

DEFENCE SPACE CTF-2017

ÇÖZÜMÜ:

İp taraması yaparak başlıyorum işe ve kalinin bağlı olduğu ip yi direk görüyorum.

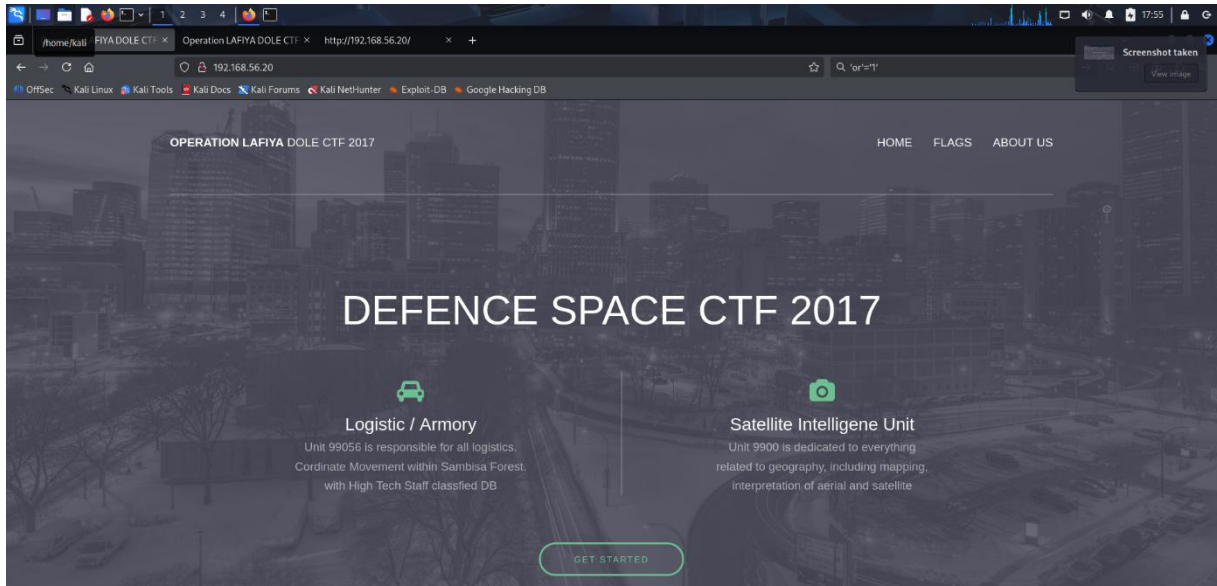
```
root@kali: ~  
Currently scanning: Finished! | Screen View: Unique Hosts  
6 Captured ARP Req/Rep packets, from 3 hosts. Total size: 360  
-----  
IP            At MAC Address  Count  Len  MAC Vendor / Hostname  
-----  
192.168.56.1  0a:00:27:00:00:2d  1      60  Unknown vendor  
192.168.56.28 08:00:27:57:61:ef  4      240 PCS Systemtechnik GmbH  
192.168.56.108 08:00:27:50:0c:51  1      60  PCS Systemtechnik GmbH
```

Daha sonrasında nmap atarak devam ediyorum çünkü hangi ip lerin gerçekten çalıştığını ve açık portlarda hangi servisin çalıştığını görmem gerekiyor.

