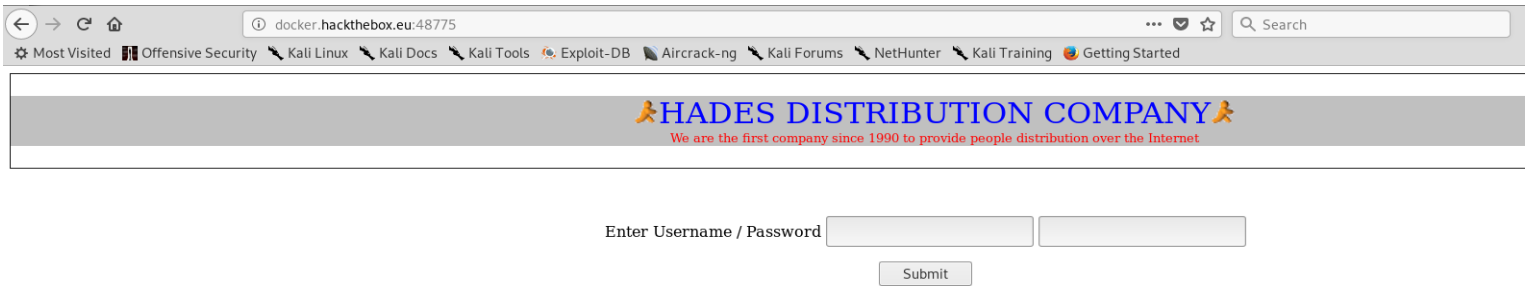
HACK THE BOX

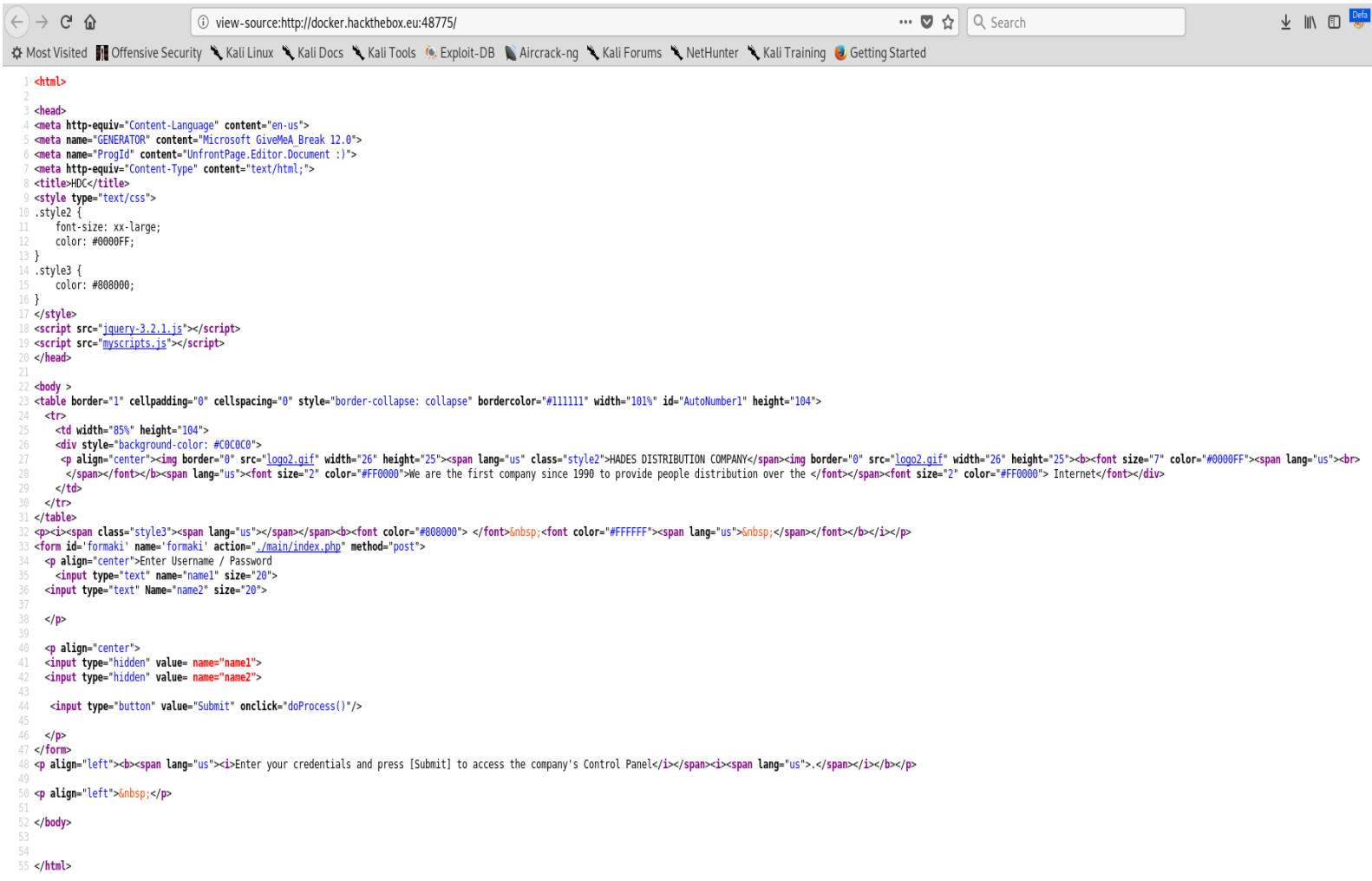
WEB CHALLENGE: HDC

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.



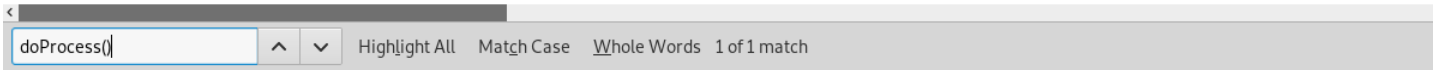
Per te gjetur username dhe password, fillimisht kerkova ne View Page Source qe te gjeja formen qe permban username dhe password, shoh qe username eshte i ruajtur si name1 dhe password si name2 ne form id=’formaki’, dhe funksioni doProcess()




```
<html>

<head>
