HGAME 2022 Week4 writeup by nerowander

眨眼之间，week4 就已经结束了，期间还是学到了不少东西，希望在接下来的 hgame-final 能不交白卷，学以致用。

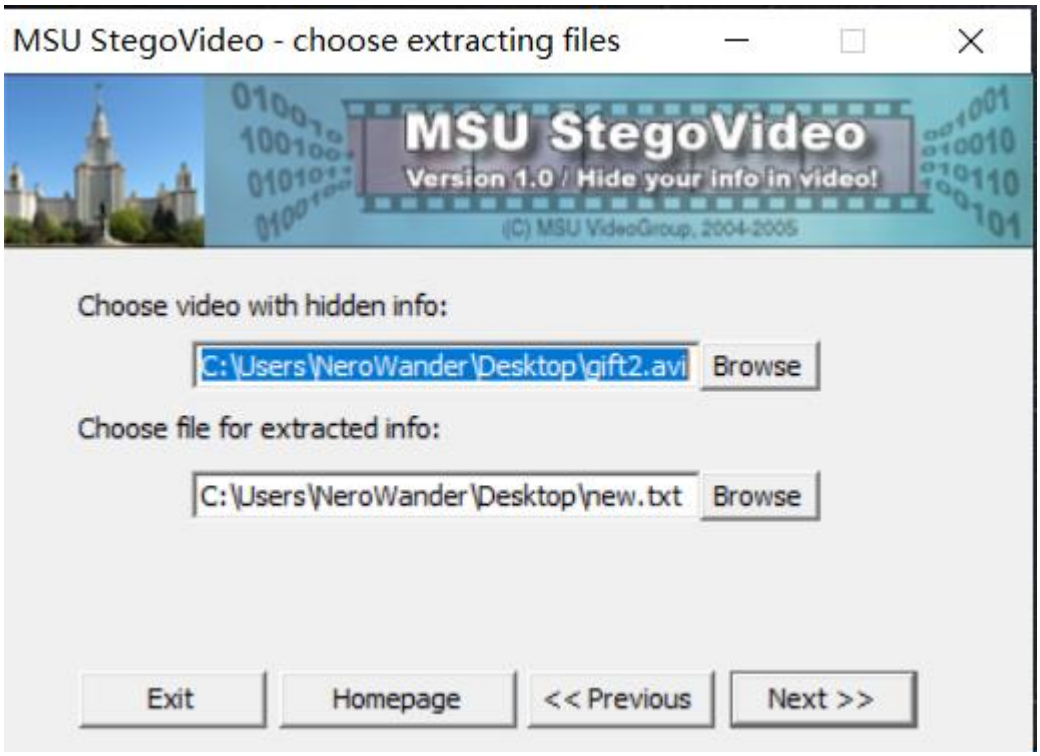
MISC

At0m 的给你们的(迟到的)情人节礼物

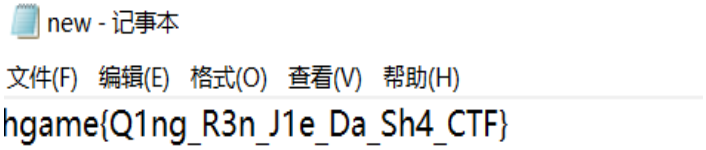
首先观察第一个视频，其实它不仅是 go 语言那道题的 hint（虽然 go 语言那道题我没做出来）