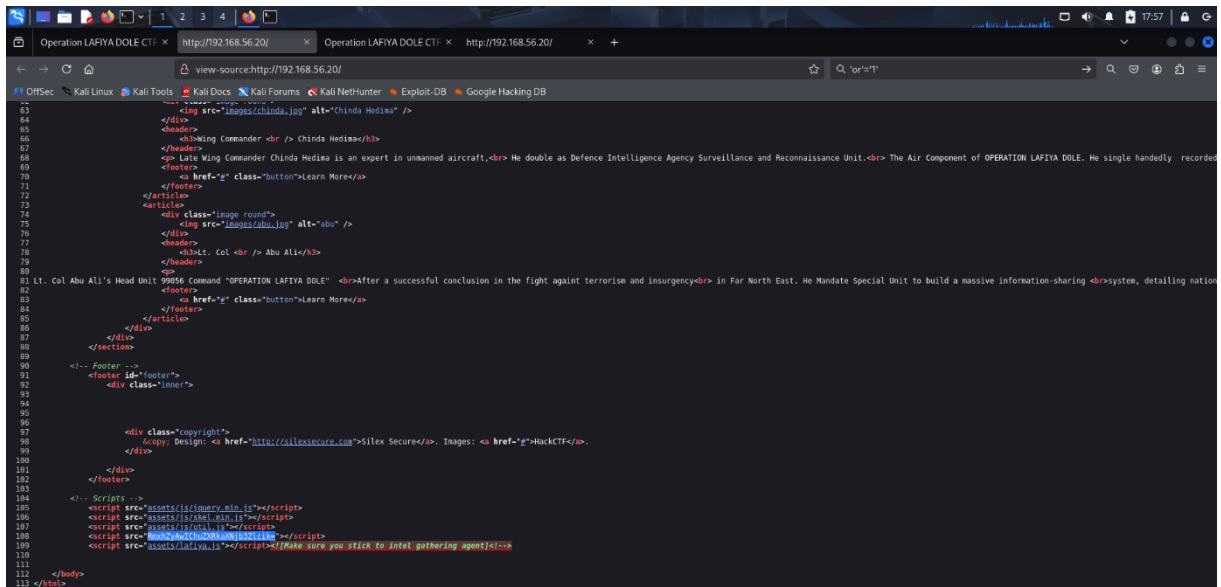
```
root@kali: ~  
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers  
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 88.54% done; ETC: 17:03 (0:00:02 remaining)  
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 88.54% done; ETC: 17:03 (0:00:02 remaining)  
Stats: 0:00:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 94.95% done; ETC: 17:03 (0:00:01 remaining)  
Stats: 0:00:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 97.24% done; ETC: 17:03 (0:00:00 remaining)  
Stats: 0:00:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 98.21% done; ETC: 17:03 (0:00:00 remaining)  
Stats: 0:00:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 99.45% done; ETC: 17:03 (0:00:00 remaining)  
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 58.00% done; ETC: 17:04 (0:00:06 remaining)  
Nmap scan report for 192.168.56.28  
Host is up (0.007s latency).  
Not shown: 65532 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
80/tcp    open  http  Apache httpd 2.4.18 ((Ubuntu))  
|_ http-title: Operation LAPTYA DOLE CTF 2017 - INFILTRATE THE OPERATION COMM ...  
|_ http-server-header: Apache/2.4.18 (Ubuntu)  
443/tcp   open  ssl/http Apache httpd 2.4.18 ((Ubuntu))  
|_ http-title: Operation LAPTYA DOLE CTF 2017 - INFILTRATE THE OPERATION COMM ...  
|_ ssl-cert: Subject: commonName=Flag3[19c562a30aeb455d093baf5236f]-[39 39 30]/organizationName=Silex Secure Lab Ltd/stateOrProvinceName=Abuja/countryName=NG  
|_ Not valid before: 2017-01-24T12:54:41  
|_ Not valid after: 2018-01-24T12:54:41  
|_ ssl-date: TLS randomness does not represent time  
|_ tls-alpn:  
|_ http/1.1  
|_ http-server-header: Apache/2.4.18 (Ubuntu)  
2225/tcp  open  ssh      OpenSSH 7.3p1 Ubuntu 1 (Ubuntu Linux; protocol 2.0)  
|_ ssh-hostkey:  
|_ 2048 f6:08:08:c9:4d:18:2d:fde7:88:51:d7:06:57:48:56 (RSA)  
|_ 256 c2:2b:6e:83:8a:00:67:c2:39:62:16:5e:f9:01:ee:fe (ECDSA)  
|_ 256 dc:8f:7f:6e:11:76:35:77:dc:bc:39:28:6d:5b:3f:23 (ED25519)  
MAC Address: 08:00:27:57:61:ef (PCS Systemtechnik/Oracle Virtualbox virtual NIC)  
Device type: general purpose  
Running: Linux 3.x/4.x  
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4  
OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16  
Network Distance: 1 hop  
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
TRACEROUTE  
Hop RTT Address
```

Burda flag3 ü yakalıyorum ve abuali diye bir kahramandan söz edildiğini görüyorum. Bu ismi unutmuyorum. SSH servisinin açık olduğunu da görüyorum. Daha sonrasında ip yi görüyorum

ve bu ip yi tarayıcıya yazıyorum.



