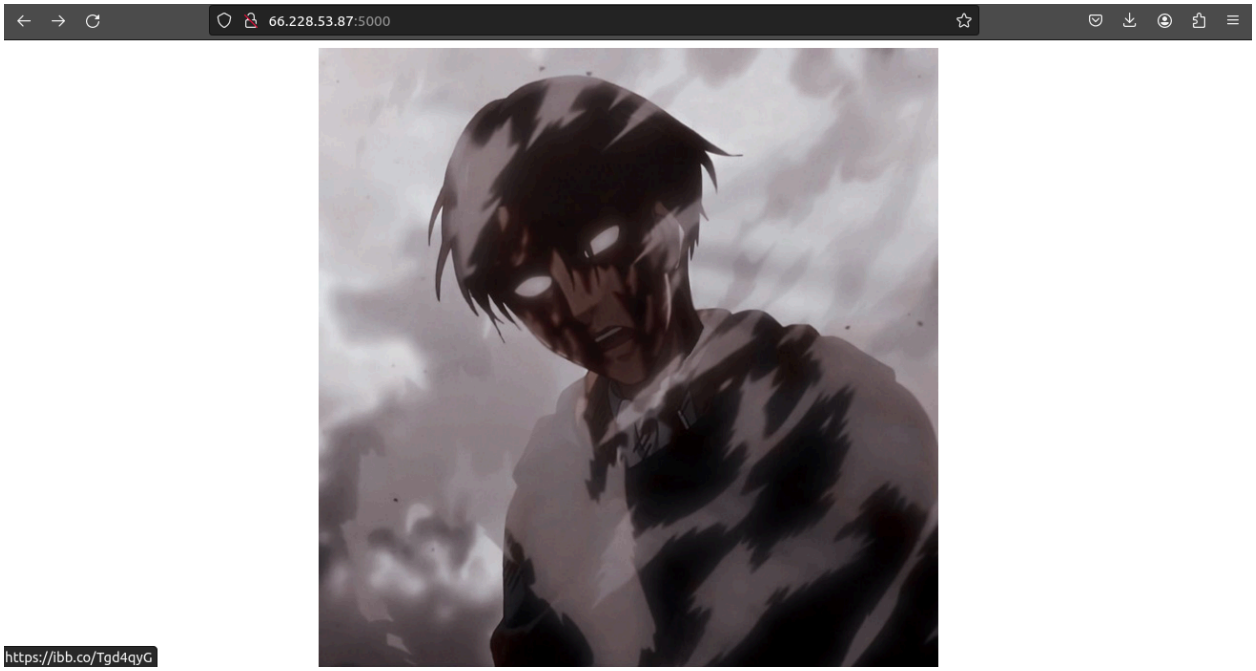
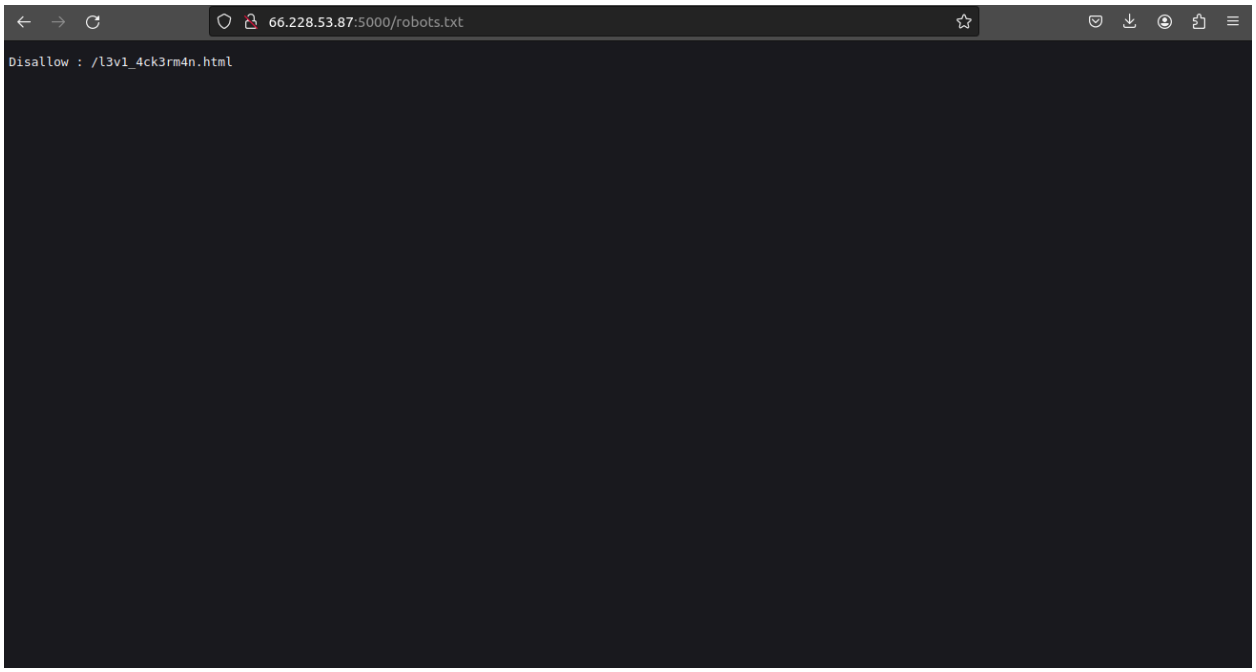
SWE 4504, Bonus Marks Assignment: Mirza Mohammad Azwad, 200042121
Write Up Knight CTF 2024

