

[hackinglab][CTF][综合关][2020] hackinglab 综合关 writeup

原创

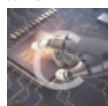
[CryptWinter](#) 于 2021-01-21 10:39:18 发布 310 收藏

分类专栏: [CTF](#) 文章标签: [writeup](#) [hackinglab](#) [2020](#) [CTF](#) [综合关](#)

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/dadongwudi/article/details/112900610>

版权



[CTF 专栏收录该内容](#)

17 篇文章 2 订阅

订阅专栏

[hackinglab][CTF][解密关][2020] hackinglab 上传关 writeup

综合关 1 渗透测试第一期

概要: 在于绑定admin用户, 进行修改密码! (手机号码仔细!!!)

知识点: 在进行绑定的操作时, 没有对用户名最开始的密码进行验证, 导致可以伪装其他用户。进行绑定手机, 然后进行修改密码操作。修改密码操作也没有对原密码进行验证, 导致漏洞。

步骤:

https://blog.csdn.net/qq_46091464/article/details/106423371

<https://www.cnblogs.com/Easyoung/p/14202707.html>

综合关 2 没有注入到底能不能绕过登录

概要: robots.txt 保持登陆的Session会话

知识点: 后台对登陆状态没有验证, 仅仅验证了登陆用户的权限, 保持登陆的Session会话, 然后去访问后台地址就OK

步骤: <https://blog.csdn.net/liushulin183/article/details/79041549>

综合关 3 美图闪亮亮交友平台

概要: 写脚本 url 反向监听

知识点:

步骤: <https://blog.csdn.net/xzz2333/article/details/109514039>

综合关 4 最简单的数字取证1

概要: IDA搜索key 或 磁盘恢复工具DiskGenius打开

知识点:

步骤: <https://www.pianshen.com/article/3422676301/>

综合关 5 最简单的数字取证2

概要: 磁盘恢复工具DiskGenius打开

步骤: <https://www.pianshen.com/article/2652676116/>

综合关 6 小明学习代码审计writeup

概要: 脚本

步骤: <https://www.cnblogs.com/kevinbruce656/p/11209125.html>

综合关 7 HackingLab首台rootkit题目虚拟机[公测]

概要: strings

知识点:

步骤: <https://blog.40huo.cn/blog/hackinglab-comp.html>

综合关 8 代码审计与综合利用

概要: getshell

步骤: <https://blog.40huo.cn/blog/hackinglab-comp.html>

综合关 9 代码审计重置任意用户密码

步骤: 暂无

综合关 10 不拦截攻击的奇怪的WAF

概要: WAF

步骤: 暂无