

# HACK THE BOX

## WEB CHALLENGE: HDC

We believe a certain individual uses this website for shady business. Can you find out who that is and send him an email to check, using the web site's functionality?

Note: The flag is not an e-mail address.

Linku <http://docker.hackthebox.eu:48775>, per web challenge HDC na jep kete login page, i cili kerkon username dhe password, per ta aksesuar me tutje Hades Distribution Company.



Enter Username / Password

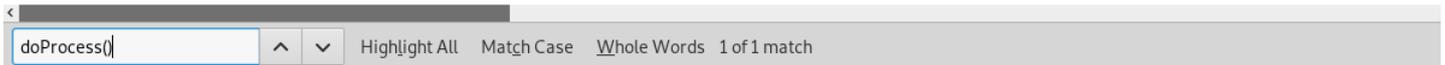
Enter your credentials and press [Submit] to access the company's Control Panel.

Per te gjetur username dhe password, fillimisht kerkova ne View Page Source qe te gjeja formen qe permban username dhe password, shoh qe username eshte i ruajtur si name1 dhe password si name2 ne form id='formaki', dhe funksioni doProcess()

```
view-source:http://docker.hackthebox.eu:48775/
1 <html>
2
3 <head>
4 <meta http-equiv="Content-Language" content="en-us">
5 <meta name="GENERATOR" content="Microsoft GiveMeA Break 12.0">
6 <meta name="ProgId" content="UnfrontPage.Editor.Document :)">
7 <meta http-equiv="Content-Type" content="text/html;">
8 <title>HDC</title>
9 <style type="text/css">
10 .style2 {
11     font-size: xx-large;
12     color: #0000FF;
13 }
14 .style3 {
15     color: #008000;
16 }
17 </style>
18 <script src="jquery-3.2.1.js"></script>
19 <script src="myscripts.js"></script>
20 </head>
21
22 <body >
23 <table border="1" cellpadding="0" cellspacing="0" style="border-collapse: collapse" bordercolor="#111111" width="101%" id="AutoNumber1" height="104">
24 <tr>
25 <td width="85%" height="104">
26 <div style="background-color: #C0C0C0">
27 <p align="center"><span lang="us" class="style2">HADES DISTRIBUTION COMPANY</span><b font size="7" color="#0000FF"><span lang="us"><br>
28 </span></font></b><span lang="us"><font size="2" color="#FF0000">We are the first company since 1990 to provide people distribution over the </font></span><font size="2" color="#FF0000"> Internet</font></div>
29 </td>
30 </tr>
31 </table>
32 <p><i><span class="style3"><span lang="us"></span></span><b font color="#808000"> </font><span font color="#FFFFFF"><span lang="us"><span></font></b></i></p>
33 <form id="formaki" name="formaki" action="/main/index.php" method="post">
34 <p align="center">Enter Username / Password
35 <input type="text" name="name1" size="20">
36 <input type="text" Name="name2" size="20">
37
38 </p>
39
40 <p align="center">
41 <input type="hidden" value= name="name1">
42 <input type="hidden" value= name="name2">
43
44 <input type="button" value="Submit" onclick="doProcess()"/>
45
46 </p>
47 </form>
48 <p align="left"><b><span lang="us"><i>Enter your credentials and press [Submit] to access the company's Control Panel</i></span><i><span lang="us"></i></b></p>
49
50 <p align="left"><span></p>
51
52 </body>
53
54
55 </html>
```