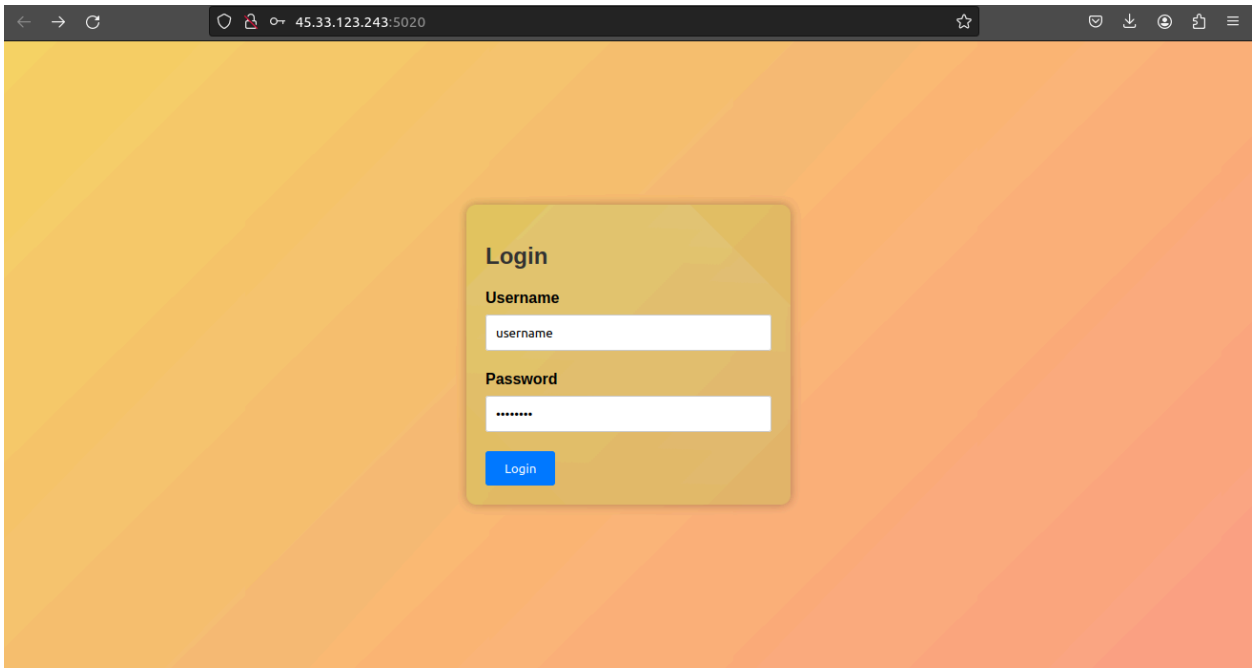
1. **Web-Levi Ackerman**
   The hint provided was Levi Ackerman is a robot, by is a I thought it might be a path in the website, the paths I tried was /robot,/robots, /robots.jpeg, /robots.png, /robots.txt, /robot.txt. The path /robots.txt gave the path /l3v1_4ck3rm4n.html and upon accessing this path we got the flag: KCTF{1m_d01n6_17_b3c4u53_1_h4v3_70}
   The idea is simply an example of **path traversal attack**

