

# “F1rry” week2 web write up

## 草莓社区-1:

<http://118.25.18.223:10011/>

题目描述如下

### Description

flag在../flag.php中

知识点：LFI

URL <http://118.25.18.223:10011/>

Base Score 100

Now Score 100

User solved 84

因为是 LFI,所以要想拿到 flag, 需要找到有关参数进行修改。  
打开界面, 发现并没有能修改的参数。



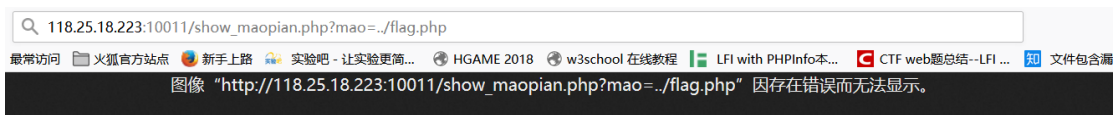
点击猫片 2 发现 url 中可以对 mao 进行修改



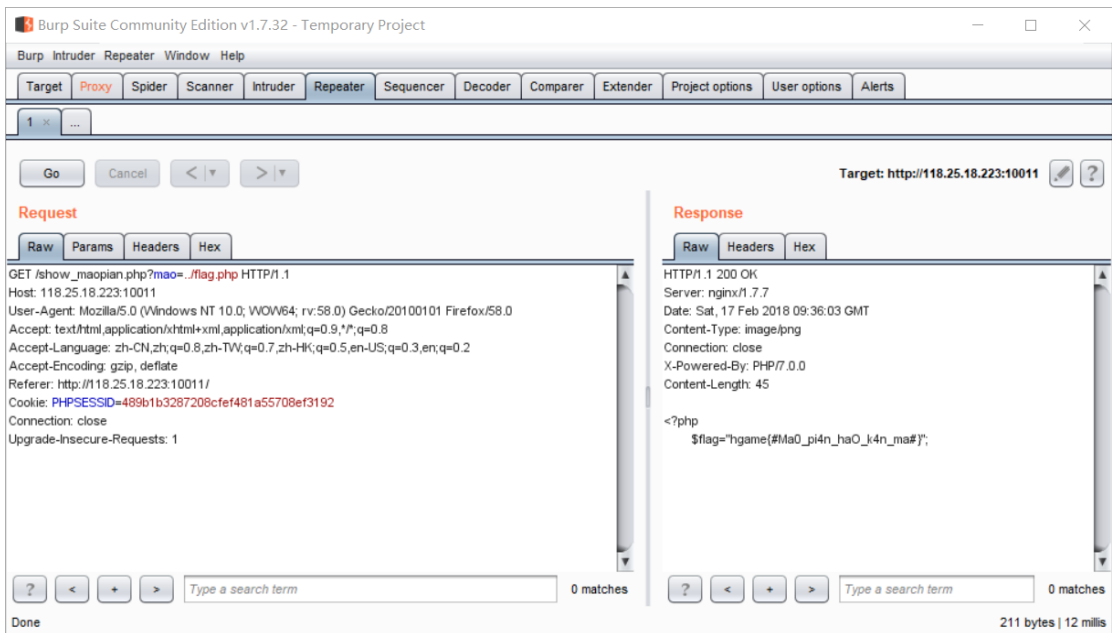
修改如下:

[118.25.18.223:10011/show\\_maopian.php?mao=../flag.php](http://118.25.18.223:10011/show_maopian.php?mao=../flag.php)

存在错误无法显示?



于是抓个包来看看，得到 flag.



XSS-1:

<http://118.25.18.223:10013/>

打开界面发现:

## Try to alert(1)

```
function charge(input) {
    input = input.replace(/script/gi, '_');
    input = input.replace(/image/gi, '_');
    input = input.replace(/\(/, '_');

    return '<article>' + input + '</article>';
}
```

try to input something...

通过 charge 函数将 input 里面的 script,image,"(" 字符过滤掉了，其中 script,image 为全局

替代，并且大小写不敏感。‘(’ 只会替换一次。

所以要达成 `alert(1)`，需要解决 2 个问题，一是要用除 `<script><img>` 以外的标签来执行 XSS，二是解决 ‘(’ 被替换的问题。

针对第一个问题，百度了以后发现 XSS 攻击可以凭借 `<a>`、`<img>`、`<video>`、`<audio>` 标签 和 `onclick`: 点击触发 `onerror`: 当 src 加载不出来时触发 `onload`: 当 src 加载完毕触发 事件来触发以及 `iframe` 标签，写入后网页加载自动执行。

而针对第二个问题，只要在之前输入 ‘(’ 即可具体 payload 如下：

## Try to alert(1)

```
function charge(input) {  
    input = input.replace(/script/gi, '_');  
    input = input.replace(/image/gi, '_');  
    input = input.replace(/\(/, '_');  
  
    return '<article>' + input + '</article>';  
}
```

```
<img src='#' name="("onerror='alert(1)' >
```

请带着payload找fantasyqt(QQ 744399467)

## XSS-2:

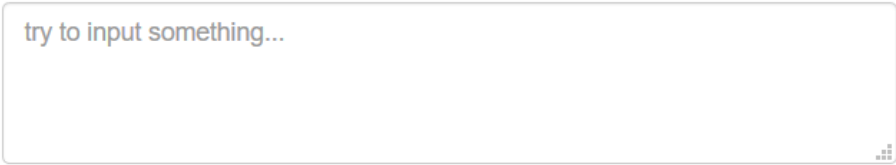
<http://118.25.18.223:10014/>

打开界面如下：

---

## Try to alert(1)

```
function charge(input) {  
    input = input.replace(/script/gi, '_');  
    input = input.replace(/img/gi, '_');  
    input = input.replace(/image/gi, '_');  
    input = input.replace(/\(/, '_');  
    input = input.replace(/\>/, '_');  
    return '<input value="' + input + '" type="text">';  
}
```



这比上一个题目多了 2 个问题，一个是它将>也过滤掉了，不过方法同上，只要在之前输入(>即可；

第二个是 return 语句：由于单双引号的存在他会将你输入的内容直接返回到页面，同时会干扰到触发事件时需要用到的引号以及运用标签时的‘>’，要想保证 XSS 的成功，只要在前面运用>">即可,第一个‘>’会被替换成'\_',而第二个‘>’会闭合 input 标签，所以要用到两个>>,再加上后面的语句

Return 语句就会变成

```
Return '<input value="' + ' ' __ ><video src='#' onerror='alert(1)'></ video> '" type="text">';
```

成功触发：

# Try to alert(1)

```
function charge(input) {  
    input = input.replace(/script/gi, '_');  
    input = input.replace(/img/gi, '_');  
    input = input.replace(/image/gi, '_');  
    input = input.replace(/\(/, '_');  
    input = input.replace(/\>/, '_');  
    return '<input value="' + input + '" type="text">';  
}
```



">( ><video src='#' onerror='alert(1)'></ video>

请带着payload找fantasyqt(QQ 744399467)

## 简单的 sql 题:

<http://118.25.18.223:10015/>

题目描述说只有 admin 才能登陆

### Description

Only admin can get flag!!!!

所以只要在用户名内输入 admin'-- (ps: '-' '-' 中间无空格, 后面有一空格, 此为注释符号)

密码随意输即可

因为应用程序将执行以下查询:

```
SELECT*FROM users WHERE username = 'admin'-- ' AND password = '1'
```

因为运用到了注释符号, 等同于

```
SELECT*FROM users WHERE username = 'admin'
```

获得 flag