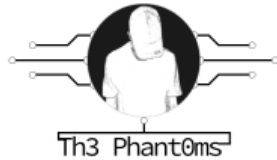


We are the rarest common race on earth.....!
Meet us we are the **HACKERS**.....!!!

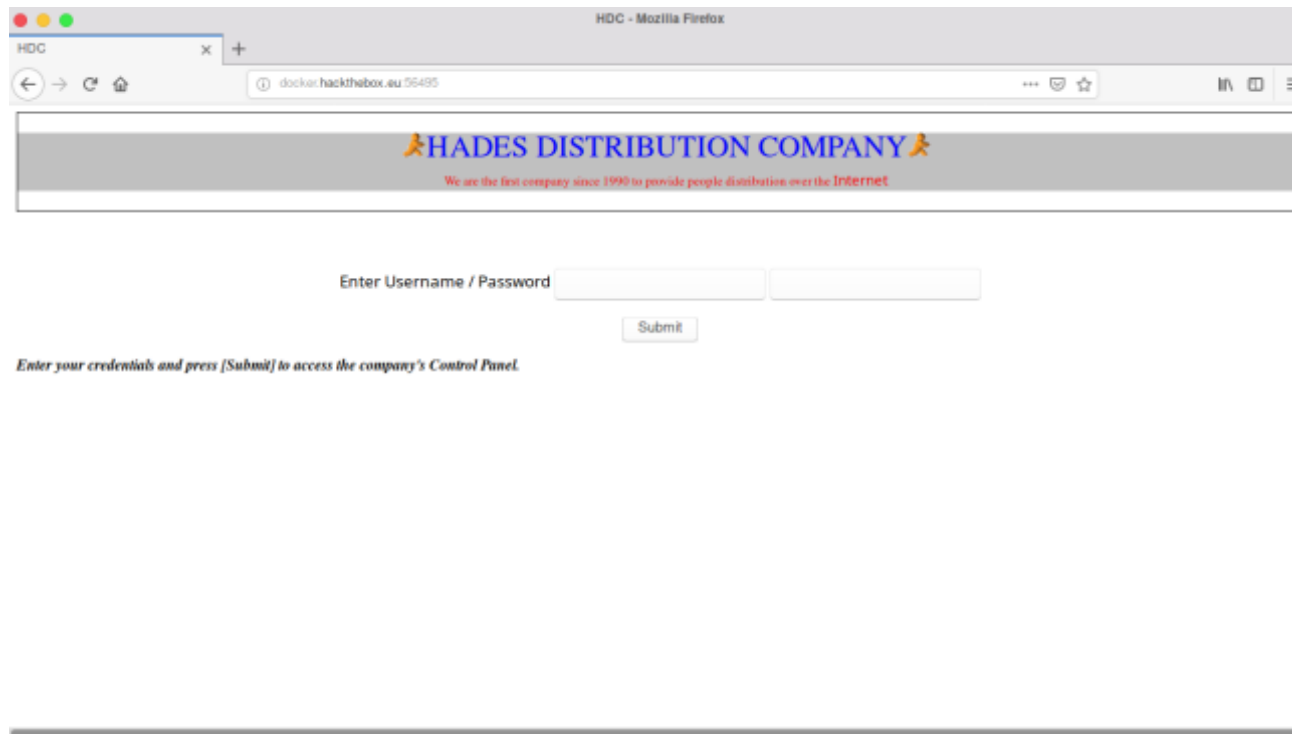


MENU

PHANTOM INFOSEC

[Hackthebox] Web challenge – HDC

Posted on [December 22, 2018](#) by [Phantom Michael \(ခန့်ခွဲခန့်ခွဲ\)](#)



So now! we are going to the third challenge of web challenge on hackthebox.eu, this challenge is hard a bit, okay!!! let's start now, connect to your target and you know the first thing that we always do is check source code, when I look into the source code I marked 2 places like a bellow.

```
<script src="jquery-3.2.1.js"></script>  
<script src="myscripts.js"></script>
```

these script tags

```
<input type="hidden" value= name="name1">  
<input type="hidden" value= name="name2">
```

