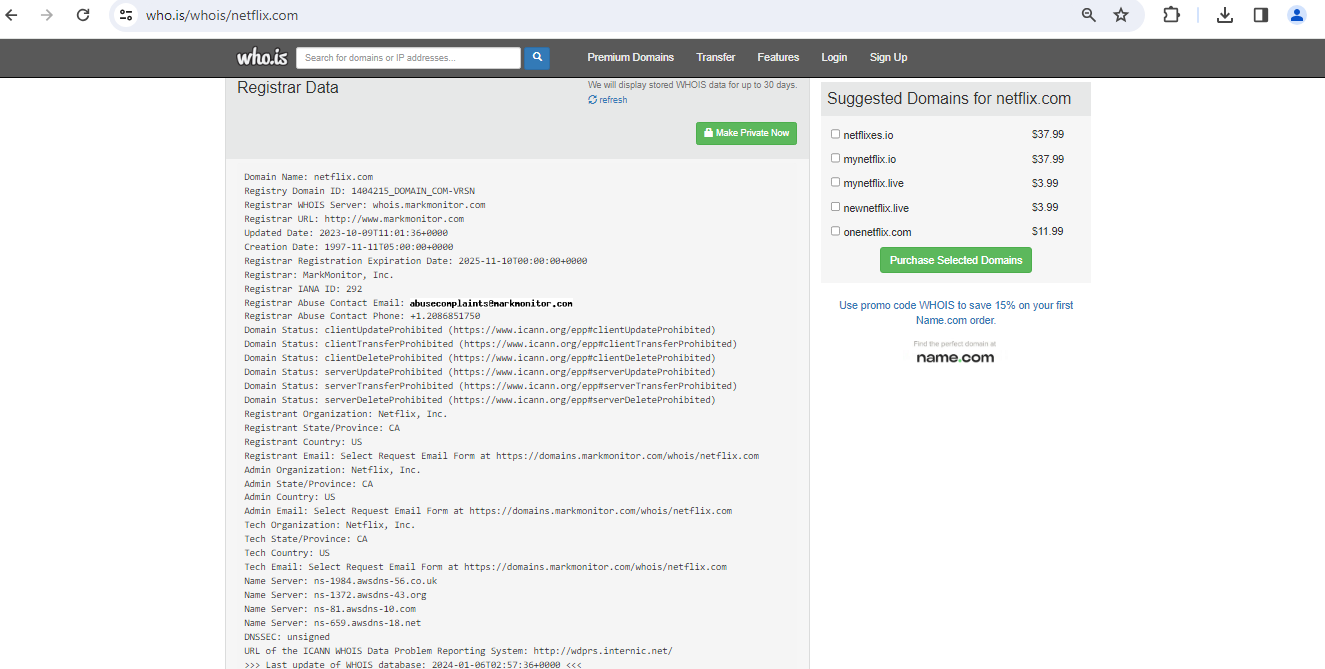
