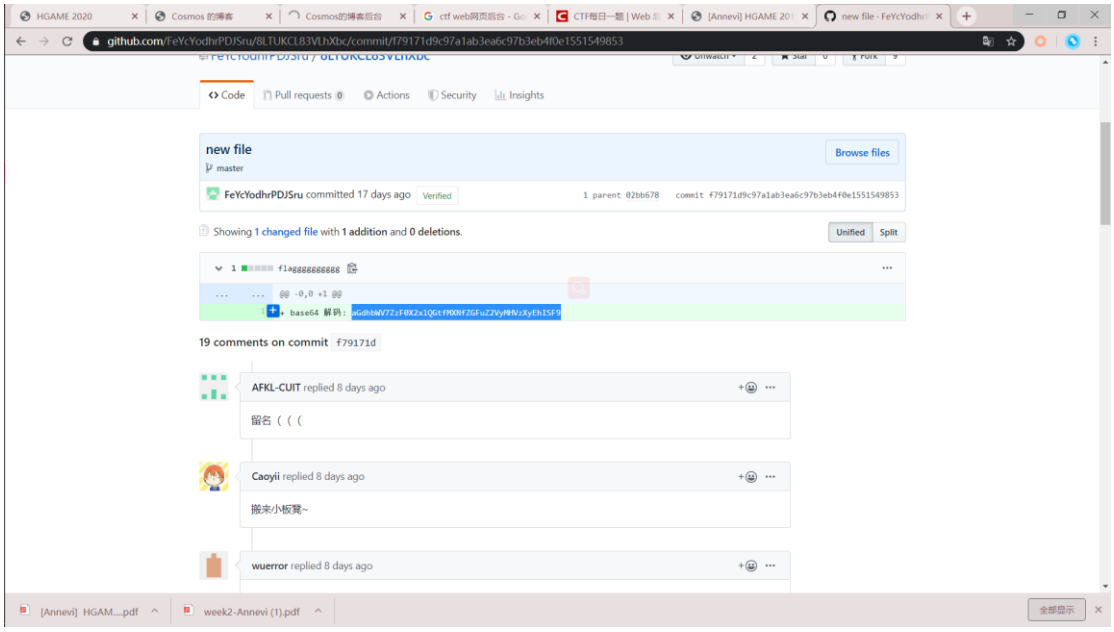
Week1　lupin111

Web:

