

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

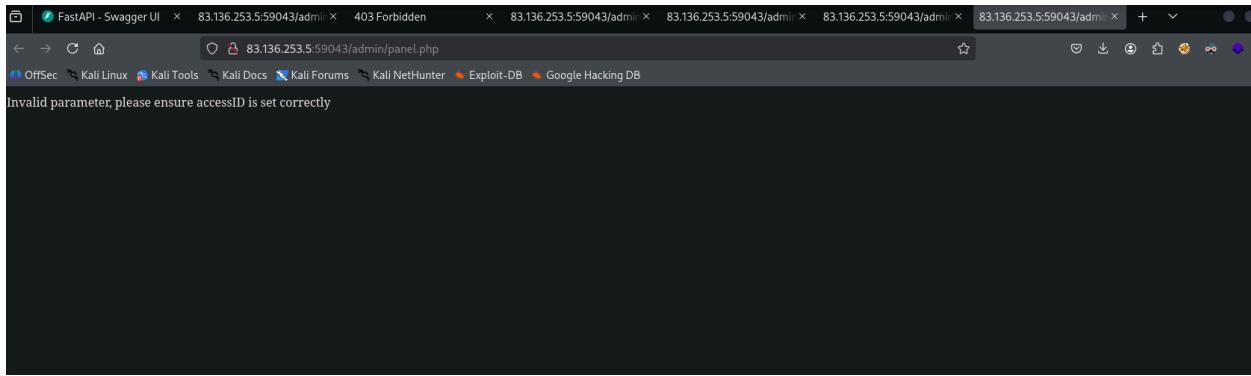
After completing all steps in the assessment, you will be presented with a page that contains a flag in the format of HTB{...}. What is that flag?

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

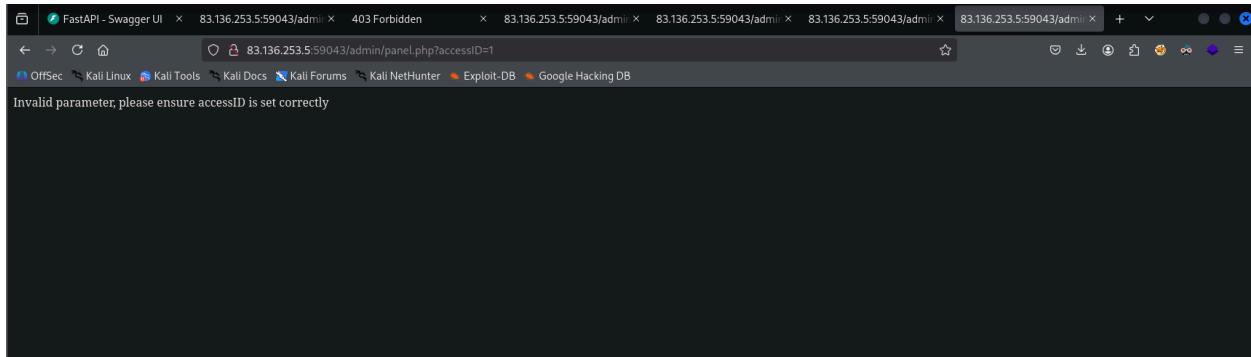
Navigating to http://83.136.253.5:59043/admin/panel.php



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

The screenshot shows the CAIDO application interface. On the left, there's a sidebar with various tools like Overview, Sitemap, Scopes, Filters, Proxy, Intercept, HTTP History, WS History, Match & Replace, Testing, Replay, Automate, Workflows, Assistant, Environment, Logging, Search, Findings, Exports, and Workspace. The 'Automate' section is currently selected. In the main area, there are two tabs: 'Session 1' (2025-11-14 23:54:54) and 'Session 2' (2025-11-14 23:56:24). A search bar at the top says 'Enter an HTTPQL query...'. Below it is a table titled 'ID Pay... Status Length ▲ Round-trip Time (ms)' with several rows of data. To the right of the table is a '4746 requests' section with 'Pretty' and 'Raw' tabs. Under 'Request', there's a multi-line code block showing an HTTP GET request. Under 'Response', there's another multi-line code block showing the server response. The response includes the message 'Head on over to the fuzzing_fun.htb host for some more fuzzing fun!'