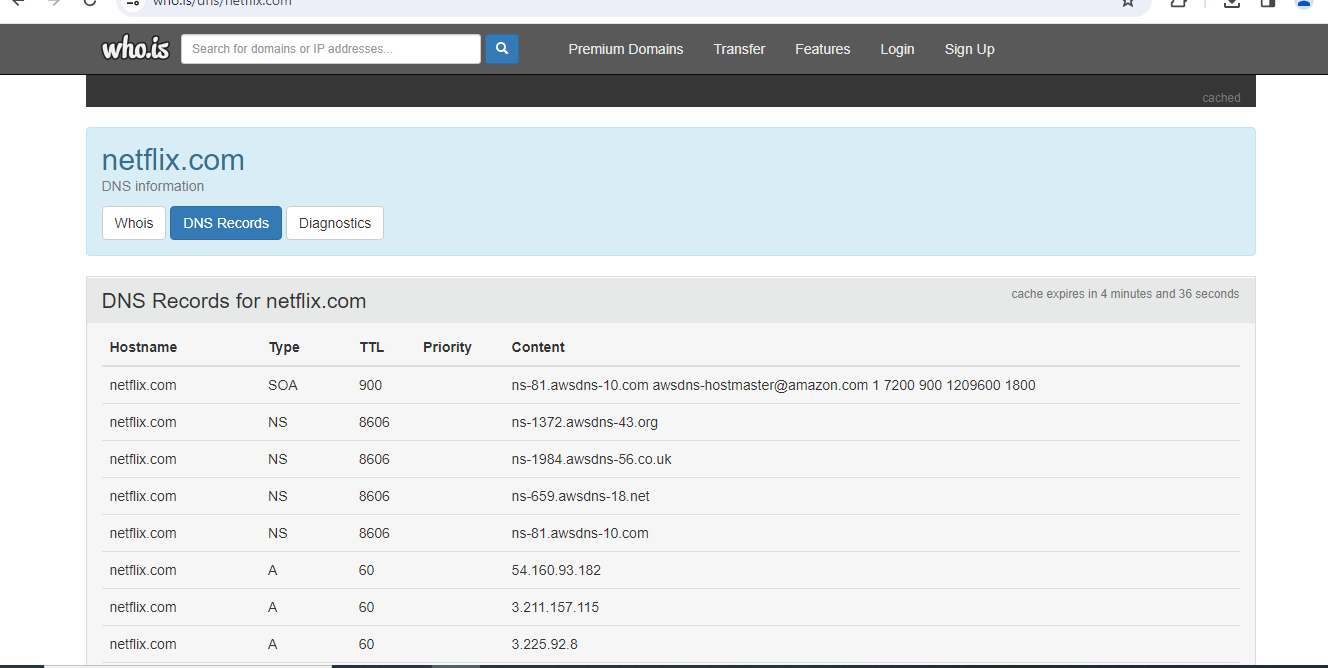
**Prc1**

