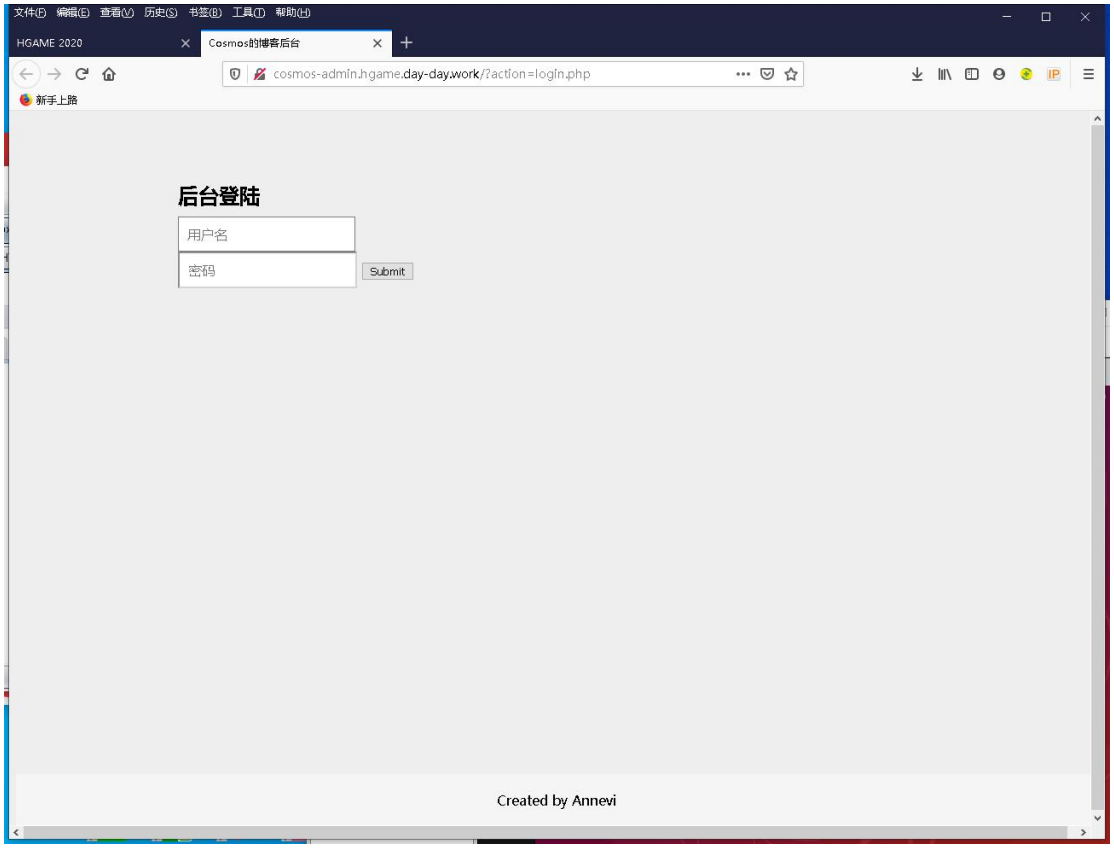
HGAME WRITEUP WEEK2——泛舟当歌

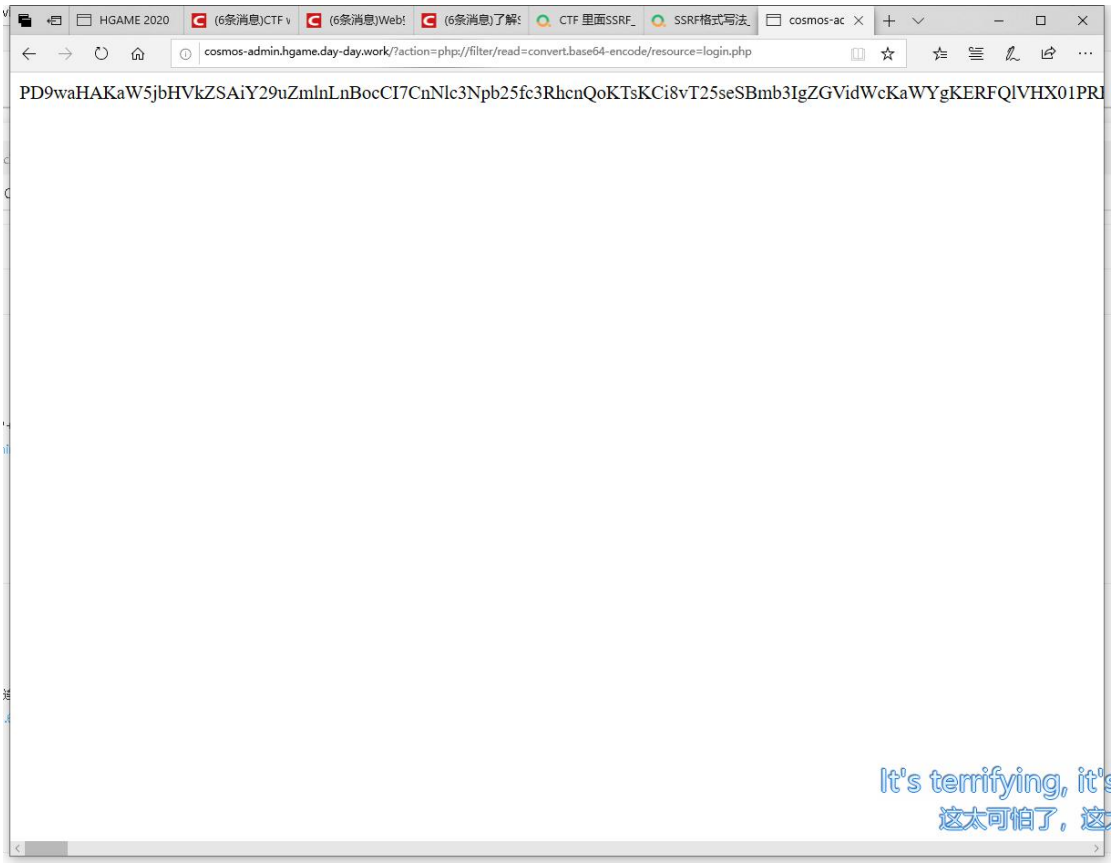
WEB （0/4）

0x01 Cosmos 的博客后台

（首先致歉 E99 学长，后面真的是耐心的手把手教我，可惜最后还是没解出来，基础知识太匮乏了，实在无法触类旁通。头皮都抓破了，不过还是能解一解前面的，写下来把，虽然没解出来，但是还是学到了很多）



首先查看源码等皆无收获，然后通过 URL 里意外发现了有个 action 参数，感觉是伪协议，走一波，然后发现源码



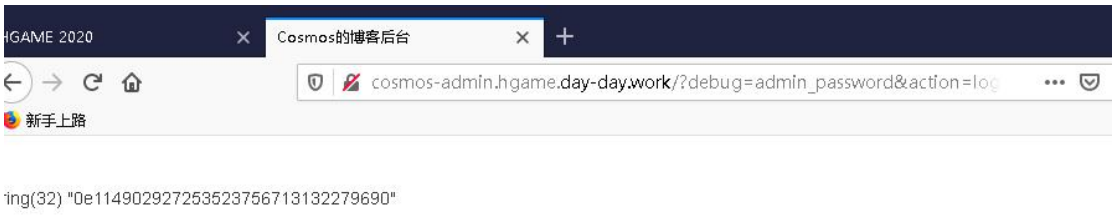
BASE64 解码后，查看源码

```
'
<?php
include "config.php";
session_start();

//Only for debug
if (DEBUG_MODE){
    if(isset($_GET['debug'])) {
        $debug = $_GET['debug'];
        if (!preg_match("/^[a-zA-Z_\x7f-\xff][a-zA-Z0-9_\x7f-\xff]*$/", $debug)) {
            die("args error!");
        }
        eval("var_dump($$debug);");
    }
}

if(isset($_SESSION['username'])) {
    header("Location: admin.php");
    exit();
}
else {
    if (isset($_POST['username']) && isset($_POST['password'])) {
        if ($admin_password == md5($_POST['password']) && $_POST['username'] === $admin_username){
            $_SESSION['username'] = $_POST['username'];
            header("Location: admin.php");
            exit();
        }
        else {
            echo "用户名或密码错误";
        }
    }
}
?>
```