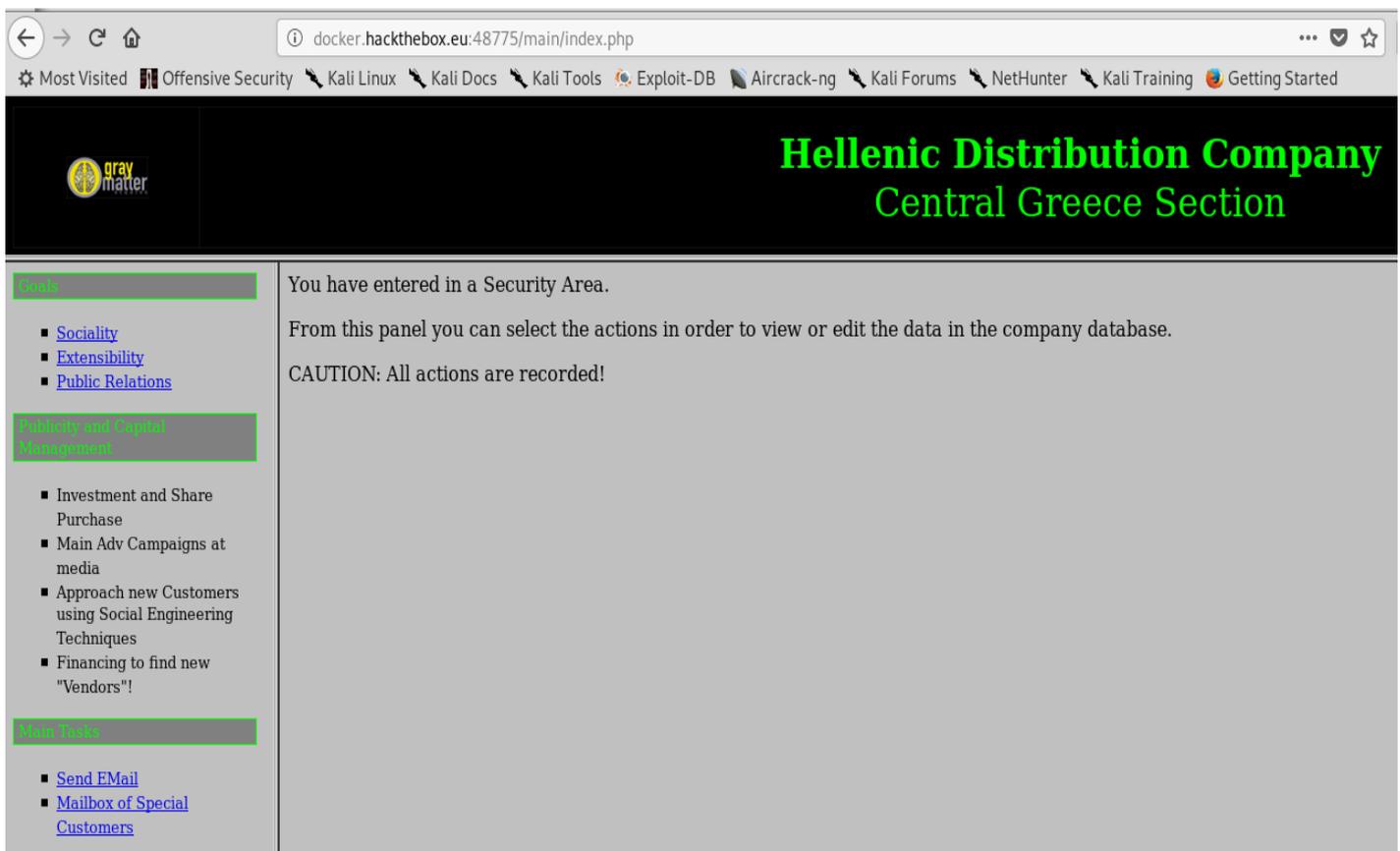
Kerkoj per funksionin doProcess() ne file [jquery-3.2.1.js](#), dhe gjej username dhe password

```
function doProcess()  
{var form=document.createElement("form"); form.setAttribute("method","post"); form.setAttribute("action","main/index.php");  
  
function getData( data ) {  
    if ( data === "true" ) {  
        return true;  
    }  
  
    if ( data === "false" ) {  
        return false;  
    }  
  
    if ( data === "null" ) {  
        return null;  
    }  
}
```