一　　Cosmos 的博客点题目连接进去就说 git 版本库　发现页面里有页脚 hgame

所以去 github 搜 cosmos hgame

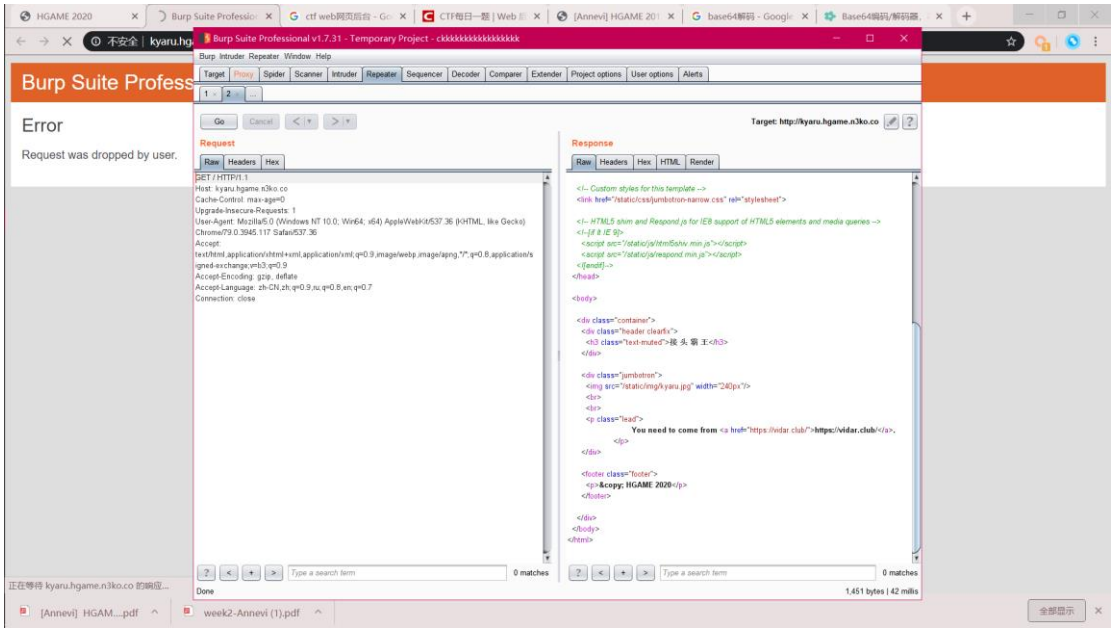


aGdhbWV7ZzF0X2xlQGtfMXNfZGFuZ2VyMHVzXyEhISF9 base64 解密 okk　hgame{g1t_le@k_1s_danger0us_!!!!}

