hack the box challenge-web-HDC writeup

原创

唐仔橙 于 2020-11-24 14:44:18 发布 122 收藏 1
分类专栏： hackthebox 文章标签： 安全 安全漏洞 网络安全 信息安全

任务目标：

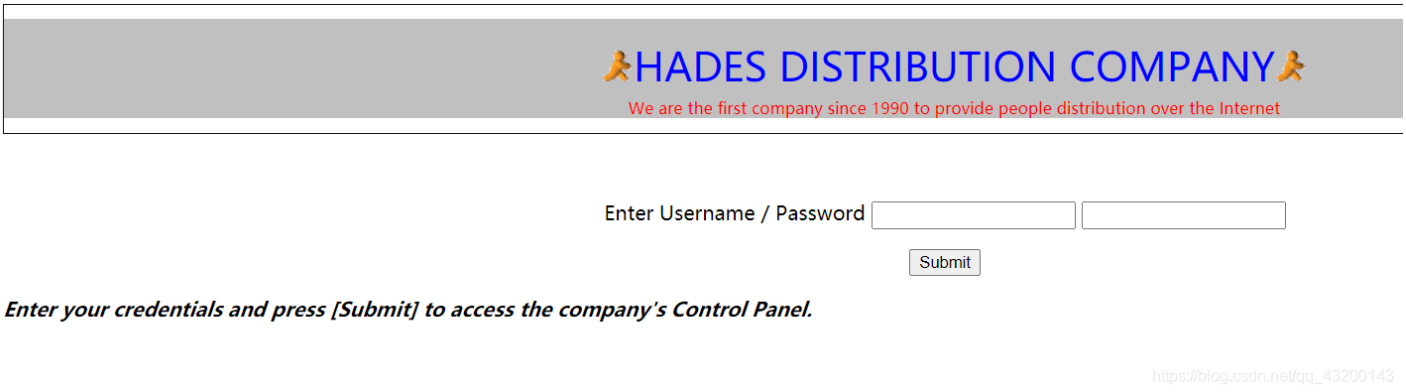
We believe a certain individual uses this website for shady business. Can you find out who that is and send him an email to check, using the web site's functionality?

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

寻找到正确的邮箱，然后给他发消息。

1.寻找突破口

首页进入后是这个样子，然后查看一下源代码



不安全 | view-source:178.62.0.100:30142

```
<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="#11
  <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=
      </span></font></b><span lang="us"><font size="2" color="#FF0000">We are the first company sinc
    </td>
  </tr>
</table>
<p><i><span class="style3"><span lang="us"></span></span><b><font color="#808000"> </font> <fon
<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">
```


发现有一个自己的js文件，查看一下

```
function doProcess()
{
        document.forms["formaki"].submit();
}
```