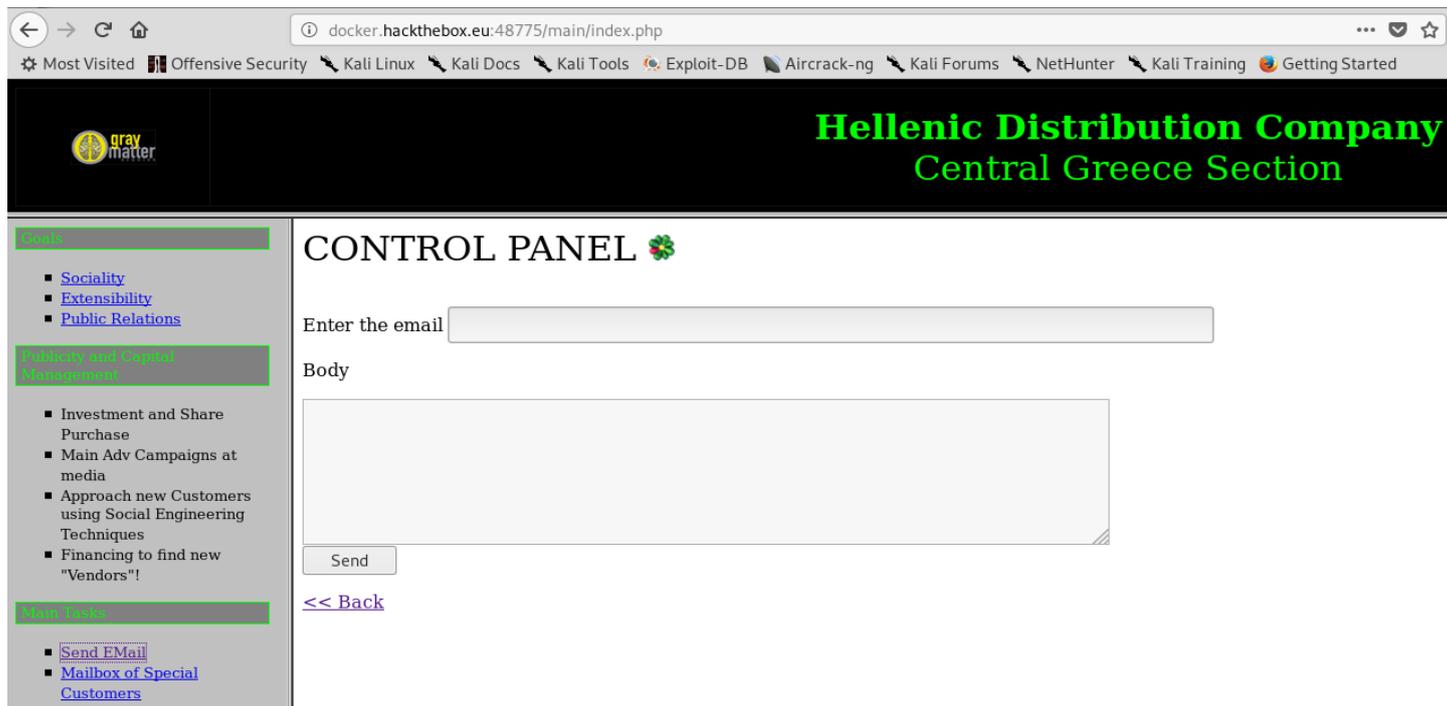


```
hiddenField.setAttribute("type","hidden"); hiddenField.setAttribute("name","name1"); hiddenField.setAttribute("value","TXlMaXR0bGU");  
hiddenField2.setAttribute("type","hidden"); hiddenField2.setAttribute("name","name2"); hiddenField2.setAttribute("value","cDB3bml1");
```

I jap username dhe password : TXlMaXR0bGU/cDB3bml1 ne faqen loguese, dhe logohem.

