

遇到的ctf 套路 记录（长期）

原创

[White-小白](#) 于 2018-09-20 08:45:29 发布 894 收藏 3

文章标签: [ctf study](#)

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/weixin_42214273/article/details/82780813

版权

掌控安全封神台:

伪造本来用户登录

burp抓包 修改 Host和Referer参数 改成127.0.0.1即可

存储型xss

利用xss漏洞平台创建xss语句插入存在存储型xss漏洞的位置, 在xss平台等待响应

上传木马

用cmd创建一句话木马 copy 1 .jpg/b + 1 .php/a 2 .jpg 查看上传允许文件类型 发现可以上传cer文件 可利用iis6.0漏洞 将木马后缀名改为.cer上传成功

提权

在菜刀中发现可以上传文件利用cmd和pr进行提权 在菜刀终端中利用cmd允许pr进行提权 (在终端允许cmd, cmd中允许pr.exe"cmd指令") 即可创建超级用户

查看windows下明文密码

在远程连接选项中选择共享 将mimikatz拖入终端 privilege::debug sekurlsa::logonpasswords 查看即可



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)