<meta http-equiv="Content-Language" content="en-us">
<meta name="GENERATOR" content="Microsoft GiveMeA Break 12.0">
<meta name="ProgId" content="UnfrontPage.Editor.Document :)">
<meta http-equiv="Content-Type" content="text/html;">
<title>HDC</title>
<style type="text/css">
.style2 {
    font-size: xx-large;
    color: #0000FF;
}
.style3 {
    color: #808000;
}
</style>
<script src="jquery-3.2.1.js"></script>
<script src="myscripts.js"></script>
</head>

<body >
<table border="1" cellpadding="0" cellspacing="0" style="border-collapse: collapse" bordercolor="#111111" width="101%" id="AutoNumber1" height="104">
  <tr>
    <td width="85%" height="104">
    <div style="background-color: #C0C0C0">
     <p align="center"><img border="0" src="logo2.gif" width="26" height="25"><span lang="us" class="style2">HADES DISTRIBUTION COMPANY</span><img border="0" src="logo2.gif" width="26" height="25"><b><font size="7" color="#0000FF"><span lang="us"><br>
      </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>
    </td>
  </tr>
</table>
<p><i><span class="style3"><span lang="us"></span></span><b><font color="#808000"> </font> <font color="#FFFFFF"><span lang="us"> </span></font></b></i></p>
<form id='formaki' name='formaki' action="./main/index.php" method="post">
  <p align="center">Enter Username / Password
    <input type="text" name="name1" size="20">
  <input type="text" Name="name2" size="20">

  </p>

