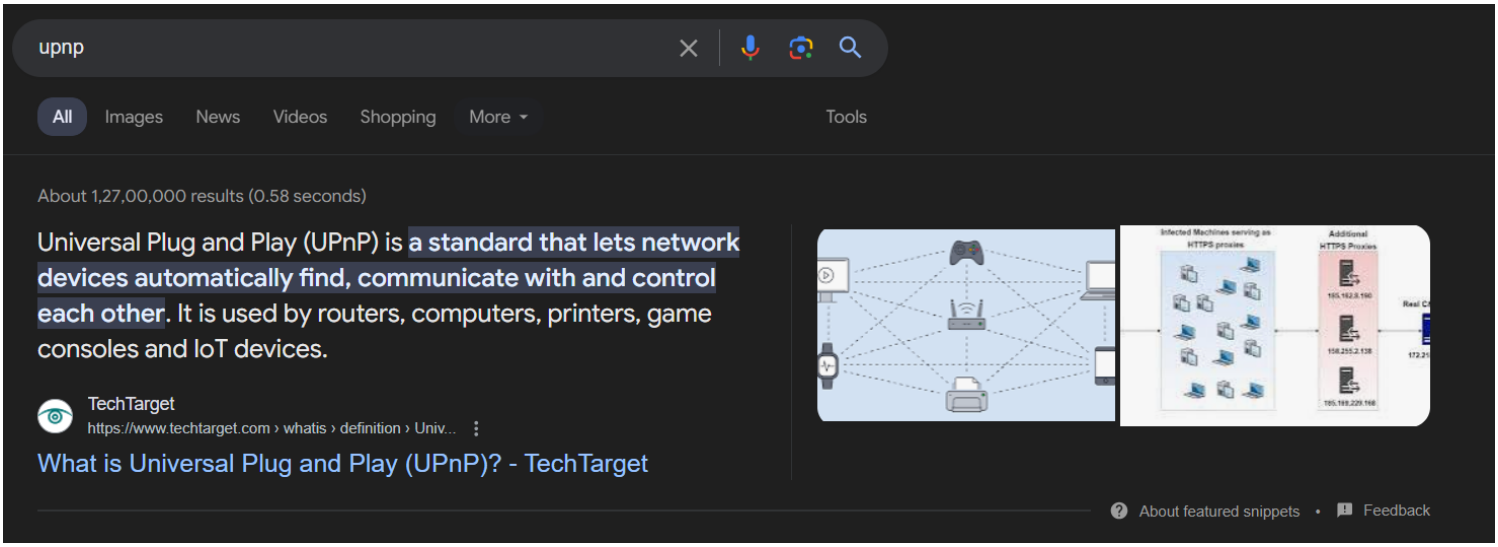
Information Gathering

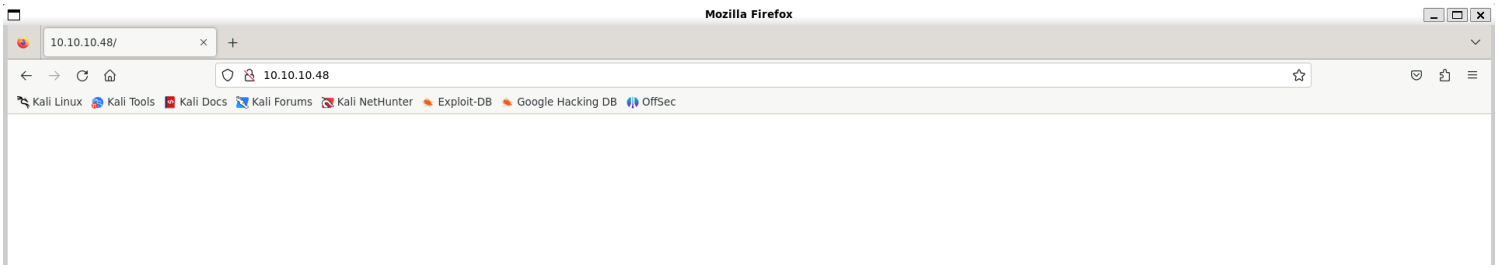
1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~/Pwn/Challenges]
└─$ sudo nmap 10.10.10.48 -p- -sV --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-24 19:36 IST
