Hackthis!! Writeup——Javascript Level

原创

Roverdoge 于 2019-03-05 11:27:22 发布 200 收藏

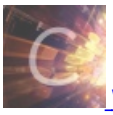
分类专栏： hackthis WP

本文链接：https://blog.csdn.net/qq_43148462/article/details/88173814

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:

查看源代码，搜索script，发现以下一段代码：

```
$(function(){ $('.level-form').submit(function(e){ e.preventDefault(); if(document.getElementById('pass').value == correct) { document.location = '?pass=' + correct; } else { alert('Incorrect password') } })})
```

这段代码判断输入的值是否等于变量"correct"的值，于是我们去找correct的值。搜索correct，发现

```
var correct = 'jrules'
```

于是填入jrules，通过。

Level 2:

依旧先查看源代码，搜索script，发现以下代码：

```
$(function(){ $('.level-form').submit(function(e){ e.preventDefault(); if ($('.level-form #pass')[0].value.length == length) { document.location = "2?x=" + length; } else { alert('Incorrect Password'); } }); });
```

这段代码是判断我们的密码的位数是否与“length”相等，于是去找length，发现了一段代码：

```
var length = 5; var x = 3; var y = 2; y = Math.sin(118.13); y = -y; x = Math.ceil(y); y++; y = y+x+x; y *= (y/2); y++; y++; length = Math.floor(y);
```

这里 没必要去算，直接拖进控制台里执行得到结果就ok了，然后填入指定位数的密码，通过。

Level 3:

同上，得到以下代码：

```
var thecode = 'code123'; $(function(){ $('.level-form').submit(function(e){ e.preventDefault(); if ($('.level-form #pass')[0].value == thecode) { document.location = "?pass=" + thecode; } else { alert('Incorrect Password'); } }); });
```

很明显是判断我们填入的密码是否为code123。但是我们填入code123，却提示不正确。这里其实是变量覆盖，由于在main.js中也声明了thecode=getinthere，则该变量的值被覆盖为getinthere。具体的覆盖规则我也还没有搞懂，还需要多加学习啊。。

另外，这里其实可以直接在控制台里alert(thecode)来获取这个变量的值。

Level4:

和上面一样，先查看源代码，这次什么都没有发现。。。
于是用fiddler抓一下包，发现该网页经过了一次跳转：先进入的是
https://www.hackthis.co.uk/levels/javascript/4
然后经过
`document.location = '?input';`
的跳转进入最终显示的页面 。
回到跳转前的页面，在源代码中得到密码：
The password is: smellthecheese

Level5:

这次上来直接弹窗要密码。我们还是先查看源代码，发现源代码中没有，于是我们思考是不是放在单独的js文件里。在firefox开发者工具中有调试器，发现有main.js和extra_xxxxxxx.js两个js。分别搜索password，最后在第二个js中发现以下代码：
`p=prompt("Password:","");if(p==d){window.location="?pass="+p;}else{window.location="/levels/";}`
于是直接alert(d)，找到d的值，填入通过。