  <p align="center">
  <input type="hidden" value= name="name1">
  <input type="hidden" value= name="name2">

   <input type="button" value="Submit" onclick="doProcess()"/>

  </p>
</form>
<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">.</span></i></b></p>

<p align="left"> </p>

</body>


</html>
```

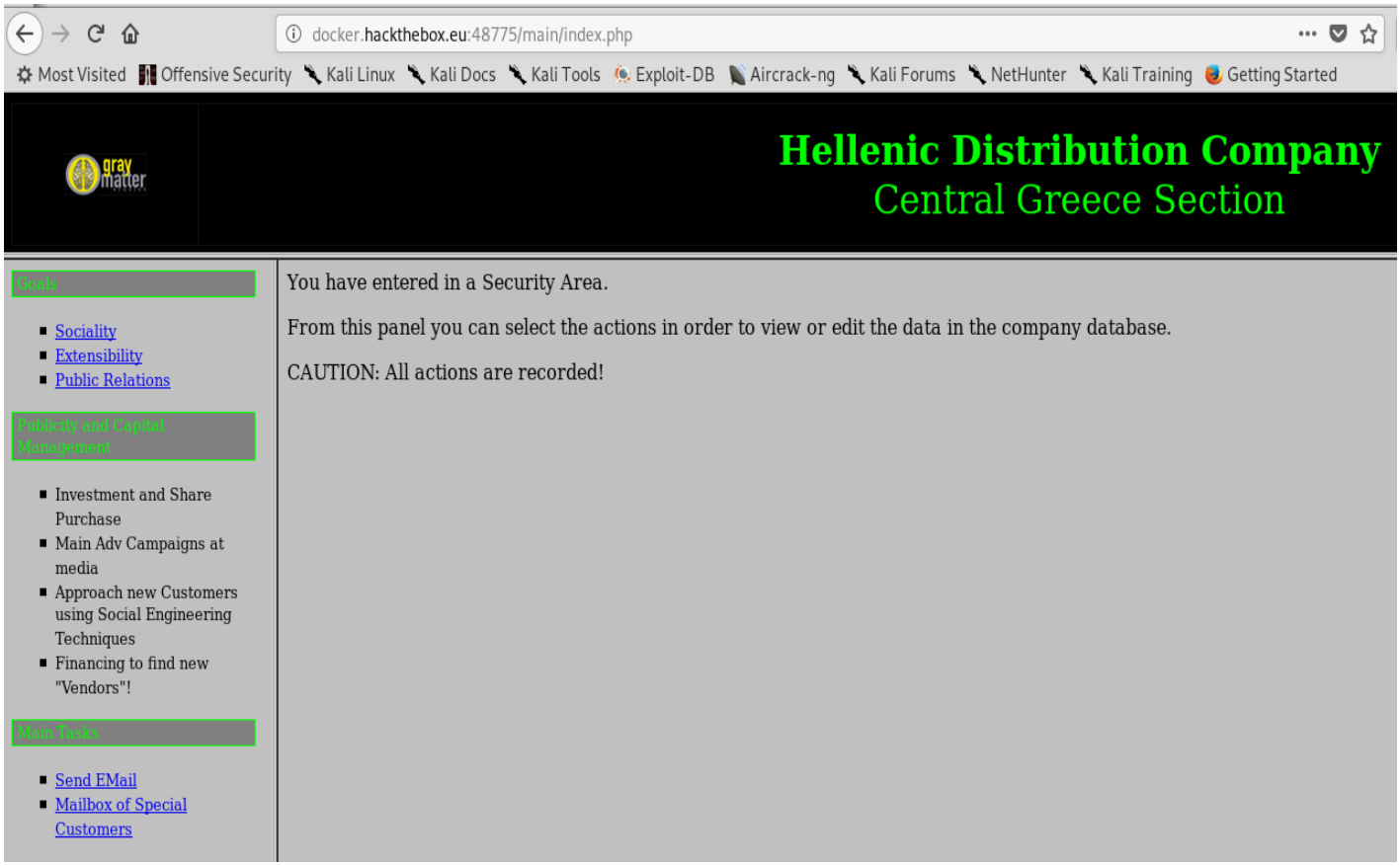
Kerkoj per funksionin doProcess() ne file jquery-3.2.1.js, dhe gjej username dhe password

```
