Skills Assessment

To complete this Skills Assessment, you will need to apply the multitude of tools and techniques showcased throughout this module. All fuzzing can be completed using the common.txt SecLists Wordlist, found at /usr/share/seclists/Discovery/Web-Content on Pwnbox, or via the SecLists GitHub.

Target: 83.136.253.5:59043

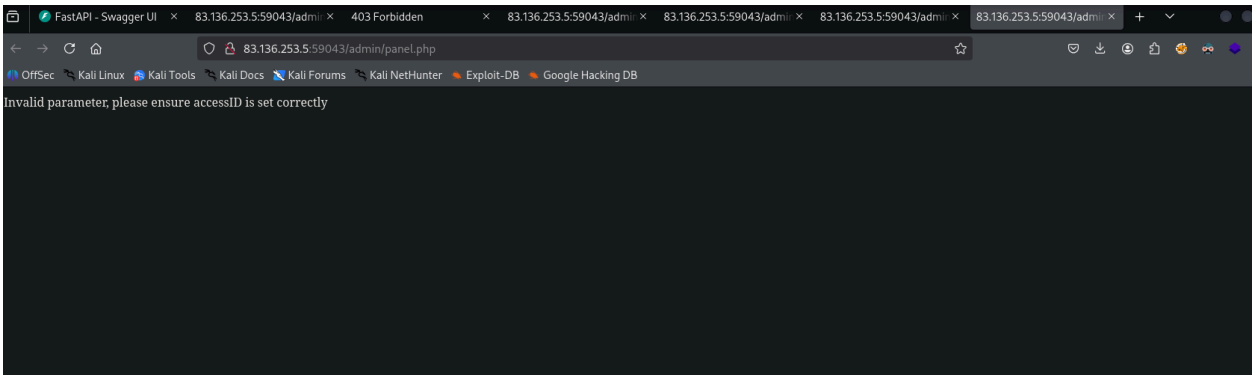
After completing all steps in the assessment, you will be presented with a page that contains a flag in the format of HTB{...}. What is that flag?

Starting off by running feroxbuster against the target endpoint

```
feroxbuster -u http://83.136.253.5:59043 -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt  -x "php" -k -q -e -r -t 200


404      GET        9l       31w      277c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter403      GET        9l       28w      280c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filterScanning: http://83.136.253.5:59043/
200      GET        1l        2w       13c http://83.136.253.5:59043/admin/
200      GET        1l        2w       13c http://83.136.253.5:59043/admin/index.php
200      GET        1l        8w       58c http://83.136.253.5:59043/admin/panel.php
Scanning: http://83.136.253.5:59043/
Scanning: http://83.136.253.5:59043/admin/
```

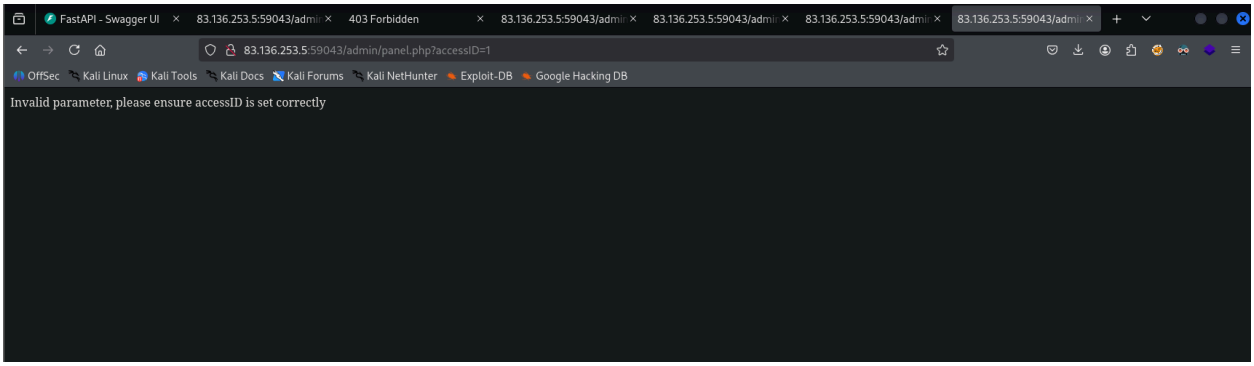
Navigating to http://83.136.253.5:59043/admin/panel.php