发现里面含有一个这个函数，然后从jquery里面找一下这个函数的具体信息

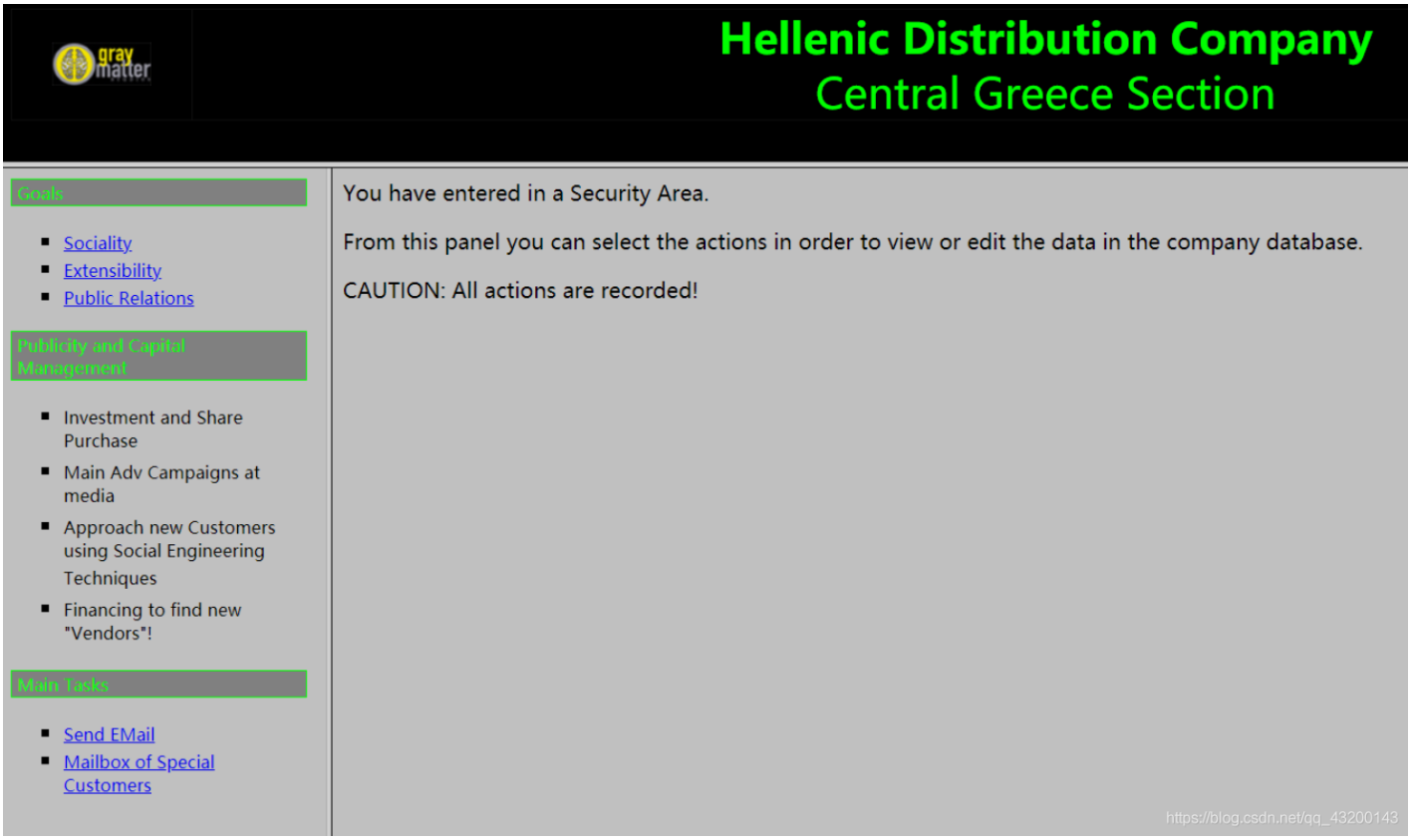
发现了账户名和密码

```
return jQuery;
} );

function doProcess()
{var form=document.createElement("form");      form.setAttribute("method","post");     form.setAttribute("action","main/index.php");     form.setAttribute("target","view");     var hiddenField=document.createElement("input");
hiddenField.setAttribute("type","hidden");      hiddenField.setAttribute("name","name1");       hiddenField.setAttribute("value","TXlMaXR0bGU");        var hiddenField2=document.createElement("input");
hiddenField2.setAttribute("type","hidden");     hiddenField2.setAttribute("name","name2");      hiddenField2.setAttribute("value","cDB3bml1");  form.appendChild(hiddenField2);        form.appendChild(hiddenField);
form.appendChild(hiddenField2); document.body.appendChild(form);                window.open('','view'); form.submit();}


function getData( data ) {
```