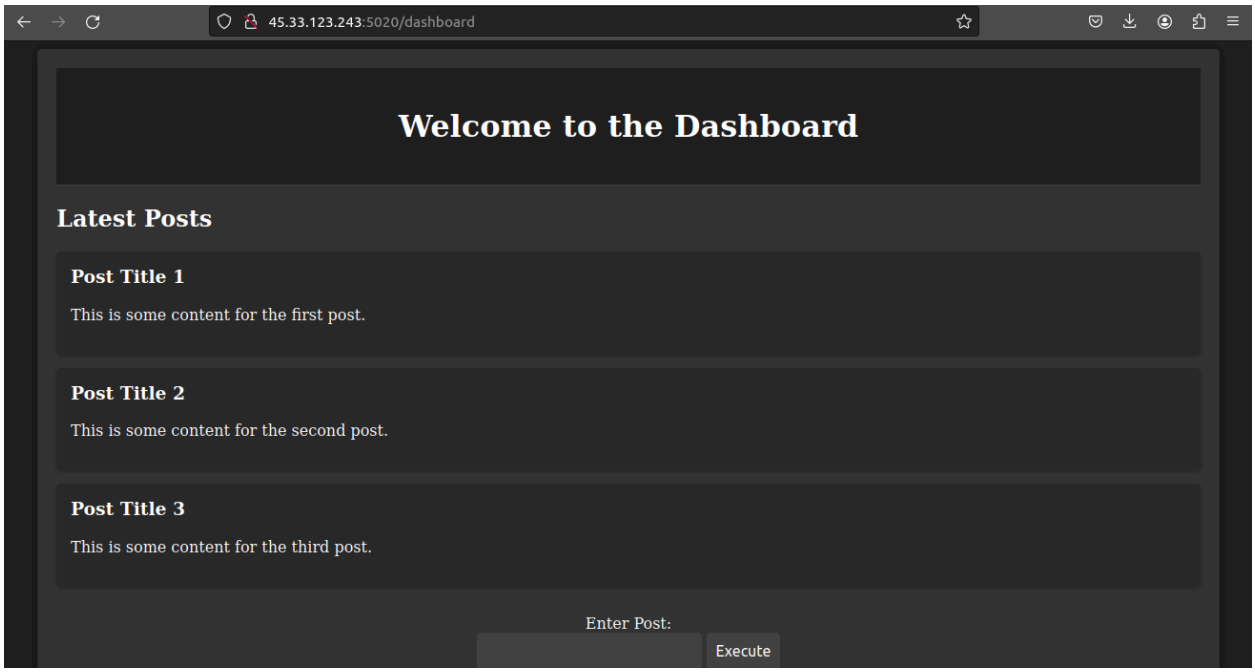


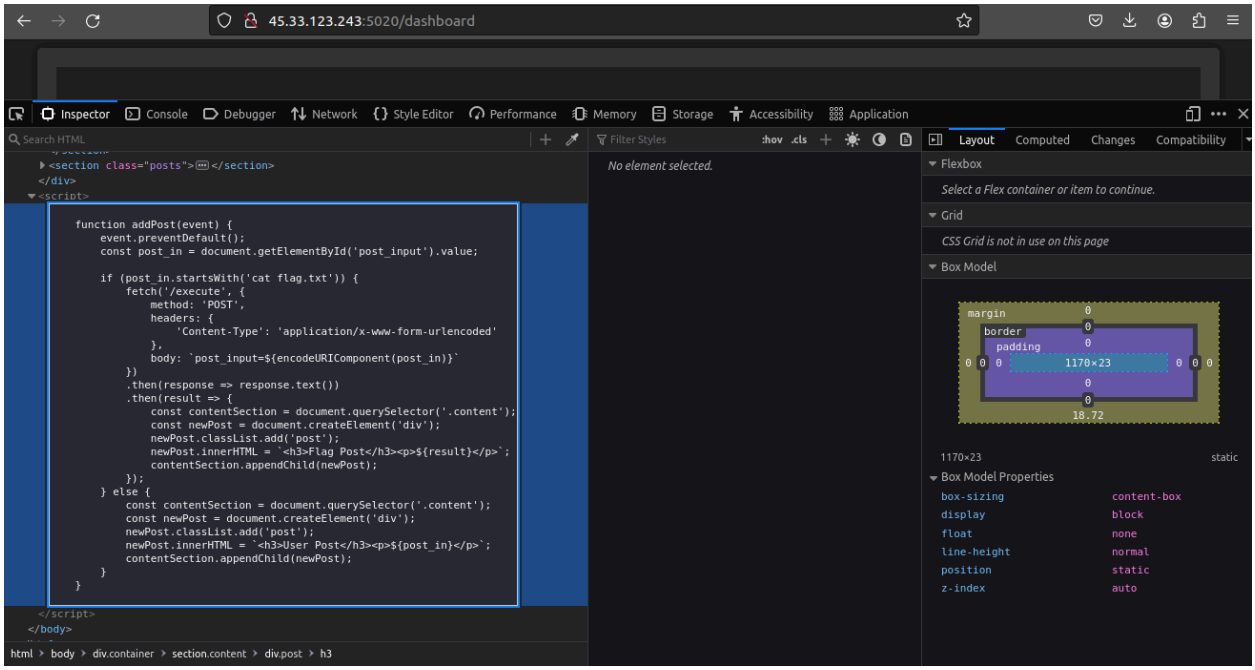


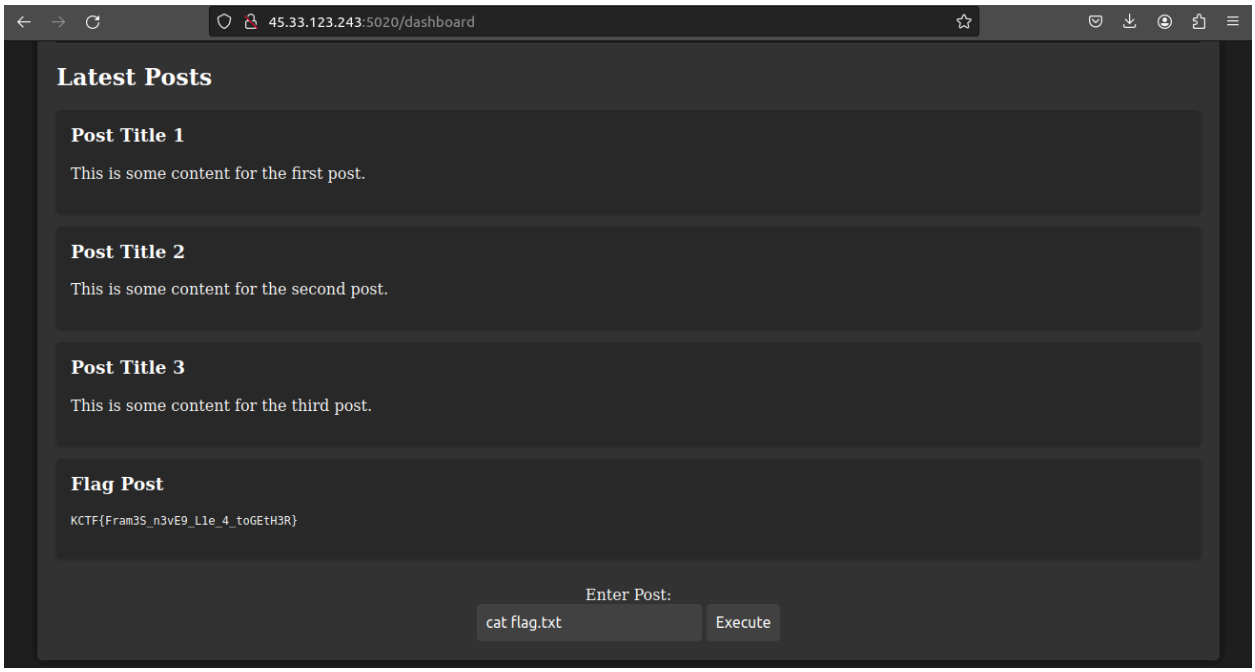
2. **Web-Kitty**

In this problem the username was password was “username” and “password” respectively but I ended up overthinking and trying to find an SQLi vulnerability which it did have in the password field. But that was unnecessary due to the most secure username and password being assigned here.