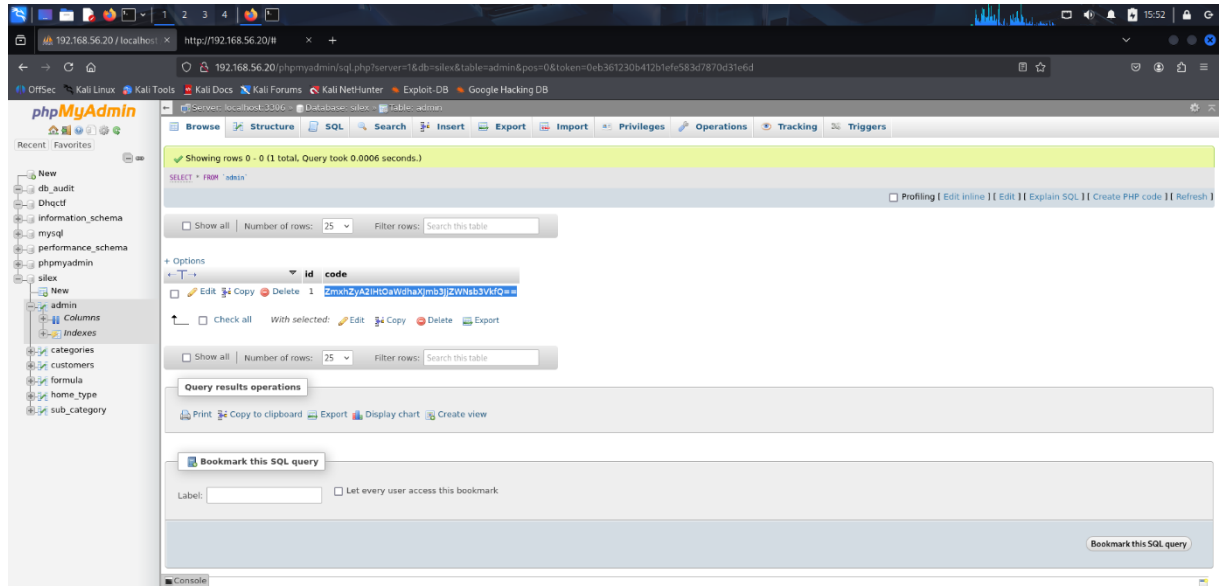
Tarayıcıya yazdıktan sonra ekranı inceliyorum flag sekmesine basıyorum ama hiçbir şey olmuyor. Sonra sayfanın kaynağına gidiyorum.