Nmap scan report for 10.10.10.48
Host is up (0.22s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
53/tcp    open  domain  dnsmasq 2.76
80/tcp    open  http    lighttpd 1.4.35
1364/tcp  open  upnp    Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)
32400/tcp open  http    Plex Media Server httpd
32469/tcp open  upnp    Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 80.19 seconds
```



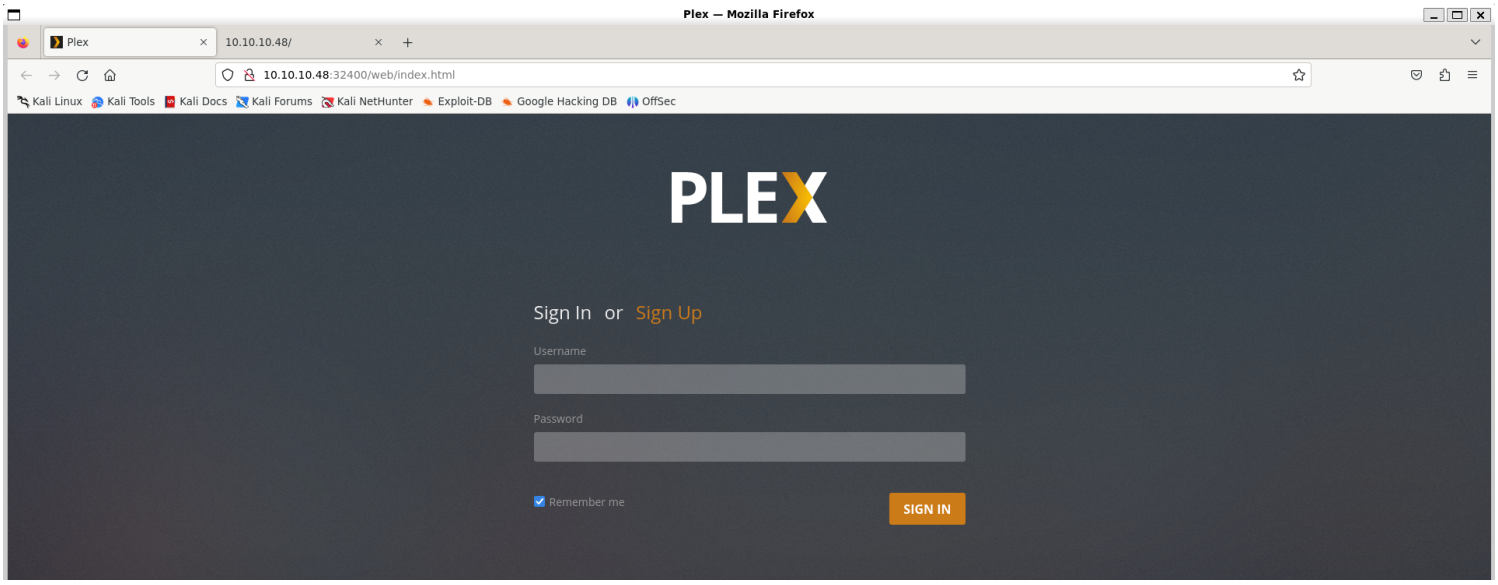
2) Checked the web ports

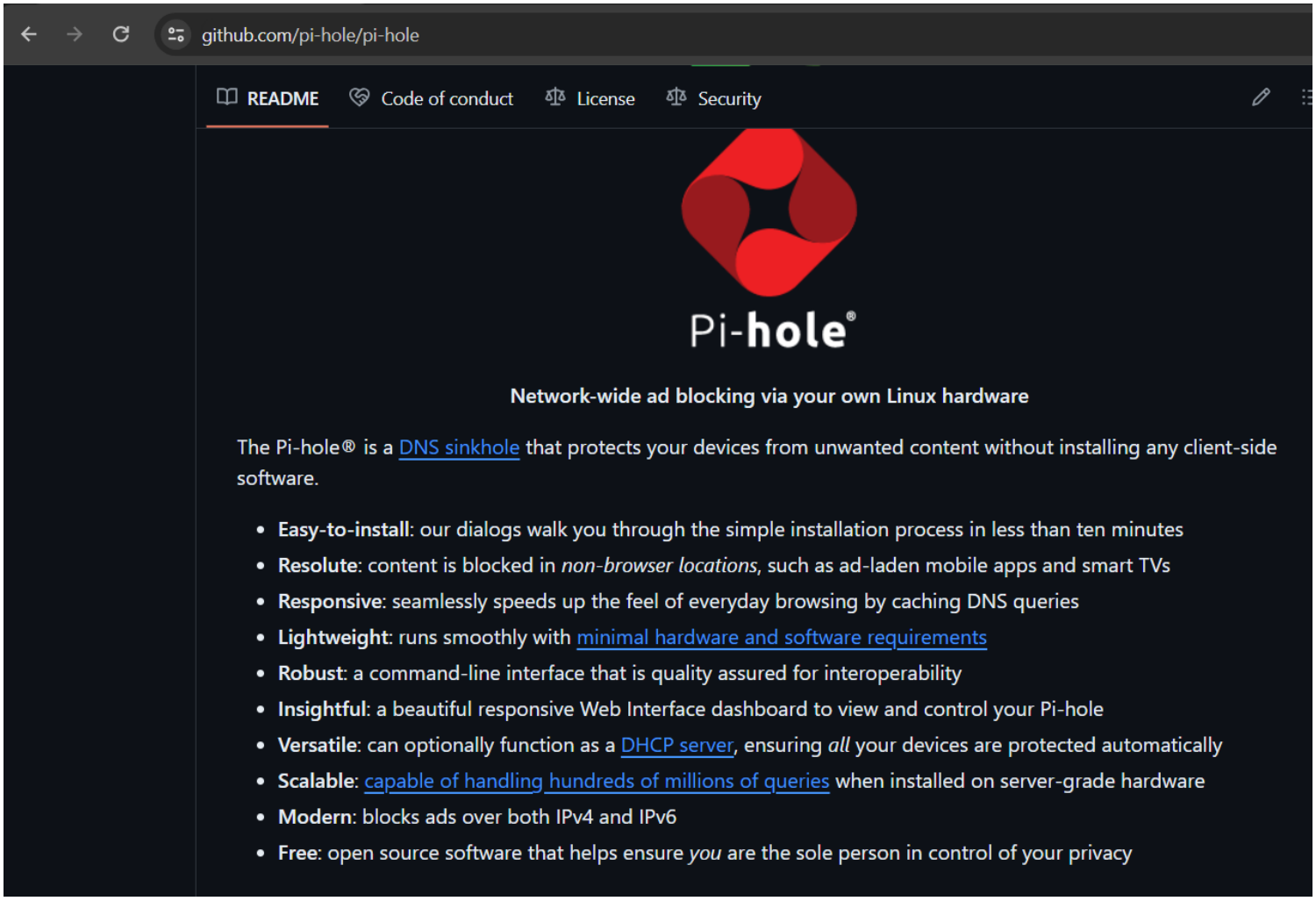


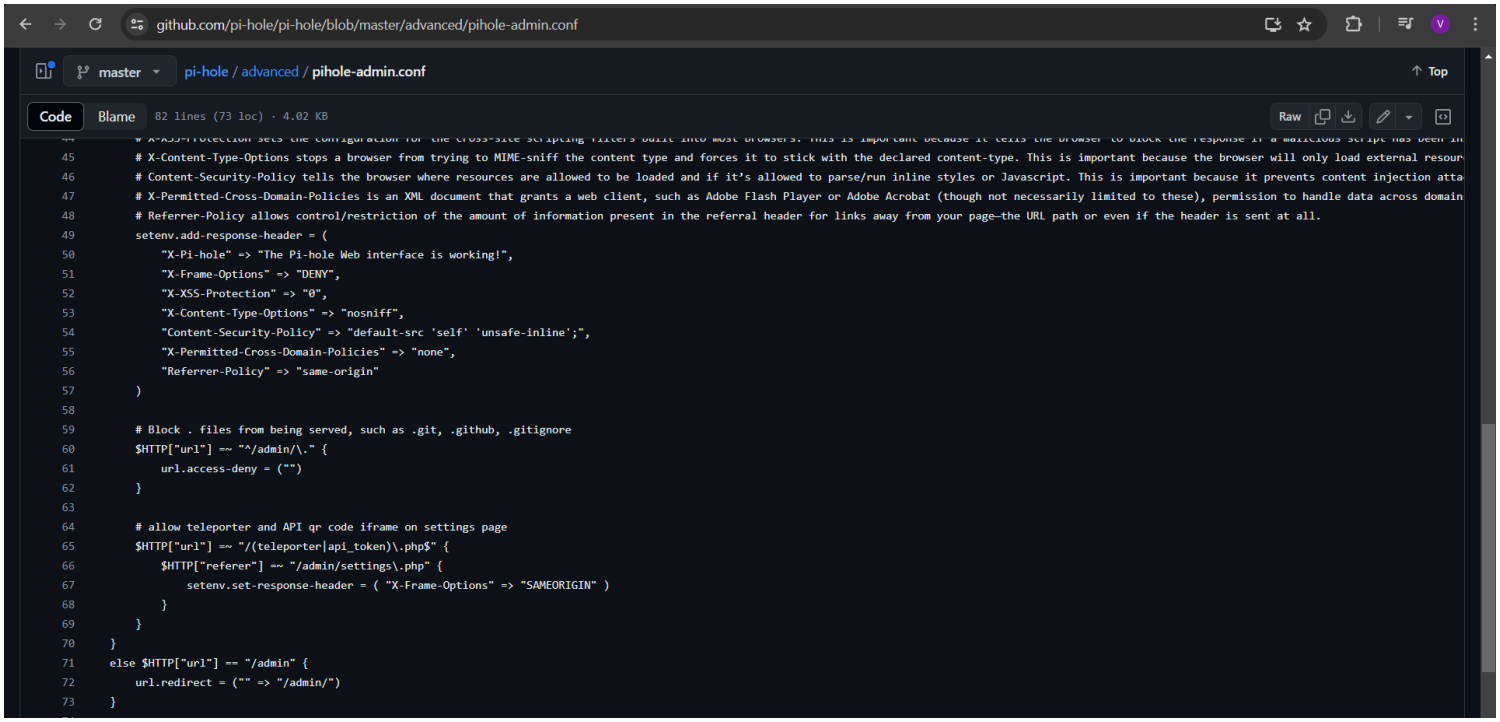
Response

Pretty Raw Hex Render