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;
    }
```

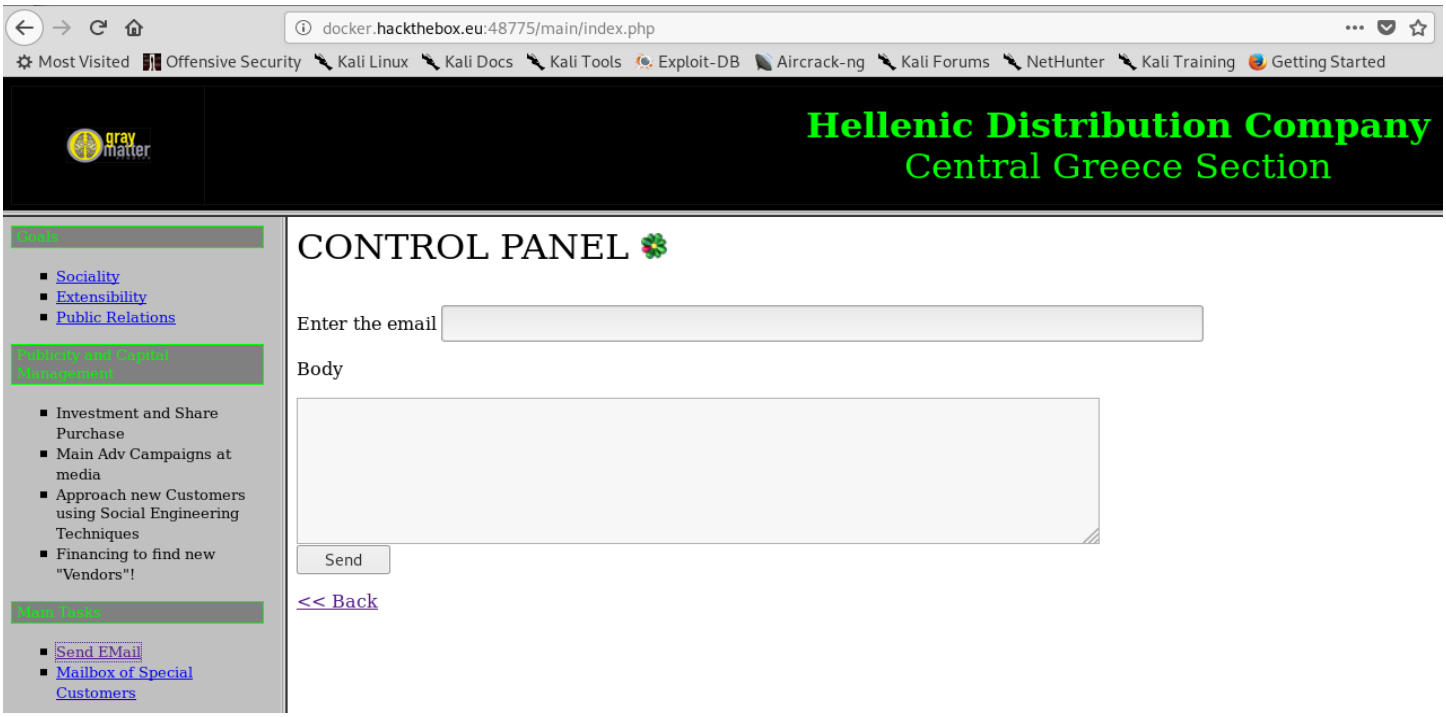



```
hiddenField.setAttribute("type","hidden");  hiddenField.setAttribute("name","name1");   hiddenField.setAttribute("value","TXlMaXR0bGU");

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

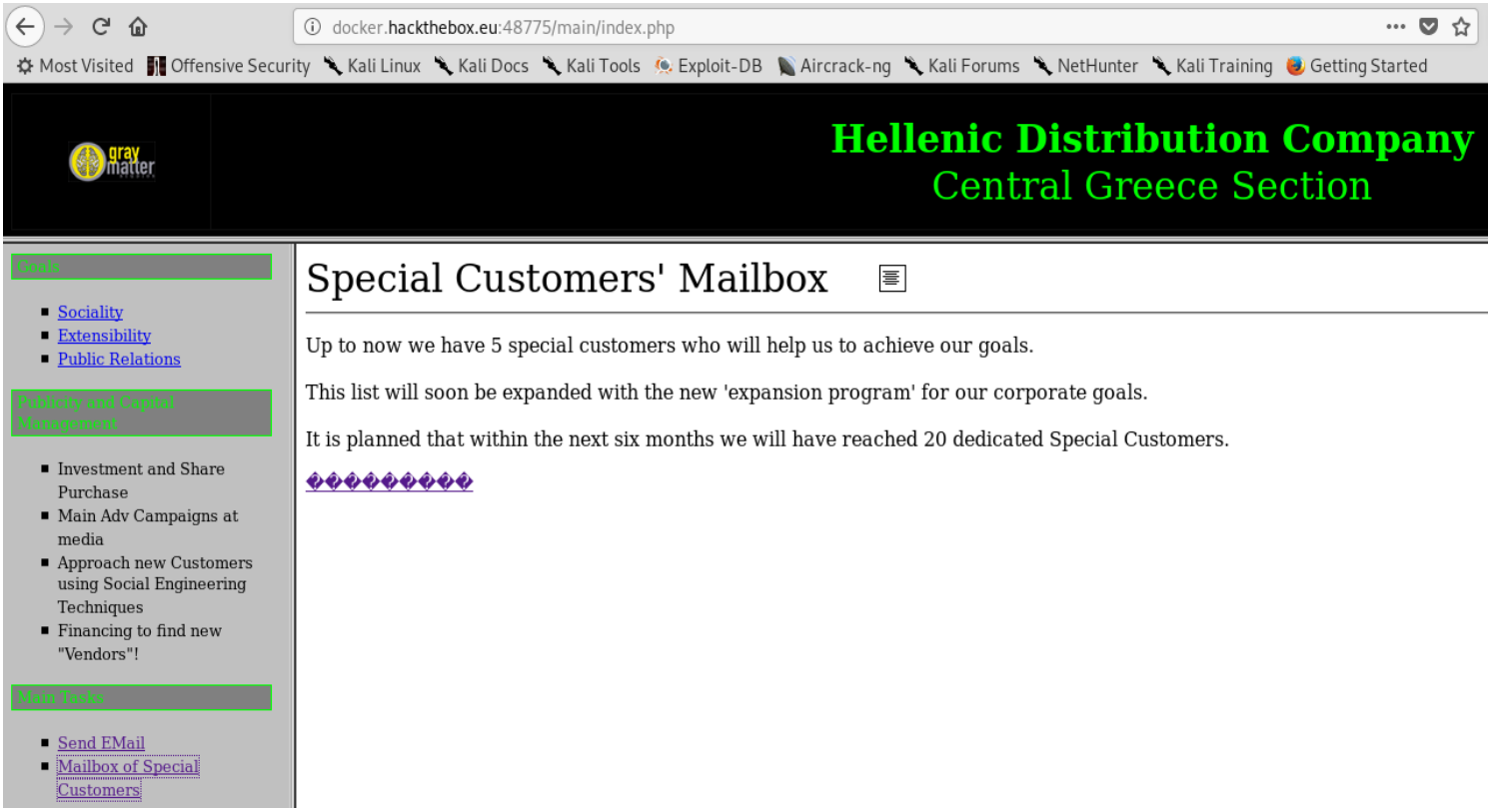
I jap username dhe password : TXlMaXR0bGU/cDB3bmll ne faqen loguese, dhe logohem.



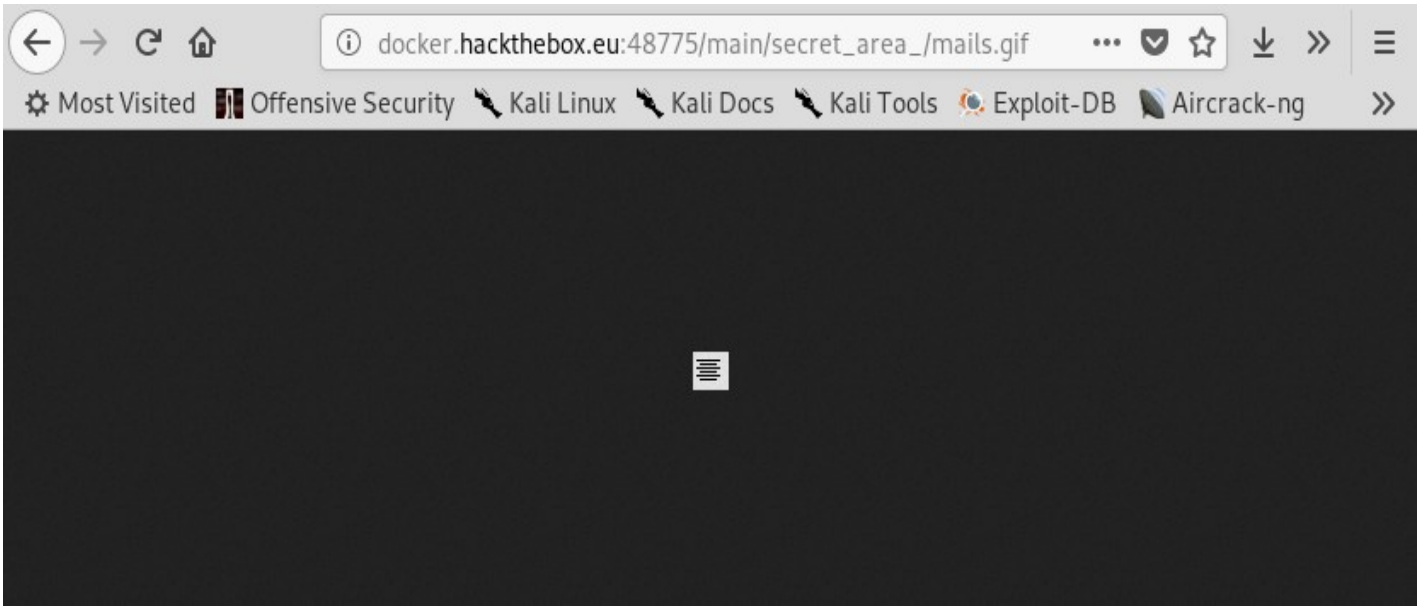
