ACTF writeup

原创

sec_lee 于 2014-04-17 10:29:44 发布 2994 收藏
分类专栏： 网络攻防比赛 ctf 文章标签： 安全 actf ctf


网络攻防比赛 同时被 2 个专栏收录
3 篇文章 0 订阅
订阅专栏


ctf
1 篇文章 0 订阅
订阅专栏

先挖个坑把题目列出来，后续把解题思路慢慢填到坑里...

[已解决] RE?

说好的逆向题呢？出题人还没吃早饭呢，你们急什么。出门左转，乖乖做Web题，OK不？

[已解决] 古老

```
本题flag不在ACTF{}中。
oivqmqgn, yja vibem naarn yi yxbo sqnyab yjqo q zixuea is gaqbn qdi. ykra jqn zira yi baseazy yjqy qeni ko
```

[已解决] 餐前甜点

```
nc 218.2.197.236 2009
crypto200.tar.gz
```

[已解决] 社(song)工(fen)

听说参加ACTF的屌丝都喜欢上贴吧:)

[已解决] flag之路

```
少年，不来一发么。http://218.2.197.236:2005/index.php
```

[已解决] 买不到票的怨念

买不到TI4的门票觉得人生好灰暗。。crypto200.tar.gz

[已解决] 杀猪吃肉

```
nc 218.2.197.236 2010
crypto200.tar.gz
```

[已解决] 讨厌的管理员

FLAG在admin的手里！http://218.2.197.236:2005/web200/index.php

[未解决] S4ndb0x

http://218.2.197.236:2015

[未解决] 抓(zhua)包(zhu)

猪头在自习室用手机的流量被全部抓到了！看看流量里有什么有意思的东西？
链接：http://pan.baidu.com/s/1ntrzThB 密码：cbf2

[已解决] 喵喵喵喵

管理员小陆搭了个服务器，但是好像漏洞蛮多哟。
http://218.2.197.236:2001/index.html

[未解决] 老大哥aay的秘密

老大哥aay给了你一个神秘文件，你看着办吧flag.rar

[未解决] 找(ri)bug(猪)

猪头喜欢上oschina，找死猫要了一个安卓客户端，不过死猫居心叵测在里面留了一个后门。听说猪头在oschina用私信约了一个妹妹，现
http://218.2.197.236:2007
提示
猪头的用户id是1581834
注意后门在死猫给的客户端里

[未解决] 赞助商

你大家快来看赞助商！hidden.png

[未解决] 贡丸酱

web300没做出来的话这题做出来的希望不大，你以为你是可爱的贡丸酱么(つ•̀ω•́)つ
（贡丸酱到底算不算提示呢）
(web300和web400都不需要使用扫描器)
(本题flag并不是ACTF形式的，你提交的flag中也不需要包含任何形式的括号)
http://218.2.197.236:2003

提示
现在可以公开的情报：
管理员是个很懒的人，他的笔记几乎没有任何废话。

[未解决] Verify

链接: http://pan.baidu.com/s/1GOO3c 密码: 6q9f

补充说明：本题不提供回显，发送请求后需要关闭socket，只有有效的请求会被接受
提示
RTFM <-- 这是最关键的提示
-----BEGIN PUBLIC KEY-----
ME4wEAYHKoZIzj0CAQYFK4EEACEDOgAEPUnnLOYk4sKVDwPQlbtJ/CTLuyeoMXkL
nsrFPFQjt5mIHYVnnfcDpZTfb+Qw8bwfz8znToVhA+g=
-----END PUBLIC KEY-----

bash only

[未解决] 木(tou)马(kui)

上次被日之后猪头提高了警惕，现在他不允许其他人给他的小破手机(Android2.3)装有联网权限的应用了。这次他放心地在sd卡上放了x
注意:猪头手机有两个网卡，eth0, eth1。有时候一个不行尝试下另外一个~

提示
flanker:猪头，你这Android2.3可是非常老，听说2.3里有些联网操作都不需要申请权限，不怕约炮视频被偷？ 猪头：没事，偷了也就

[未解决] 丧心病狂的黑客

管理员小陆搭的服务器被人日穿了(见web300)，小陆被boss骂了个狗血淋头。然后boss勒令小陆再搭一遍，小陆在某内网换了个架构(原

接受挑战，hackers，日穿这台位置未知的内网服务器！！！
(本题和之前的web题有紧密联系！！！)
(部分关键文件每十分钟重置一次！！！)
(本题flag不包含有ACTF字样，不包含有任何括号！！！)
(Drink All The Booze , Hack All The Things！！！)

提示
第一步先确定服务器位置

[未解决] Chaos

Download: http://pan.baidu.com/s/1i3GA4zr
Password: ophk

ATQA (SENS_RES): 00 04
UID (NFCID1): AD EA DC A7
SAK (SEL_RES): 08

请你帮这只死猫计算出 0 扇区的 KeyA 和 3 扇区的 KeyB
Flag = (Sector_0_KeyA + Sector_3_KeyB).encode('hex').upper()

提示
exported and non-exported entries can ease your life

Log => Code Path, Google => Document, Server => Secret, Reuse => No More Reverse

[未解决] NonStandard

链接: http://pan.baidu.com/s/1pJO5QeZ 密码: lk1d
写不出 Keygen 都不好意思说自己是搞逆向的
请写出 Keygen 发送至 ACTF.NonStandard@gmail.com，解决“暗桩”有额外加分

提示
看标题