Web1

1. ?action　php 伪协议任意文件读取 读取 login.php

php://filter/read=convert.base64-encode/resource=login.php

读出一段 base64 解码　发现$$ 百度搜索 php $$得知 可以构造

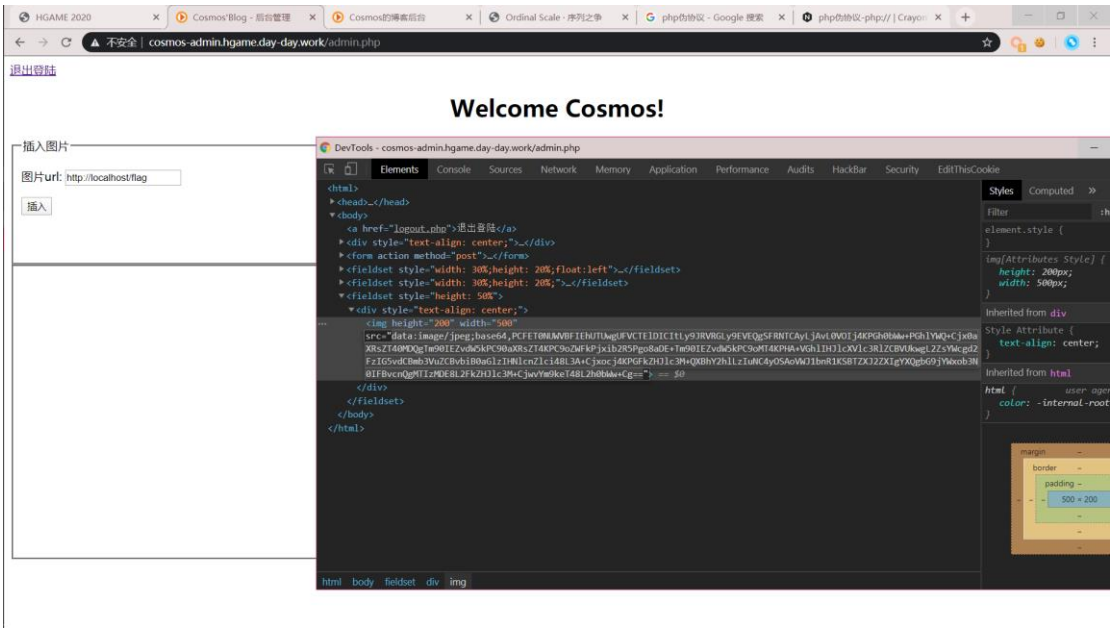
Debug = GLOBALS

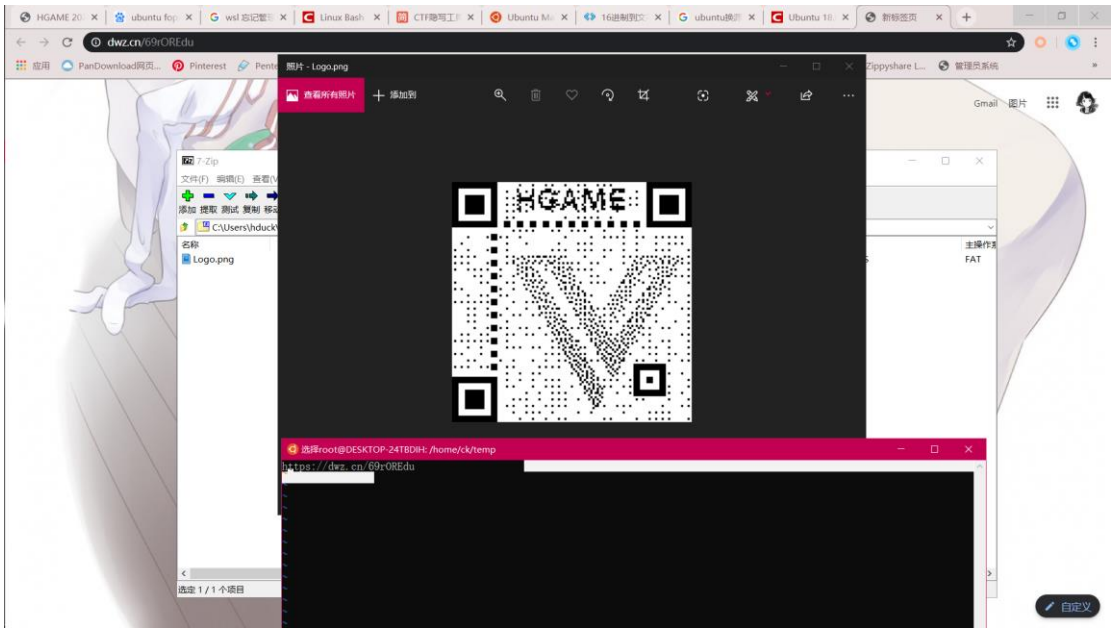
得到 账号 Cosmos！　密码为 md5 加密后 0e 开头　随便找了一个 s878926199a