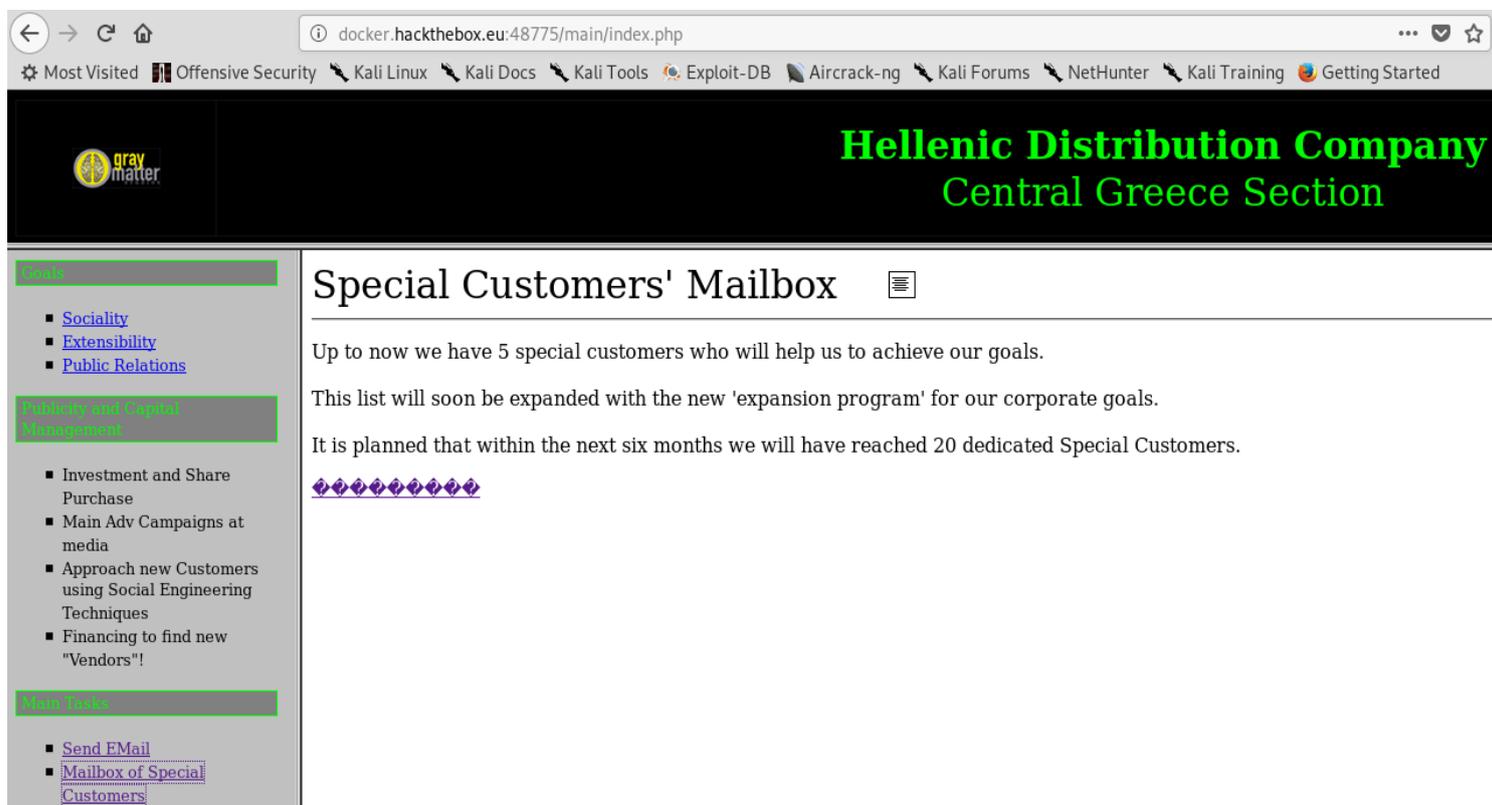


Filloj te shfletoj secilen faqe pas login-it, sidomos send Email dhe Mailbox of Special Customers, sipas pershkrimet qe me eshte dhene ne challenge, por pa ndonje rezultat per te vazhduar me tutje, keshtu qe filloj te shikoj imazhet qe jane ne kete web challenge.



