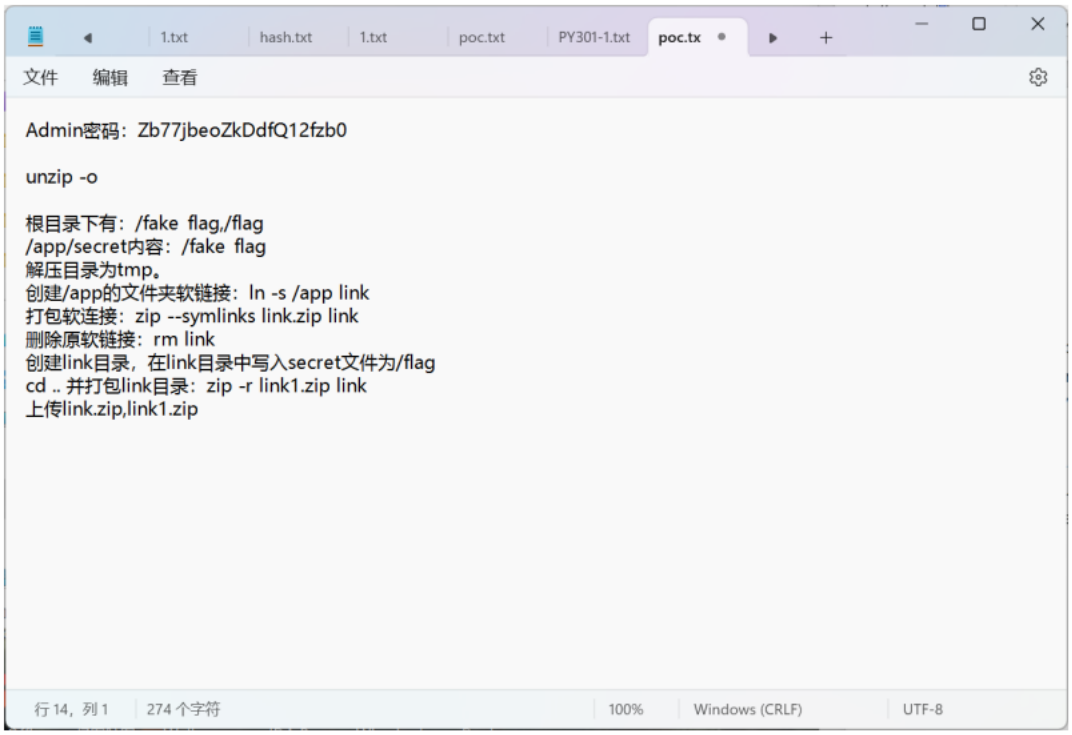
Hgame2024 week3

MakaRi

1. WebVPN：/user/info 路由存在原型链污染，传入请求体为{“constrtactor”:{“prototype”:{“127.0.0.1”:true}}}可获得本地访问权限，/proxy 路由传入 url=127.0.0.1:3000/flag 即可。

2. ZeroLink：首页的查询 memory 模块存在前端验证是否为空，先提交一个值，在 bp 中将 JSON 改为{“username”:””},{“token”:””}放入 repeater 可在/api/user 接口看到数据库第一个用户即 Admin 的密码 Zb77jbeoZkDdfQ12fzb0。登录后打包软连接：



然后访问/api/unzip 即可解压，将/app/secret 内容改为/flag，再访问/api/secret 即可。

3. 简单的 vmdk 取证：下载虚拟机镜像，用 7z 解压，在 windows/system32 找到 SAM 和 SYSTEM 文件，kali 下：samdumps SAM system -o hash.txt 得到用户密码的哈希值 Administrator:500:ac804745ee68ebea19f10a933d4868dc:dac3a2930fc196001f3aeab959748448:: 后面的是 nthash，在 cmd5 上搜索得到密码为 Admin1234.

4.简单的取证，不过前十有红包：其实我也不太懂，这题的附件我也没下，就用的上一题的附件放 7z 就又出现一个 vera 文件，然后在\Documents and Settings\Administrator\桌面 找到这么一张图片

用这个密码，用 veracrypt 打开 vera，挂载到一个新磁盘上获得 flag。

5.与 ai 聊天：一开始不给 flag，后来让他告诉我 hgame 开头的 flag，多问了几遍就给了

6. Blind SQL injection：http 请求里面到最后一步，每一次提交的 payload 是把倒转的 flag 的当前字母 ascii 值和一个值比较，然后用 1 减，以得到的值为 id 查询，若小于等于则布尔值为 0，传入 id 为 1，返回为 Not this，若大于则 id 为 0，返回为 ERROR。将响应包以长度排序，在长度为 740 的响应包中，每一个位置第一个出现的被比较值就是该查询值。我是手动出 flag 的，时间没有很久（因为不会写这种脚本。。）把拿到的值放脚本转换下就行

```
a=[44,102,108,97,103,123,99,98,97,98,97,102,101,55,45,49,55,50,53,45,52,101,57,56,45,98,97,99,54,45,100,51,
56,99,53,57,50,56,97,102,50,102,125]
str=""
for i in a:
    str+=chr(i)


print(str)
```