**背景：**

企业在内部使用或限制使用的某些帐号/密码时常因为有意或无意被泄露到公网中，造成风险或损失。对于通过企业内部分析已经得出泄漏信息后，对于泄漏源进行追查和销毁是非常必要的。所以泄漏帐密信息的方向和方法挖掘也是数安治理人员的技能之一。

**赛题介绍：**

互联网上的学习类知识类网站或代码托管平台，是各公司帐密信息泄漏的主要外部源头。现已提前布置多套帐密信息做为泄漏内容，安放在各类平台中，需由考生在公网进行挖掘和分析，将这些帐密信息泄漏的URL做为flag进行提交。该题包含5组帐密信息，分别放在不同的渠道中，考生找出条目越多分数越高。

泄漏信息：DataSecurityBox公司开发了“青莓”（green berry）项目（即时通讯工具），并使用python语言开发后台登陆服务程序，由于发现该项目内部的5个帐密有异常使用，怀疑内部人员通过程序代码共享、云端保存或项目宣传时造成了帐密泄漏，该项目的这5个帐号如下：

kUn3E5QQXE5wMjp5239L、hYmVsVbda44ztf4nEUMm、CUmLtwVT3YYEJsrHvWGD、XfNBHgmcgYwvZVnWpjyw、Rk2zb295UrY3UB8uEsSr

注：人为方式泄露可按场景来判断可能的泄漏渠道，如代码可能会在国内外开源代码平台（github、gitee等）上公开、代码片段可能在语雀、飞书等公开记录平台展示等。另外，关于项目信息、代码信息可能都有意进行了变形，如项目名称也可能是英文、拼音等。