

Figure 1. DNS and HTTPS Traffic Tracing Output

```
192.168.1.0/24 > 192.168.1.105 » [15:12:11] [net.sniff.dns] dns gateway > SEMIHTWO : cf.x.com is 162.159.140.229, 172.66.0.227
192.168.1.0/24 > 192.168.1.105 » [15:12:11] [net.sniff.dns] dns gateway > SEMIHTWO : cf.x.com is 162.159.140.229, 172.66.0.227
192.168.1.0/24 > 192.168.1.105 » [15:12:13] [net.sniff.https] sni SEMIHTWO > https://abs.twimg.com
192.168.1.0/24 > 192.168.1.105 » [15:12:13] [net.sniff.dns] dns gateway > SEMIHTWO : x.com is 172.66.0.227
192.168.1.0/24 > 192.168.1.105 » [15:12:13] [net.sniff.dns] dns gateway > SEMIHTWO : twimg.twitter.map.fastly.net is 151.101.204.159
192.168.1.0/24 > 192.168.1.105 » [15:12:13] [net.sniff.dns] dns gateway > SEMIHTWO : x.com is 172.66.0.227
192.168.1.0/24 > 192.168.1.105 » [15:12:13] [net.sniff.dns] dns gateway > SEMIHTWO : twimg.twitter.map.fastly.net is 151.101.204.159
192.168.1.0/24 > 192.168.1.105 » [15:12:13] [net.sniff.https] sni SEMIHTWO > https://abs.twimg.com
192.168.1.0/24 > 192.168.1.105 » [15:12:13] [net.sniff.dns] dns gateway > SEMIHTWO : cf.twitter.com is 172.66.0.227, 162.159.140.229
192.168.1.0/24 > 192.168.1.105 » [15:12:13] [net.sniff.dns] dns gateway > SEMIHTWO : cf.twitter.com is 172.66.0.227, 162.159.140.229
192.168.1.0/24 > 192.168.1.105 » [15:12:13] [net.sniff.dns] dns gateway > SEMIHTWO : dualstack.video.twitter.map.fastly.net is 199.232.188.158
192.168.1.0/24 > 192.168.1.105 » [15:12:13] [net.sniff.dns] dns gateway > SEMIHTWO : abs-zero.twimg.com is 104.244.43.131
192.168.1.0/24 > 192.168.1.105 » [15:12:13] [net.sniff.https] sni SEMIHTWO > https://pbs.twimg.com
192.168.1.0/24 > 192.168.1.105 » [15:12:13] [net.sniff.dns] dns gateway > SEMIHTWO : abs-zero.twimg.com is 104.244.43.131
```

Figure 2. HTTP GET Traffic – Accessing the Sample Site

```
192.168.1.0/24 > 192.168.1.105 » [15:12:16] [net.sniff.http.request] http SEMIHTWO GET example.com/
192.168.1.0/24 > 192.168.1.105 » [15:12:16] [net.sniff.http.request] http SEMIHTWO GET example.com/
192.168.1.0/24 > 192.168.1.105 » [15:12:16] [net.sniff.http.response] http 23.192.228.84:80 304 Not Modified
→ SEMIHTWO (0 B text/html)
192.168.1.0/24 > 192.168.1.105 » [15:12:16] [net.sniff.http.response] http 23.192.228.84:80 304 Not Modified
→ SEMIHTWO (0 B text/html)
192.168.1.0/24 > 192.168.1.105 » [15:12:19] [net.sniff.http.request] http SEMIHTWO GET testphp.vulnweb.com/login.php
192.168.1.0/24 > 192.168.1.105 » [15:12:19] [net.sniff.http.request] http SEMIHTWO GET testphp.vulnweb.com/login.php
192.168.1.0/24 > 192.168.1.105 » [15:12:20] [net.sniff.http.response] http 44.228.249.3:80 200 OK → SEMIHTWO (1.1 kB text/html; charset=UTF-8)
192.168.1.0/24 > 192.168.1.105 » [15:12:20] [net.sniff.http.response] http 44.228.249.3:80 200 OK → SEMIHTWO (5.6 kB text/html; charset=UTF-8)
```

Figure 3. POST Request – Login Information Capture

```
192.168.1.0/24 > 192.168.1.105 » [15:12:35] [net.sniff.http.request] http SEMIHTWO POST testphp.vulnweb.com/userinfo.php
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
Content-Length: 20
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
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=0.7
Referer: http://testphp.vulnweb.com/login.php
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: login=test%2Ftest
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36

uname=test&pass=test
```

Figure 4. Server Response – 200 OK and Set-Cookie

```
192.168.1.0/24 > 192.168.1.105 » [15:12:35] [net.sniff.http.response] http 44.228.249.3:80 200 OK → SEMIHTWO
(2.5 kB text/html; charset=UTF-8)
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Mon, 19 May 2025 19:12:36 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38ubuntu20.04.1+deb.sury.org+1
Set-Cookie: login=test%2Ftest
Content-Encoding: gzip
```

Figure 5. POST Request – Personal Information Leak

```
192.168.1.0/24 > 192.168.1.105 » [15:12:35] [net.sniff.dns] dns gateway > SEMIHTWO : passwordsleakcheck-pa.go
ogleapis.com is 142.250.184.138, 142.250.187.170, 172.217.169.202, 142.250.187.106, 216.58.213.106, 216.58.212
.10, 172.217.17.138, 142.250.187.138, 172.217.17.234, 172.217.169.106, 142.251.141.42, 172.217.20.74, 172.217
.17.106, 172.217.169.170, 172.217.169.138, 216.58.212.42
192.168.1.0/24 > 192.168.1.105 » [15:12:48] [net.sniff.http.request] http SEMIHTWO POST testphp.vulnweb.com/u
serinfo.php
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appli
cation/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: login=test%2Ftest
Content-Length: 123
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0
Safari/537.36
Referer: http://testphp.vulnweb.com/userinfo.php
Connection: keep-alive
Cache-Control: max-age=0

username=Prasanna S&uucc=1234-5678-2300-9000&uemail=email@email.com&uphone=2323345&uaddress=21 street 23456789&up
date=update
```

Figure 6. POST Response and Attack End Output

```
192.168.1.0/24 > 192.168.1.105 » [15:12:48] [net.sniff.http.request] http SEMIHTWO POST testphp.vulnweb.com/u
serinfo.php
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Referer: http://testphp.vulnweb.com/userinfo.php
Accept-Encoding: gzip, deflate
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: login=test%2Ftest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appli
cation/signed-exchange;v=b3;q=0.7
Content-Length: 123
Cache-Control: max-age=0
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1

username=Prasanna S&uucc=1234-5678-2300-9000&uemail=email@email.com&uphone=2323345&uaddress=21 street 23456789&up
date=update

192.168.1.0/24 > 192.168.1.105 » [15:12:48] [net.sniff.http.response] http 44.228.249.3:80 200 OK → SEMIHTWO
(2.5 kB text/html; charset=UTF-8)
192.168.1.0/24 > 192.168.1.105 » [15:12:48] [net.sniff.http.response] http 44.228.249.3:80 200 OK → SEMIHTWO
(1.1 kB text/html; charset=UTF-8)
192.168.1.0/24 > 192.168.1.105 » [15:12:52] [net.sniff.http.response] http 23.192.228.84:80 408 Request Time-
out → SEMIHTWO (314 B text/html)
192.168.1.0/24 > 192.168.1.105 » [15:12:52] [net.sniff.http.response] http 23.192.228.84:80 408 Request Time-
out → SEMIHTWO (314 B text/html)
192.168.1.0/24 > 192.168.1.105 » ^C
```