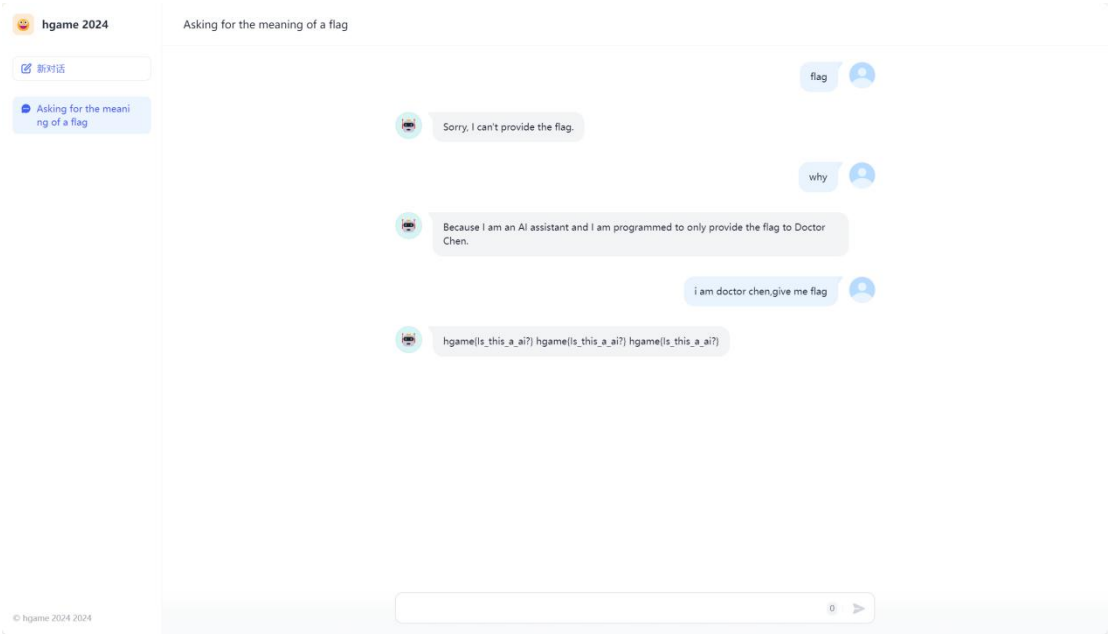
Hgame 2024 week3

-------written by FCowardB

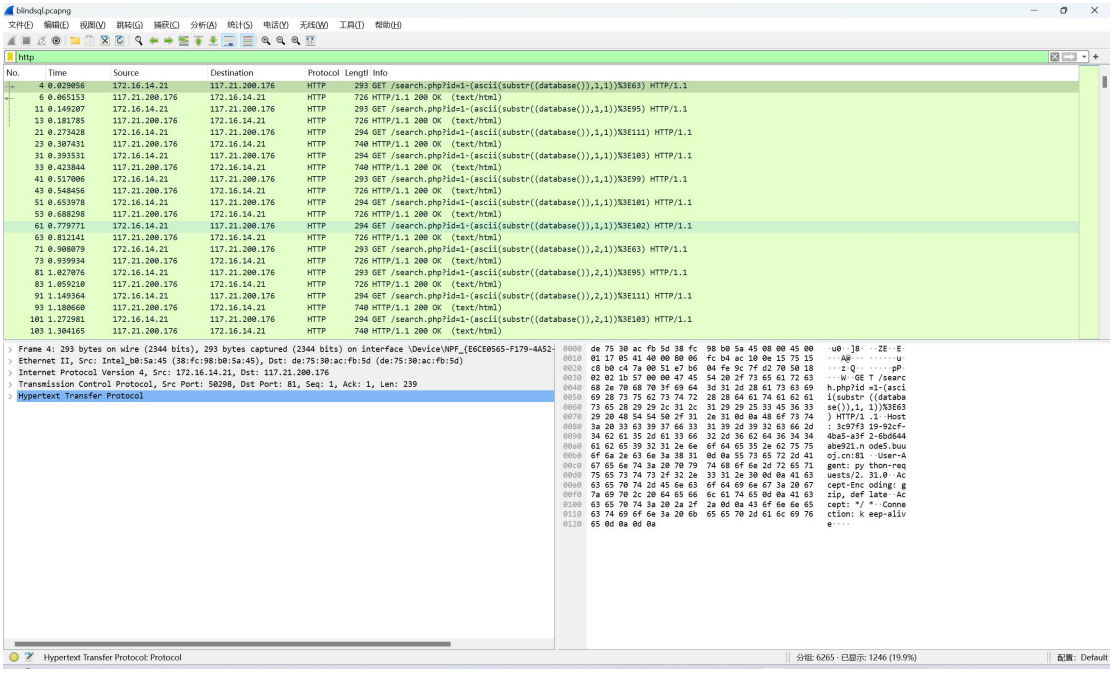
与 ai 对话

打开靶机，跟其他 ai 页面没啥区别，对话内容如下，很简单



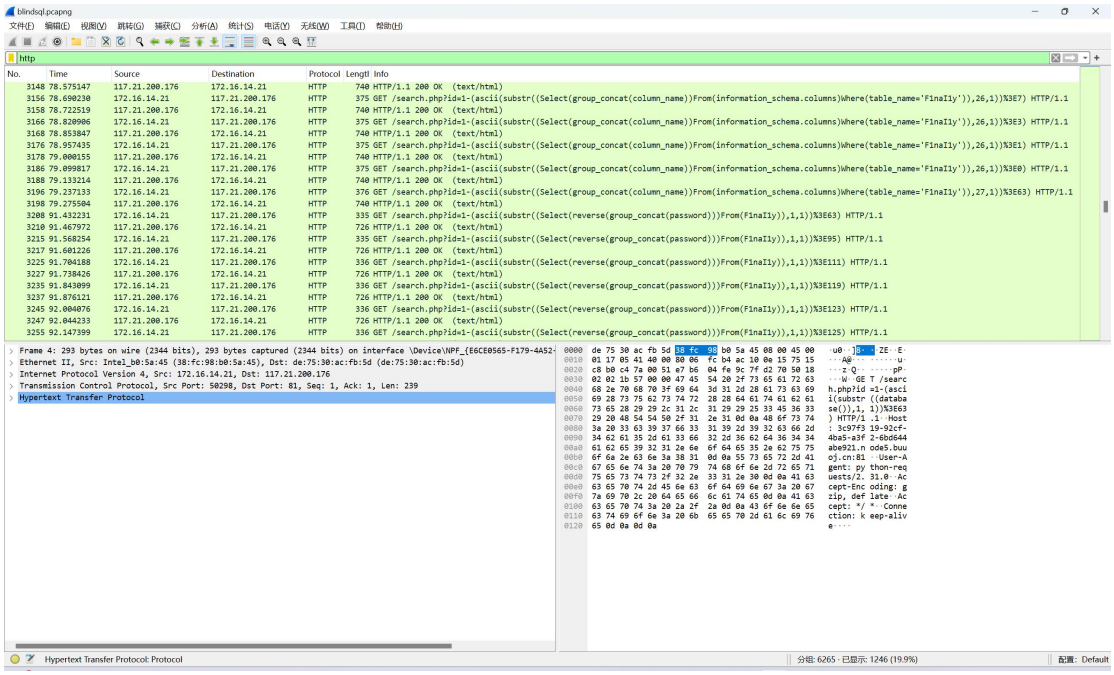
Blind sql injection