Filloj te shfletoj secilen faqe pas login-it, sidomos send Email dhe Mailbox of Special Customers, sipas pershkrimit qe me eshte dhene ne challenge, por pa ndonje rezultat per te vazhduar me tutje, keshtu qe filloj te shikoj imazhet qe jane ne kete web challenge.



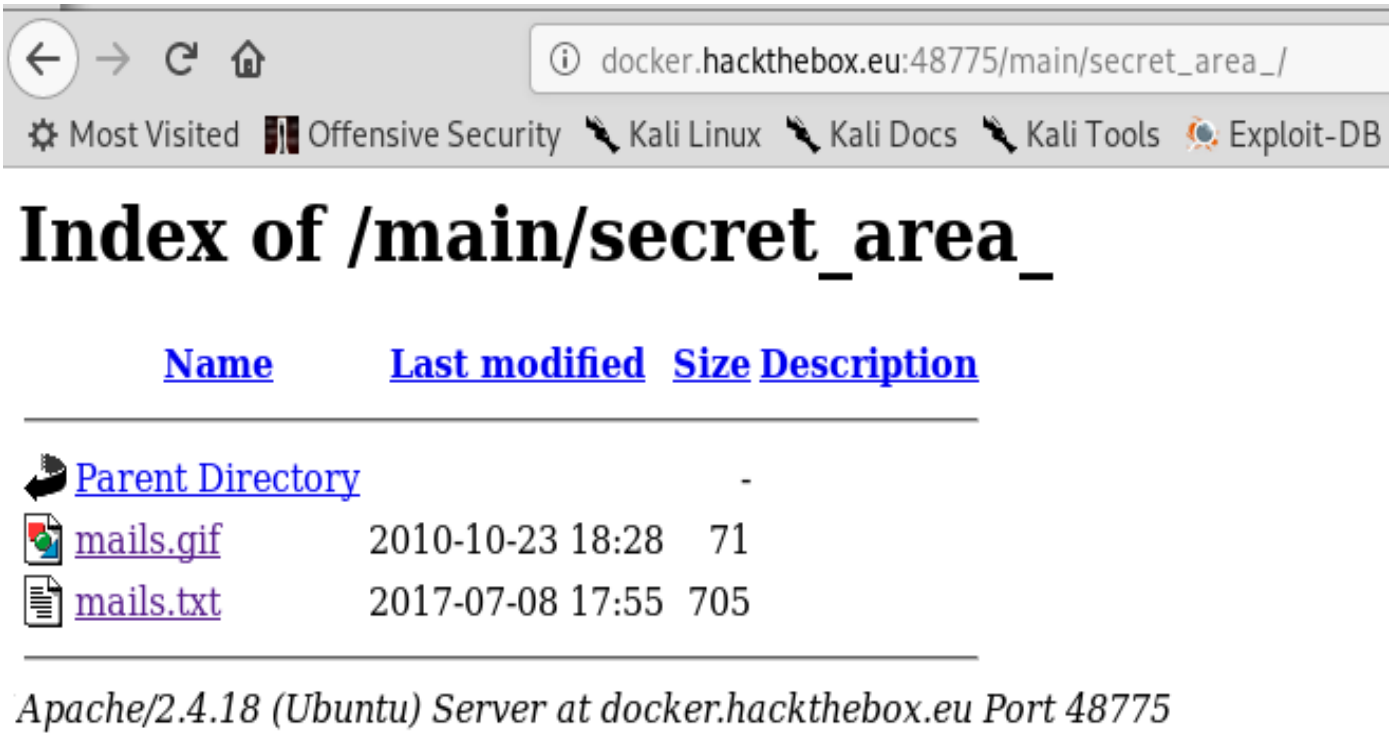
Fillova te klikoj secilin imazh ne site per te gjetur ndonje gje, por prape pa ndonje rezultat dhe me pas shoh ne Special Customers' Mailbox, qe imazhi nuk mund te klikohet dhe provoj me View Image