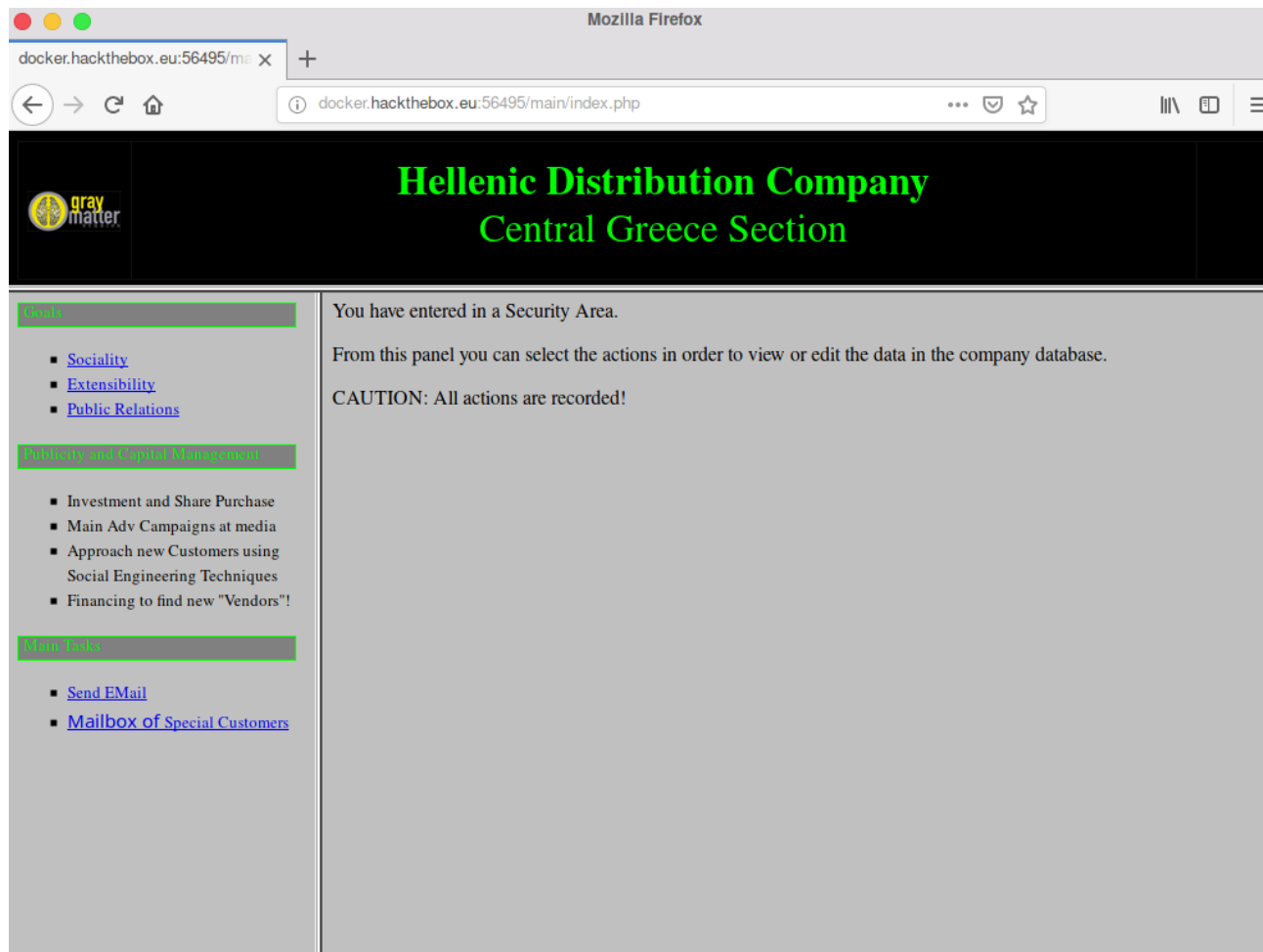
these hidden fields

Why i marked them ??? first,i marked script tags because it may give us some useful info,you should learn to read or check some src Js inside the page it may give you solution for your problem.Second,at hidden fields they give us values each field that like a hint for us.Brushed them aside,let's go to these script tags and check code inside it,open the first script that's "jquery-3.2.1.js",i'm searching for credential so i will search for username and password and it give me nothing,back to these hidden fields,look those values that's "name1" and "name2",i used it to search in the jquery script and get something cool.

```
hiddenField.setAttribute("name","name1"); hiddenField.setAttribute("value","TXIMaXR0bGU");
```

```
hiddenField2.setAttribute("name","name2"); hiddenField2.setAttribute("value","cDB3bmll");