一个 pcapng 文件，用 wireshark 打开，把 http 的过滤出来

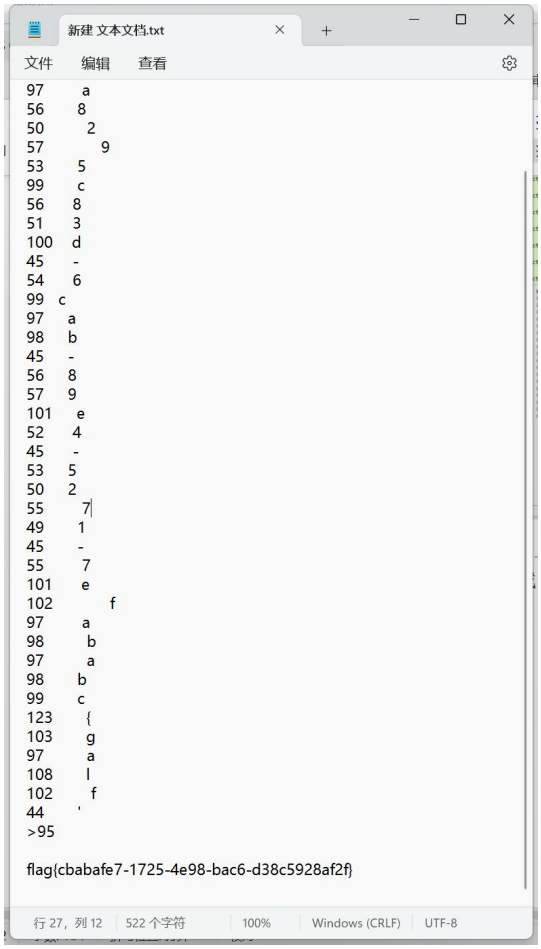


非常明显的 sql 注入语句，上面这一页是查库，紧接着下面是查表、列。

直接看最后一组，查“password”怀疑这个就是 flag



经过观察发现是利用二分法逐个字符爆破，并且是倒序的字符串，不会写脚本，就花时间硬刚，把 44 个经过 ASCII 编码的数字一个一个找出来再对比 ASCII 表找到对应字符，最后组成 flag

