

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_43200143/article/details/110076650

版权



[hackthebox](#) 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

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



Enter Username / Password

Submit

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

https://blog.csdn.net/qq_43200143

```
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: #808000;
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="#11
24 <tr>
25 <td width="85%" height="104">
26 <div style="background-color: #COCOCO">
27 <p align="center"><span lang="us" class=
28 </span></font></b><span lang="us"><font size="2" color="#FF0000">We are the first company sinc
29 </td>
30 </tr>
31 </table>
32 <p><i><span class="style3"><span lang="us"></span></span><b><font color="#808000"> </font>&nbsp;<font
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
```

https://blog.csdn.net/qq_43200143

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");
    hiddenField.setAttribute("type","hidden");
    hiddenField2.setAttribute("type","hidden");
    form.appendChild(hiddenField2);
    document.body.appendChild(form);
    form.setAttribute("method","post");
    hiddenField.setAttribute("name","name1");
    hiddenField2.setAttribute("name","name2");
    window.open("","view");
    form.setAttribute("action","./main/index.php");
    hiddenField.setAttribute("value","TXlMaXRObGUGU");
    hiddenField2.setAttribute("value","cB83bm1l");
    form.setAttribute("target","view");
    var hiddenField=document.createElement("input");
    var hiddenField2=document.createElement("input");
    form.appendChild(hiddenField2);
    form.appendChild(hiddenField);
    form.submit();
}
```

https://blog.csdn.net/qq_43200143

登录成功!!!

The screenshot shows a web application interface for the Hellenic Distribution Company, Central Greece Section. The header features the 'gray matter' logo on the left and the company name in green text on the right. The main content area is divided into a left sidebar and a right main panel. The sidebar contains three sections: 'Goals' with links for 'Sociality', 'Extensibility', and 'Public Relations'; 'Publicity and Capital Management' with links for 'Investment and Share Purchase', 'Main Adv Campaigns at media', 'Approach new Customers using Social Engineering Techniques', and 'Financing to find new "Vendors"!'; and 'Main Tasks' with links for 'Send EMail' and 'Mailbox of Special Customers'. The main panel displays a security warning: 'You have entered in a Security Area. From this panel you can select the actions in order to view or edit the data in the company database. CAUTION: All actions are recorded!'. A URL 'https://blog.csdn.net/qq_43200143' is visible in the bottom right corner of the screenshot.

2.进一步探索

注意到这里

This is a close-up screenshot of the 'Main Tasks' section from the previous image. It shows a list of two items: 'Send EMail' and 'Mailbox of Special Customers', both underlined. The URL 'https://blog.csdn.net/qq_43200143' is visible at the bottom of the screenshot.

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

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](#)

CONTROL PANEL

Enter the email

Body

[<< Back](#)

https://blog.csdn.net/qq_43200143

看到这里，发现了那些人的邮箱！F12查看

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](#)

Special Customers' Mailbox

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.

It is planned that within the next six months we will have reached 20 dedicated Special Customers.



https://blog.csdn.net/qq_43200143

"Vendors!"

Main Tasks

- Send EMail
- Mailbox of Special Customers

Special Customers' Mailbox

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 corp

It is planned that within the next six months we will have reached 20 dedicate

Elements Console Sources Network Performance Memory Application Security Lighthouse

```

<style type="text/css">...</style>
<style type="text/css">/* This is not a zero-length file! */</style>
</head>
<body>
  <font size="6">
    <span lang="en-us">Special Customers' Mailbox</span>
  </font>
  <b>...</b>
   == $0
  <hr>
  <p>
  </p>
  </body>

```

https://blog.csdn.net/qq_43200143

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!!!

← → ↻ ▲ 不安全 | 178.62.0.100:30142/main/secret_area_ /

Index of /main/secret_area_

Name	Last modified	Size	Description
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 178.62.0.100 Port 30142

https://blog.csdn.net/qq_43200143

All good boys are here... hehehehehe!

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
Theseas Sparrow Pirates@mail.gr
Black Dreamer SupaHacka@mail.com
Callme Daddy FuckthemALL@mail.com
Aggeliki Lykolouli FwsStoToune1@Traino.pourxetai
Kompinatoros Yarrnnis YannisWith4N@rolf.com
Serafino Titamola Ombrax@mail.gr
Joe Hard Soft@Butter.gr
Bond James MyNameIsBond@JamesBond.com
Endof Text EndOfLine@mail.com https://blog.csdn.net/qq_43200143

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。。。

The screenshot shows a web interface. On the left, there is a sidebar with a list of tasks:

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

The "Main Tasks" section is highlighted with a green border, containing:

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

The main content area on the right displays the following text:

Re: Hello there!

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

Congratz my friend!!

The flag is:

[HTR/... \(with the flag!!\)](#)

https://blog.csdn.net/qq_43200143

成功获得flag!