

攻防世界bug

原创

[从0到1 渗透之路](#)



于 2020-06-02 09:57:41 发布



565



收藏

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：<https://blog.csdn.net/xiaoqi199915/article/details/106489832>

版权

bug  31 最佳Writeup由Fvck·小北提供

难度系数： 5.0

题目来源：[RCTF-2015](#)

题目描述：暂无

题目场景：[点击获取在线场景](#)

题目附件：暂无

<https://blog.csdn.net/xiaoqi199915>

尝试弱口令和万能密码

首先你应该登录 进行注册 但是自己没有注册成功

登录自己的账号密码 并未发现什么 需要管理员权限进行登录

进行忘记密码进行秘密 burp 进行抓包

账号名改成admin 密码是自己注册的密码进行发包 登陆成功 admin权限 点manage发现出现IP

IP问题 进行X-Forwarded-For :127.0.0.1

进行审查源码 发现index.php?module=filemanage&do=???

那么do后面能是什么呢 猜测upload

写一个php代码

改为jpg格式进行上传 burp进行抓包改包 55.php 进行发包 PHP 文件名绕过 555.PHP 或者php4

或者js代码进行绕过