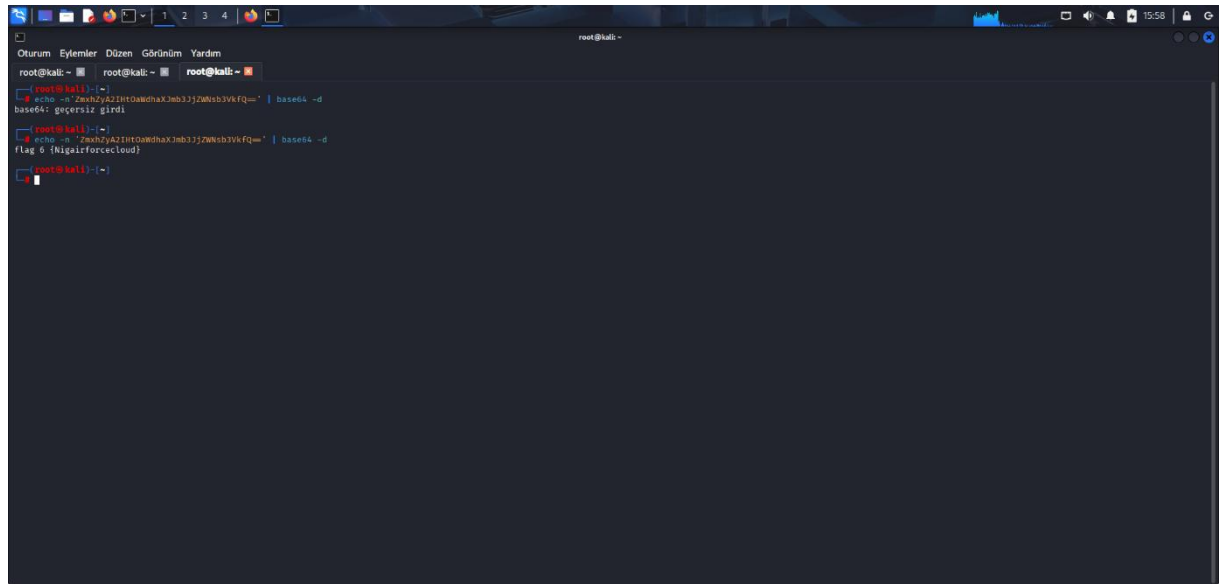
The screenshot shows a web browser window with the address bar displaying '192.168.56.20/assets/'. The website, 'AIRFORCEPORTAL', has a dark theme and a sidebar with navigation links: DASHBOARD, AIR BASE, CONTROL, WIDGETS, JET CHARTS, MENU, and Login Page. The main content area displays a 'Dashboard' with a 'flage 7: 3aa652f41d8b4a23e17937149c784868' and a list of items: 1. Home, 2. Dashboard, 6.674, 7.538, 4.362, 1.426, and WEAPON RELEASE. Below this is a section titled 'NORTHERN NIGERIA : MAIDUGURI SAMBISA FOREST' with a small map icon. On the right side of the browser window, there are three notification popups: 'You have 6 pending letter', 'You have 5 new messages', and 'You have 4 new notifications'. The notifications list various tasks and messages, including 'Shokau location', 'Project 3 Completed', 'Mick appreciated your work Today', and 'Wing Commander Chinda Hedima'.

Flag 7 yi de bulduktan sonra ne yapmam gerektiğini düşünüyorum ve aklıma portswigger da tarayıcıya admin yazmanın bazen işe yaradığı geliyor.Sadece admin işe yaramadı ve biraz

araştırarak phpmyadmin yazmam gerektiğini görüyorum ve ekliyorum.