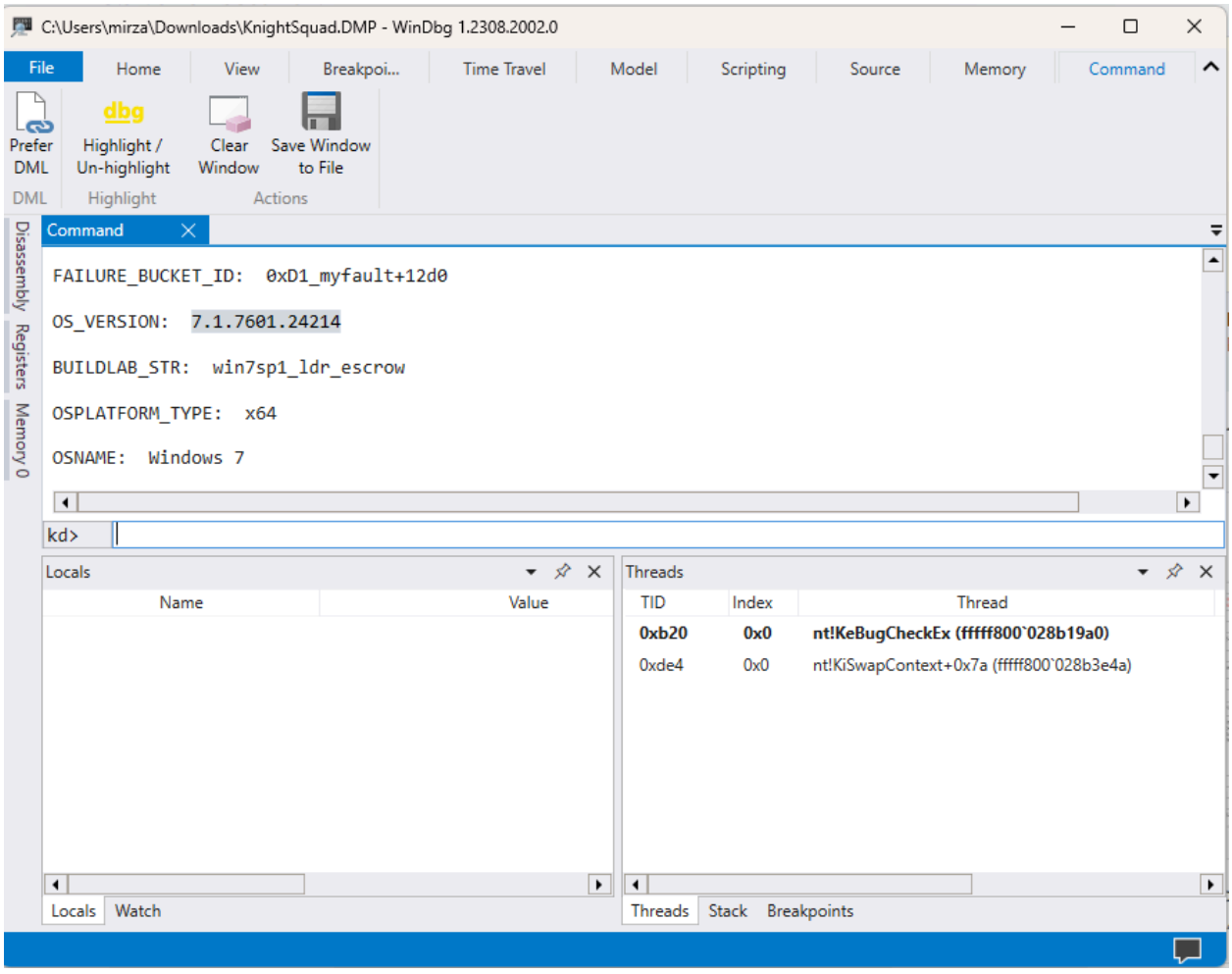


Upon entering the dashboard I tried to inspect the contents upon which I came across a script tag and within that tag we had JS which if we entered cat flag.txt the post retrieved the flag as per the script which checks if the post starts with flag.txt

3. Digital Forensics-OS

   I used the tool Windbg, all I had to do was take the crash