# 2018年“骇极杯” web3 GOOD JOB writeup 两种解法

原创

HyyMbb 于 2019-10-17 00:58:25 发布 522 收藏

分类专栏： ctf



本文链接：https://blog.csdn.net/a3320315/article/details/102597551





## 0x01 贴出源码

```php
<?php
    //error_reporting(0);
    //$dir=md5("icq" . $_SERVER['REMOTE_ADDR']);
    $dir=md5("icq");
    $sandbox = '/var/sandbox/' . $dir;
    @mkdir($sandbox);
    @chdir($sandbox);

    if($_FILES['file']['name']){
        $filename = !empty($_POST['file']) ? $_POST['file'] : $_FILES['file']['name'];
        if (!is_array($filename)) {
            $filename = explode('.', $filename);
        }
        $ext = end($filename);
        if($ext==$filename[count($filename) - 1]){
            die("emmmm...");
        }
        $new_name = (string)rand(100,999).".".$ext;
        move_uploaded_file($_FILES['file']['tmp_name'],$new_name);
        $_ = $_POST['hehe'];
        if(@substr(file($_)[0],0,6)==='@<?php' && strpos($_,$new_name)===false){
            include($_);
        }
        unlink($new_name);
    }
    else{
        highlight_file(__FILE__);
    }
```

## 0x02 过程分析

从上面的代码可以看出，代码的功能是上传一个文件，并且满足两个条件就可以包含这个文件

```php
if($ext==$filename[count($filename) - 1])
```

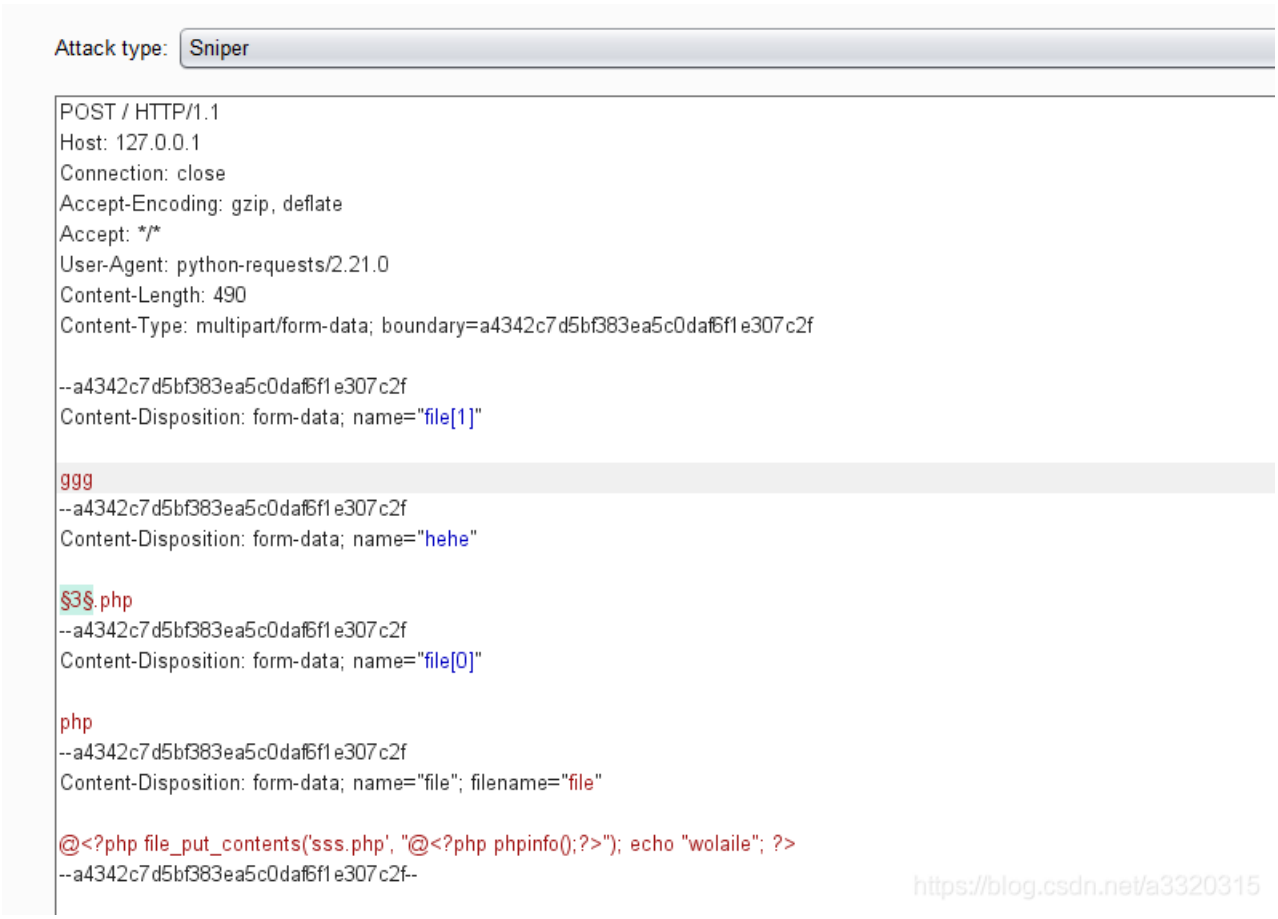
```php
if (@substr(file($_)[0], 0, 6) === '@<?php' && strpos($_, $new_name) === false)
```

