Hackthis!! Writeup——Intermediate Level

原创

Roverdoge 于 2019-03-04 16:49:00 发布 322 收藏 1

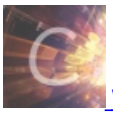
分类专栏： hackthis WP

本文链接：https://blog.csdn.net/qq_43148462/article/details/88124199

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

Level1:

> Use the GET method to send the password 'flubergump' to this page

要求用get的方式向网站发送password，于是我们直接访问

https://www.hackthis.co.uk/levels/intermediate/1?password=flubergump

便可以过关。

Level2:

> Use the POST method to send the password 'flubergump' to this page

要求用post的方式发送password，在这里可以上网搜一个post的网站，我这里用的是firefox的插件，直接post password=flubergump 即可过关。

Level3:

打开之后，扑面而来的是一张写着danger，restricted area的警告图片，下面有一个enter site的超链接。直接点击了话会返回"invalid details"，于是猜测这里有某种判断。于是打开fiddler进行抓包

```
GET https://www.hackthis.co.uk/levels/intermediate/3?enter HTTP/1.1
Host: www.hackthis.co.uk
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:65.0) Gecko/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,
Accept-Encoding: gzip, deflate, br
Referer: https://www.hackthis.co.uk/levels/intermediate/3?enter
Connection: keep-alive
Cookie: restricted_login=false; _ga=GA1.3.589989448.1545123388; PHPS
Upgrade-Insecure-Requests: 1
```

发现在cookie中这么一个东西，果断修改为ture，过关。

Level4:

> Bypass the filter and execute exactly this code:

```
<script>alert('HackThis!!');</script>
```

这是一道有显示的过滤，首先我们把这段代码扔进去试试他过滤了什么。输入这段代码后，返回了

```
alert('HackThis!!');
```

初步判断服务器端将script标签消去了。于是输入

```
 <scr<script>ipt>alert('HackThis!!');</s</script>cript>
```

通过

Level5:

> An automatic banning script is running on a target server. The script works by parsing log files for failed login attempts. The script locks out any IP address for 10 seconds after every failed login attempt. The log output will be displayed below. Attempt to login while avoiding detection.

考查内容为log注入。
这里有一篇比较详细的总结，转载给大家
https://www.cnblogs.com/coderzh/archive/2008/12/15/1355530.html
这道题使用了这篇文章中的第一种换行注入的方法，直接输入\n就能过

Level6:

> This login screen is trying something a bit different and is not using SQL. Try and login as the user whose real name is ‘Sandra Murphy’.

给出的题目中说不是用的sql，然后在hint中给了一段xml，说明这道题的登录是用的xml，于是这里考虑xpath注入攻击。
由于我也是刚刚开始学习，这里先贴上一篇大佬的文章
https://www.cnblogs.com/backlion/p/8554749.html
我个人的理解，这个其实和sql注入是一个原理，只不过查询语句不同。
根据sql注入和xpath查询语句，构造出payload
Username:’ or’1’=’1
Password:’ or ‘1’=‘1’ and realname/text()=’Sandra Murphy
通过。