This redirects me to the fuzzing_fun.htb

Add this to my /etc/hosts file

```
kali@kali: ~
kali@kali: ~
kali@kali: ~ 127x42
GNU nano 8.6
/etc/hosts *

127.0.1.1      kali
::1            localhost ip6-localhost ip6-loopback
ff02::1        ip6-allnodes
ff02::2        ip6-allrouters

#192.168.152.27 bullybox.local
#192.168.135.225 marketing.pg www.marketing.pg mail.marketing.pg smtp.marketing.pg pop3.marketing.pg customers-survey.r
#192.168.152.163 exfiltrated.offsec
#192.168.248.57 Quackerjack
#192.168.130.229 workaholic.offsec
#192.168.190.91 onlyrands teams.onlyrands.com
#192.168.162.187 access.offsec dc.access.offsec server.access.offsec hostmaster.access.offsec
#192.168.186.40 dc.hokkaido-aerospace.com hokkaido-aerospace.com
#192.168.248.122 hutchdc.hutch.offsec hutch.offsec
#192.168.108.141 ms01.oscp.exam
#10.10.68.142 ms02.oscp.exam
#10.10.68.140 dc01.oscp.exam oscp.exam
#10.10.85.147 ms01.oscp.exam
#10.10.85.146 dc01.oscp.exam oscp.exam
#10.10.85.148 ms02.oscp.exam
#192.168.178.186 bitforge.lab plan.bitforge.lab
#192.168.175.153 ms01.oscp.exam
#10.10.135.152 dc01.oscp.exam
#10.10.135.154 ms02.oscp.exam

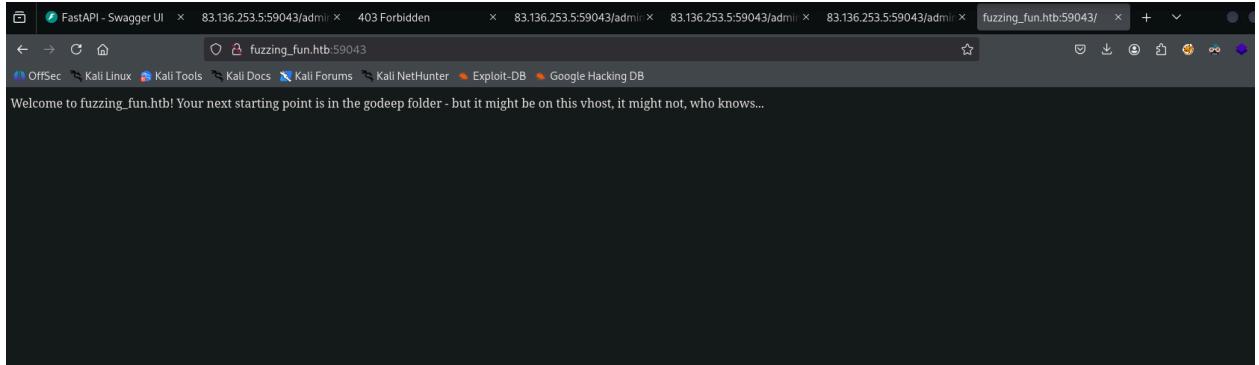
#192.168.62.206 ws26.oscp.exam
#172.16.62.200 dc20.oscp.exam
#172.16.62.202 srv22.oscp.exam

#192.168.62.110 webmarketingnow.com

#192.168.62.111 PowerShellWebAccessTestWebSite
#192.168.62.111 oscp
#192.168.62.112 thestationeryware.house

83.136.253.5 fuzzing_fun.htb
```