```

After use those values i passed login screen,and redirected to new page.



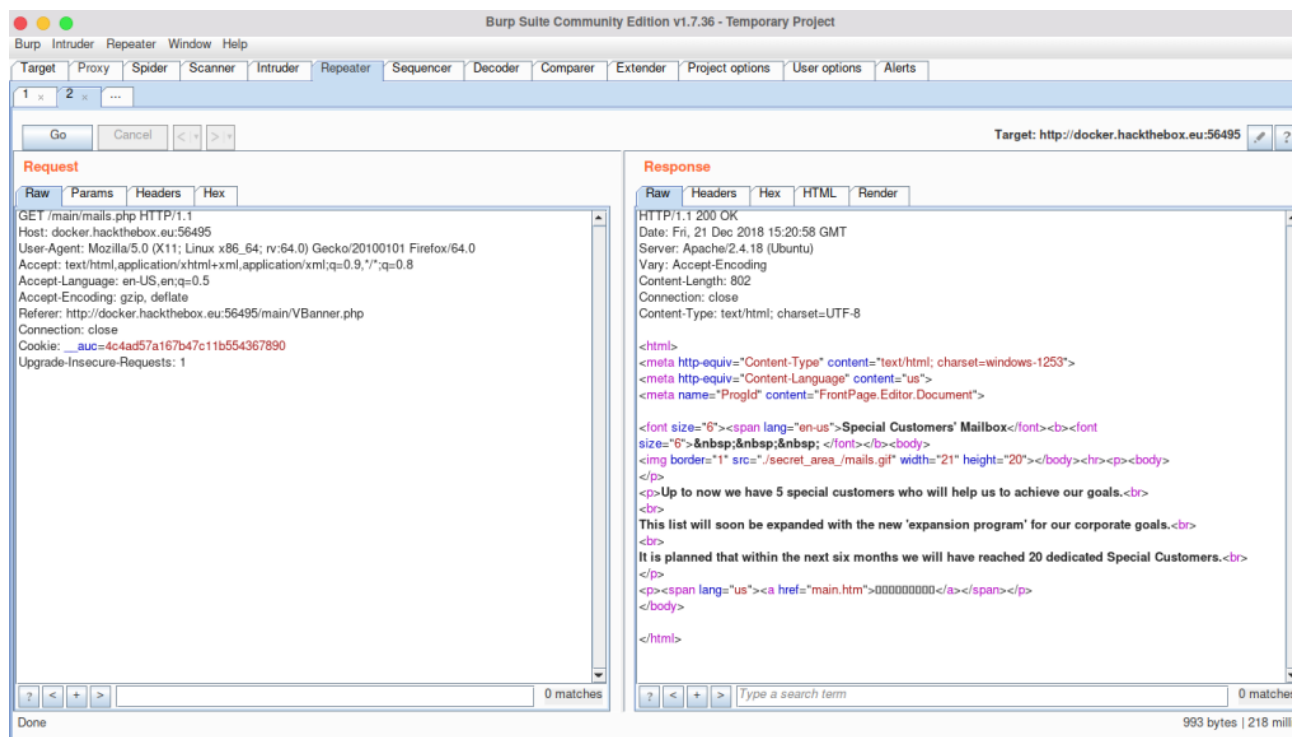
Okay, my task now is finding email address send a message and get the flag, so I forward to *Mailbox of Special Customers* to get email, but in that page it not showed any email address just a normal page, not much thinking I went to check the source code for more information, when I opened the source code page it show me this.

```
</frameset>  
<noframes>  
<body>
```

```
<p>This page uses frames, but your browser doesn't support them.</p>
```

```
</body>  
</noframes>  
</frameset>
```

That's cause my browser not support their frames so i can't see what is in the frames,i used firefox browser,never mind to it i was doing request to that page again on burp suite and i could get clearly information from that page.