memory dump and open it in the windbg application and then executed he command **!analyze -v**. This gives us the OS version that being in this case the flag which can be written as

KCTF{7.1.7601.24214} as per the flag format specified in the question



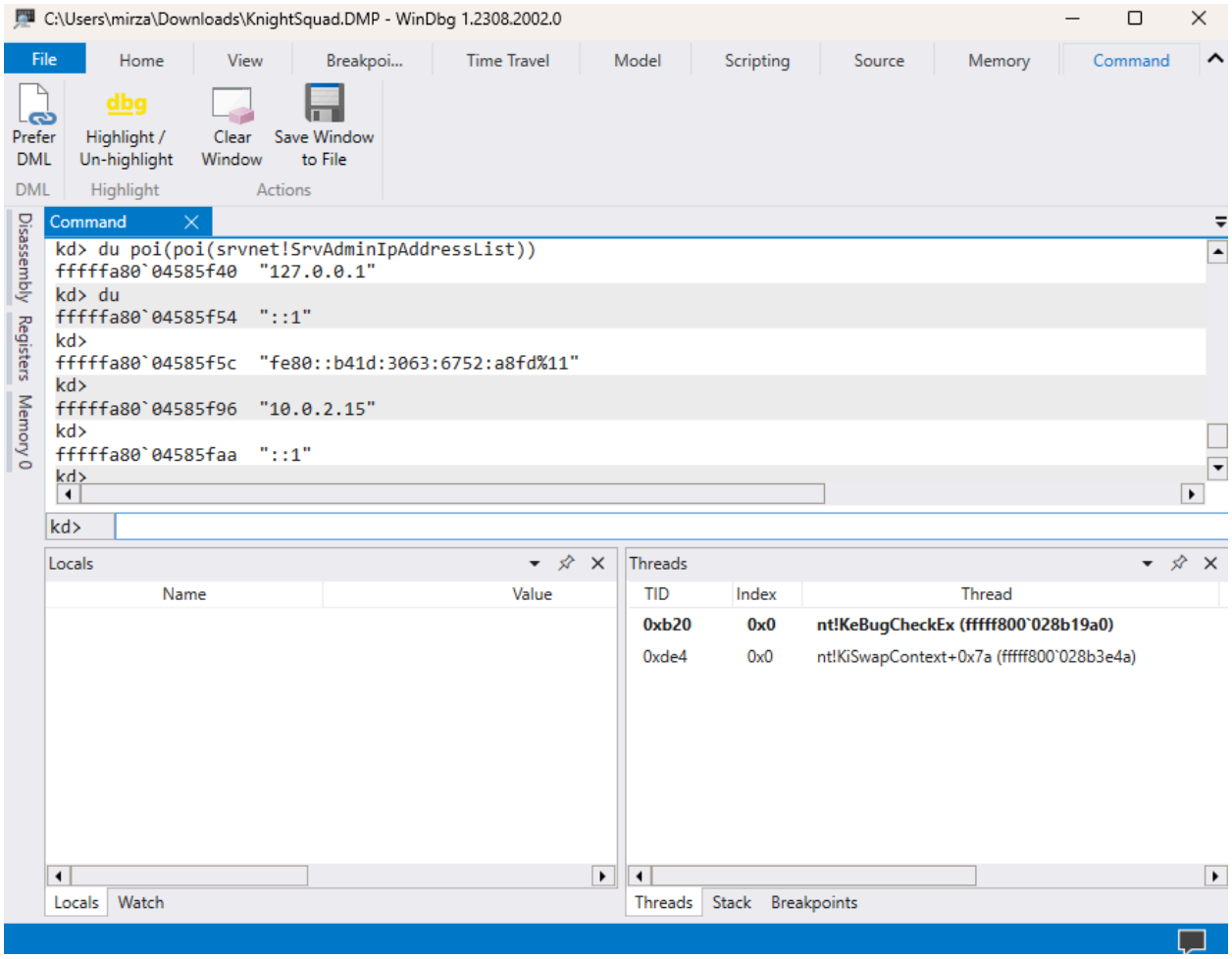
4. Digital Forensics-IP Addr
   I followed this tutorial to find the IP address using windbg