然后据学长提示发现 DEBUG 那很可疑，通过了 2 小时速成 PHP 后，发现了

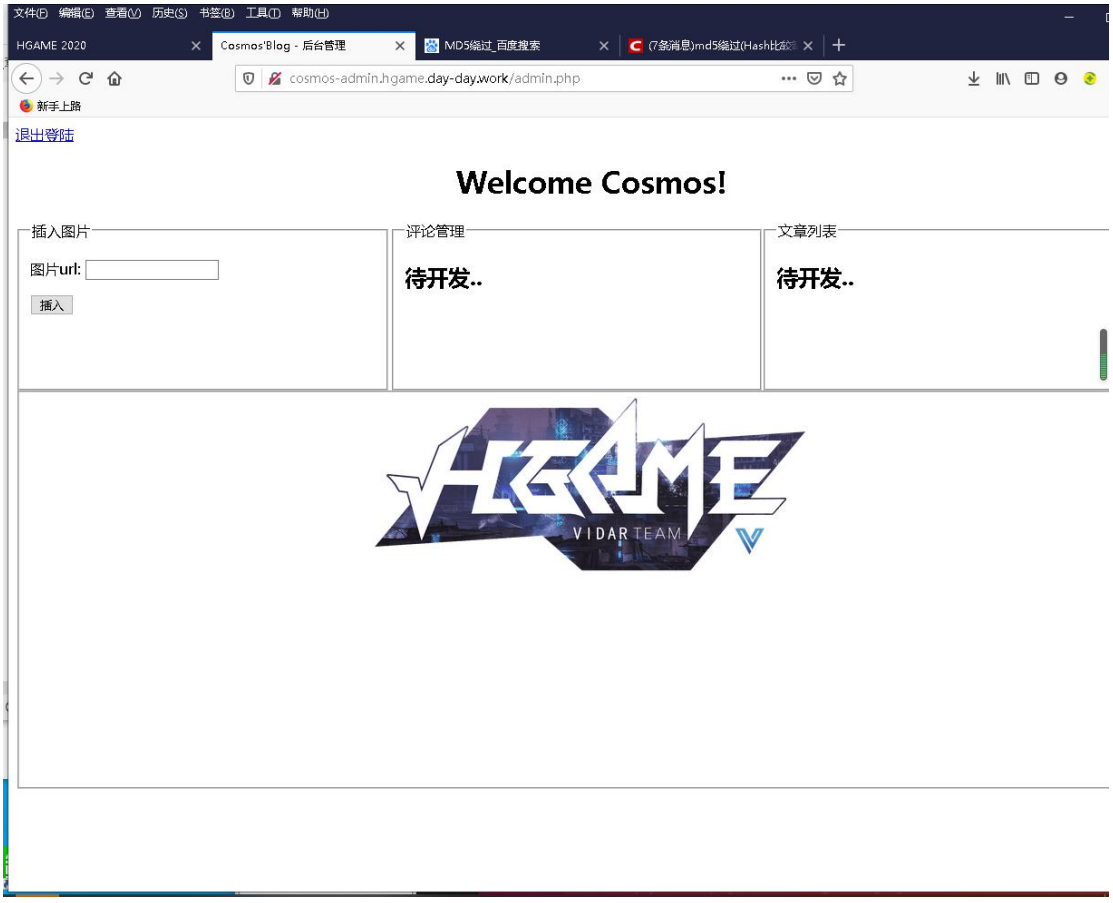
```
eval("var_dump($$debug);");
```

有泄露嫌疑，只要把 dubug 的参数赋值 admin_username 那不就会输出打印$admin_username 的值了嘛，好的试一试，果然出现了，Username 是 Cosmos!, Password 如下



ing(32) "0e114902927253523756713132279690"