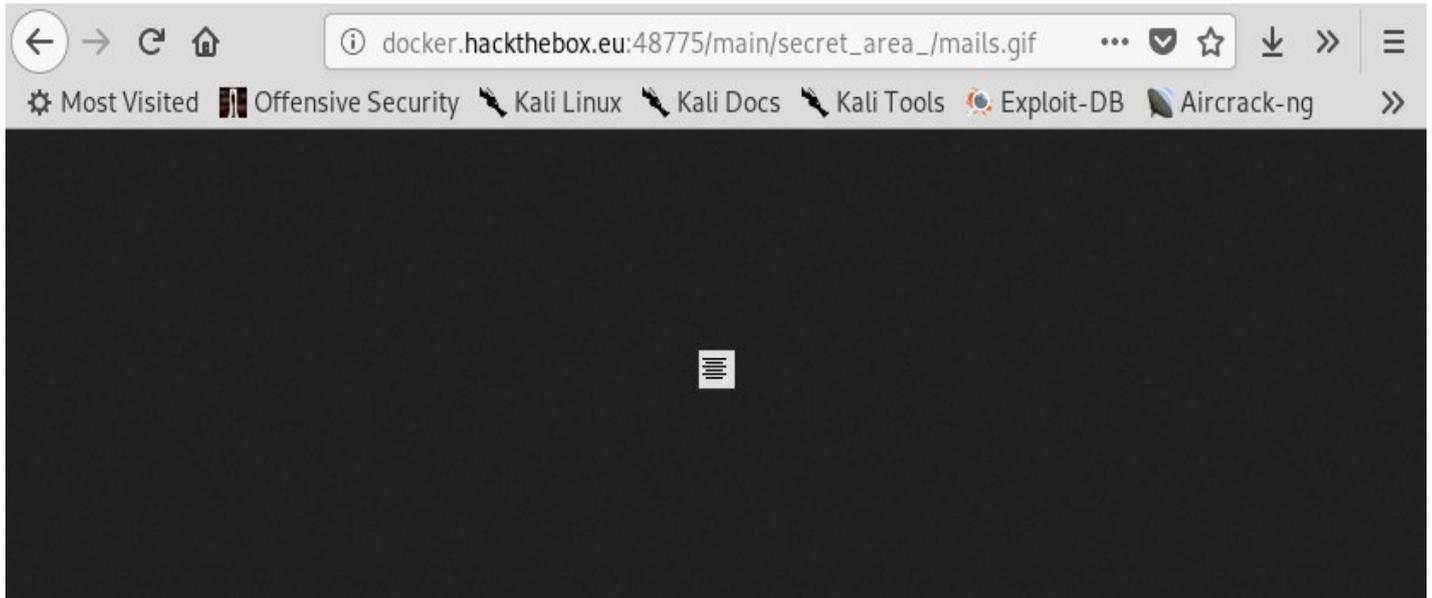
The screenshot shows a web browser window with the URL `docker.hackthebox.eu:48775/main/index.php`. The page header features the "aray matter" logo and the text "Hellenic Distribution Company Central Greece Section". The main content area is titled "CONTROL PANEL" and contains a form for sending an email. The form has a field for "Enter the email" and a larger "Body" field. A "Send" button is located below the form, and a "<< Back" link is positioned below the "Send" button. On the left side, there is a sidebar with a "Goals" section containing links for "Sociality", "Extensibility", and "Public Relations". Below this is a "Publicity and Capital Management" section with a list of tasks: "Investment and Share Purchase", "Main Adv Campaigns at media", "Approach new Customers using Social Engineering Techniques", and "Financing to find new 'Vendors'!". At the bottom of the sidebar is a "Main Tasks" section with links for "Send EMail" and "Mailbox of Special Customers".