**Output :-**

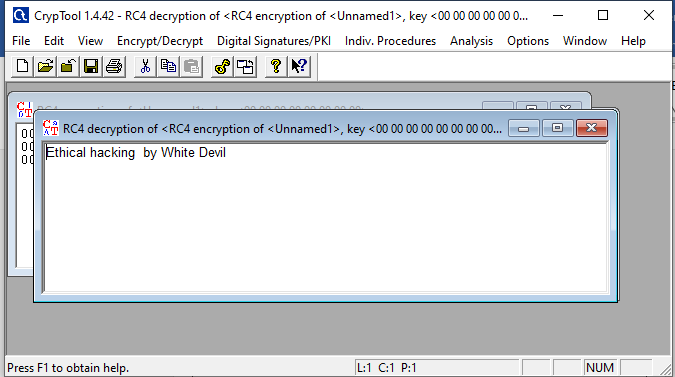


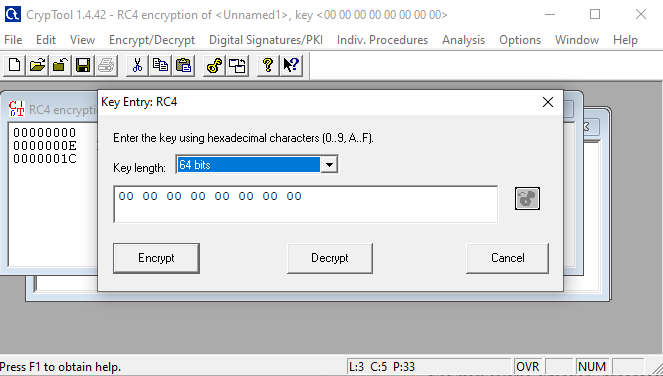


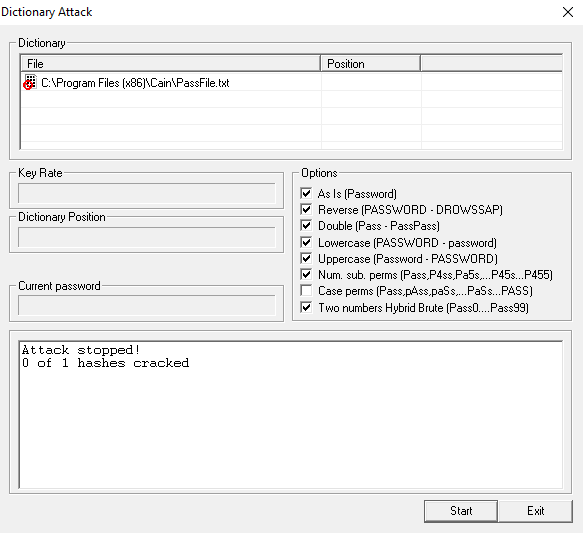
**Prc2**

**Output :-**

**Decryption Using RC4 with 64bits**

****

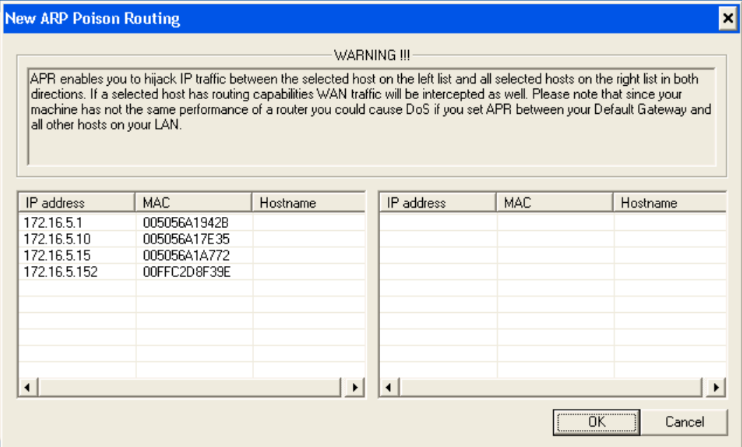
****

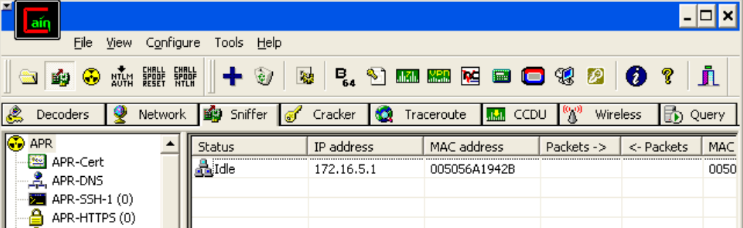
**Output :-**

**Prc3**

**Output :-**

Click on the IP and then click on the button shown in the image to start ARP Poisoning