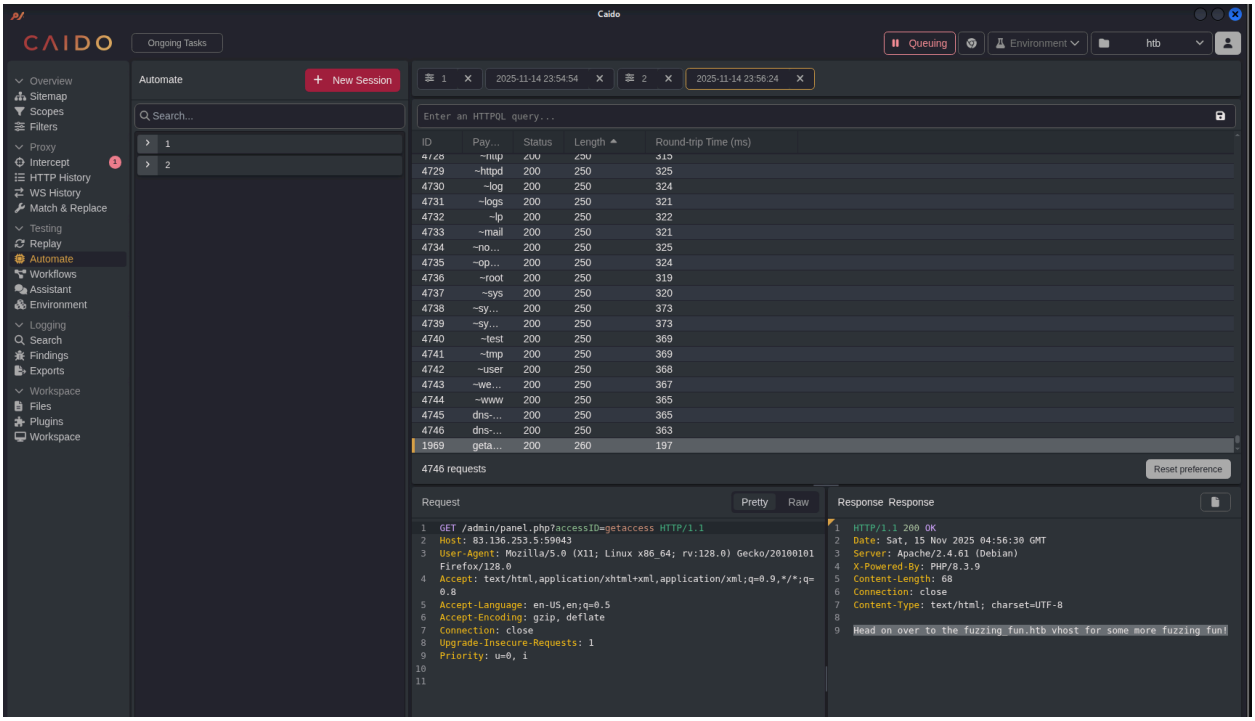
This error indicates that I should fuzz values for a parameter called accessID

To fuzz for parameters I want to learn Caido so I am going to turn on my proxy in foxy proxy and redirect request to caido

To make bruteforcing in caido a bit easier first I sent a request in my browser utilizing the accessID parameter and setting it to a dummy value of 1

