

# RESTAURANT UYGULAMASI ZAFİYETLERİ

## 1-Unrestricted File Upload (Sınırsız Dosya Yükleme)

Kayıt olurken firma eklerken vb resim yüklenen yerlerde yeterli bir kısıtlama olmadığından kaynaklı php dosyaları da yükleyip Shell çalıştırabiliyoruz

### Profil

 Profil Resmi

Ad: sefa

Soyad: sefa

Kullanıcı Adı: sefa

Bakiye: 5000

Kayıt Tarihi: 2024-10-04 08:26:15

[Şifreyi Güncelle](#) [Profili Güncelle](#) [Bakiye Ekle](#) [Ana Sayfa](#)

POWERCATALYTIC

```
www.data@ecba58ec41:~/uploads/users# cd
```

```
www.data@ecba58ec41:~/uploads/users# ls
```

```
1727809626.png  
1727558360.png  
1727558368.png  
1727558674.png  
1727558720.png  
1727558845.png  
1727558848.png  
1727558895.png  
1727558897.jpg  
1727558988.png  
1727558989.png  
1727558990.png  
1727558999.jpg  
1728830374.php  
1728830525.php
```

```
www.data@ecba58ec41:~/uploads/users#
```

Zafiyet kritik bir zafiyet olduđu için Shell i çalıştırdıktan sonra yetki yükseltme ile istenilen yapılabilir buradan sonrası zafiyet bulan kişinin hayal gücüne kalıyor

Çözümü için sisteme yüklenen dosyaların uzantılarının whitelist blacklist gibi kontroller ile kısıtlama yapılabilir.

CVSS Skoru :7.5 – 9.0