显然是通过了 MD5 加密，再回看源码 ($admin_password == md5($_POST['password']) & ==是弱类型比较，很好，那么随便输入一个 MD 加密后是 0e 开头的就会被 PHP 认为是 0=0 而发生 MD5 绕过（hash 缺陷）了，这里我输入了 QNKCDZO，成功进入了里面



欸，flag 还没出来嘛？哇，太难了把，好吧只能继续查看 admin 的源码（方法同上）

```php
<?php
include "config.php";
session_start();
if(!isset($_SESSION['username'])) {
    header('Location: index.php');
    exit();sta
}

function insert_img() {
    if (isset($_POST['img_url'])) {
        $img_url = @$_POST['img_url'];
        $url_array = parse_url($img_url);
        if (@$url_array['host'] !== "localhost" && $url_array['host'] !== "timgsa.baidu.com") {
            return false;
        }
        $c = curl_init();
        curl_setopt($c, CURLOPT_URL, $img_url);
        curl_setopt($c, CURLOPT_RETURNTRANSFER, 1);
        $res = curl_exec($c);
        curl_close($c);
        $avatar = base64_encode($res);

        if(filter_var($img_url, FILTER_VALIDATE_URL)) {
            return $avatar;
        }
    }
    else {
        return base64_encode(file_get_contents("static/logo.png"));
    }
}
?>
```

这里没有什么思路了，然后茄子学长提示我了解一下 SSRF，再次速成后，发现可以通过 file:// 等协议访问服务器内部的文件，然后又因为这里有限制条件

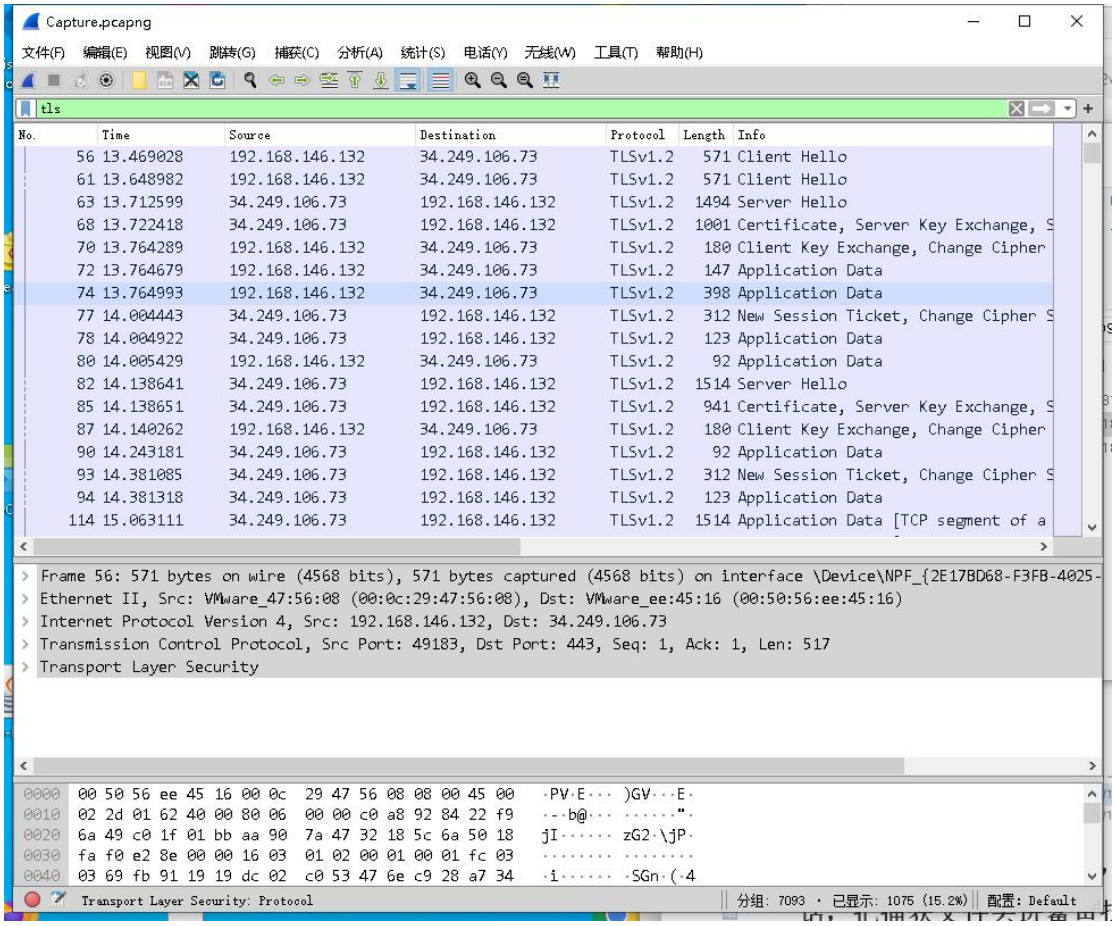
```php
if (@$url_array['host'] !== "localhost" && $url_array['host'] !== "timgsa.baidu.com") {
    return false;
}
```

