

Bugku Writeup —文件上传2(湖湘杯)

转载

[diyuling2121](#) 于 2018-11-04 23:06:00 发布 119 收藏

文章标签: [php](#)

原文链接: <http://www.cnblogs.com/X1a0/p/9906510.html>

版权

我们先来看下题目, 题目说明是文件上传



Upload your own png file

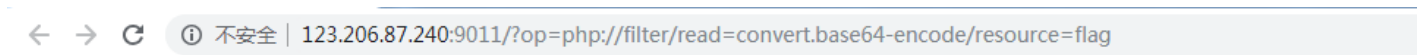
Image file (max 100x100): 未选择文件。

2017 © All rights reserved.

我们可以尝试通过构造payload来进行测试

`php://filter/read=convert.base64-encode/resource=flag`

获取到flag, 之后进行解码, 得到真正的flag



PD9waHANCiRmbGFnPSJmbGFne2UwMGY4OTMxMDM3Y2JkYjI1ZjZiMWQ4MmRmZTU1NTJmfSI7DQo/Pg==

2017 © All rights reserved.

总结:

题目考察的是文件包含漏洞。

如果不懂payload意思的小伙伴可以自行百度一下

转载于:<https://www.cnblogs.com/X1a0/p/9906510.html>