It still like nothing, but when you look carefully you will see a `` tag include a weird src.

```
</body><hr><p><body>
```

that path i never see before, not wait anymore i'm going to secret_area to check if have somethings on that.

Index of /main/secret_area_

| Name | Last modified | Size | Description |
|--|-------------------------------|----------------------|-----------------------------|
| <hr/> | | | |
|  Parent Directory | | - | |
|  mails.gif | 2010-10-23 18:28 | 71 | |
|  mails.txt | 2017-07-08 17:55 | 705 | |

Apache/2.4.18 (Ubuntu) Server at docker.hackthebox.eu Port 56495

Inside secret_area it include file mails.txt which stored emails address.

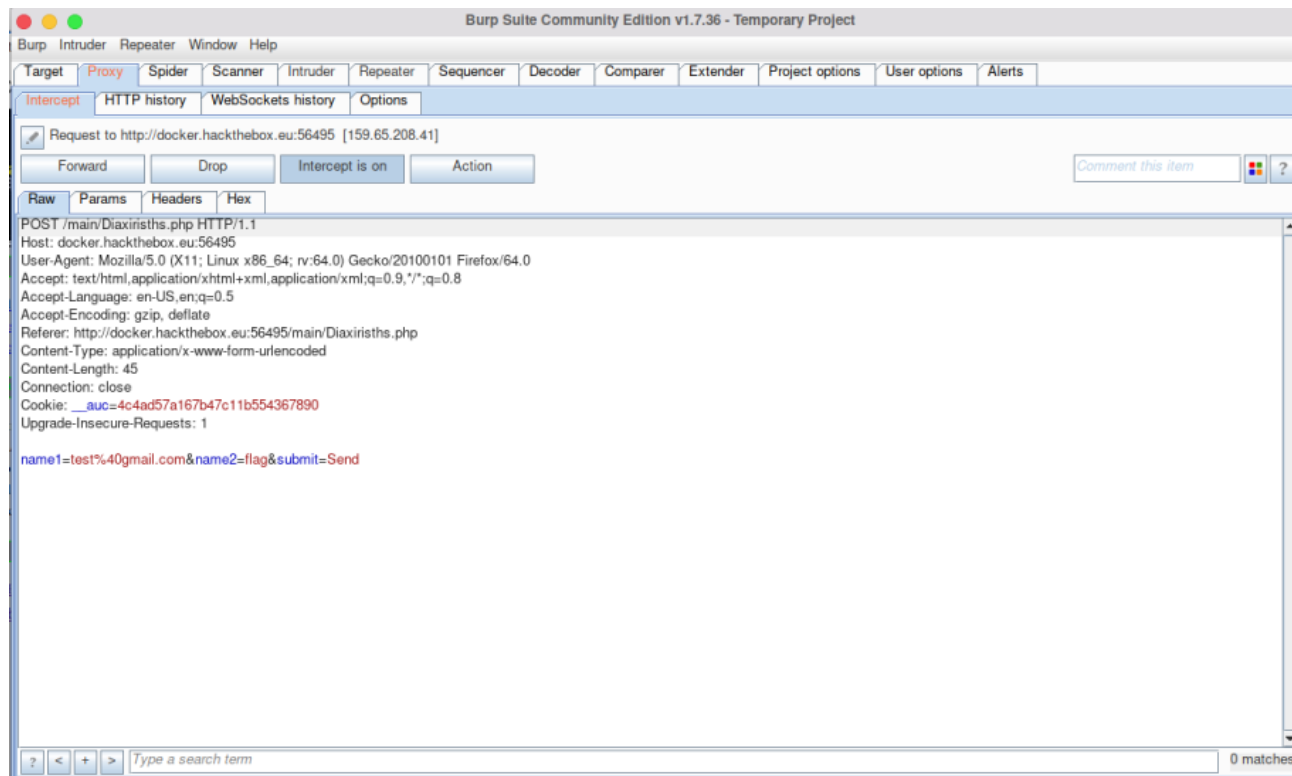
All good boys are here... hehehehehehe!