Bruce_Dang Member - All Emails
Posts: **8**
October 2011

here you go:

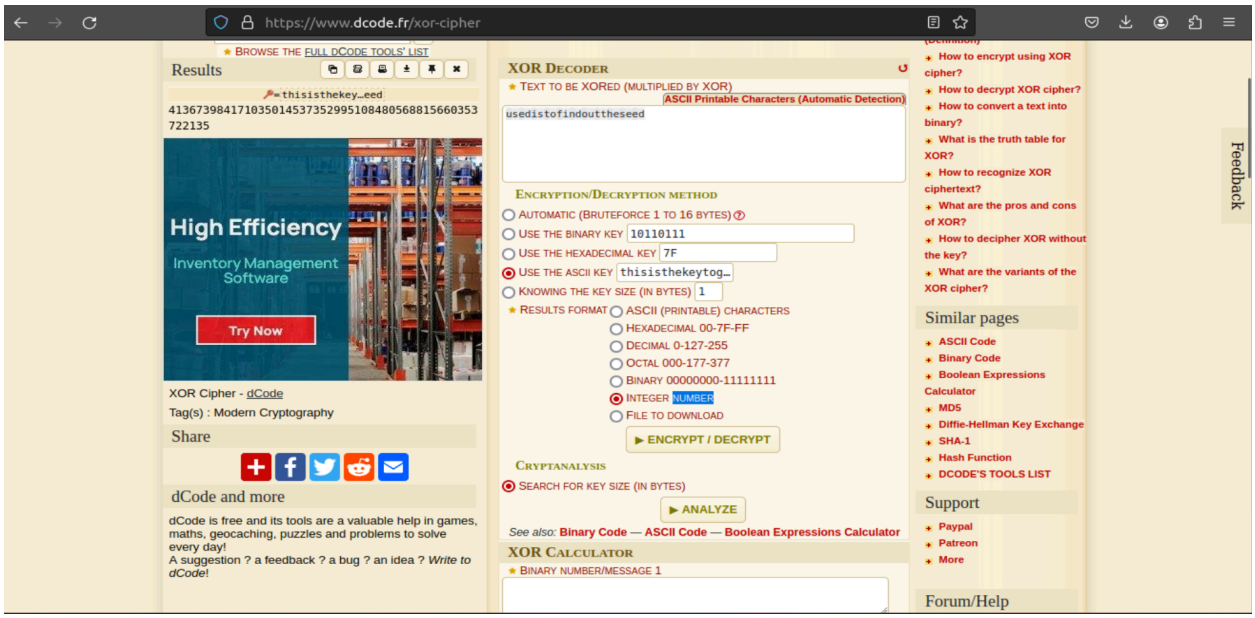
```
2: kd> x srvnet!SrvAdminIpAddressList
81fb06b8 srvnet!SrvAdminIpAddressList = <no type information>
2: kd> du poi(poi(srvnet!SrvAdminIpAddressList))
85c52090 "127.0.0.1"
2: kd> du
85c520a4 "::1"
2: kd>
85c520ac "192.168.47.132"
```