Fillova te klikoj secilin imazh ne site per te gjetur ndonje gje, por prape pa ndonje rezultat dhe me pas shoh ne Special Customers' Mailbox, qe imazhi nuk mund te klikohet dhe provoj me View Image

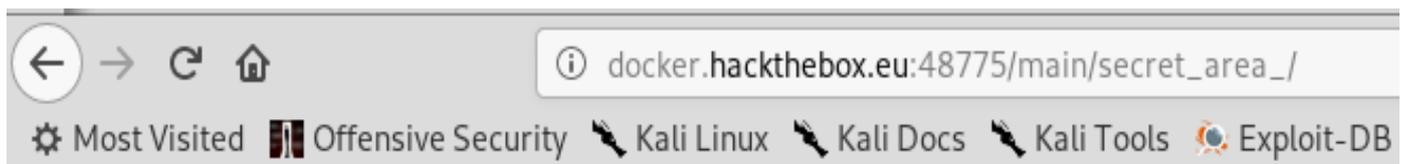


The screenshot shows the "Special Customers' Mailbox" page. The header is identical to the previous screenshot. The main content area is titled "Special Customers' Mailbox" and contains the following text: "Up to now we have 5 special customers who will help us to achieve our goals.", "This list will soon be expanded with the new 'expansion program' for our corporate goals.", and "It is planned that within the next six months we will have reached 20 dedicated Special Customers." Below the text is a row of ten diamond-shaped icons, each with a different color and pattern. The sidebar on the left is also identical to the previous screenshot, with the "Main Tasks" section containing links for "Send EMail" and "Mailbox of Special Customers".

Dhe me ane te View Image gjej direktorine secret\_area\_ , e cila ka dy file:



Klikoj ne file mails.txt dhe me jep listen e email-ve:

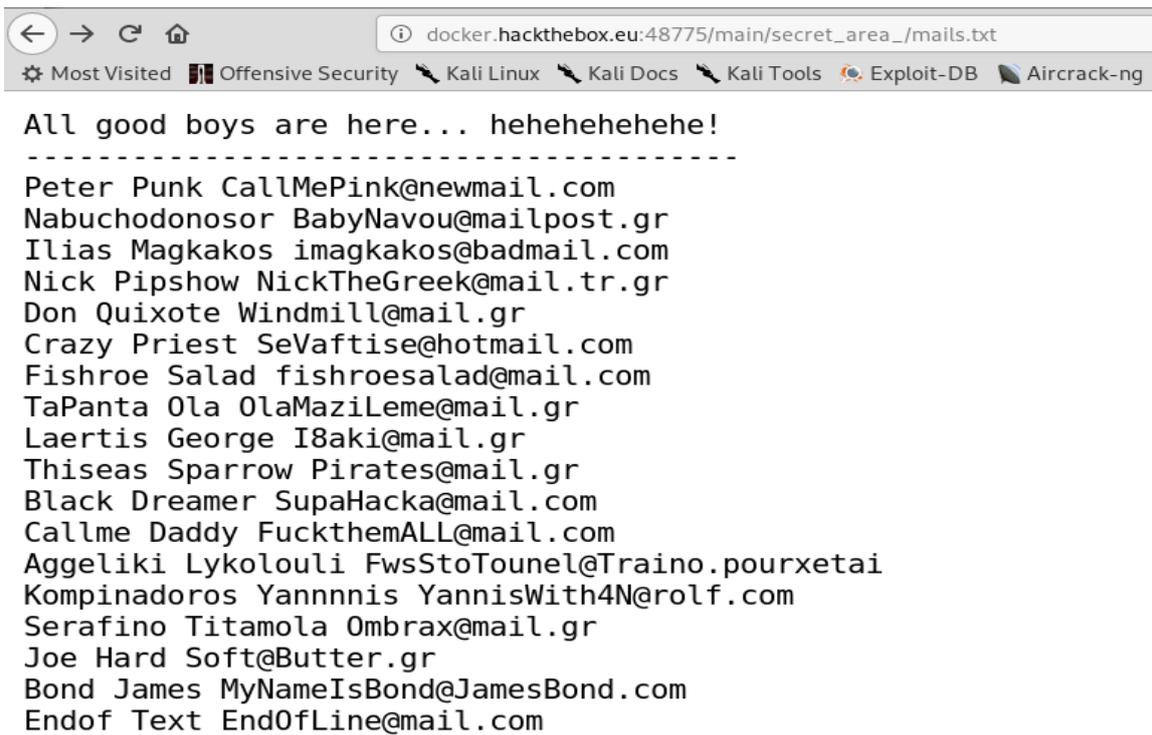


## Index of /main/secret\_area\_

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">mails.gif</a>	2010-10-23 18:28	71	
 <a href="#">mails.txt</a>	2017-07-08 17:55	705	

*Apache/2.4.18 (Ubuntu) Server at docker.hackthebox.eu Port 48775*

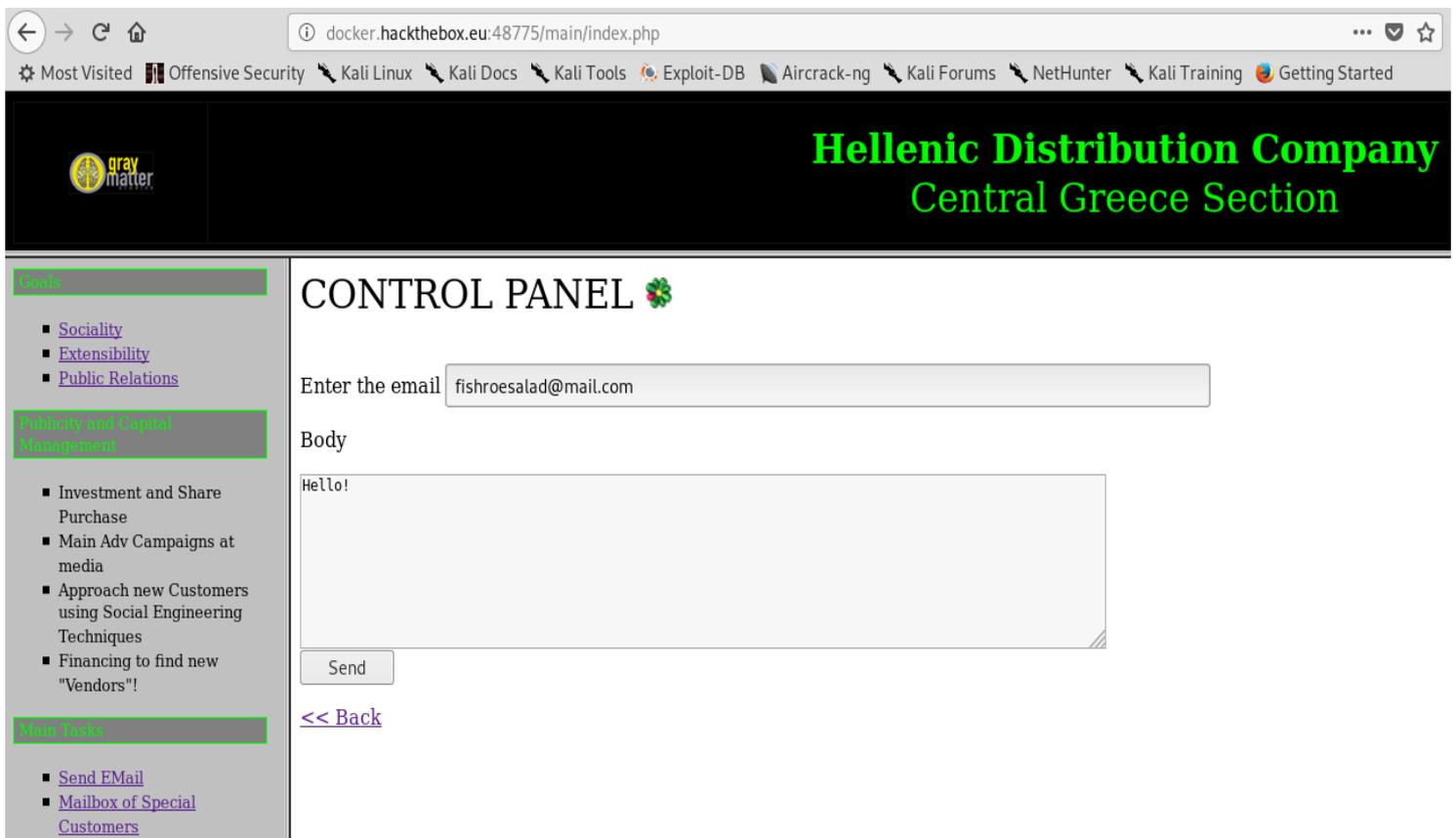
Pasiqe tanime kam listen e email-ave, duhet te dergoj email tek secili ne kete liste qe te provoj se cila eshte nga keto email adresa qe do me jap flag-un.



