Hackthis!! Writeup——Main Level

原创

Roverdoge 于 2018-12-30 23:52:51 发布 239 收藏 1

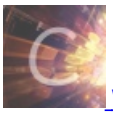
分类专栏： hackthis WP 文章标签： hackthis writeup main

本文链接：https://blog.csdn.net/qq_43148462/article/details/85413695

hackthis 同时被 2 个专栏收录

5 篇文章 0 订阅

订阅专栏



WP

5 篇文章 0 订阅

订阅专栏

Level 1:

最常见的查看源代码，然后可以轻易地找到注释中的username和Password

```
<link href="/favicon.png" rel="icon" id="basic-favicon" type="images/png" />
<link rel="shortcut icon" href="/favicon.ico" type="image/vnd.microsoft.icon" />
<link rel="icon" href="/favicon.ico" type="image/vnd.microsoft.icon" />

<meta property="fb:app_id" content="163820353667417" />
<meta name='twitter:site' content='@hackthisuk'>
<meta property='og:site_name' content='HackThis!!'>

<link href='https://fonts.googleapis.com/css?family=Orbitron%7CLato%3A400%2C700' rel='stylesheet' type='text/css'>

<link rel='stylesheet' href='/files/css/min/dark/main.css?1492506645' type='text/css' />
<link rel='stylesheet' href='/files/css/min/dark/extra_d33b50696e.css?1492506645' type='text/css' />

<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.9.1/jquery.min.js"></script>
<!-- <script src="https://cdn.socket.io/socket.io-1.2.1.js"></script> -->
<!-- username: in, password: out -->
<script src="https://d3t63mlrxnixd2.cloudfront.net/files/js/modernizr-2.6.2.min.js"></script>
<!--[if lt IE 9]>
<script src="https://d3t63mlrxnixd2.cloudfront.net/files/js/respond.min.js"></script>
<script src="https://d3t63mlrxnixd2.cloudfront.net/files/js/html5shiv.js"></script>
<![endif]-->

</head>
<body class='theme-dark ' data-username='roverdoge' data-key='69552bfb202a5ce8'>


<div class="page-wrap">
<div id="header-wrap" class="container clr">
<header>
<div class="col span_11 banner">
```

PASS 高亮全部(A) 区分大小写(C) 匹配词句(W) 第 1 项，共找到 6 个匹配项 到达页尾，从页首继续

Level 2:

同样是查看源代码，然后就隐藏在代码行中

```
<form method="POST">
            <fieldset>
                <label for="user">Username:</label> <span style="color: #000000">resu</span>
                <input type="Text" name="user" id="user" autocomplete="off"><br>
                <label for="user">Password:</label> <span style="color: #000000">ssap</span>
                <input type="Password" name="pass" id="pass" autocomplete="off"><br>
                <input type="submit" value="Submit" class="button">
```

Level 3:

同样是查看源代码，这次是一个JS代码验证（然而关掉JS并绕不过。。服务器端应该也有验证）

```
ction(){ $('.level-form').submit(function(e){ if(document.getElementById('user').value == 'heaven' && document.getElementById('pass').value == 'hell')
r clr">
```

Level4:

```
                <label for="user">Username:</label>
                <input type="Text" name="user" id="user" autocomplete="off"><br>
                <label for="user">Password:</label>
                <input type="Password" name="pass" id="pass" autocomplete="off"><br>
                <input type="hidden" name="passwordfile" value="../../extras/ssap.xml">
                <input type="submit" value="Submit" class="button">
```

同样是查看源代码，这次给了一个网页 直

```
- <user>
    <name>Admin</name>
    <username>999</username>
    <password>911</password>
  </user>
```