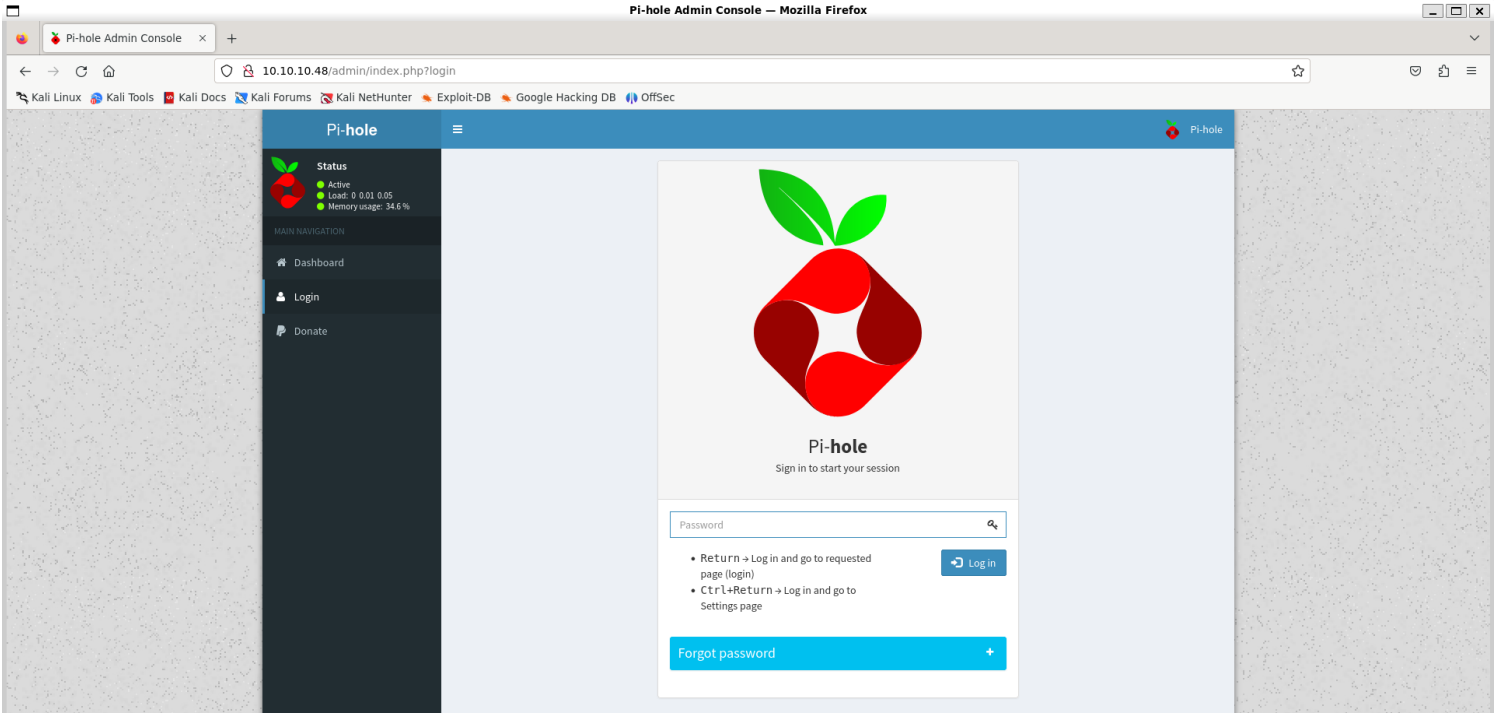
```
1 HTTP/1.1 404 Not Found
2 X-Pi-hole: A black hole for Internet advertisements.
3 Content-type: text/html; charset=UTF-8
4 Content-Length: 0
5 Connection: close
6 Date: Fri, 24 May 2024 14:41:23 GMT
7 Server: lighttpd/1.4.35
8
9
```