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
```

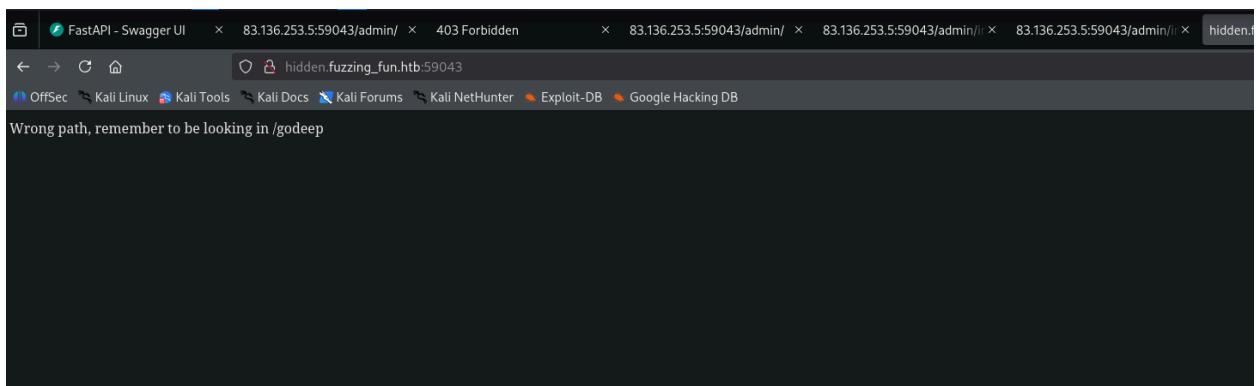
```
=====
Starting gobuster in VHOST enumeration mode
=====
hidden.fuzzing_fun.htb:59043 Status: 200 [Size: 45]
lost+found.fuzzing_fun.htb:59043 Status: 400 [Size: 308]
~adm.fuzzing_fun.htb:59043 Status: 400 [Size: 308]
~guest.fuzzing_fun.htb:59043 Status: 400 [Size: 308]
~ftp.fuzzing_fun.htb:59043 Status: 400 [Size: 308]
~admin.fuzzing_fun.htb:59043 Status: 400 [Size: 308]
~apache.fuzzing_fun.htb:59043 Status: 400 [Size: 308]
~administrator.fuzzing_fun.htb:59043 Status: 400 [Size: 308]
~amanda.fuzzing_fun.htb:59043 Status: 400 [Size: 308]
~bin.fuzzing_fun.htb:59043 Status: 400 [Size: 308]
~http.fuzzing_fun.htb:59043 Status: 400 [Size: 308]
~logs.fuzzing_fun.htb:59043 Status: 400 [Size: 308]
~httpd.fuzzing_fun.htb:59043 Status: 400 [Size: 308]
~lp.fuzzing_fun.htb:59043 Status: 400 [Size: 308]
~log.fuzzing_fun.htb:59043 Status: 400 [Size: 308]
~nobody.fuzzing_fun.htb:59043 Status: 400 [Size: 308]
~sysadm.fuzzing_fun.htb:59043 Status: 400 [Size: 308]
~mail.fuzzing_fun.htb:59043 Status: 400 [Size: 308]
~operator.fuzzing_fun.htb:59043 Status: 400 [Size: 308]
~root.fuzzing_fun.htb:59043 Status: 400 [Size: 308]
~sys.fuzzing_fun.htb:59043 Status: 400 [Size: 308]
~test.fuzzing_fun.htb:59043 Status: 400 [Size: 308]
~webmaster.fuzzing_fun.htb:59043 Status: 400 [Size: 308]
~tmp.fuzzing_fun.htb:59043 Status: 400 [Size: 308]
~sysadmin.fuzzing_fun.htb:59043 Status: 400 [Size: 308]
~user.fuzzing_fun.htb:59043 Status: 400 [Size: 308]
~www.fuzzing_fun.htb:59043 Status: 400 [Size: 308]
Progress: 4746 / 4746 (100.00%)
=====
Finished
=====
```

This finds hidden.fuzzing_fun.htb:59043

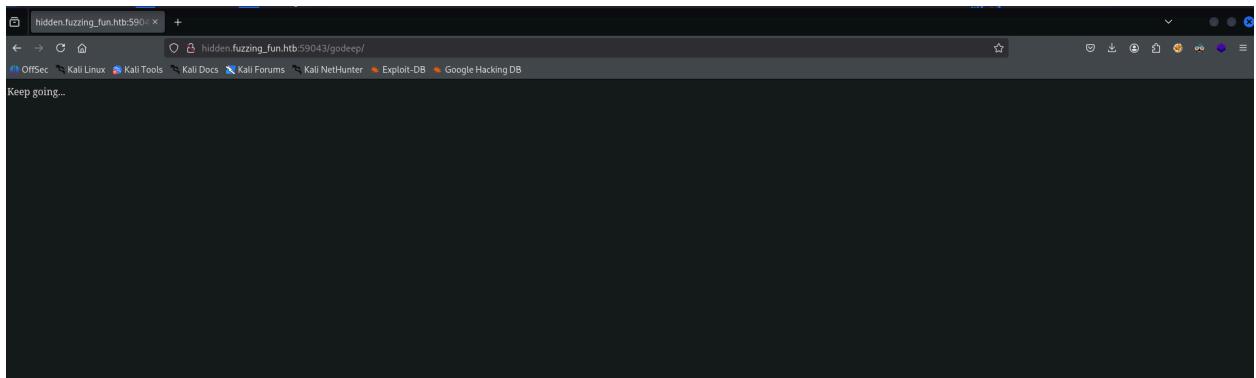
I need to add this to my /etc/hosts file as well

```
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/w
rdlists/seclists/Discovery/Web-Content/common.txt -x "php" -k -q -e -r -t 20
0
```

```
(kali㉿kali)-[~]
$ 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

404      GET      9l      31w      287c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
403      GET      9l      28w      290c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
Scanning: 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.

