

Tier 0 - Preignition

In this lab, we gain access to a poorly configured Word Press to retrieve the flag. We do this by brute forcing directories on the target web server using GoBuster.

Enumeration

The first move we make is pinging the target to check if its online and reachable.

```
└─ [★]$ ping 10.129.90.75
PING 10.129.90.75 (10.129.90.75) 56(84) bytes of data.
64 bytes from 10.129.90.75: icmp_seq=1 ttl=63 time=78.7 ms
64 bytes from 10.129.90.75: icmp_seq=2 ttl=63 time=78.5 ms
64 bytes from 10.129.90.75: icmp_seq=3 ttl=63 time=78.5 ms
64 bytes from 10.129.90.75: icmp_seq=4 ttl=63 time=78.7 ms
64 bytes from 10.129.90.75: icmp_seq=5 ttl=63 time=78.5 ms
64 bytes from 10.129.90.75: icmp_seq=6 ttl=63 time=78.6 ms
^C64 bytes from 10.129.90.75: icmp_seq=7 ttl=63 time=78.6 ms
64 bytes from 10.129.90.75: icmp_seq=8 ttl=63 time=78.7 ms
^C
--- 10.129.90.75 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7012ms
rtt min/avg/max/mdev = 78.474/78.596/78.737/0.101 ms
```

After we have confirmed its reachable we do an nmap scan.

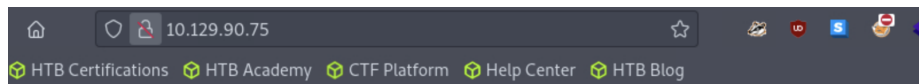
```
sudo nmap -sV {Target_IP}
```

```
└─ [★]$ sudo nmap -sV 10.129.90.75
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-05 02:02 BST
Nmap scan report for 10.129.90.75
Host is up (0.098s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx 1.14.2

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.98 seconds
```

We see that port 80/HTTP is open.

Inputing the target ip into our search engine of choice we see this page.



Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

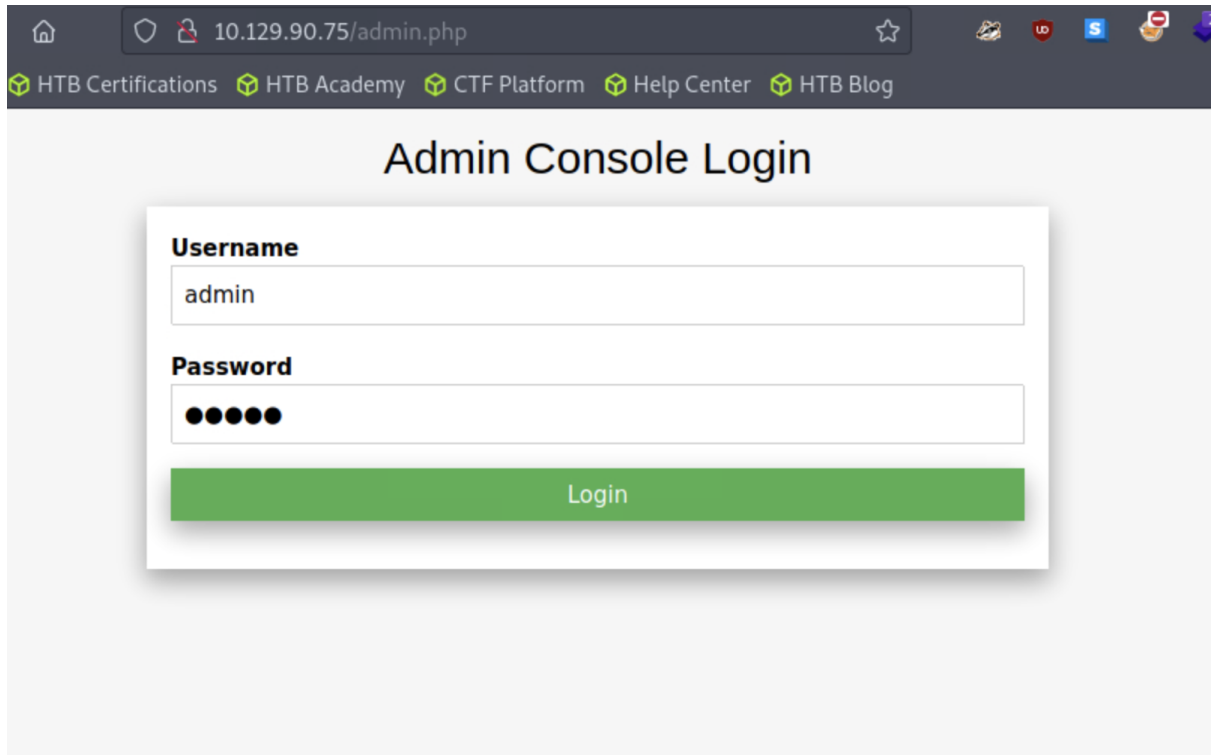
This leads us to a web server. Using GoBuster we will enumerate directories using a wordlist.

```
sudo gobuster dir -w /usr/share/wordlists/dirb/common.txt -u
```

```
[*]$ sudo gobuster dir -w /usr/share/wordlists/dirb/common.txt -u 10.129.90.75
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.129.90.75
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s
=====
2024/04/05 02:20:58 Starting gobuster in directory enumeration mode
=====
/admin.php (Status: 200) [Size: 999]
=====
2024/04/05 02:21:35 Finished
=====
```

