buuctf [ACTF2020 新生赛]Include

原创

Fatesec 于 2021-03-03 16:40:21 发布 68 收藏 1

分类专栏： buuctf web 文章标签： 网络安全

本题主要考查了利用php://filter伪协议进行文件包含

进入题目根据Tip进入正题，可以看到URL中存在文件包含

tips

Can you find out the flag?

首先尝试php://input伪协议：

hacker!

发现被过滤了

然后尝试使用**php://filter**伪协议来继续包含，使用“**php://filter"伪协议**”来进行包含。当它与包含函数结合时，**php://filter流会被当作php文件执行**。所以我们一般对其进行编码，阻止其不执行。从而导致任意文件读取。

php://filter

`php://filter` 是一种元封装器，设计用于数据流打开时的筛选过滤应用。 这对于一体式（all-in-one）的文件函数非常有用，类似 readfile()、 file() 和 file_get_contents()， 在数据流内容读取之前没有机会应用其他过滤器。

`php://filter` 目标使用以下的参数作为它路径的一部分。 复合过滤链能够在一个路径上指定。详细使用这些参数可以参考具体范例。

php://filter 参数

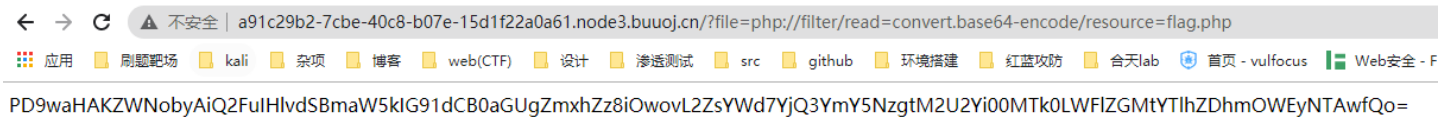
名称	描述
resource=<要过滤的数据流>	这个参数是必须的。它指定了你要筛选过滤的数据流。
read=<读链的筛选列表>	该参数可选。可以设定一个或多个过滤器名称，以管道符（|）分隔。
write=<写链的筛选列表>	该参数可选。可以设定一个或多个过滤器名称，以管道符（|）分隔。
<；两个链的筛选列表>	任何没有以 *read=* 或 *write=* 作前缀 的筛选器列表会视情况应用于读或写链。

构造payload

```
?file=php://filter/read=convert.base64-encode/resource=flag.php
```

这里需要注意的是使用php://filter伪协议进行文件包含时，需要加上**read=convert.base64-encode**来对文件内容进行编码

发送请求得到base64编码后的flag.php文件源码



PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7YjQ3YmY5NzgtM2U2Yi00MTk0LWFlZGMtYTlhZDhmOWEyNTAwfQo=

将其进行base64解码得到：

```
<?php
echo "Can you find out the flag?";
//flag{b47bf978-3e6b-4194-aedc-a9ad8f9a2500}
```