Peter Punk CallMePink@newmail.com
Nabuchodonosor BabyNavou@mailpost.gr
Ilias Magkakos imagkakos@badmail.com
Nick Pipshow NickTheGreek@mail.tr.gr
Don Quixote Windmill@mail.gr
Crazy Priest SeVaftise@hotmail.com
Fishroe Salad fishroesalad@mail.com
TaPanta Ola OlaMaziLeme@mail.gr
Laertis George I8aki@mail.gr
Thiseas Sparrow Pirates@mail.gr
Black Dreamer SupaHacka@mail.com
Callme Daddy FuckthemALL@mail.com
Aggeliki Lykolouli FwsStoTounel@Traino.pourxetai
Kompinadoros Yannnnis YannisWith4N@rolf.com
Serafino Titamola Ombrax@mail.gr
Joe Hard Soft@Butter.gr
Bond James MyNamelsBond@JamesBond.com
Endof Text EndOfLine@mail.com

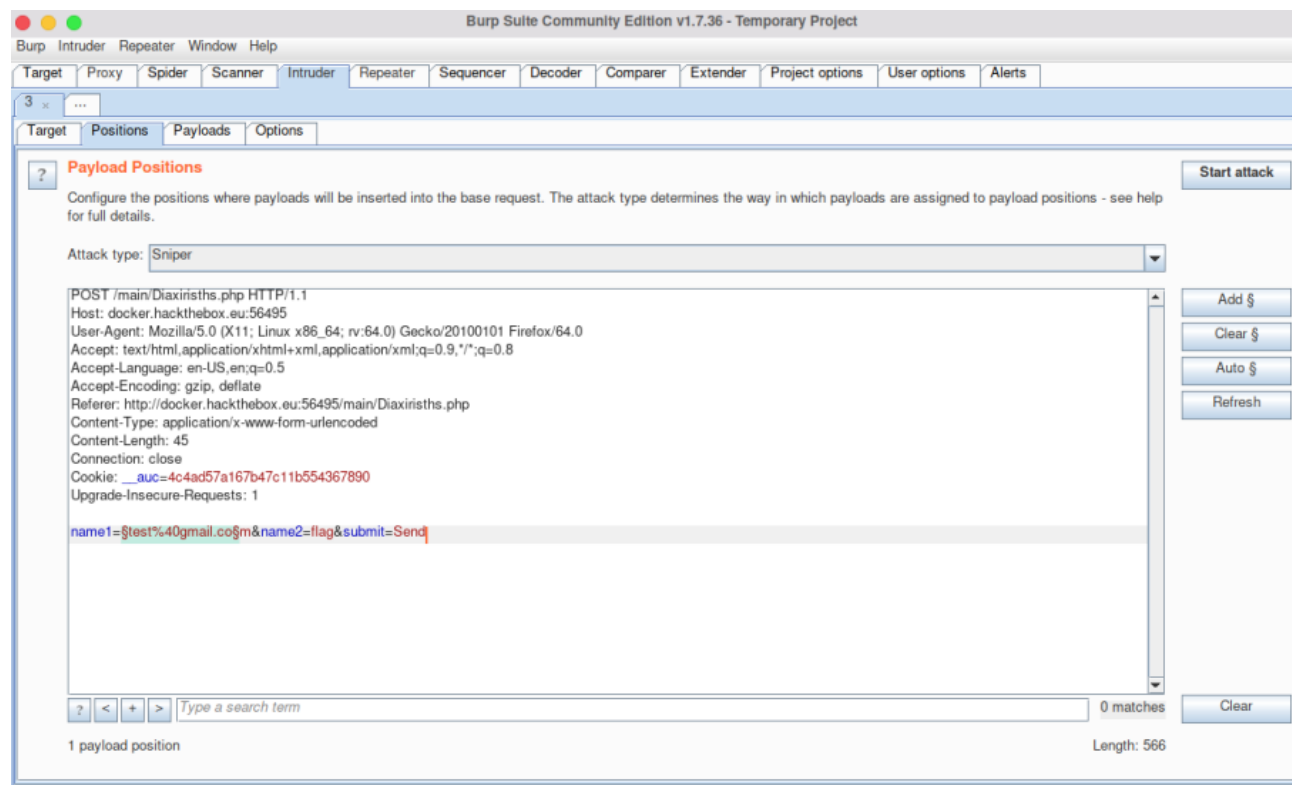
I got mails list now i need to check the correct email address to get the flag by sending message to per mail at *Send EMail* before doing that u should create a list email address,here is my python code to do that.


```
import requests
r = requests.get('http://docker.hackthebox.eu:56495/main/secret_a
content = r.content.decode('utf-8').strip('\n').split()
with open('mails.txt','a') as file:
    for text in content:
        if '@' in text:
            file.write(text+'\n')
```