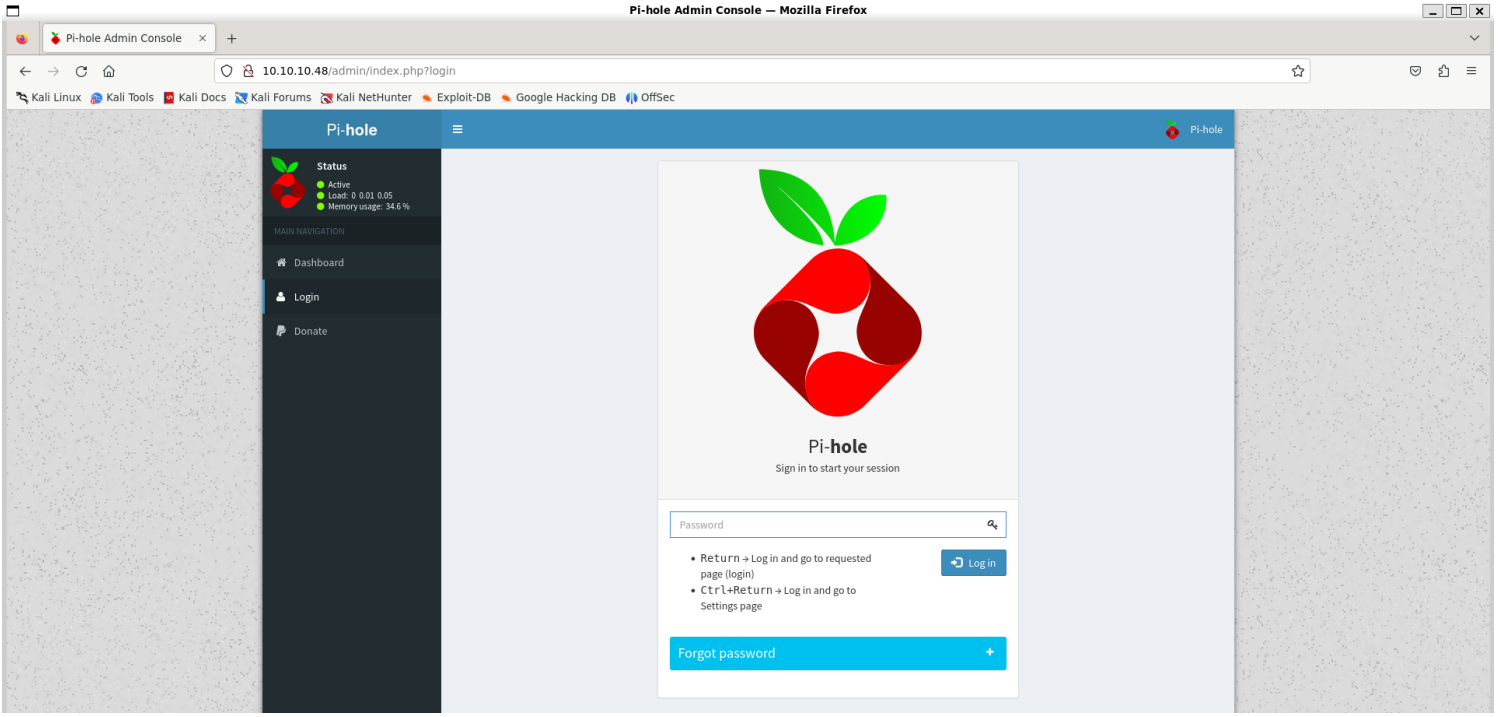


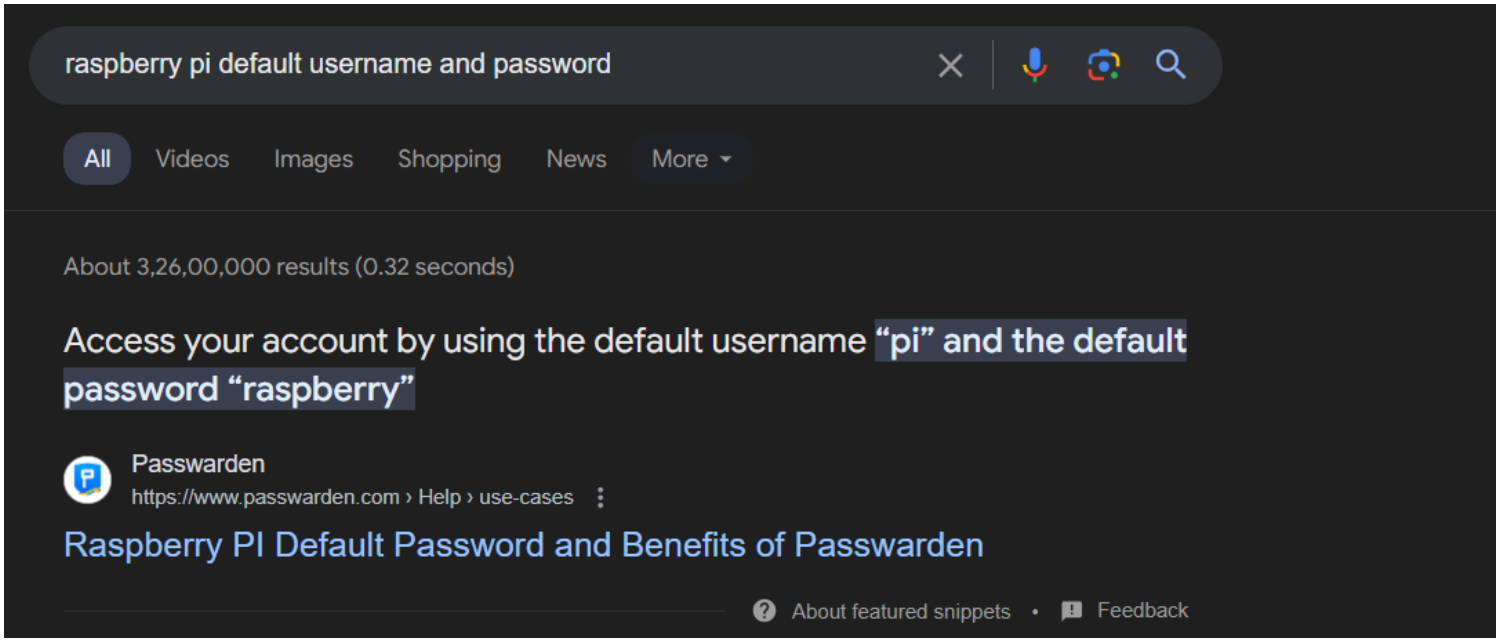
3) Found admin console



Vulnerability Assessment

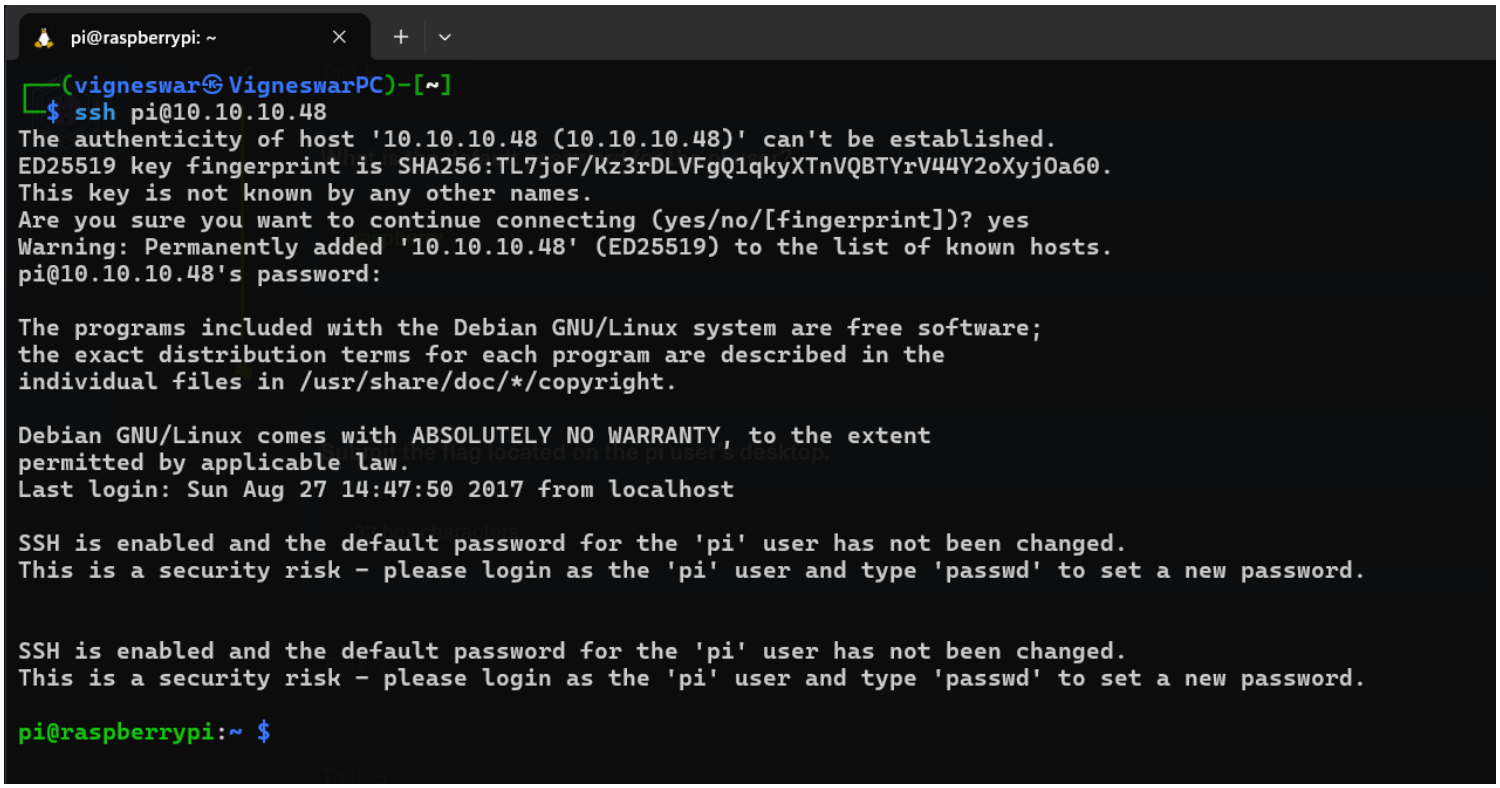
1) Checked for default password





Exploitation

1) The raspberry pi is vulnerable to common credentials usage



Privilege Escalation

1) The user has full sudo rights

```
pi@raspberrypi:~/Desktop $ sudo -l
Matching Defaults entries for pi on localhost:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User pi may run the following commands on localhost:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: ALL
pi@raspberrypi:~/Desktop $
```

```
pi@raspberrypi:~/Desktop $ sudo su
root@raspberrypi:/home/pi/Desktop# cd ~
root@raspberrypi:~# ls
root.txt
root@raspberrypi:~# cat root.txt
I lost my original root.txt! I think I may have a backup on my USB stick...