二：

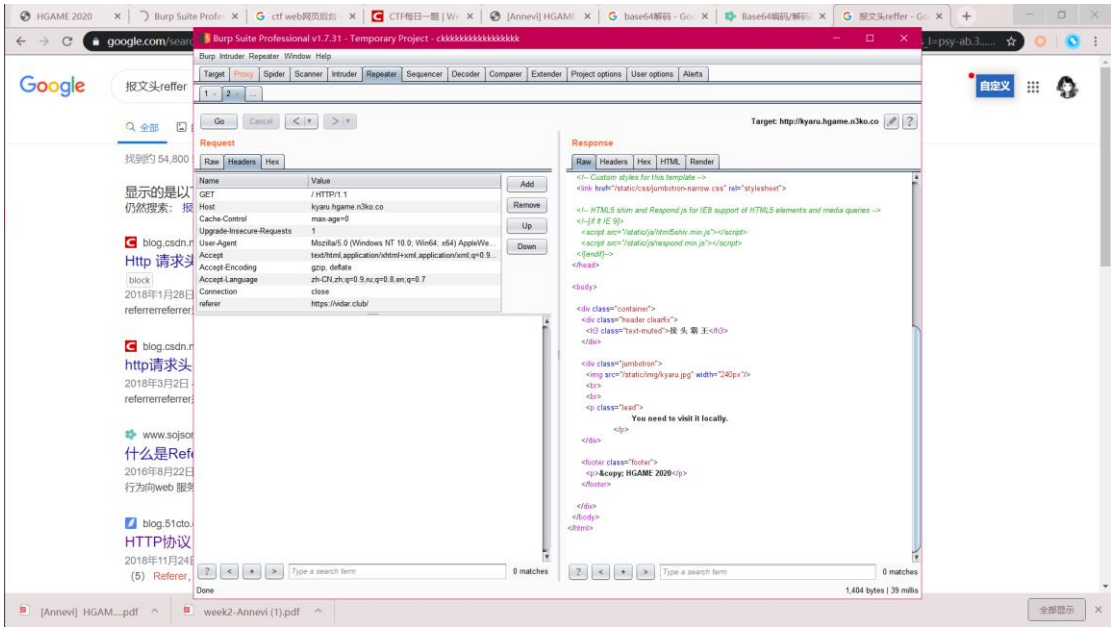
街头霸王

接头？



用 bp 一步步走下去

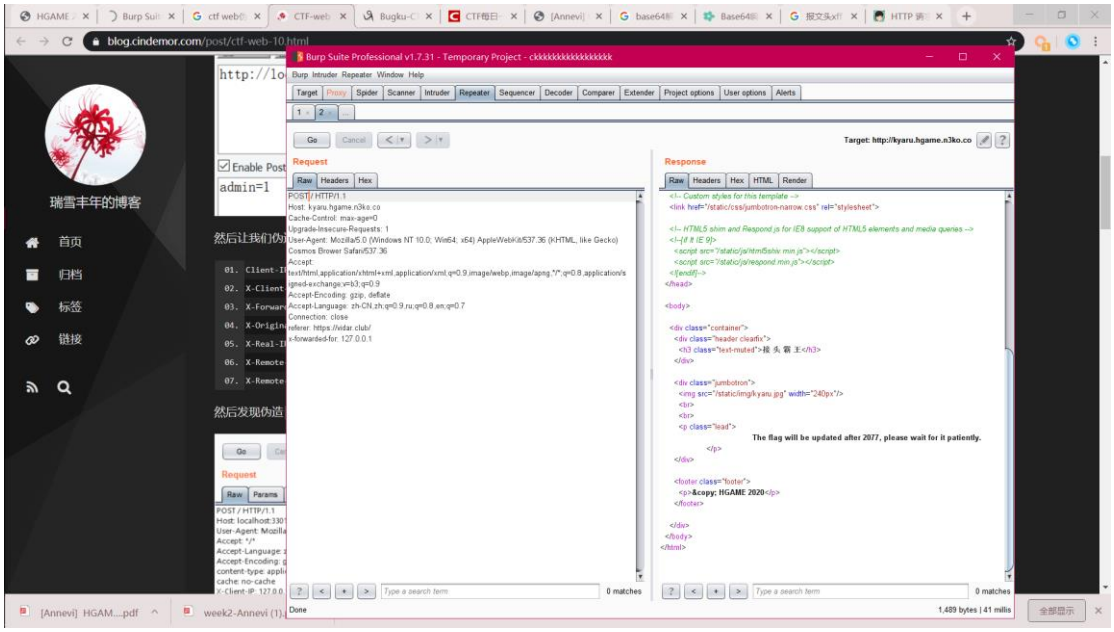
用到了 reffer



Local xff 。

后面省略了 一步 改浏览器 和 请求方式

下面这步卡了好久 0.0 最后 py 茄子 出来的 modify



If nomo sin

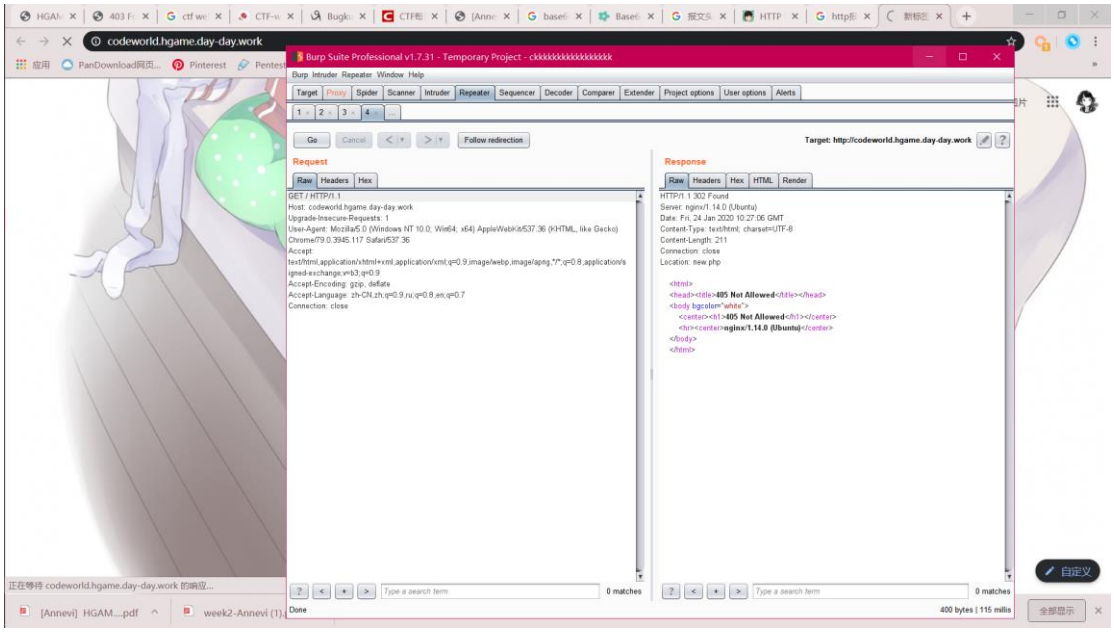
If mo sin

