

攻防世界web PHP2 writeup

原创

[Sprint#51264](#) 于 2020-07-11 18:28:18 发布 118 收藏

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_45837896/article/details/107288675

版权

先前的无思路

题目页面



Can you authenticate to this website?

https://blog.csdn.net/qq_45837896

问我能不能登陆上这个网站

但是没有登录入口，于是F12查看network

状态	方法	域名	路径	响应内容
200	GET	220.249.52.133:...	/	browsing-...

发现接收方

式为GET

于是盲猜应该有id字段

输入id=admin进行尝试



not allowed!

惊奇地发现，

页面发生了变化，再尝试传入密码无果

尝试burpsuite 爆破无果

尝试sqlmap 注入?? 无果

最终查看别人的writeup了解了...

正确思路

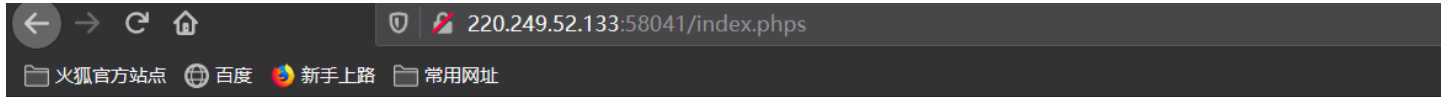
index.phps（正确思路）

url后跟index.php查看源码

（好吧新知识记下来）

知识点：phps文件就是php的源代码文件，通常用于提供给用户（访问者）查看php代码，因为用户无法直接通过Web浏览器看到php文件的内容，所以需要phps文件代替。其实，只要不用php等已经在服务器中注册过的MIME类型为文件即可，但为了国际通用，所以才用了phps文件类型。它的MIME类型为：text/html, application/x-httpd-php-source, application/x-httpd-php3-source。

出现以下页面



not allowed!

```
"); exit(); } $_GET[id] = urldecode($_GET[id]); if($_GET[id] == "admin") { echo "
```

Access granted!

```
"; echo "
```

Key: xxxxxxxx

```
"; } ?> Can you authenticate to this website?
```

https://blog.csdn.net/qq_45837896

通过源码我们了解到，页面接收通过url传入的id参数并对id参数进行一系列操作。

- 1.首先对id进行一次url解码
- 2.如果解码后的结果是admin还会禁止登陆

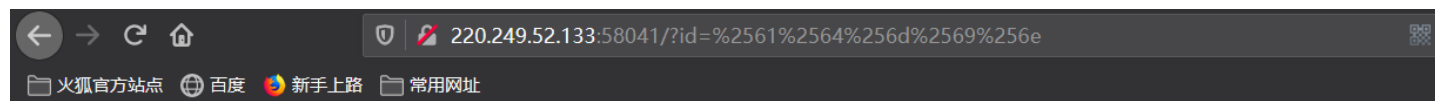
但是通过刚刚的尝试发现只有id为admin才可以登录

说明id必须为admin，由此，想出将admin进行二次url编码

admin二次url十六进制编码后变为

%25%36%31%25%36%34%25%36%64%25%36%39%25%36%65

重新尝试输入该id值得



Access granted!

Key: cyberpeace{5552cb510a1b16b20e69e92ae4e0b8d0}

Can you authenticate to this website?

https://blog.csdn.net/qq_45837896

得到flag...