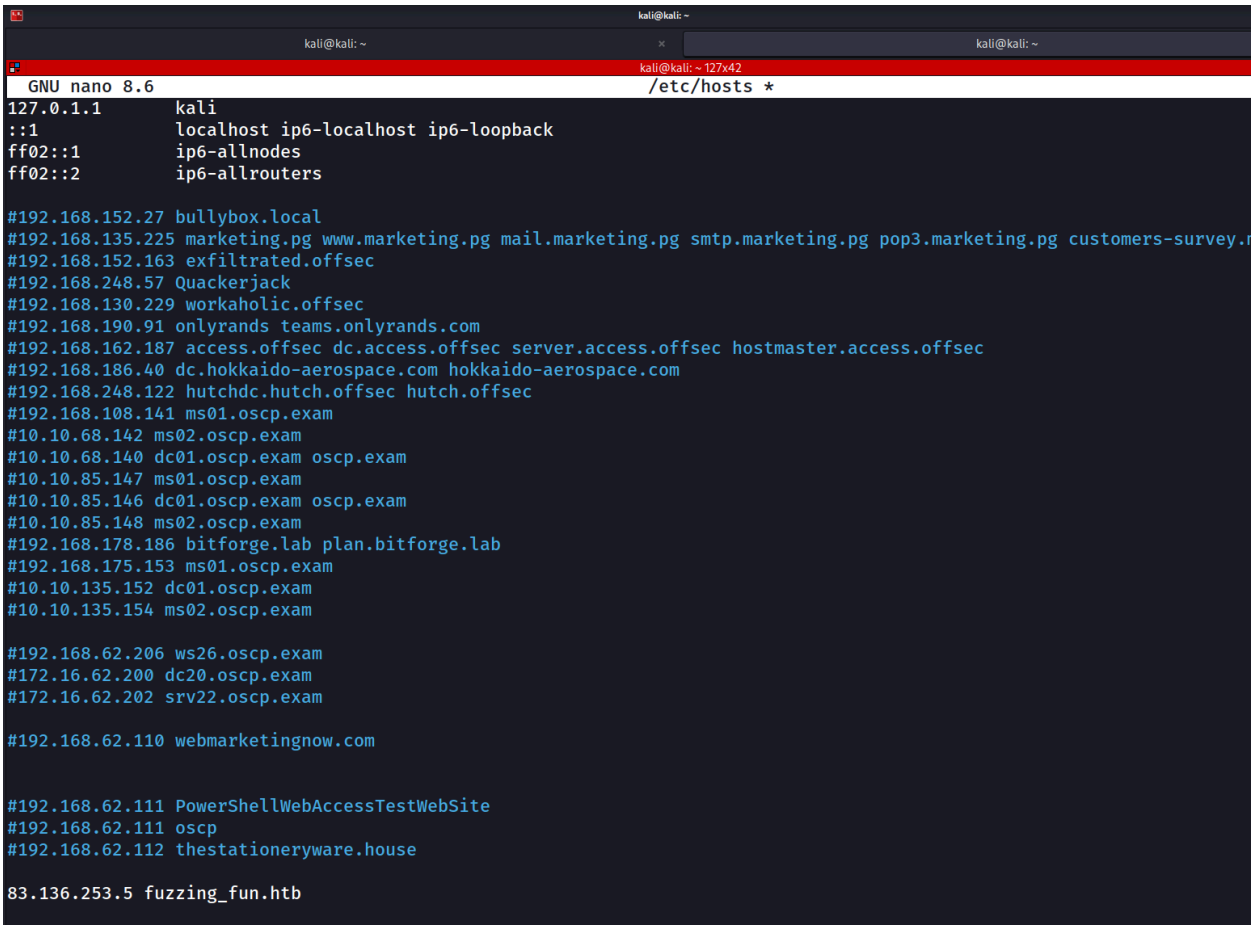


I sent the captured request → sent it to replay → sent it to automate → highlighted the 1 and clicked + → made the worked 100 to speed it up