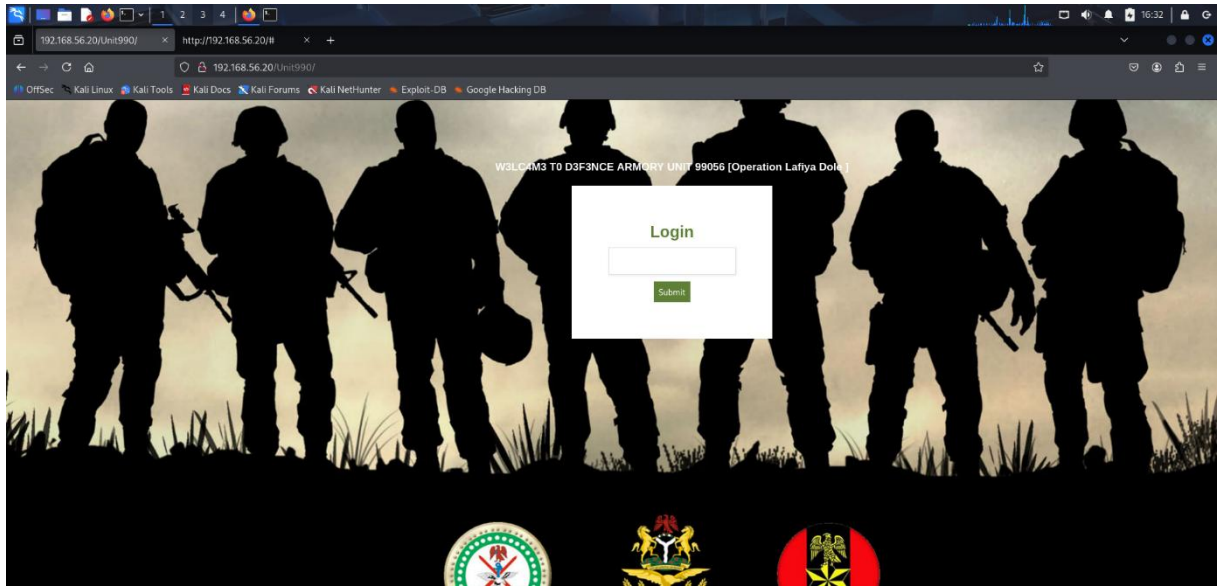


Bu sayfaya girmeye çalışırken benden şifre istiyor ve afallıyorum sonra chatgpt den bu gibi lablarda hazır şifreler kullanıldığını öğreniyorum ve bu şifreleri deniyorum. Root & root işe yarıyor ve sayfaya erişiyorum. Bu sayfayı dolanıyorum ve silex in altında admin diye bir şey var ona tıklıyorum. Burda yine bir yazı var ve bunu decode ediyorum.