## 0x03 题解

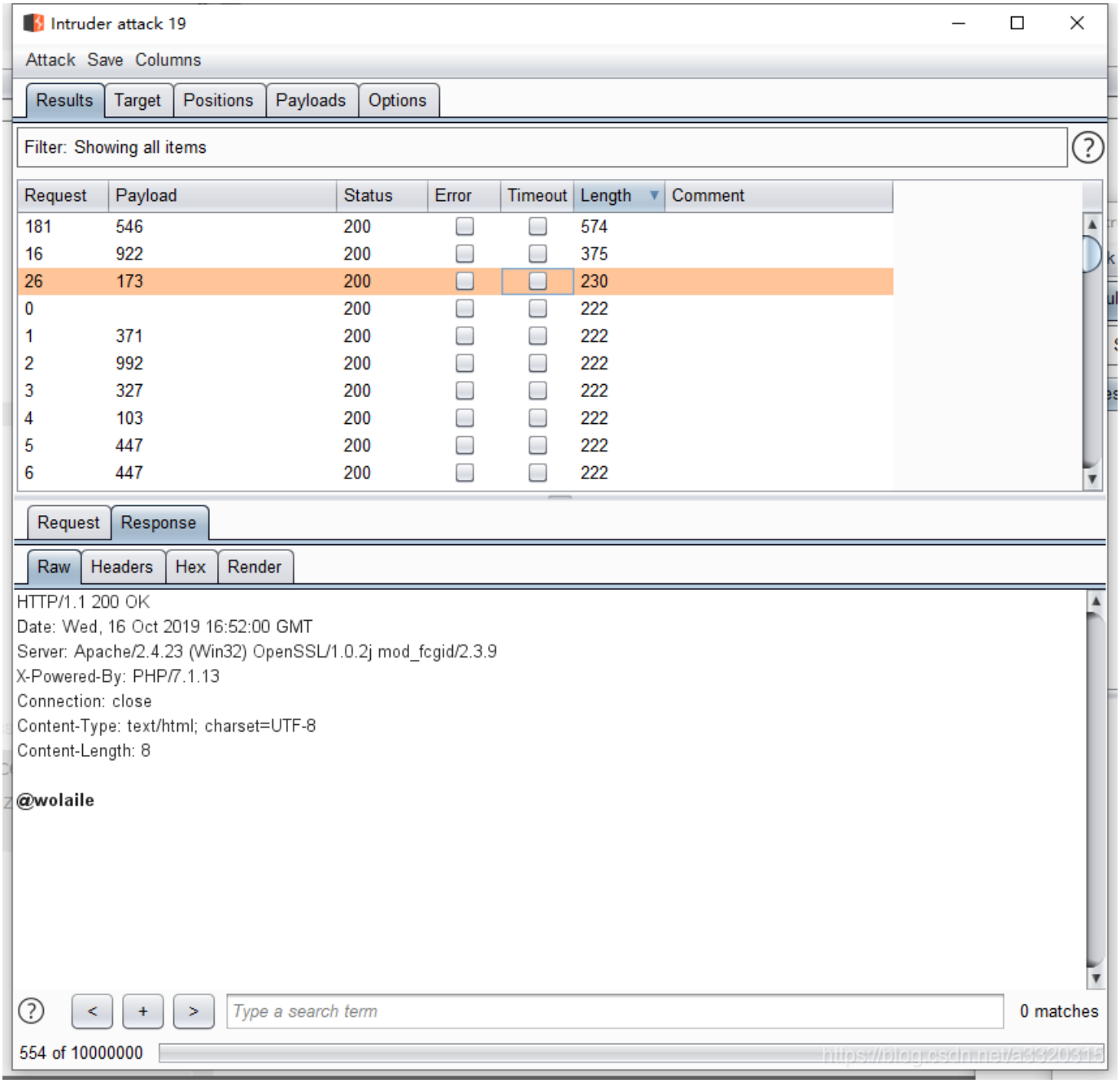
第一个条件可以通过数组绕过
第二个条件`strpos($_, $new_name) === false`，假如只上传一次不能绕过

### 解法一：

我们可以进行条件竞争，整个代码流程为`上传=》包含=》删除`，我们可以多线程上传文件，在上传和删除的间隔中，另外一个线程来包含这个文件。由于随机数只是在100-999，用burpsuite开三个intruder，几分钟就可以碰撞成功。




图片一




图片二

碰撞成功!

## 解法二

利用 `/.` 绕过 `unlink`

我们只需要上传一次文件，然后unlink不会删除此文件，我们再进行爆破包含文件就ok了。