可能是学长故意露出的一些细节，让我发现了一些提示

问题在于，想用这个工具提取文件中的密文，需要一个 6 位数字的密码，看了一下 8889 端口，尝试了 888999 密码，然后就成功了



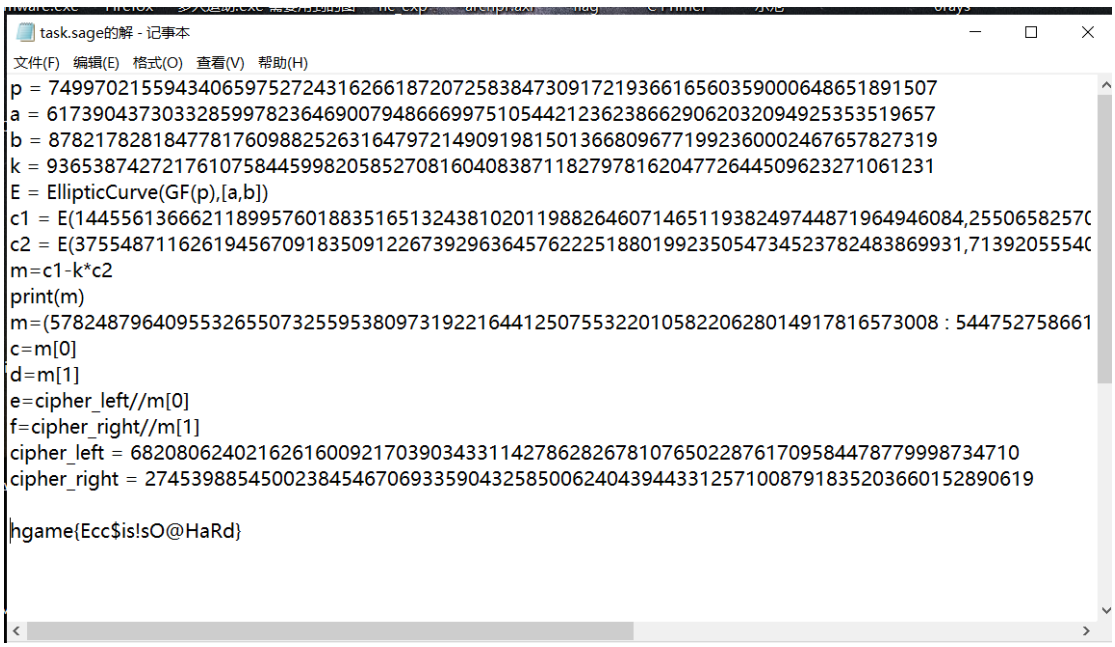
啊这，我也没想到这就猜出来了，还是需要一定的猜测能力的（~~情人节的浪漫~~）



CRYPTO

ECC

思路如下，解出 flag，关键是掌握基本的概念和网上的一些解法就可以了

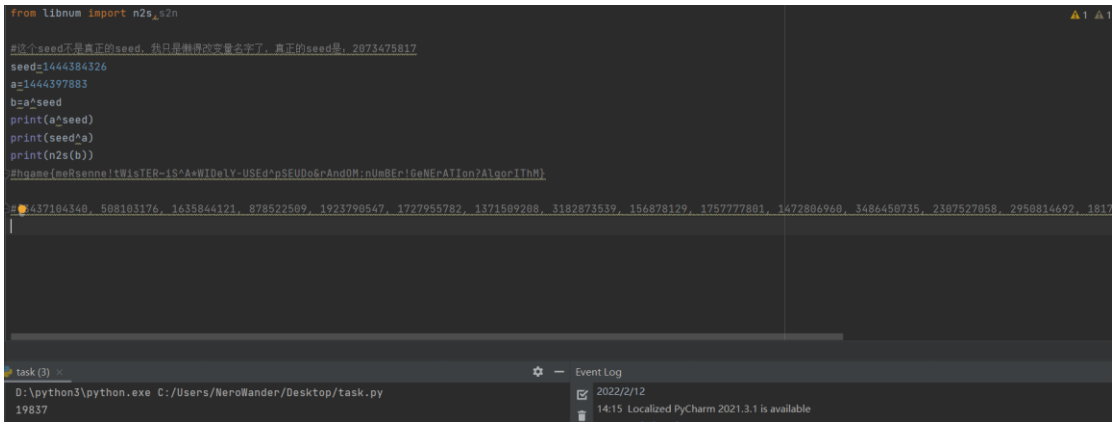


PRNG

这道题其实挺有意思的，卡了我半天

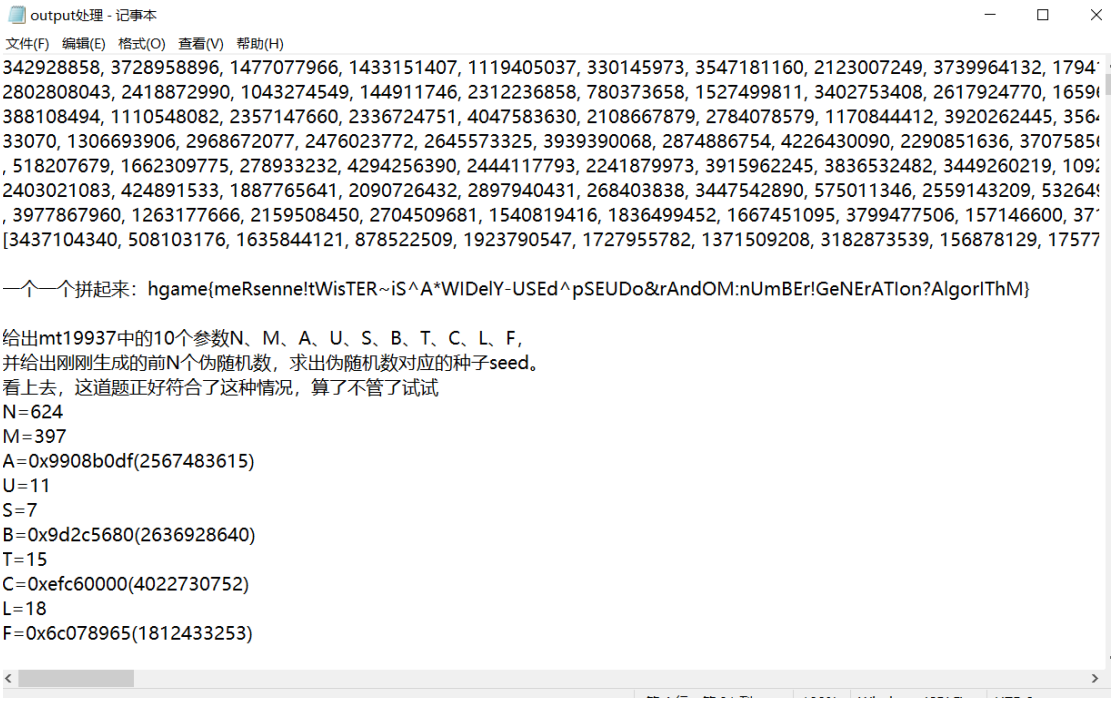
首先得读懂原来的 python 代码，可以得出是 flag 转换成数字序列之后以 4 个数字为一个部分（part）和接下来生成的随机数（从第 625 个随机数开始）作异或，异或是可逆的，问题不大，重点是知道接下来的随机数是什么

可以根据已有的 624 个随机数，根据 mt19937 算法生成接下来的随机数，也可以找出这已知的 624 个随机数的 seed（随机数种子）写出来接下来的随机数，不过我根据网上的方法得出了种子，但是没有找到用种子写的方法，所以还是采用了第一种方法



根据已有 624 个随机数推接下来的随机数的方法：
https://googles.plus/2022/01/16/mt19937-mei-sen-xuan-zhuan-suan-fa/#toc-heading-4