We have enumerated the directory and have found a /admin.php directory.

Inputting that into our search engine we are prompted with a login page. Using admin,admin as login



10.129.90.75/admin.php

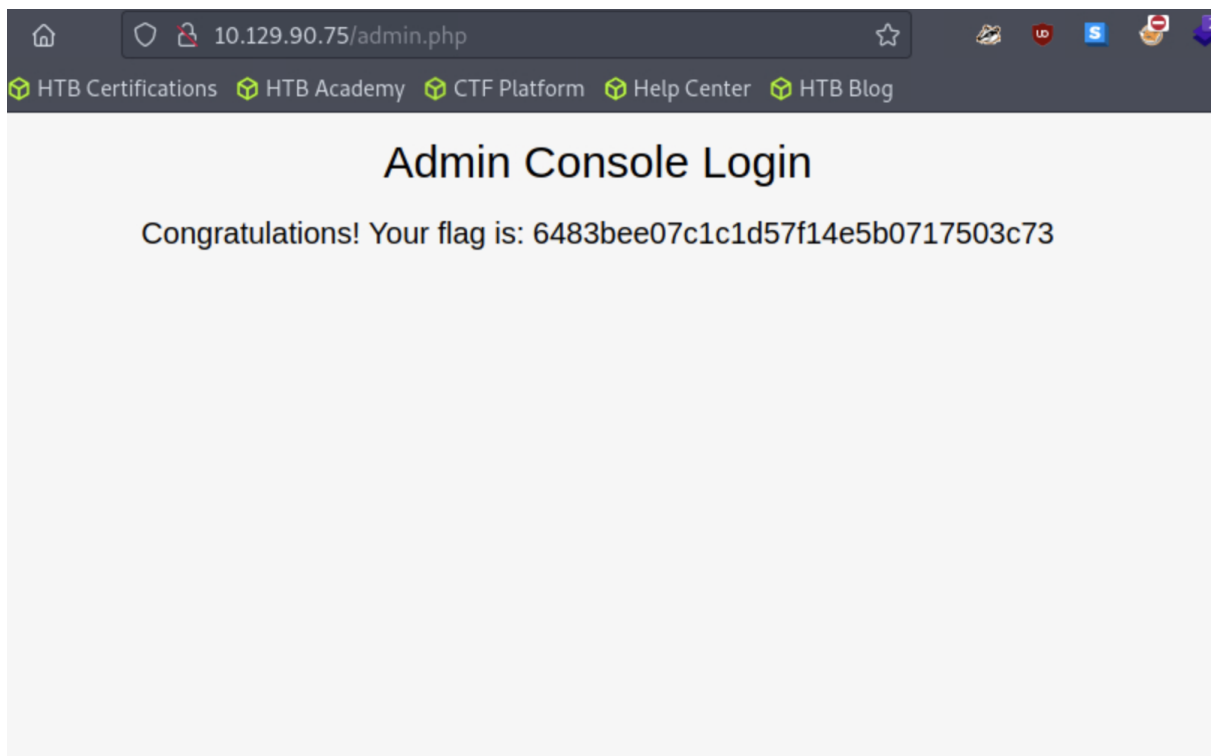
HTB Certifications HTB Academy CTF Platform Help Center HTB Blog

Admin Console Login

Username

Password

Login



10.129.90.75/admin.php

HTB Certifications HTB Academy CTF Platform Help Center HTB Blog

Admin Console Login

Congratulations! Your flag is: 6483bee07c1c1d57f14e5b0717503c73

After a successful login we have retrieved the flag.