HTTP 协议中的 `If-Unmodified-Since` 消息头用于请求之中，使得当前请求成为条件式请求：只有当资源在指定的时间之后没有进行过修改的情况下，服务器才会返回请求的资源，或是接受 POST 或其他 non-safe 方法的请求。如果所请求的资源在指定的时间之后发生了修改，那么会返回 412 (Precondition Failed) 错误

三：点连接 死活找不到 302

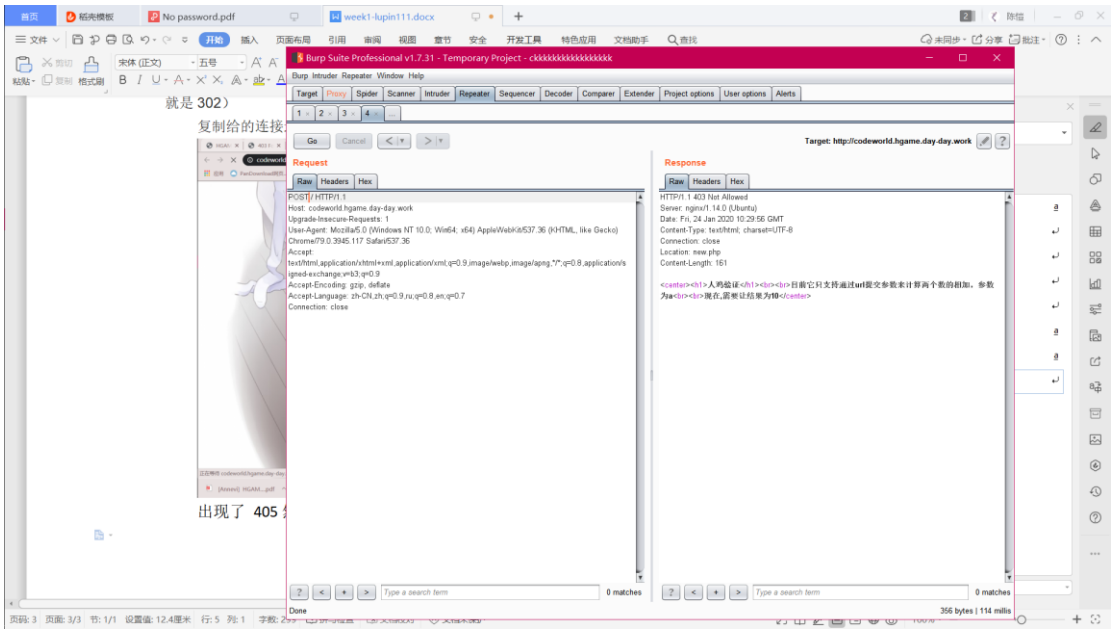
后来突然发现 给的连接和点进去的连接有差别 (一开始我觉得页面都这样的,后来才知道原来这就是 302）