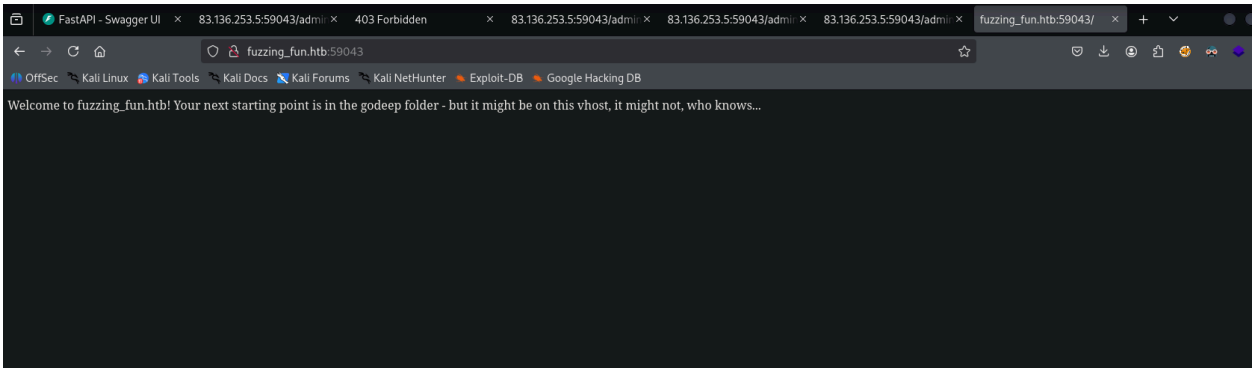


This redirects me to the fuzzing_fun.htb

Add this to my /etc/hosts file



Loading this page



It hints to me that recursive fuzzing will be required and that I might need to fuzz for other vhost

Fuzzing for additional vhost with gobuster

```
gobuster vhost -u http://fuzzing_fun.htb:59043/ -w /usr/share/seclists/Discovery/Web-Content/common.txt --append-domain
```

Running gobuster without filtering out 403 status codes returned alot of content so I filtered that out

Running gobuster without filtering out a content lenght of 305 gave alot of content so I filtered that out

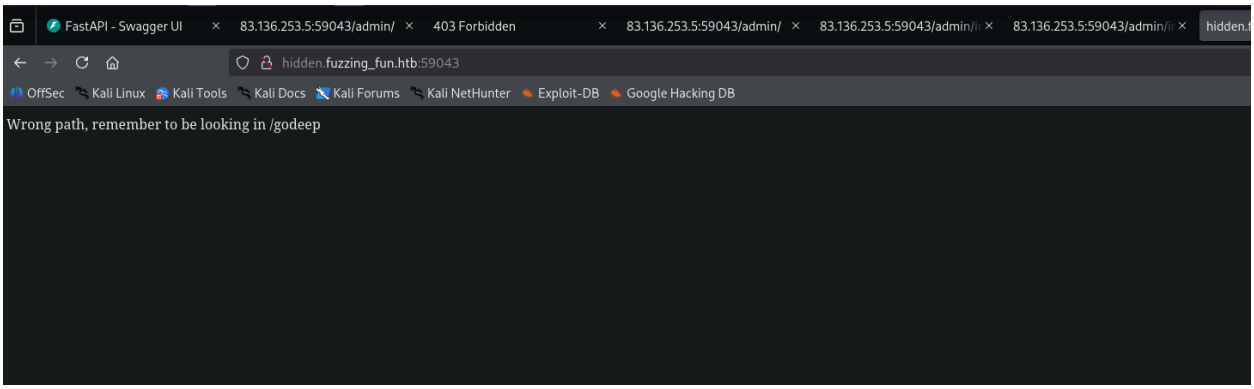
```
gobuster vhost -u http://fuzzing_fun.htb:59043/ -w /usr/share/seclists/Discovery/Web-Content/common.txt --append-domain -xs 403 -xl 305
```