root@raspberrypi:~#
```

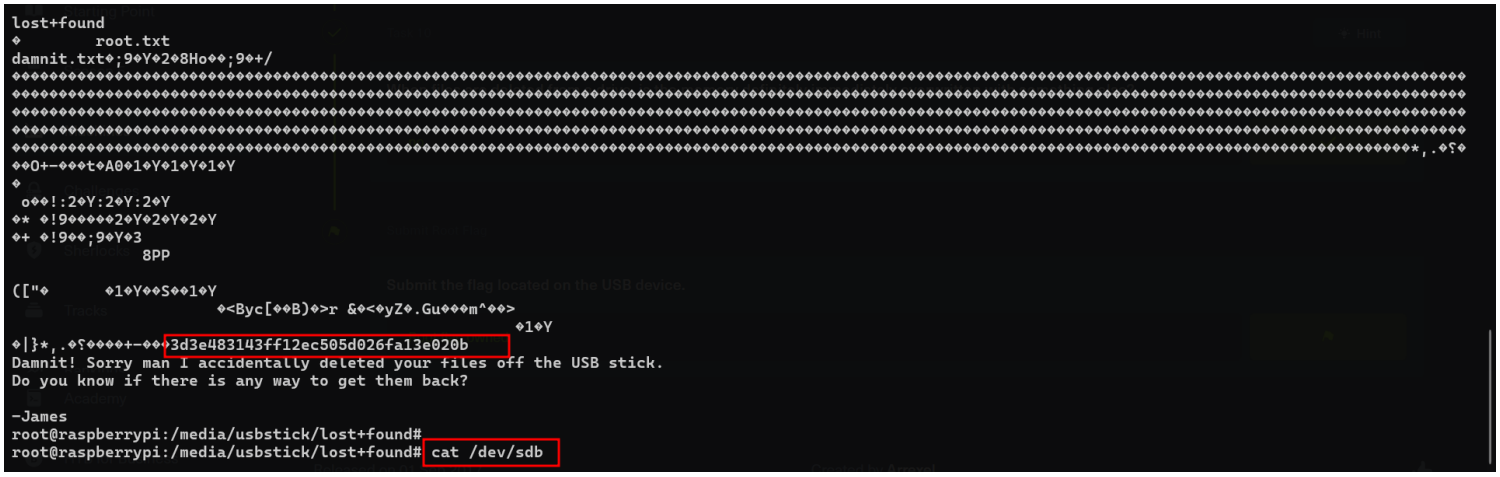
2) Found the usb mount

```
root@raspberrypi:~# mount
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
tmpfs on /run type tmpfs (rw,nosuid,relatime,size=102396k,mode=755)
/dev/sda1 on /lib/live/mount/persistence/sda1 type iso9660 (ro,noatime)
/dev/loop0 on /lib/live/mount/rootfs/filesystem.squashfs type squashfs (ro,noatime)
tmpfs on /lib/live/mount/overlay type tmpfs (rw,relatime)
/dev/sda2 on /lib/live/mount/persistence/sda2 type ext4 (rw,noatime,data=ordered)
aufs on / type aufs (rw,noatime,si=292bd95b,noxino)
devtmpfs on /dev type devtmpfs (rw,nosuid,size=10240k,nr_inodes=58955,mode=755)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,release_agent=/lib/systemd/systemd-cgroups-agent,nam
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_cls,net_prio)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=22,pgrp=1,timeout=300,minproto=5,maxproto=5,direct)
mqueue on /dev/mqueue type mqueue (rw,relatime)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,relatime)
/dev/sdb on /media/usbstick type ext4 (ro,nosuid,nodev,noexec,relatime,data=ordered)
tmpfs on /run/user/999 type tmpfs (rw,nosuid,nodev,relatime,size=51200k,mode=700,uid=999,gid=997)
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,size=51200k,mode=700,uid=1000,gid=1000)
```

```
root@raspberrypi:/media/usbstick# cat damnit.txt
Damnit! Sorry man I accidentally deleted your files off the USB stick.
Do you know if there is any way to get them back?

-James
```

3) The file is still in memory


lost+found
root.txt
damnit.txt
3d3e483143ff12ec505d026fa13e020b
Damnit! Sorry man I accidentally deleted your files off the USB stick.
Do you know if there is any way to get them back?
-James
root@raspberrypi:/media/usbstick/lost+found#
root@raspberrypi:/media/usbstick/lost+found# cat /dev/sdb