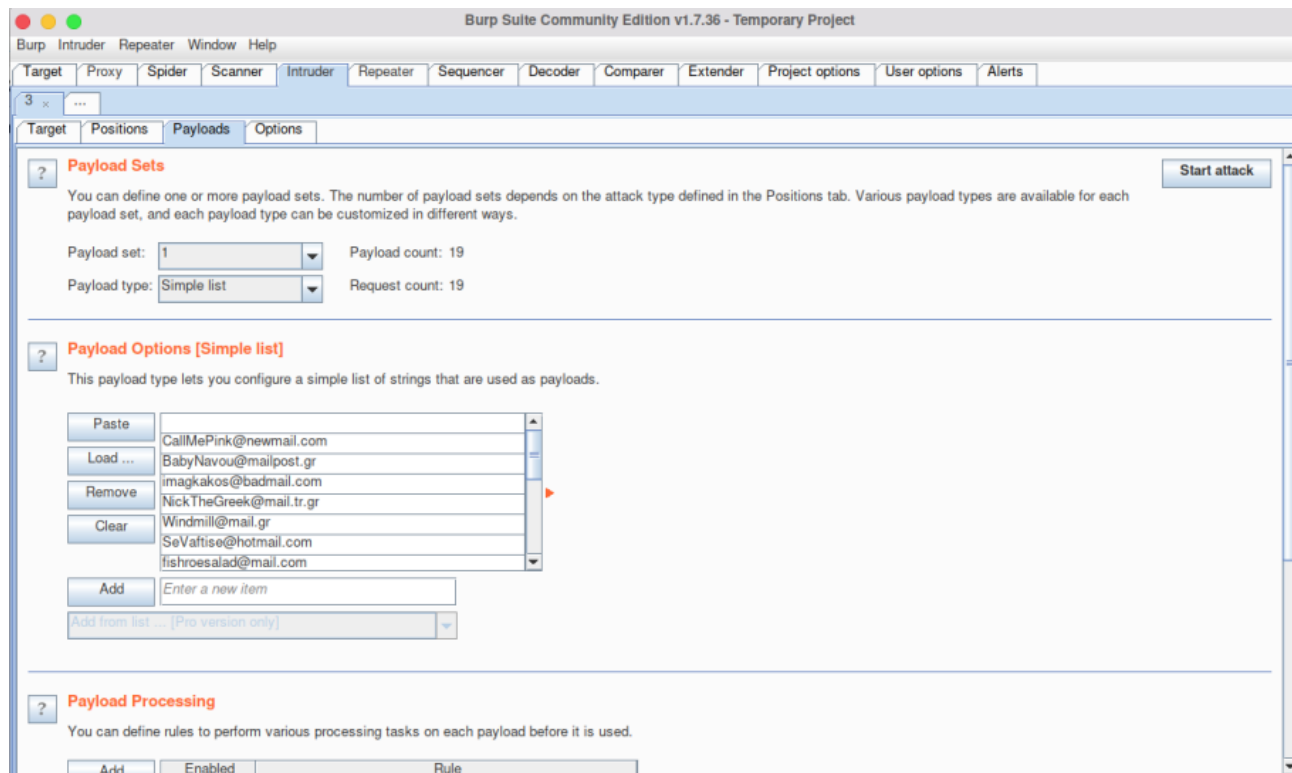
After have the list,do send email process with burp suite,catch request on *Send EMail* and send it to Intruder in burp suite.