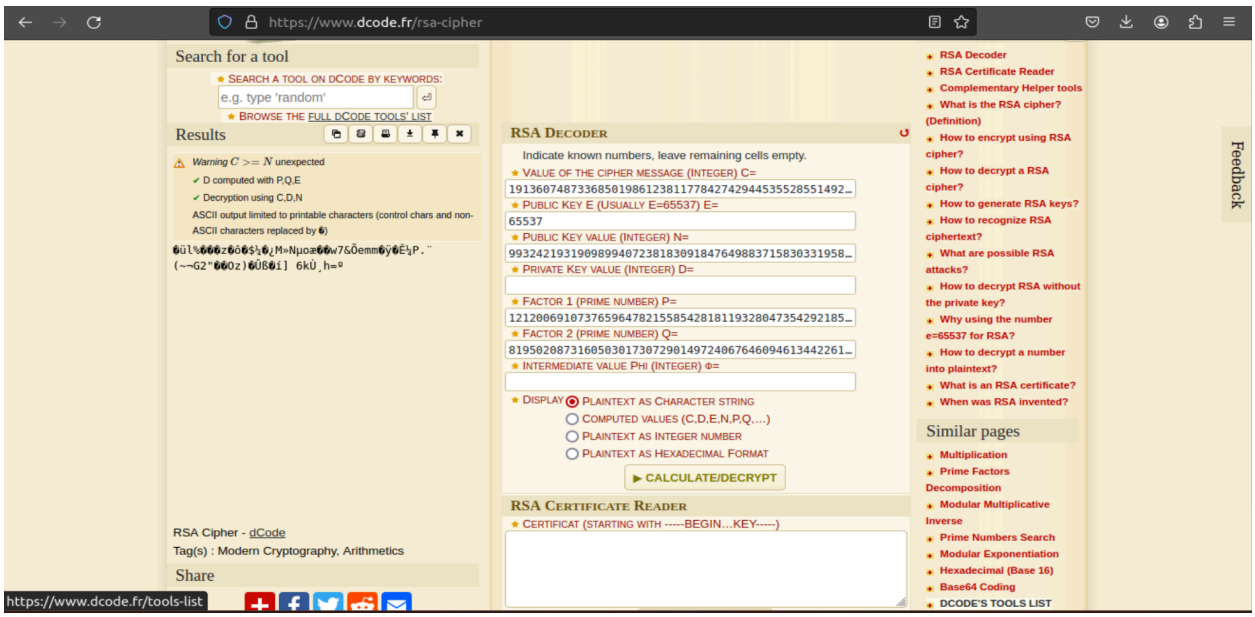
The link is given here:
https://community.osr.com/discussion/214844/how-to-get-ip-address-in-windbg



5. **Attempted Random Shamir Adleman from Cryptography**

In this problem I had the q value and the default e value along with the hint being Axe-Or which hints towards xor cipher. So I tried feeding the results to dcode.fr
I obtained a value for the seed, but the p value was a 256 bit prime number so I tried to generate a 256 bit number using hashlib and secrets in python alongside the seed that I obtained but the numbers I generated could not be used to get a proper ASCII representation as outlined in the screenshots below. As per the logic of RSA encryption I computed n as the product of p and q. As well as the phi_n as the product of p-1 and q-1 but still the result was not satisfactory. Some screenshots are provided as evidence. I apologize for not being able to crack this solution.





Being greedy I wanted this 500 to standout but failed miserably and I spent most of my time trying to crack, this but undoubtedly I learnt a lot from this about RSA encryption

algorithms and even managed to write my own python script for encrypting and decrypting RSA by trying out different prime number generated from the seed.