攻防世界web PHP2 writeup

原创

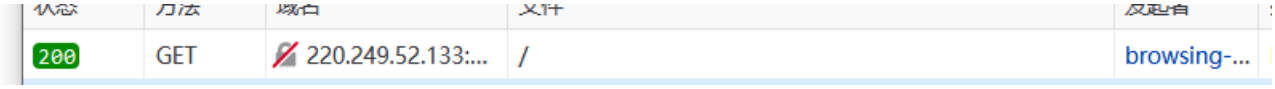
Sprint#51264 于 2020-07-11 18:28:18 发布 118 收藏

先前的无思路

题目页面

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



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

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

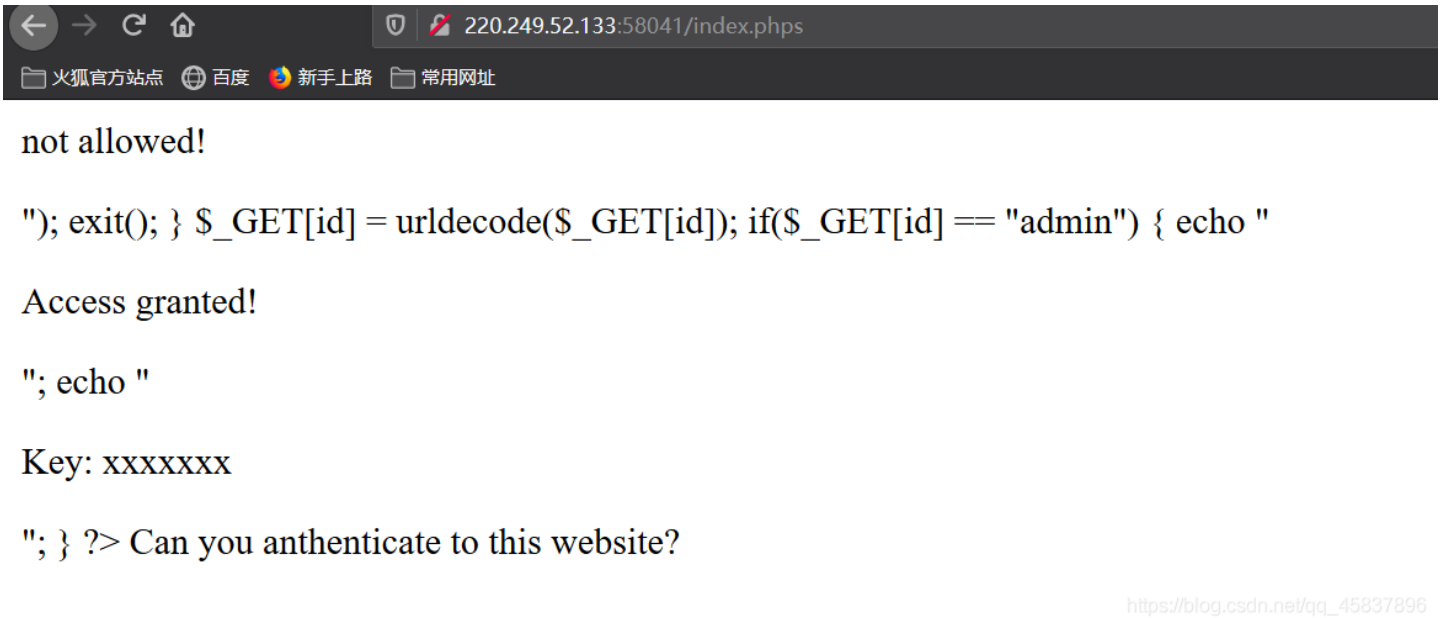
最终查看别人的wirteup了解了…

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，所以需要用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



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。

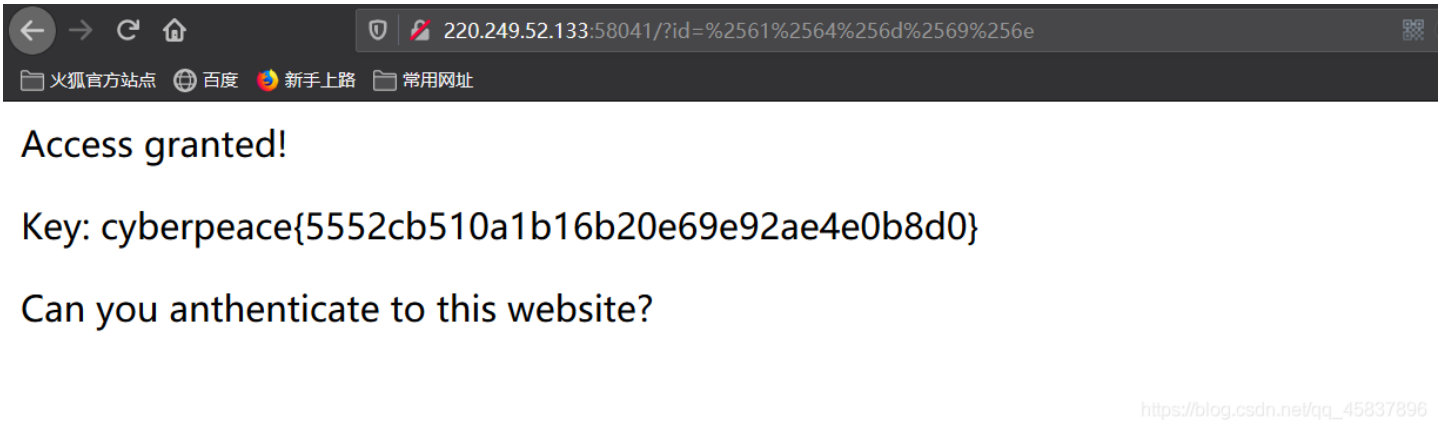
1.首先对id进行一次url解码
2.如果解码后的结果是admin还会禁止登陆

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



得到flag…