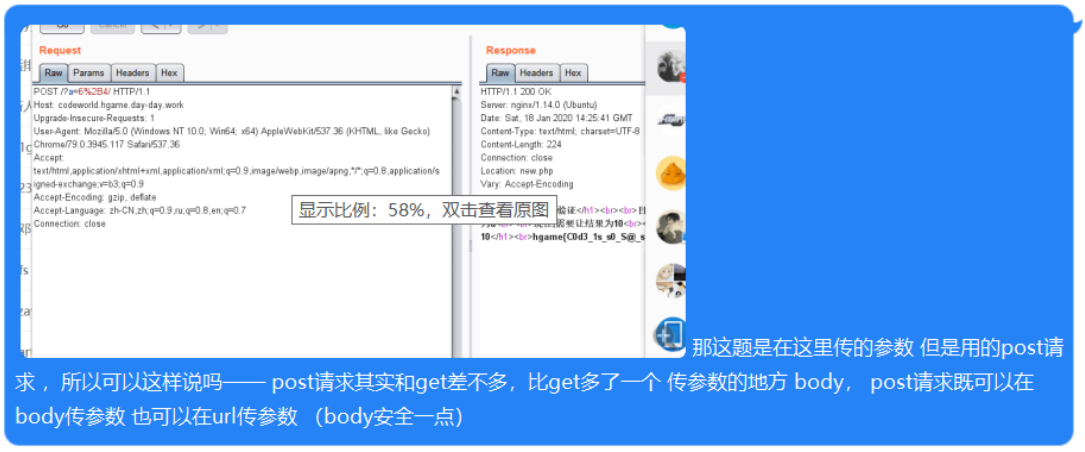
复制给的连接地址 bp 抓包



出现了 405 然后又懵了

去百度了 405 说请求问题 修改为 post 来到人机验证





那这题是在这里传的参数 但是用的post请求，所以可以这样说吗—— post请求其实和get差不多，比get多了一个 传参数的地方 body， post请求既可以在body传参数 也可以在url传参数 （body安全一点）

原来 post 也能 url 传参数。

四：

这题我二话没说 改包 然后过了。。问了茄子一下，哈哈投机取巧。

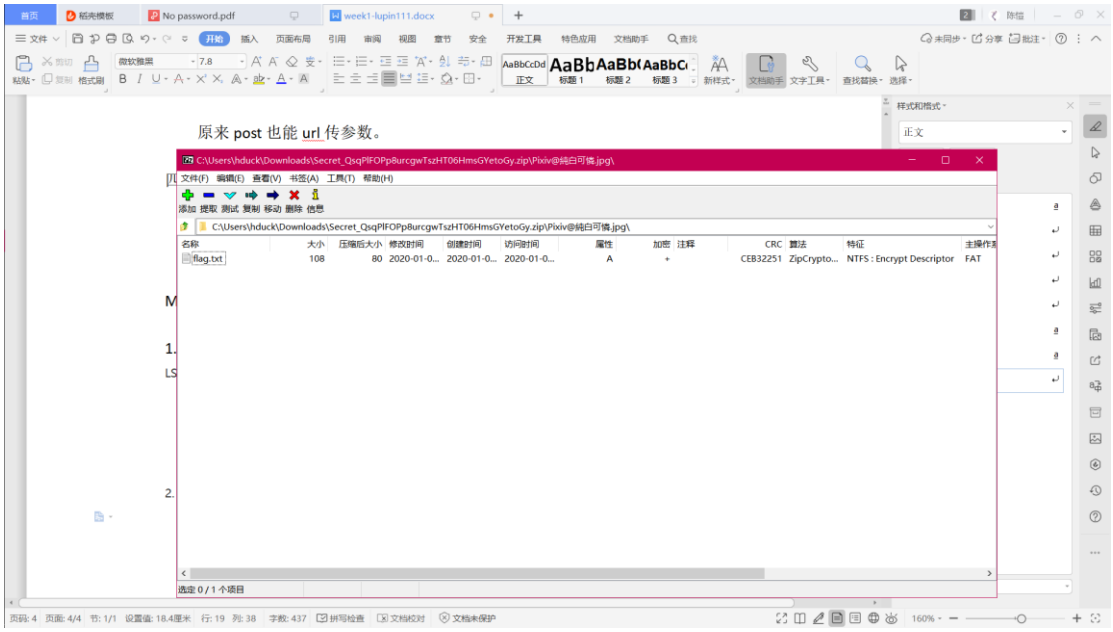
Misc： 我就说一下解决过程吧， 很多文件都删了 只留了一些工具（0.0）

1. Li0tIC4uLi0tIC4tLi4gLS4tLiAtLS0tLSAtLSAuIC4uLS0uLSAtIC0tLSAuLi0tLi0gLi4tLS0gLS0tLS0gLS0tLS0gLi4tLS0gLS0tLS0gLi4tLS4tIC4uLi4gLS0uIC4tIC0tIC4uLi0t