接访问这个url，得到密码

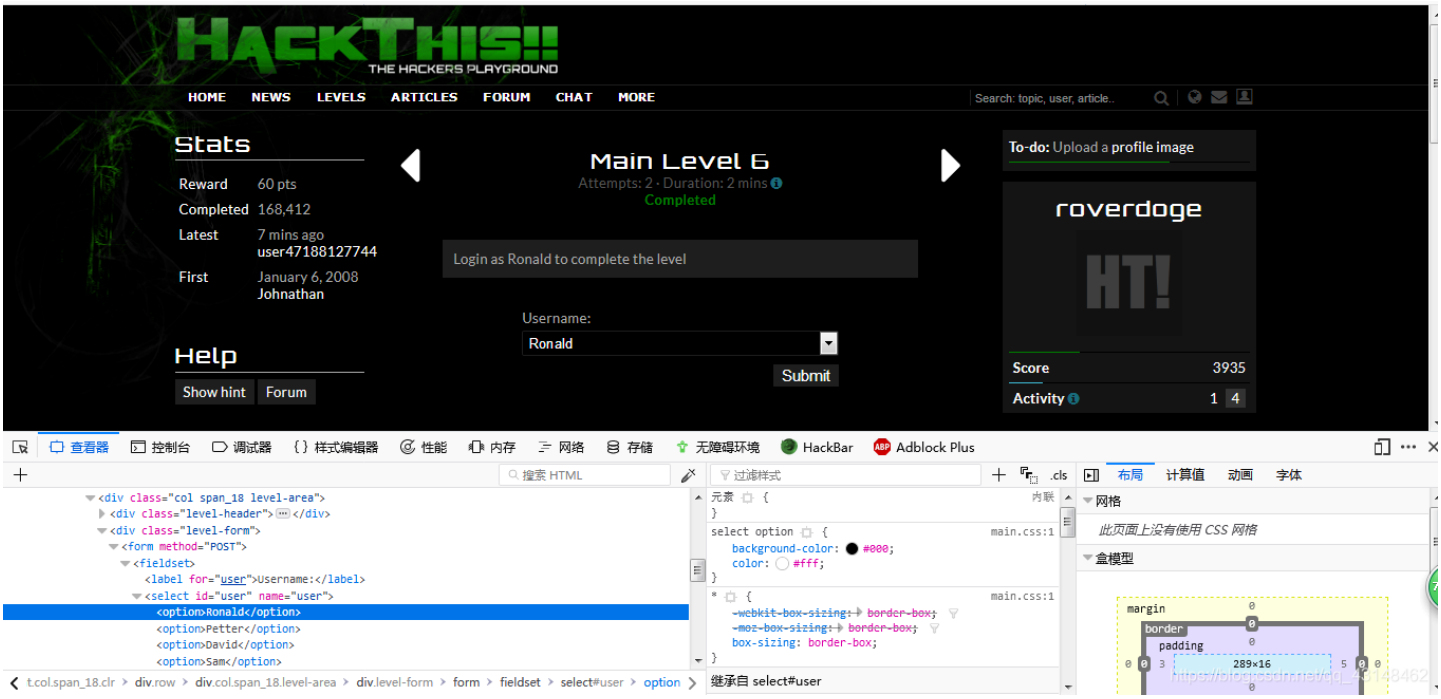
Level 5:

```
    <div class='level-form'>
script language="JavaScript" type="text/javascript">
    var pass;
    pass=prompt("Password","");
    if (pass=="9286jas") {
        window.location.href="/levels/main/5?pass=9286jas";
    }
```

同样是查看源代码，然后可以发现以下JS代码：
这里是通过修改url来用GET方法通关

Level 6:

首先我们可以看到，要求用户选择为Ronald，而选项框中没有Ronald。
因此，我们可以有两条思路：
1，通过修改html来得到Ronald的选项，如下图。



我是用的firefox的开发工具（F12开启）
2，通过对传输数据的包进行修改，如下图。

```
POST https://www.hackthis.co.uk/levels/main/6 HTTP/1.1
Host: www.hackthis.co.uk
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Referer: https://www.hackthis.co.uk/levels/main/6
Content-Type: application/x-www-form-urlencoded
Content-Length: 9
Connection: keep-alive
Cookie: _ga=GA1.3.589989448.1545123388; autologin=%92%A5Vy%98%14e%C2%D4%E0%C4%0Az%5B%B68%E8z%FF%5B%15%8O%CC%F3%B7VC%FD%DF%A6%13%F7%86%5
Upgrade-Insecure-Requests: 1

User=Ronald
```