catch request on burp suite



set payload marker at name1



load payload from mails.txt

Press start attack button at right top and see results,you will get the flag like bellow.

Intruder attack 3

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

| Request | Payload | Status | Error | Timeout | Length | Comment |
|---------|-------------------------------|--------|-------|---------|--------|---------|
| 4 | imagakos@badmail.com | 200 | | | 1029 | |
| 5 | NickTheGreek@mail.tr.gr | 200 | | | 1029 | |
| 6 | Windmill@mail.gr | 200 | | | 1029 | |
| 7 | SaVafise@hotmail.com | 200 | | | 1029 | |
| 8 | fishroesalad@mail.com | 200 | | | 474 | |
| 9 | OiaMaziLeme@mail.gr | 200 | | | 1029 | |
| 10 | I8aki@mail.gr | 200 | | | 1029 | |
| 11 | Pirates@mail.gr | 200 | | | 1029 | |
| 12 | SupaHacka@mail.com | 200 | | | 1029 | |
| 13 | FuckthemALL@mail.com | 200 | | | 1029 | |
| 14 | FwsStoTounel@Traino.pourxetai | 200 | | | 1029 | |
| 15 | YannisWith4N@rolf.com | 200 | | | 1029 | |
| 16 | Ombrax@mail.gr | 200 | | | 1029 | |
| 17 | Soft@Butter.gr | 200 | | | 1029 | |

Request Response

Raw Headers Hex HTML Render

Vary: Accept-Encoding
Content-Length: 283
Connection: close
Content-Type: text/html; charset=UTF-8

```
<html>
<head>
<meta http-equiv="Content-Language" content="us">
<meta http-equiv="Content-Type" content="text/html">
<h1>Re: Hello there!</h1><h3>Hi, I am still alive, don't worry :)</h3><h3>Congratz my friend!!</h3><h3>The flag is:</h3>HTB{FuckTheB3stAndPlayWithTheRest!!}
```

0 matches

Finished

the flag is HTB{FuckTheB3stAndPlayWithTheRest!!}

That's all, we completed this challenge, in next post I will be going to do *I know Mag1k* [50 points] challenge.

Thanks for watching!!!



[REPORT THIS AD](#)

AUTOMATTIC

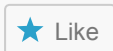
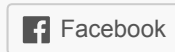
**We're hiring
backend developers.
Join us!**

[APPLY](#)



[REPORT THIS AD](#)

Share this:



One blogger likes this.

Posted in [ctf write-ups](#) Tagged [ctf write-ups](#), [hackthebox](#), [web challenge](#) [Leave a comment](#)

[\[Hackthebox\] Web challenge – Cartographer](#)

[\[Hackthebox\] Web challenge – I know Mag1k](#)

Leave a Reply

Enter your comment here...

RECENT POSTS

[\[Hackthebox\] Web challenge – Grammar write-up](#)

[\[Hackthebox\] Web challenge – I know Mag1k](#)

[\[Hackthebox\] Web challenge – HDC](#)

[\[Hackthebox\] Web challenge – Cartographer](#)

[\[Hackthebox\] Web challenge – Lernaean](#)

Advertisements

AUTOMATTIC

**We're hiring
backend developers.
Join us!**

[APPLY](#)

WordPress, Automattic, WooCommerce, and other logos

[REPORT THIS AD](#)

LOOKING FOR ANOTHER STUFFS

ctf write-ups

Linux

FOLLOW US



Powered by WordPress.com.