百度搜了一些好像有原题 base64 解完 一段摩斯密码 W3LC0METO2020HGAM3

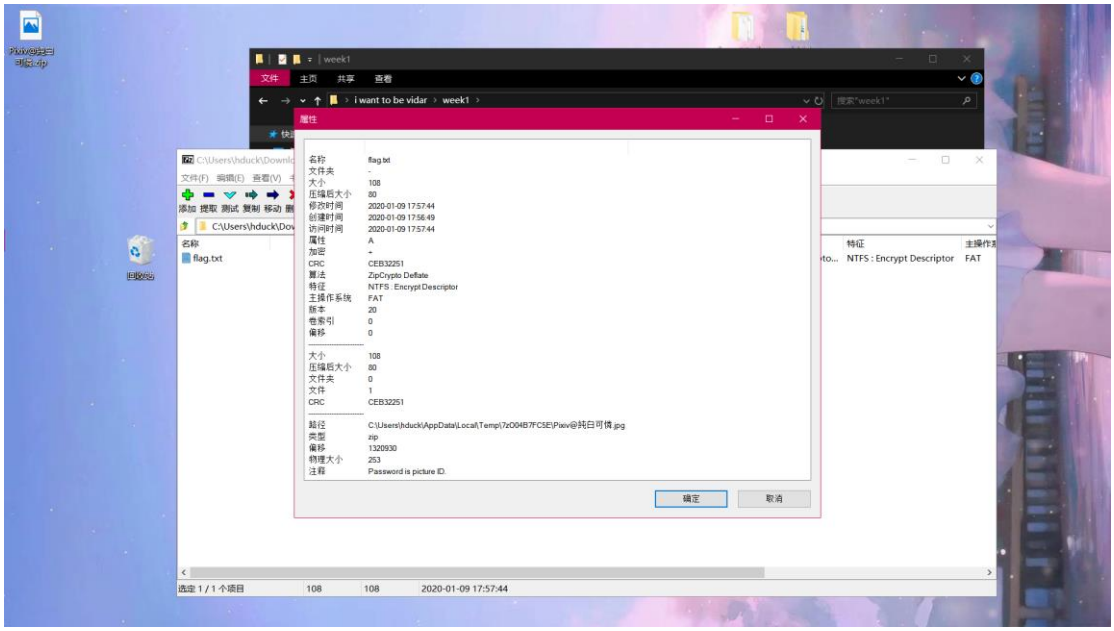
2.

拿到一张图片 在 7z 里双击这个图片 竟然 看到了 flag.txt 要密码



发现注释里 0.0

找了半天不知道 id 在哪 后来 pixivi 草 p 站 然后去搜索 id 就是 url 后面 id=



拿到这个 不熟悉编码的 去百度了

\u68\u67\u61\u6d\u65\u7b\u44\u6f\u5f\u79\u30\u75\u5f\u4b\u6e\u4f\u57\u5f\u75\u4e\u69\u43\u30\u64\u33\u3f\u7d

修改过的 unicode 编码 用 ascll 在线工具解出了 flag

3 克鲁斯神话

明文攻击

4. 每日推荐　流量分析 拿到一个压缩包 。

Crypto

1. rsa 签到题
2. 模运算还行 0.0 看了挺久 写了一个脚本跑出来

4 没找到啥规律 输入 32 字符一一比较 然后用记事本写出来

3. 没写出来 编码转换绕的有点头晕 后面几天没动脑子 0.0