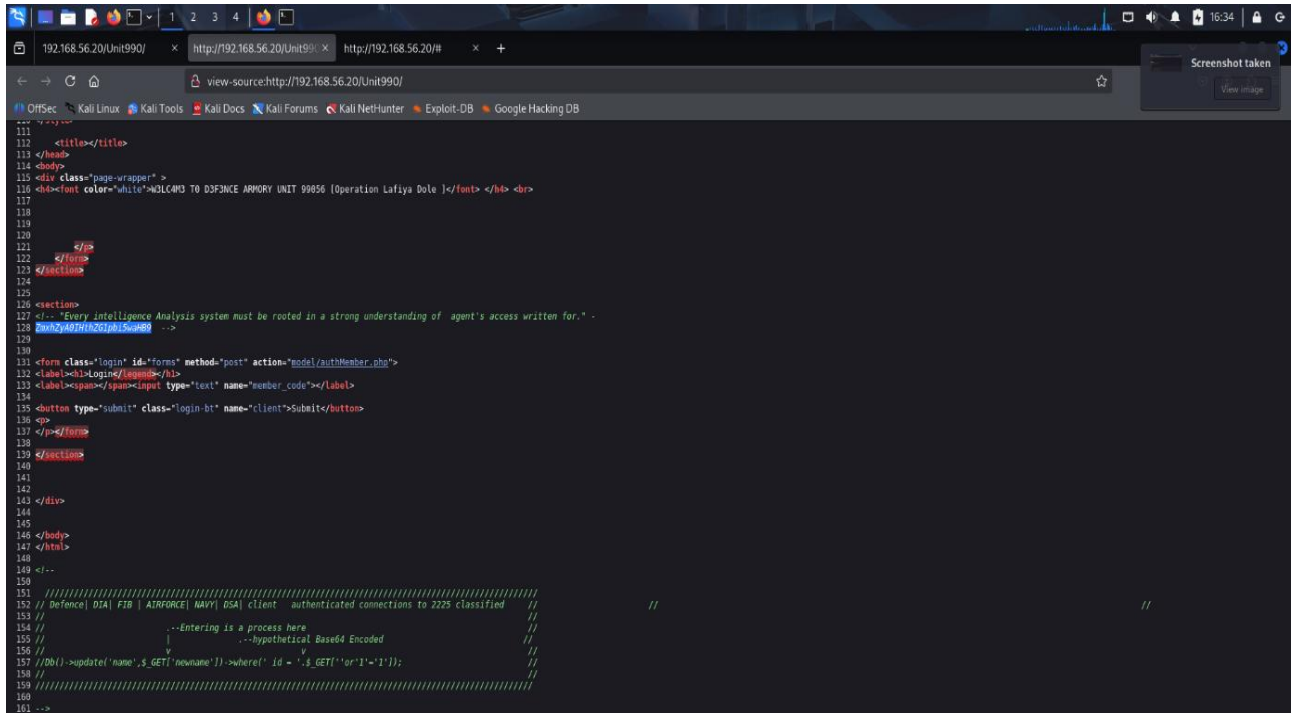


Flag 6 yı da buldum. Bir sonraki adım için yine admin sayfasını kurcaladım ama bir şey bulamadım orada. Sonraki adım için araştırma yapıyorum ve flag3 ü decode etmenin işe yarayacağını görüyorum MD5 olduğunu görüyorum. Ama flag3 ün içindeki striing 27 haneli ve ben decode etmeye çalıştıkça olmuyor sebebini araştırırken bunu Author's Walkthrough da bulurum bunun anlamı unity demekmiş. Yanında ki sayıları da hex ediyorum ordan da 990

sayısına ulaşıyorum ve bunları birleştirip tarayıcıya yazıyorum.



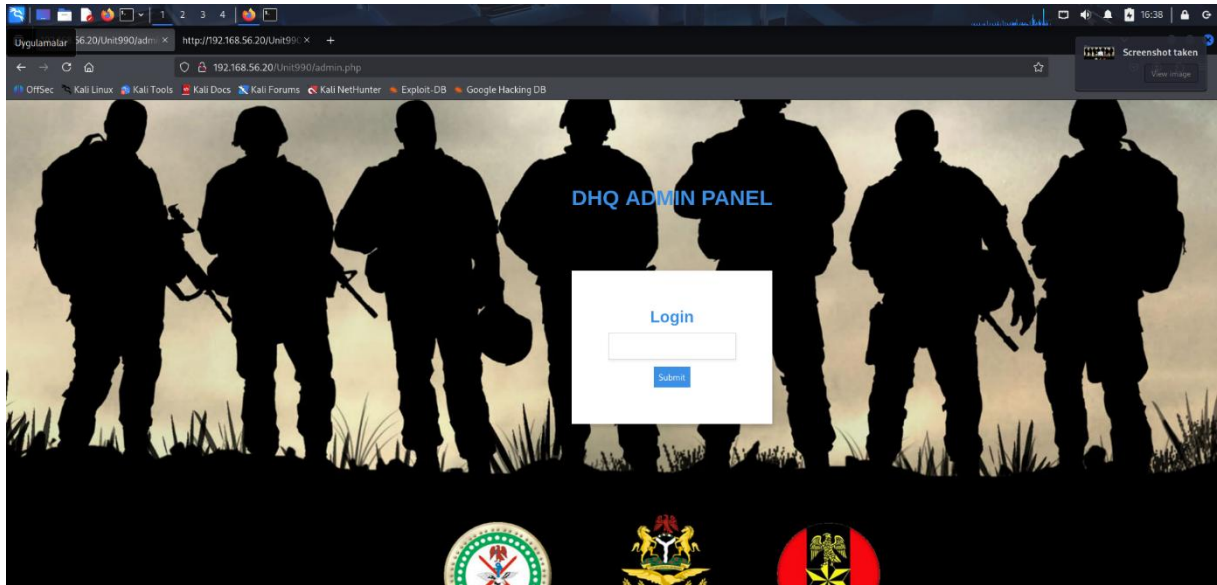
Beni böyle bir sayfaya atıyor ve direk kaynak incelemesi yapıyorum.



Burda yine bir yazı görüyorum ve decode ediyorum. Bu arada aşağıda bir SQL injection kodu görüyorum ve aklımda tutuyorum çünkü onu deneyeceğim.

```
root@kali: ~  
(root@kali) ~  
echo -n "Flag519c562a36aeb4550e93b4f5236f" | base64 -d  
Vee_1E40uyy0uc+++  
(root@kali) ~  
echo -n "Zash7y48Irh2G1pb1swaH9" | base64 -d  
flag 4 {admin.php}  
(root@kali) ~
```

Flag 4 ü de bulmuş oldum. Adının admin.php i olması ilgimi çekti ve hemen tarayıcıya admin.php yi ekledim.



The screenshot shows a web browser window with three tabs open: "http://192.168.56.20/Unit990/admin...", "http://192.168.56.20/Unit990...", and "http://192.168.56.20/Unit990...". The active tab displays the source code of the page at "view-source:http://192.168.56.20/Unit990/admin.php".

