WeChall-writeup-5-11.21(GPG;hi;Stegano Attachment)

原创

MeliodasC 于 2018-11-21 19:43:28 发布 496 收藏

分类专栏： WeChall 文章标签： WeChall writeup 安全

本文链接：https://blog.csdn.net/Crystal_bing/article/details/84328721

准时打卡！今天又交了积分~

这一次想好好写一下GPG这道题，真的遇到了好多小困难，加起来就是一个大困难…

Training: GPG

首先通过这个网页我们可以了解一下什么是GPG

这两个网站讲的特别详细，我觉得不用另外再写一遍教程了:

1.GPG密钥的生成与使用

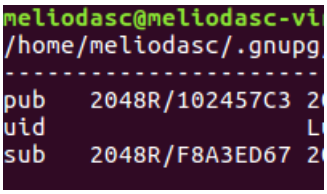
2.GpG使用指南

但是我自己在操作过程中遇到了挺多问题的…在这里分享一下:

1.pub中hash后得到的ID即 `pubID` 代替 `用户ID`

在这里 `pubID` 就是第二行的 `102457C3`

输入 `gpg --list-keys`,会出现四行，分别是：



第一行显示公钥文件名（pubring.gpg）

第二行显示公钥特征（4096位，Hash字符串和生成时间）

第三行显示"用户ID"

第四行显示私钥特征

2.gpg: 未给出公钥服务器(使用 --keyserver 选项);

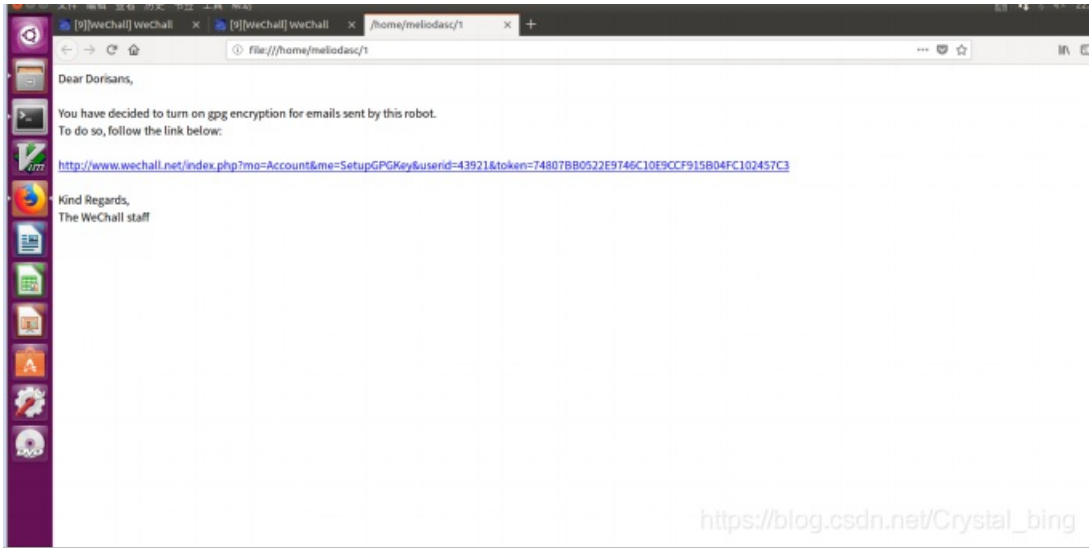
gpg: 上传至公钥服务器失败：URI 已损坏

`gpg --keyserver keys.gnupg.net --send-key pubID`

这个写法跟网上大多数教程不太一样，但是始终不能传上去的大家可以试一试…这个点真的折磨了我好久…

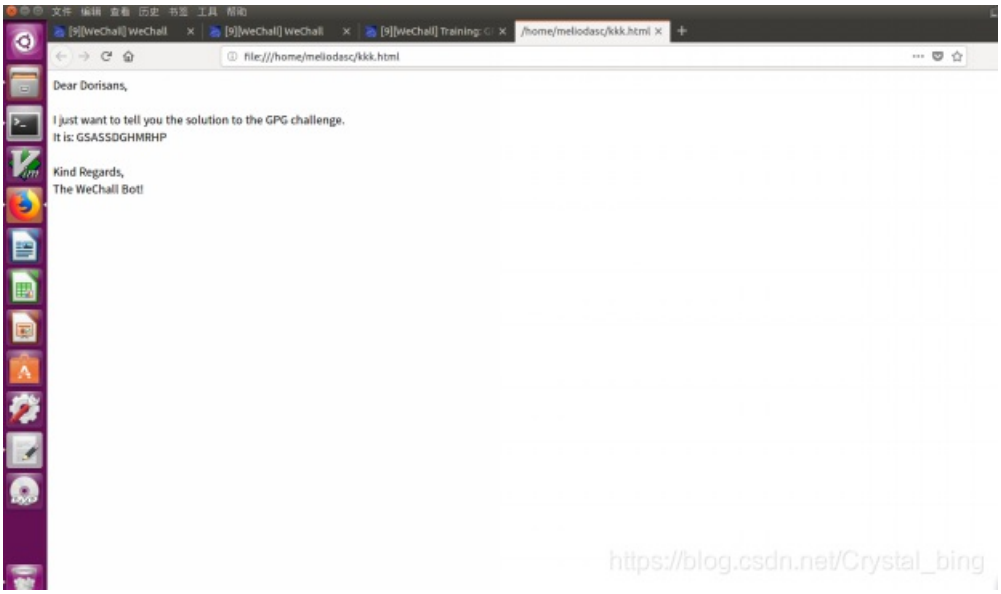
3.输出文件 `gpg --output xxx.html -d test.txt`

向wechall提交公钥后会收到一封邮件，里面是一篇密文。将它保存为txt文档。解密的输出选择格式为html。打开html文件可以直接点击链接，跳转提示已经开启了wechall的gpg。



4.最后的solution输出

跟前面的解密方式一样，提示后面最好也输出成一个html文件（我还以为会是个txt）



---

hi

一个…等差数列…

（首项+末项）*项数/2

就算一算2333

Stegano Attachment

又是一道隐写术

这道题坏坏的，文件保存下来后缀是php。这一步有点凭直觉（因为看到的是一张图片），直接把后缀改成jpg。

用010editor打开，发现最前面是`FFD8FF`，也就是jpg的开头，于是去搜`FFD9`。把之后的内容保存出来。

那么现在又有一个问题，隐藏在后面的这个文件应该是什么格式的呢，查了一下资料，`504B0304`是zip的开头，于是保存为zip格式。解压打开，得到solution。