Keeper			
Organization: Hack The Box		Type: online CTF	
Categories:	☐ Network Security ☑ Cryptography ☐ Mobile Applications	☐ Reverse Engineering ☑ Web Applications ☐ Forensics	Difficulty: Easy
Name: Kasper Verhulst		Release date: Completing date:14th August 2023	

Scanning & Reconaissance

First, let us start scanning the machine to see which services are running. As usual, let's start by running an nmap command.

```
sudo nmap -A -sS -p1-1024 $BOX_IP -oN nmap.out
```

We find the following services running on the machine:

Port	Service	Version
22/tcp open	SSH	OpenSSH 8.9p1
80/tcp open	HTTP	nginx 1.18.0

We don't find any critical vulnerabilities present in these services.

Let us try to visit the website http://$BOX_IP.

Figure 1: Home page

On the home page, there is only a hyperlink to another page to open a ticket. There is nothing else interesting present in the source code or in the HTTP headers. In order to access tickets.keeper.htb/rt, we will have to add the domain to the `/etc/hosts` file. This page seems to show a login screen to a ticketing system called Request Tracker.

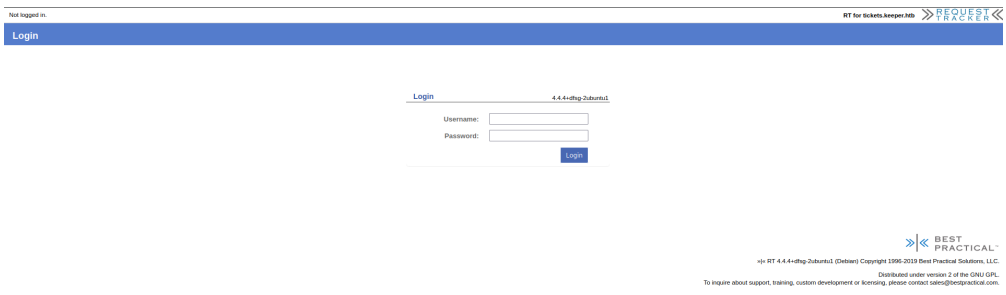

Figure 2: Home page

Before exploring the Request Tracker portal, let us enumerate the web application for more paths or hidden subdomains:

```
gobuster dir -u http://$BOX_IP -x html,py,php -w /usr/share/wordlists/dirb/
    common.txt
```

path	Status code
/index.html	200

```
gobuster vhost -u http://$BOX_IP --append-domain --domain keeper.htb -w /usr/
    share/wordlists/SecLists-master/Discovery/DNS/subdomains-top1million
    -20000.txt
```

domains	Status code
tickets.keeper.htb	200

It seems like there aren't any other web pages available on the web server, so let us try to break into the Request Tracker portal.

Gaining Access

I started by researching for vulnerabilities in the Best Practical Request Tracker v4.4.4. It seems like there are a couple of vulnerabilities like open redirection and XSS, but nothing that will grant us access to the portal. However, we can find the system has a superadmin account with default credentials 'root' and 'password'. It seems like the root password wasn't changed and we can login with the root account. Once logged in to the portal, we can see it is mostly empty, except one ticket and two users. Next to the root user, there is also a user called *lnorgaard*. In the description of that user, we find her password. The *lnorgaard* uses same password for the ticketing system as for her Linux account.

Privilege Escalation

The ticketing system also contains a ticket that explains the root user has an issue with his KeePass Windows client. He stored an export of his KeePass vault together with a Windows dump file in *lnorgaard* home directory. This seems very interesting because a password vault contains all passwords of the user.

After doing some research, I stumbled upon the recent KeePass vulnerability where the master password was stored in cleartext in memory (CVE-2023-32784). The researcher that disclosed the KeePass vulnerability wrote a PoC in .NET that retrieves the vault master password from a memory dump. Since, I was completing the box from a Linux machines, I tried the PoC from `https://github.com/CMEPW/keepass-dump-masterkey` since it is written in Python. The exploit script finds almost the entire vault password apart from a couple of characters. If we google the result we found, it refers to a Danish dessert that is the correct password to open the vault.

```
python3 poc.py -d KeePassDumpFull.dmp
```

In order to interact with the KeePass vault file, we can install a full KeePass client. Yet, I opted to install the KeePass CLI client, *kpcli*. To open the vault with the master password, you need to execute:

```
kpcli --kdb passcodes.kdbx
```

I browsed the vault using *kpcli cd* and *kpcli show* and in the Network Access, I found the putty ppk file to connect to the box as root. Because I don't use putty client, the final step was to transform the putty file into a standard openssh private key. This can be done like:

```
puttygen putty -O private-openssh -o id_rsa
```

Now we can SSH to the box, and find the root flag.

```
ssh root@$BOX_IP -i id_rsa
```