A screenshot of a web browser window. The address bar shows 'docker.hackthebox.eu:48775/main/secret\_area\_/mails.txt'. The page content is a list of email addresses, starting with 'All good boys are here... hehehehehehe!' and ending with 'Endof Text EndOfLine@mail.com'. The browser's bookmark bar includes 'Offensive Security', 'Kali Linux', 'Kali Docs', 'Kali Tools', 'Exploit-DB', and 'Aircrack-ng'.

```
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
Kompinodoros Yannnnis YannisWith4N@rolf.com
Serafino Titamola Ombrax@mail.gr
Joe Hard Soft@Butter.gr
Bond James MyNameIsBond@JamesBond.com
Endof Text EndOfLine@mail.com
```

Dhe kur arrij tek email adresa [fishroesalad@mail.com](mailto:fishroesalad@mail.com) ti dergoj email, kjo email adrese me jep flag-un.



A screenshot of a web application interface. The browser address bar shows 'docker.hackthebox.eu:48775/main/index.php'. The page header features the 'gray matter' logo and the text 'Hellenic Distribution Company Central Greece Section'. The main content area is titled 'CONTROL PANEL' and contains a form for sending an email. The 'Enter the email' field contains 'fishroesalad@mail.com' and the 'Body' field contains 'Hello!'. A 'Send' button is visible below the body field. A sidebar on the left contains navigation links for 'Goals', 'Publicity and Capital Management', and 'Main Tasks'.

**gray matter**

**Hellenic Distribution Company**  
Central Greece Section

**CONTROL PANEL** 🌸

Enter the email

Body

[<< Back](#)

**Goals**

- [Sociality](#)
- [Extensibility](#)
- [Public Relations](#)

**Publicity and Capital Management**

- Investment and Share Purchase
- Main Adv Campaigns at media
- Approach new Customers using Social Engineering Techniques
- Financing to find new "Vendors"!

**Main Tasks**

- [Send EMail](#)
- [Mailbox of Special Customers](#)

Dhe ketu kam flag-un nga dergimi i email qe bera, ne email adresen [fishroesalad@mail.com](mailto:fishroesalad@mail.com)

docker.hackthebox.eu:48775/main/index.php

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Kali Training Getting Started

 **Hellenic Distribution Company**  
Central Greece Section

**Goals**

- [Sociality](#)
- [Extensibility](#)
- [Public Relations](#)

**Publicity and Capital Management**

- Investment and Share Purchase
- Main Adv Campaigns at media
- Approach new Customers using Social Engineering Techniques
- Financing to find new "Vendors"!

**Main Tasks**

- [Send EMail](#)
- [Mailbox of Special Customers](#)

**Re: Hello there!**

Hi, I am still alive, don't worry :)

Congratz my friend!!

**The flag is:**

HTB{FuckTheB3stAndPlayWithTheRest!!}