This finds hidden.fuzzing_fun.htb:59043

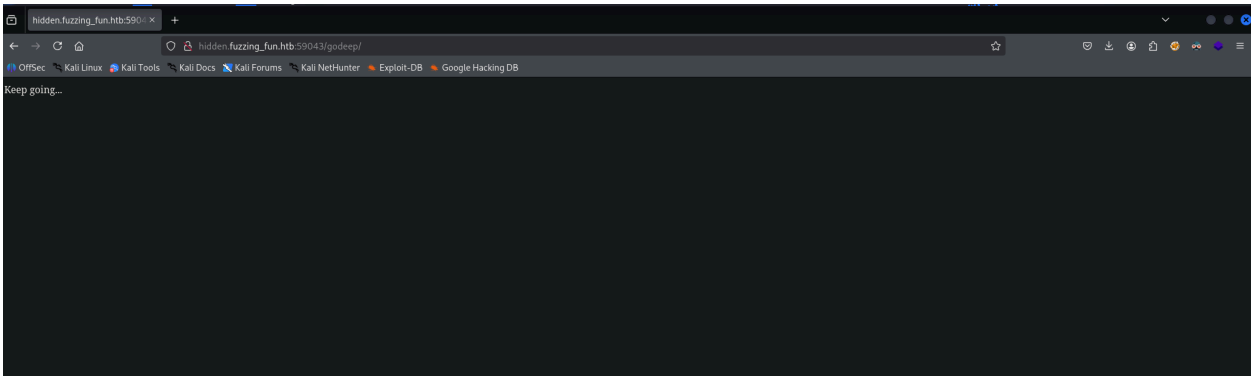
I need to add this to my /etc/hosts file as well

```
83.136.253.5 fuzzing_fun.htb hidden.fuzzing_fun.htb
```

This points me in the direction of /godeep



Going to /godeep in the hidden vhost brings me to this page



Running feroxbuster on the /godeep directory

```
feroxbuster -u http://hidden.fuzzing_fun.htb:59043/godeep/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt  -x "php" -k -q -e -r -t 200
```

```
┌──(kali㉿kali)-[~]
└─$ feroxbuster -u http://hidden.fuzzing_fun.htb:59043/godeep/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.tx
t  -x "php" -k -q -e -r -t 200


404      GET        9l       31w      287c Auto-filtering found 404-like response and created new filter; toggle off with --don
t-filter403      GET        9l       28w      290c Auto-filtering found 404-like response and created new filter; toggle off wi
th --dont-filterScanning: http://hidden.fuzzing_fun.htb:59043/godeep/
200      GET        1l        2w       13c http://hidden.fuzzing_fun.htb:59043/godeep/
200      GET        1l        2w       13c http://hidden.fuzzing_fun.htb:59043/godeep/index.php
200      GET        1l        2w       15c http://hidden.fuzzing_fun.htb:59043/godeep/stoneedge/
200      GET        1l        4w       18c http://hidden.fuzzing_fun.htb:59043/godeep/stoneedge/bbclone/
200      GET        1l        2w       15c http://hidden.fuzzing_fun.htb:59043/godeep/stoneedge/index.php
200      GET        1l        4w       18c http://hidden.fuzzing_fun.htb:59043/godeep/stoneedge/bbclone/index.php
200      GET        1l        1w       23c http://hidden.fuzzing_fun.htb:59043/godeep/stoneedge/bbclone/typo3/
200      GET        1l        1w       23c http://hidden.fuzzing_fun.htb:59043/godeep/stoneedge/bbclone/typo3/index.php
Scanning: http://hidden.fuzzing_fun.htb:59043/godeep/
Scanning: http://hidden.fuzzing_fun.htb:59043/godeep/stoneedge/
Scanning: http://hidden.fuzzing_fun.htb:59043/godeep/stoneedge/bbclone/
Scanning: http://hidden.fuzzing_fun.htb:59043/godeep/stoneedge/bbclone/typo3/

┌──(kali㉿kali)-[~]
```

The pages before the last level of recursion hint me in the direction to keep going. Doing so brings me to the flag finally.