登录后 看到一个 img_url 得知为 ssrf　再用任意文件读取 看一下 admin.php 文件的源码

然后知道 p_url 后【host】 要为 localhost　或者 timbaidu.com 中的一个

所以如图构造 playload 得知 flag 的 base64 解码以后拿到 flag





Misc1

Cosmos 的午餐

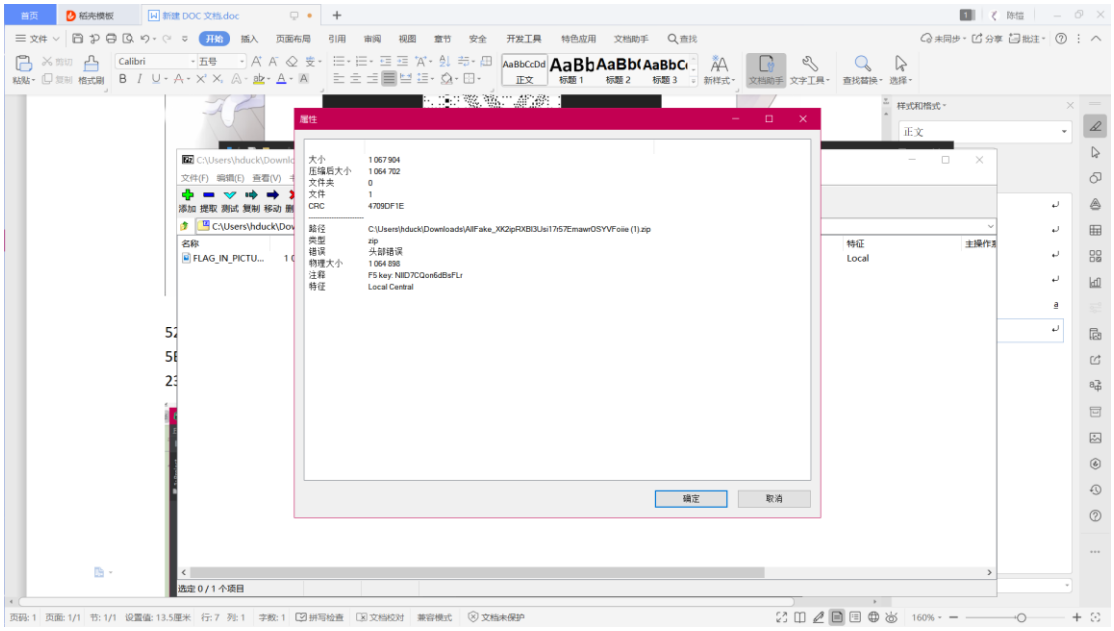
Ssl 解密后分析流量包 追踪 tls 流

得到一个 zip

打开发现名字 outguess 这里卡了好久 0.0 最后靠出题人提示解密拿到 flag

Misc2

所见为假 看了好久对联没发现什么。 最后在图片提示中找到 F5



526172211A0701003392B5E50A010506000501018080008B9527AEA2402030BA70004A70020CB

5BDC2D80000008666C61672E7478740A03029A9D6C65DFCED5016867616D657B343038375E7A236D737733344552746E46557971704B556B32646D4C505736307D1D77565103050400

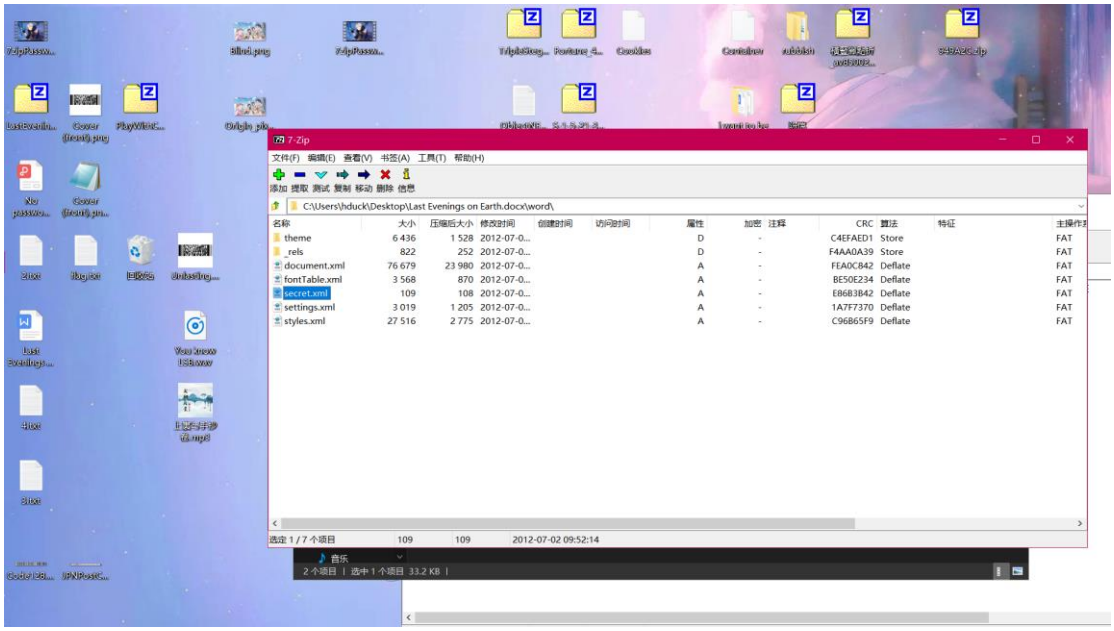
Misc3 地球最后的夜晚

进入 pdf 翻译了一下 人工智能盲水印？ 盲水印？要两张图片 没有图片现在要 解密压缩包所以 搜了一下 pdf 隐写

发现密码 OmR#O12#b3b%s*IW

然后看到一个 word 文件 搜了一下 word 隐写 发现有一个 xml

用压缩工具打开 secret.xml 文件里发现 flag



Misc4

发现码 为日本 post 编码

找一个在线网站 生成 然后根据长短 一一对照得到密码 后再解密文件 又得到一个码 这个码很长找了个工具在线识别 0.0