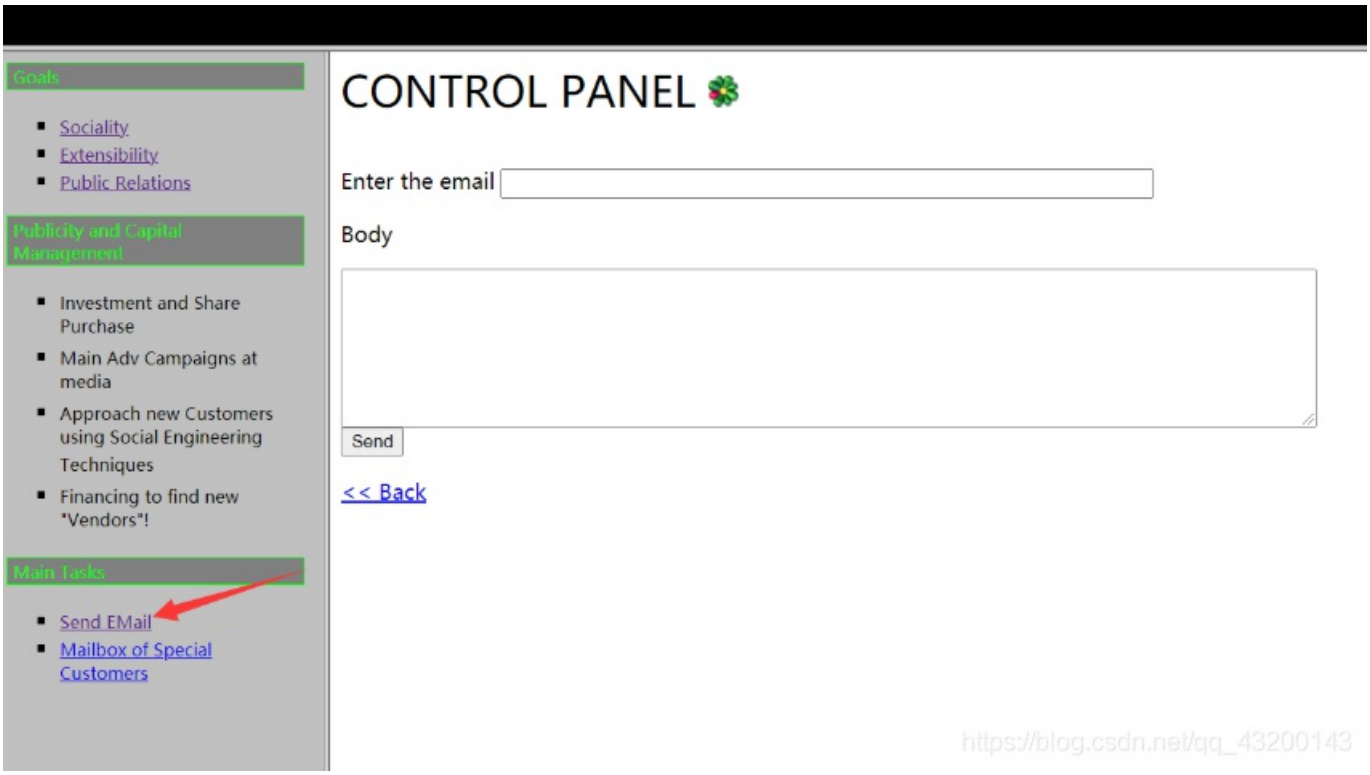
登录成功！！！



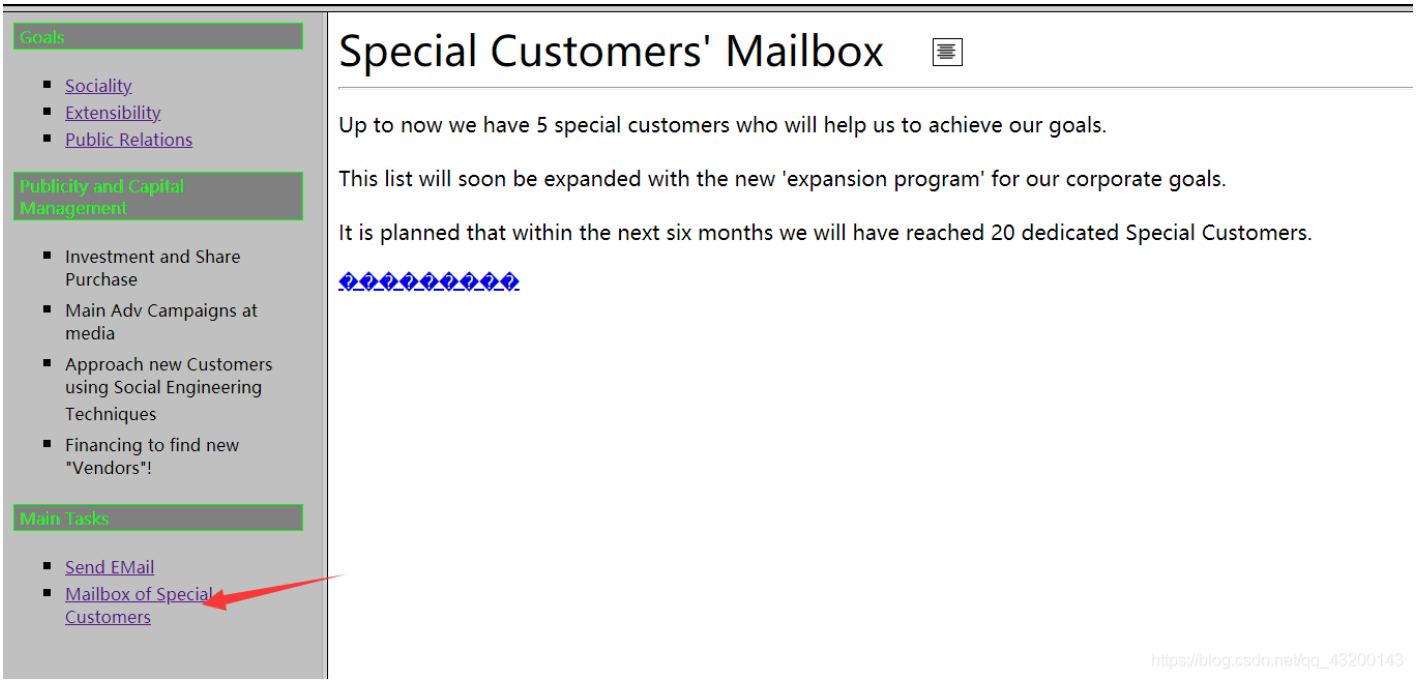
2.进一步探索

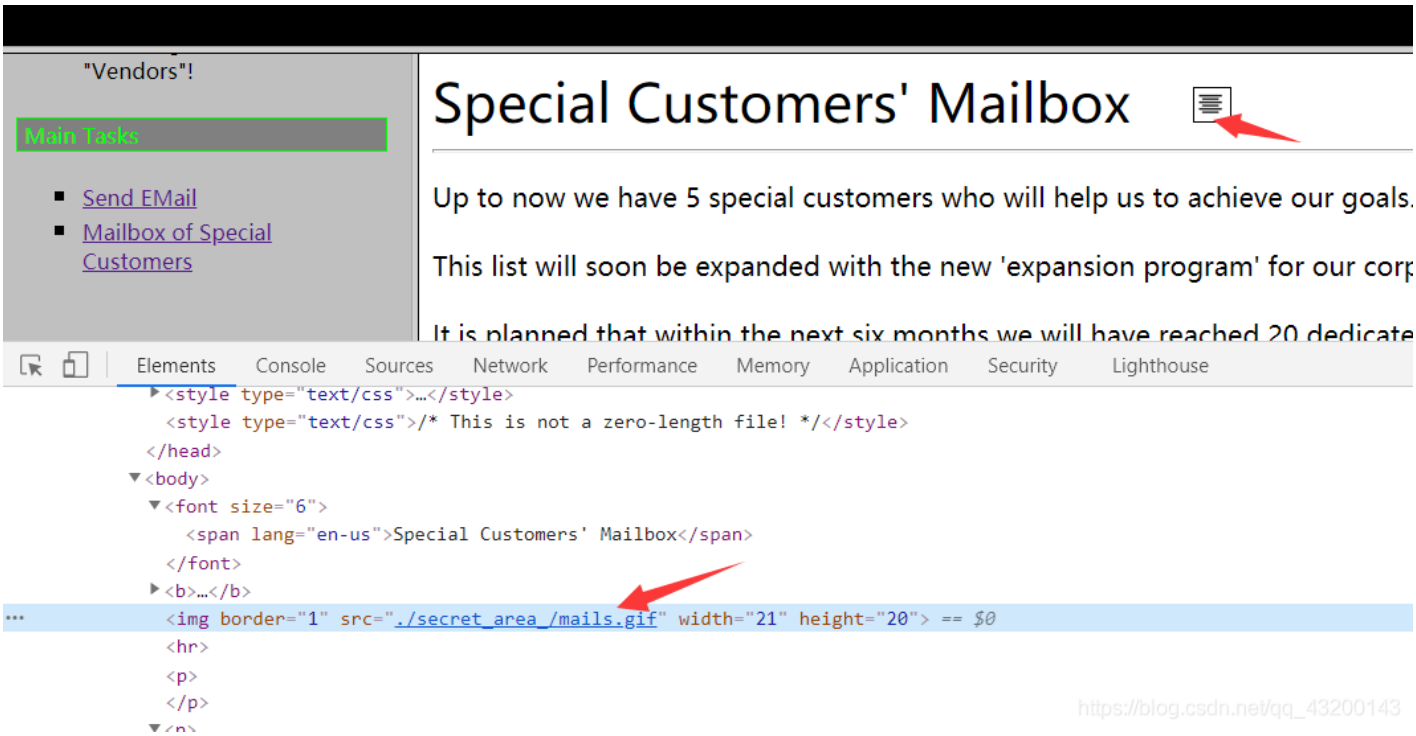
注意到这里

发现了发送邮件的地方，查看源码，发现一些东西显示不出来，那么就用F12开发者工具看吧



看到这里，发现了那些人的邮箱！F12查看





可以看到这里存在一个路径，图片的路径，

这里能够学习到的一点就是要观察页面出现的服务器的路径，可能存在目录遍历漏洞等

3.最后的寻找、获取flag!

在这里能看到邮箱txt！！！找到他了！！

```
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 MyNameIsBond@JamesBond.com
Endof Text EndOfLine@mail.com
```


然后就可以从刚才发现的页面去提交了

不算是很多，可以自己一个个尝试，也可以用bp或者自己写个脚本

都尝试了一遍。。问什么不行呢。。。

。。。。。傻了，前面是人名，，后面是邮箱。。。

成功获得flag！