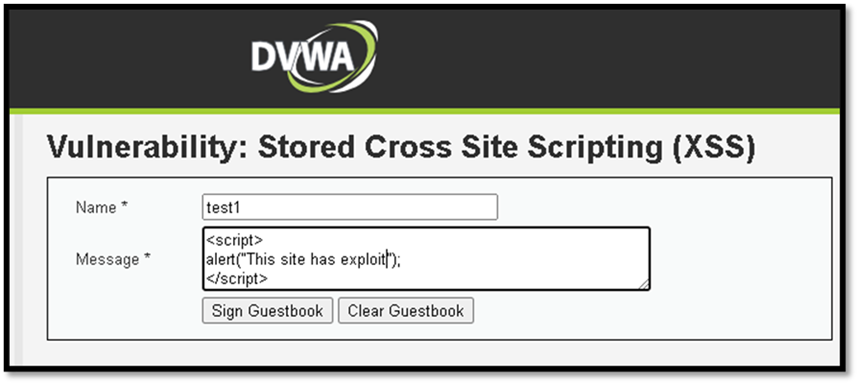
**Prac5**

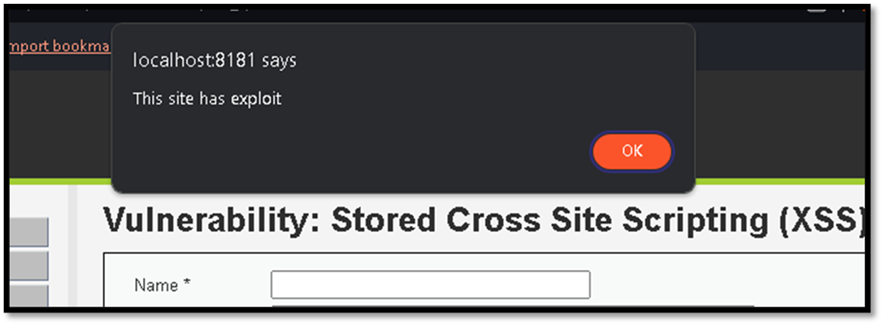
**Output :-**

|  |
| --- |
|  |
|  |  |

Here Site has Exploited

|  |
| --- |
|  |
|  |  |

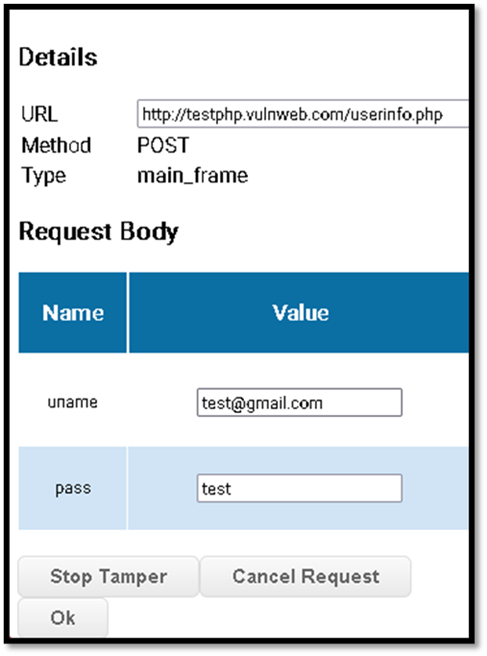




**Prac6**

**Output :-**

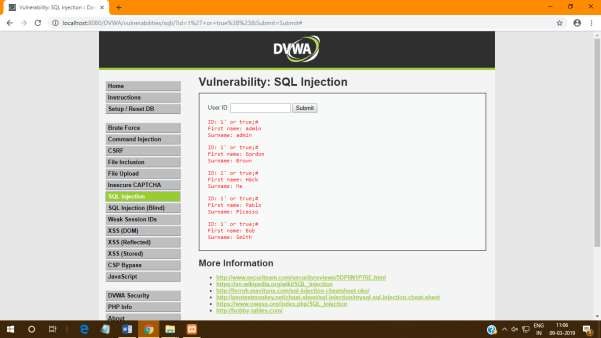
Here’s the result  of session impersonification



**Prc 7**

**Output :-**

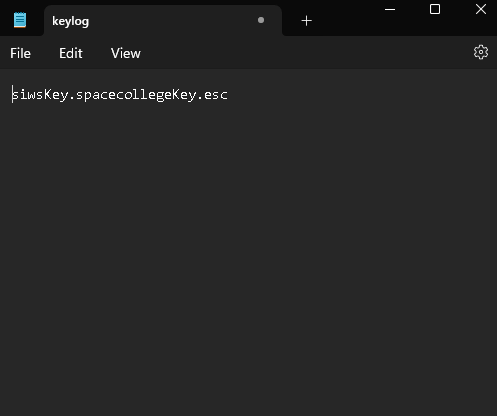
    Type 1’ or tue;# and click on submit.



**Output 8 :-**

After Executing The Python File KeyLog.txt Is Created

Open KeyLog.txt and See the Output

****