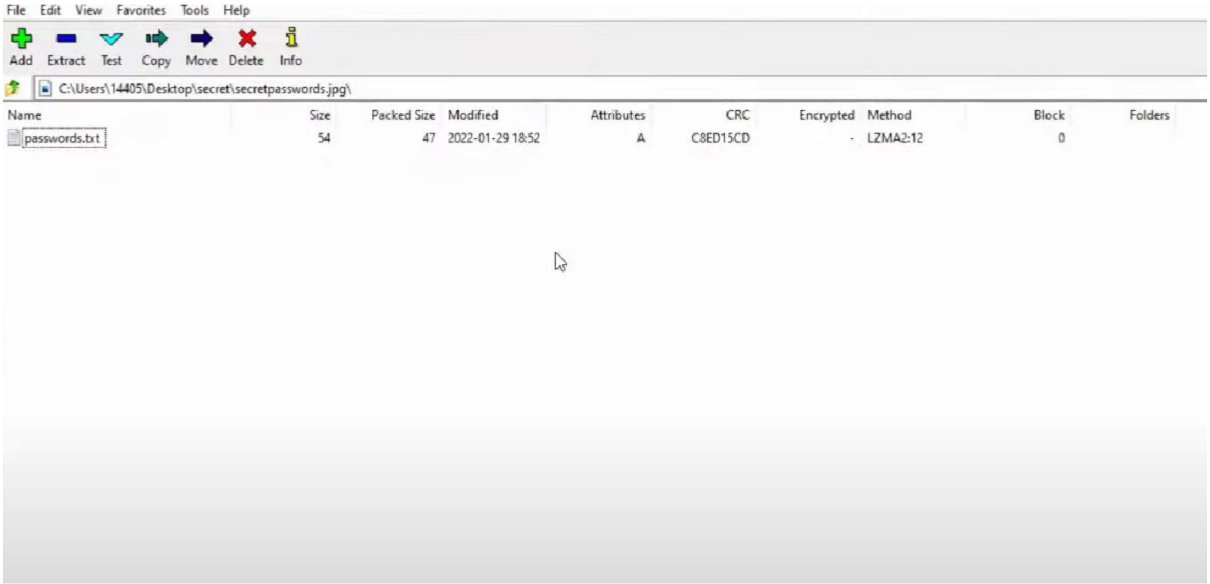
After clicking the image we cant see the real text now double click on the password files



C:\Users\14405\Desktop\secret\

Name	Size	Modified	Created	Comment	Folders	Files
passwords.7z	177	2022-01-29 18:53	2022-01-29 18:53			
passwords.txt	54	2022-01-29 18:52	2022-01-29 18:52			
secret.jpg	30 611	2021-12-05 21:19	2022-01-26 12:52			
secretpasswords.jpg	30 788	2022-01-29 18:54	2022-01-29 18:54			
supersecret.jpg	167 989	2022-01-29 18:48	2022-01-29 18:42			

inside this you will find a password.txt file



C:\Users\14405\Desktop\secret\secretpasswords.jpg\

Name	Size	Packed Size	Modified	Attributes	CRC	Encrypted	Method	Block	Folders
passwords.txt	54	47	2022-01-29 18:52	A	C8ED15CD	-	LZMA2:12	0	

----------------------------------X--------------------------------