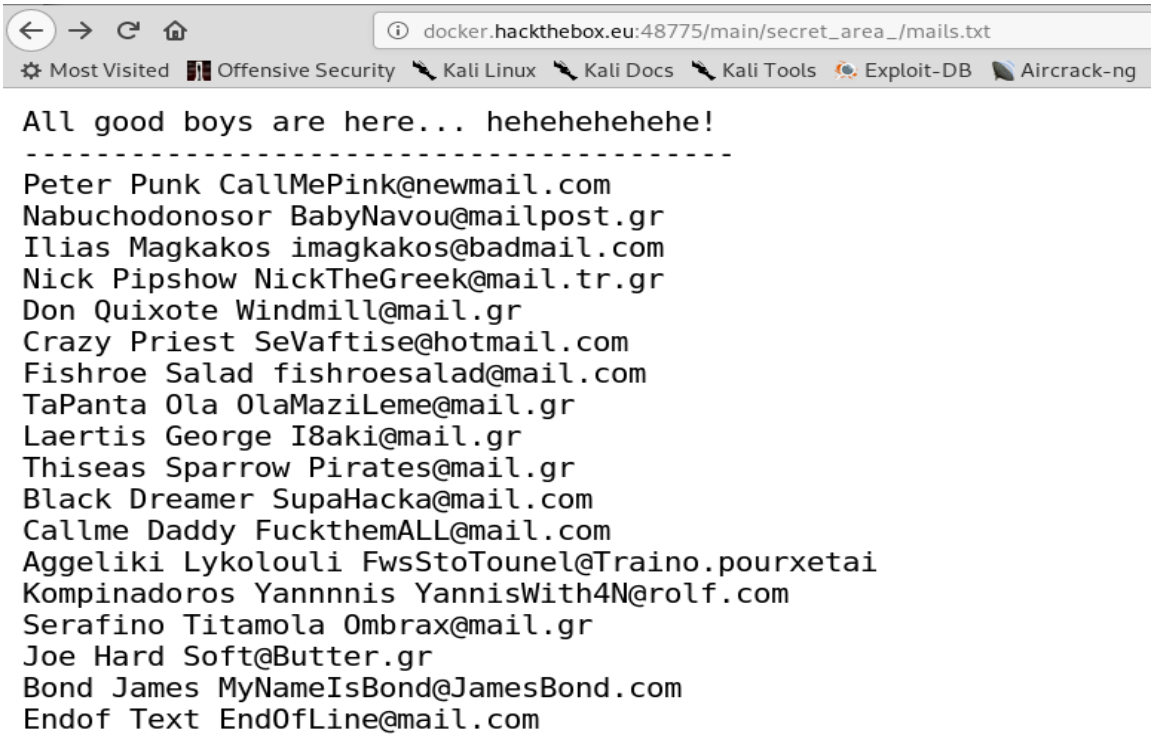
Dhe me ane te View Image gjej direktorine secret_area_ , e cila ka dy file:



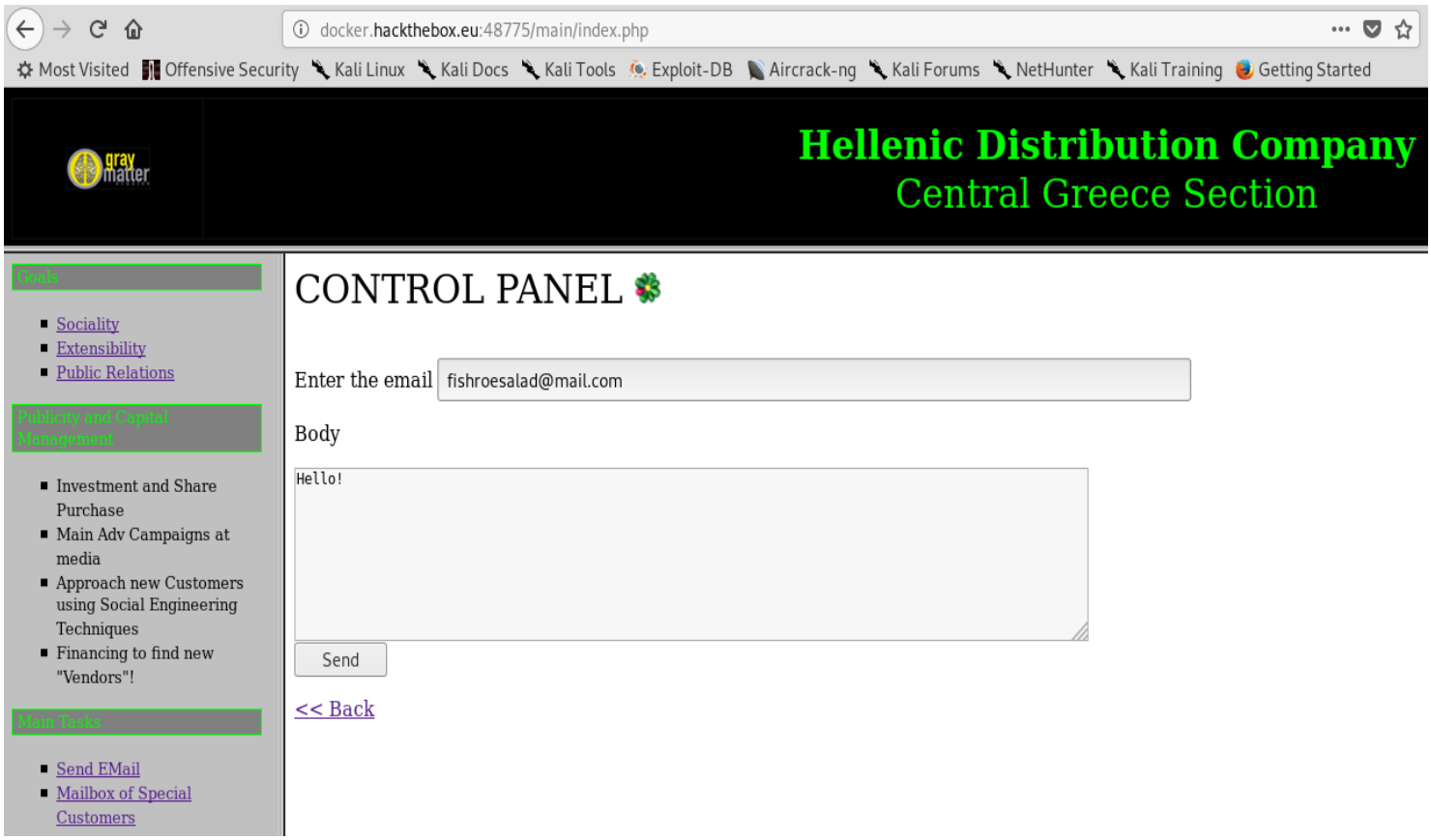
Klikoj ne file mails.txt dhe me jep listen e email-ve:



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.



Dhe kur arrij tek email adresa fishroesalad@mail.com ti dergoj email, kjo email adrese me jep flag-un.



Dhe ketu kam flag-un nga dergimi i email qe bera, ne email adresen fishroesalad@mail.com