这里我用的是Fiddler，在上传前进行截断并修改可得到Ronald。

Level 7:

同样查看源代码。。。。哦不这次好像并不是
于是看了一下hint，得到以下信息：

> The password is again stored in a txt file. This time however it is not as straight forward as viewing the source.
> You wouldn't even find the page by using a search engine as search bots have been excluded.

这个提示所给的信息指向一个关键网页：robots.txt（关于robots协议，请自行百度其功能）

```
User-agent: *
Allow: /
Disallow: /contact.php
Disallow: /inbox/
Disallow: /levels/
Disallow: /levels/extras/userpass.txt
Disallow: /users/
Disallow: /ctf/8/php/*
```

于是，我们访问这个页面，得到以下信息：
至此我们找到了这个所谓的txt文件。访问这个网页得到以下账号密码：

> 48w3756
> u3qh458

Level8：

首先依旧是查看源代码，得到以下提示：

```
    <div class='level-form'>
<form method="POST">
    <fieldset>
        <label for="user">Username:</label>
        <input type="Text" name="user" id="user" autocomplete="off"><br>
        <label for="user">Password:</label>
        <input type="Password" name="pass" id="pass" autocomplete="off"><br>
        <input type="hidden" name="passwordfile" value="extras/secret.txt">
        <input type="submit" value="Submit" class="button">
    </fieldset>
```

访问这个页面，得到以下信息：

> 1011 0000 0000 1011
> 1111 1110 1110 1101

这里需要手动将2进制转换成16进制，并按照ASCII表对应出user和pass。

Level9：

首先依旧查看源代码，发现了这个东西：

```
<div class='level-form'>
    <form method="POST">
        <fieldset>
            <label for="user">Username:</label>
            <input type="Text" name="user" id="user" autocomplete="off"><br>
            <label for="user">Password:</label>
            <input type="Password" name="pass" id="pass" autocomplete="off"><br>
            <a class='left' href='?forgot'>Request details</a>
            <input type="submit" value="Submit" class="button">
```

进入这个页面，然后继续查看源代码，得到以下信息：

```
<div class='level-form'>
    <form method="POST">
        <fieldset>
            <label for="email1">Email:</label>
            <input type="text" name="email1" id="email1" autocomplete="off"><br>
            <input type="hidden" name="email2" id="email2" value="admin@hackthis.co.uk" autocomplete="off">
            <input type="submit" value="Submit" class="button">
        </fieldset>
```

将下面这个邮箱填入框中，然后。。。。不对

```
email1=admin%40hackthis.co.uk&email2=admin%40hackthis.co.uk
```

于是，我用Fiddler抓了下包，发现他发送了两条信息 然后根据提示：

> The developer has now added a feature that allows him to get a password reminder. Can you exploit it to send you the login details instead?

得出以下结论：是需要把email2和email1都改成自己的邮箱。
更改后，通过。

Level 10:

依旧是首先查看源代码，得到以下信息：

```
    <fieldset>
        <label for="user">Username:</label>
        <input type="Text" name="user" id="user" autocomplete="off"><br>
        <label for="user">Password:</label>
        <input type="Password" name="pass" id="pass" autocomplete="off"><br>
        <input type="hidden" name="passwordfile" value="level10pass.txt">
        <input type="submit" value="Submit" class="button">
    </fieldset>
```

访问这个文件，便可以得到以下密文：

> 69bfe1e6e44821df7f8a0927bd7e61ef208fdb25deaa4353450bc3fb904abd52
> f1abe1b083d12d181ae136cfc75b8d18a8ecb43ac4e9d1a36d6a9c75b6016b61

这里使用了MD5加密，解密网站如下

> https://www.cmd5.com/

解密之后便可得到user和pass。