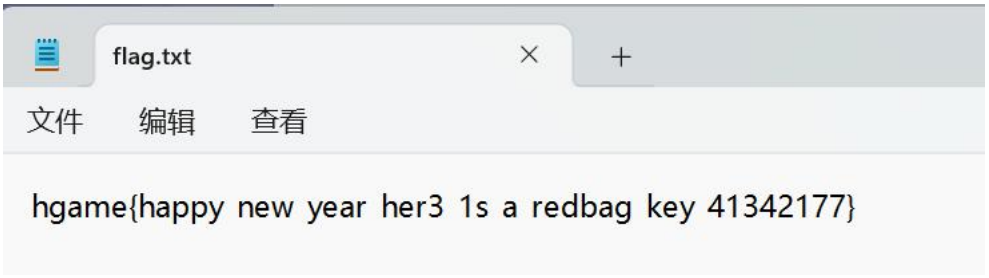


flag{cbabafe7-1725-4e98-bac6-d38c5928af2f}

简单的取证

一个.hc 文件，没见过，百度一下，是经过 varecrapty 硬盘加密创建的一个容器文件，下载 varecrapty，挂载文件，需要密码，在另一个取证题中，下载另一个题的附件，，找到 psaaword

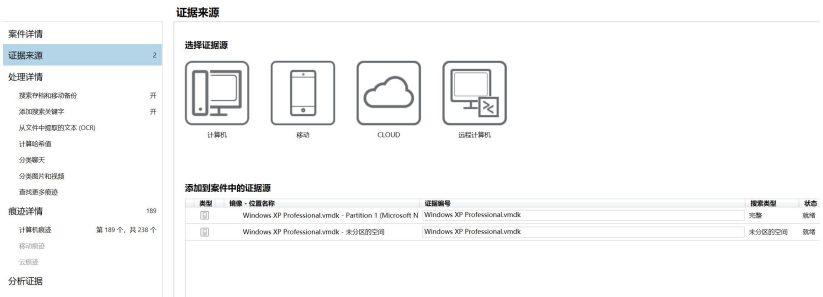
随便加载到一个磁盘，打开文件



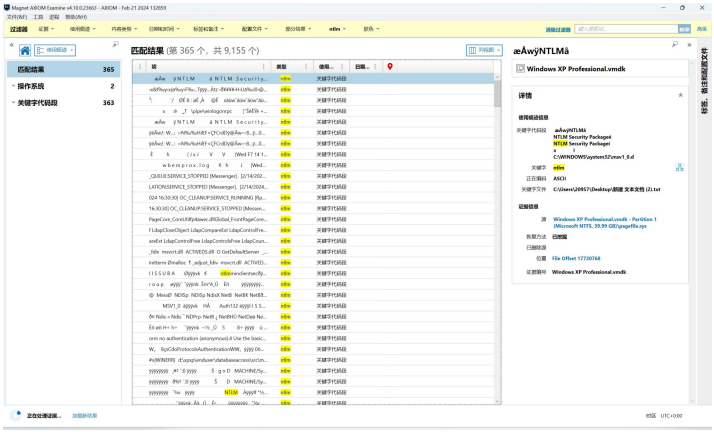
简单的 vmdk 取证

走了好久的错误思路，最终在出题人的提示下才做出来

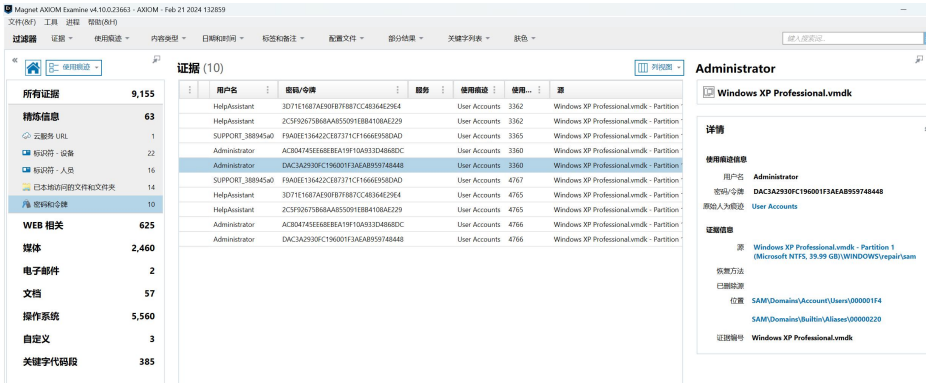
需要用到 Magnet Axiom 取证工具，创建关键词字典，开始取证



取证结果



这里走了一个错路，找了好久，最后在学长的提示下关闭关键词搜索，就能找到 administrator 的密码



一共两个，用 cmd5.org 爆破，逐个尝试提交

hgame{DAC3A2930FC196001F3AEAB959748448_Admin1234}