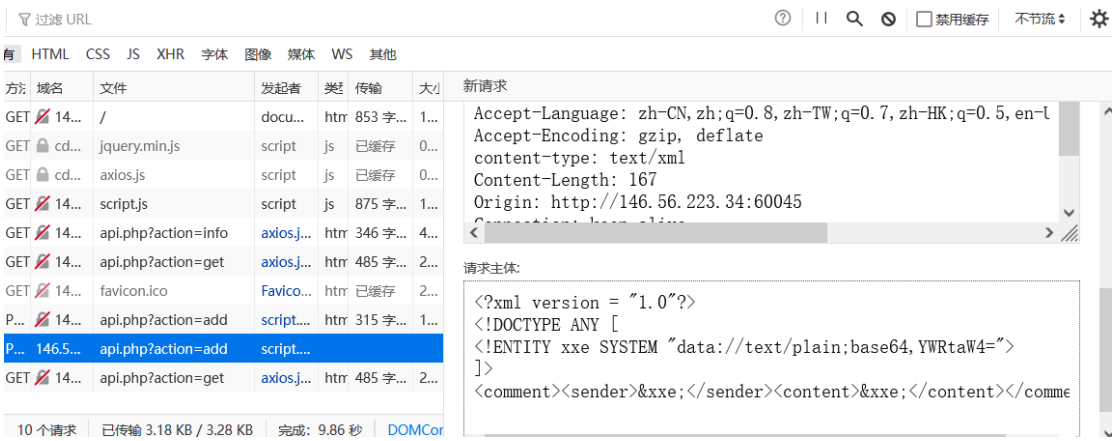
附上思路和随机数的整理



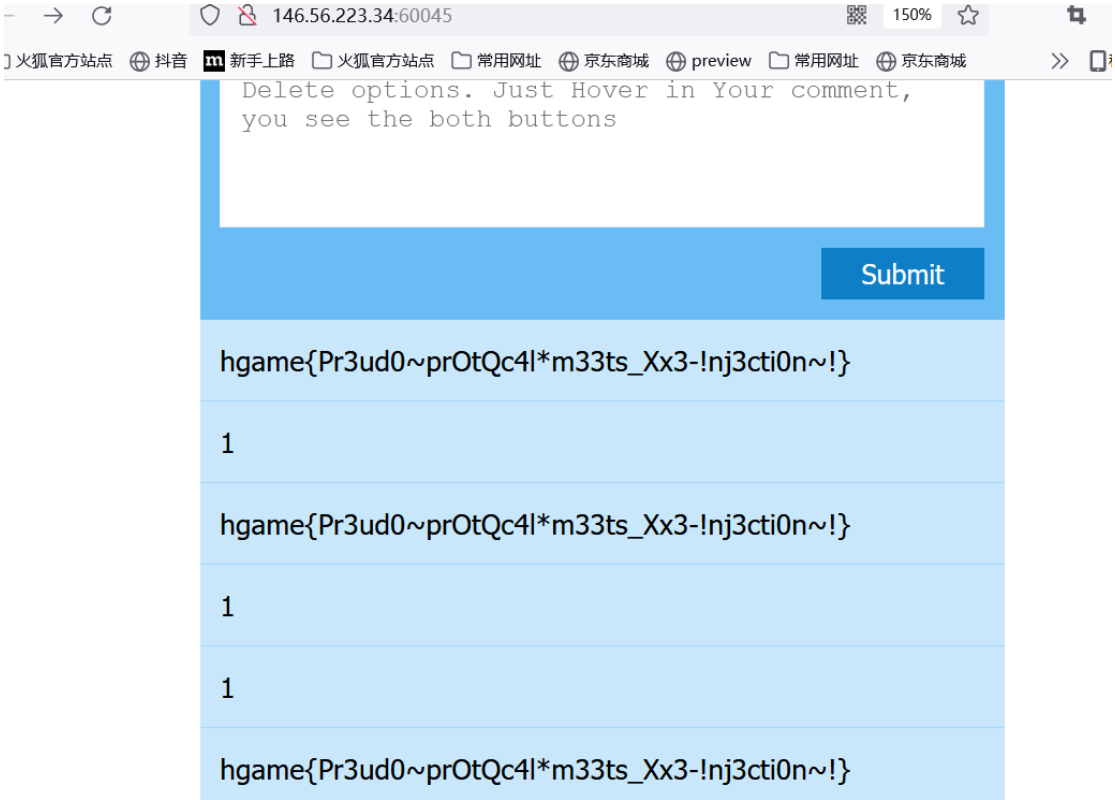
WEB

comment

根据 hint，使用 xml 格式和伪协议，以及考虑源码过滤的情况，参考网上的 xxe 漏洞的使用，以及可以考虑 data 伪协议构造”admin”的其他编码数据绕过检查得到 flag



在一个新的 post 请求主体上修改一下，用 xml 格式，刷新页面得出 flag



事实证明一点：对 web 源码审计的时候，往往需要抓住一部分，因为那一部分就是重点