The source code is as follows:

```

112 transition: 0.3s;
113 }
114 }
115 </style>
116
117 <title></title>
118 </head>
119 <body>
120 <div class="page-wrapper">
121 <div>
122 <h1> DMO ADMIN PANEL</h1>
123
124 <!--
125
126
127 ////////////////////////////////////////////////////
128 // update() sets the value of a column given a condition //
129 // //////////////////////////////////////////////////// //
130 // --escaping is automatic here //
131 // | --hypothetical: mysql_query("update users set //
132 // | // //
133 // | // //
134 // | // //
135 // | // //
136 // | // //
137 -->
138 </div>
139 </form>
140 </section>
141
142
143 <section>
144
145 <form class="login" id="form" method="post" action="model/authenticate.php">
146 <label><h3>Login/Register</h3>
147 <label><span></span><input type="password" name="admin_code"></label>
148
149 <button type="submit" class="login-bit" name="admin">Submit</button>
150 </div>
151 </div>
152 </form>
153 </section>
154
155
156 </div>
157
158
159
160 </body>
161 </html>
162

```

root@kali: ~

```

root@kali:~$ echo -n 'flag19c562a36aeb655d93b4f5236f' | base64 -d
19c562a36aeb655d93b4f5236f
root@kali:~$ echo -n 'RmshZpAB7HhZG1pb1swaH89' | base64 -d
RmshZpAB7HhZG1pb1swaH89
root@kali:~$ echo -n 'RmshZpA1HTTUlgaw7qZWbaw9ufq=' | base64 -d
RmshZpA1HTTUlgaw7qZWbaw9ufq=

```

Firefox ESR
Browse the World Wide Web

Yardm

root@kali:~

Screenshot taken
View image

Screenshot taken
View image

The screenshot shows a terminal window with the following content:

```

root@kali: ~
root@kali:~# ssh abulid192.168.56.20 -p 2225
The authenticity of host '[192.168.56.20]:2225 ([192.168.56.20]:2225)' can't be established.
ID25519 key fingerprint is SHA256:ztodr8jtyII6Fek/EvqbIV2dAgLn5P00rP5253gQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.56.20]:2225' (ID25519) to the list of known hosts.
=====
WARNING
DISCONNECT: DSS-MIG DIA-MIG - Authorized Access Only!
Disconnect IMMEDIATELY if you are not an authorized User in Operation Lafia Dole
All actions Will be Closely Monitored and Recorded by Can7
FlagsB[33cd2eb3f6d416f331de9102eb997]
=====
abulid192.168.56.20's password:

```

Öncelikle gerçekten çok güzel bir lab olmuş beni çok heyecanlandırdı ve sürükledi ki 3 günde uzun saatler harcadım bu lab için. En sonunda bitirdim. Nasıl yaptığıma gelirse kurulumu tamamladıktan sonra bu tarz lablara ilk defa başladığım ve ilk defa gördüğüm için önce bu tarz CTF lerin nasıl çözüldüğünü öğrenmek için başka CTF lerin çözümlerini bulup inceledim ve kafamda artık bir mantık oturdu. En azından nereden başlayacağımı görmüş oldum. Başladıktan sonra daha keyifli ve heyecan verici bir oyuna dönüştü sanki benim için. Bazı yerlerde çok takıldım çünkü ilk deneyim olduğu için ilerlemekte güçlük çektim. Mesela flag3 ü decode etmek çok zordu bir türlü olmuyordu ama onun farklı bir olayı varmış bunu uğraştıktan sonra öğrendim. Bazı yerlerde çok oyalandım çünkü belki bir şey çıkar düşüncesindeydim ama bu lab da hiç aynı yerde 2 tane flag elde edemedim. Yardım aldığım almam gereken yerler oldu ama elimden geldiğince inat edip yardım almamaya çalıştım ve

çoğu flag i böyle buldum. Bu dosyayı da tamamen kendi düşüncelerim ve nasıl ilerlediğimi hatırlayarak yazdım herhangi bir yerden alıntı asla yapmadım. Başlangıç için süper bir labdı.