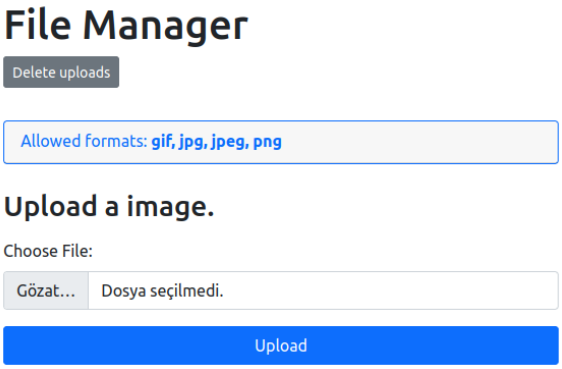
# FİLE UPLOAD

## 3.2 File Extension Filter Bypass

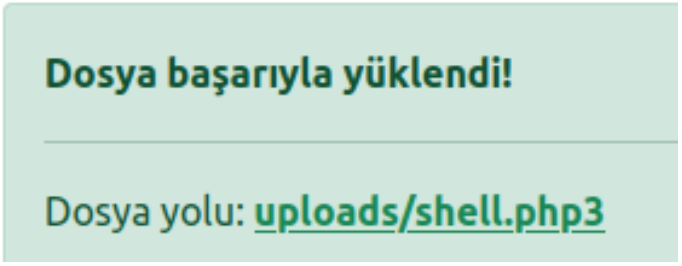
Bu zafiyetimizin bypass yeri dosyanın uzantısı olucak. Ancak edindiğimiz bilgiye göre blacklist kullanılıyor yani bazı uzantılar direkt olarak yasaklı bunu aldatmamız gerekiyor.



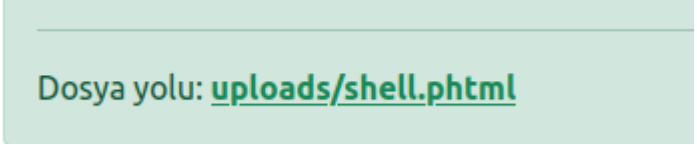

Bu bypass metodunda çok fazla faktörler vardır hepsini basitten zora doğru sıralayıp olana kadar yapalım.

Öncelikle uzantıların sonuna sayılar ekliyebiliyoruz yani;
php2 php3 php4 gibi uzantılar verebilir.
Bir diğer yöntem ise uzantı ismi sırası;
.png.php ile aldatabiliriz.
Eğer ilk uzantıya bakıyorsa noktadan anlayıp yani illa png sonda olsun diyorsa ;
.php%20.png diyebilririz bu .php den sonrasını yorum satırına almak içindi veya yanlış hatırlamıyorsam %00.

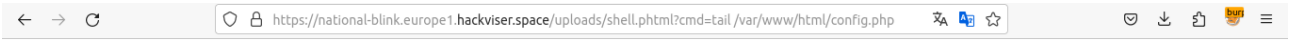
Sayılardan başlayalım




Şahsen bende pek beklemiyordum son File Upload sorusu olduğundan ötürü :) Hemen sorumuza gidelim dicektim ki komutlarımızı çalştıramıyoruz resim düzgün yüklenemedi hatası alıyorum farklı yollar arayalım
.phtml deniyorum




Ve başarıyla yüklüyoruz.Ve hemen soruyu cevaplıyorum;




$db_name = 'hv_database'; $karakter kümesi = 'utf8'; $kullanıcıadı = 'kök'; $şifre = 'Qr3eydwjjZmPpwVm'; $db = new PDO("mysql:host=$host;dbname=$db_name; charset=$charset",$username,$password); } catch(PDOException $e){ } ?>

**Soru:** **"config.php" dosyasındaki veritabanı şifresi nedir?**
**Cevap:** **Qr3eydwjjZmPpwVm**