，所以要绕过，但是这个时候尝试了很多（http://,file:// @的忽略 /的忽略都瞎几把操作了一下），都解不出来，百度了好久也查不到东西，最后只能无奈放弃，最后的 payload 是 file://localhost//flag.png，并不能解出啥东东^^

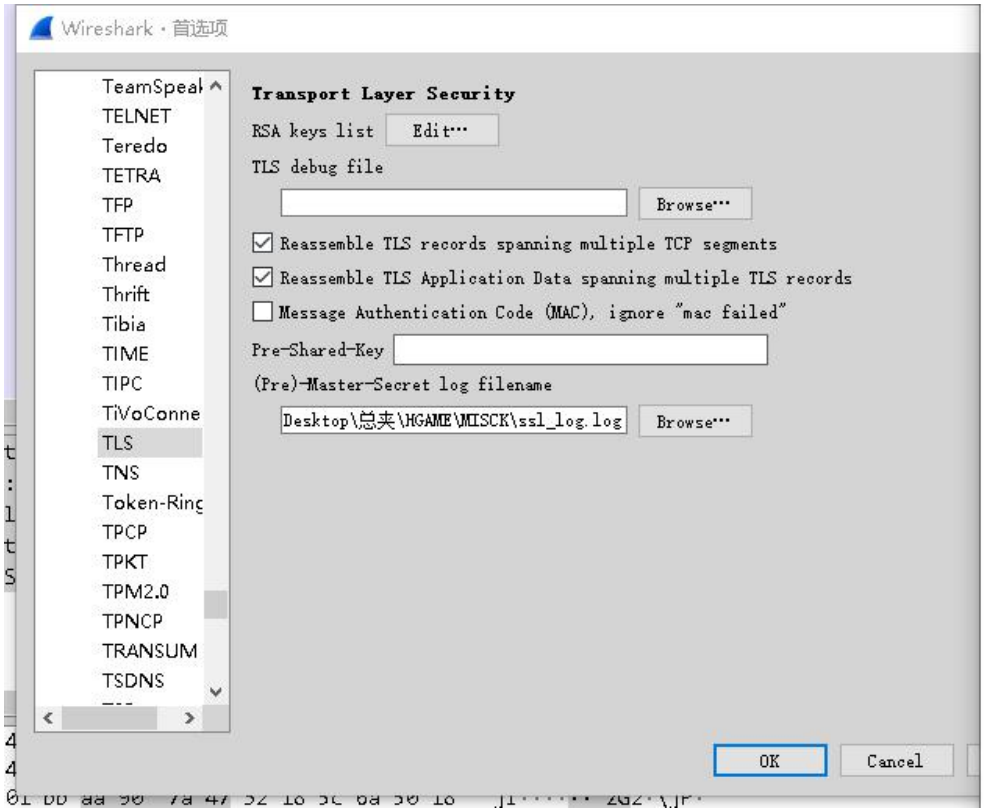
Misc （3/4）

0x01 Cosmos 的午餐

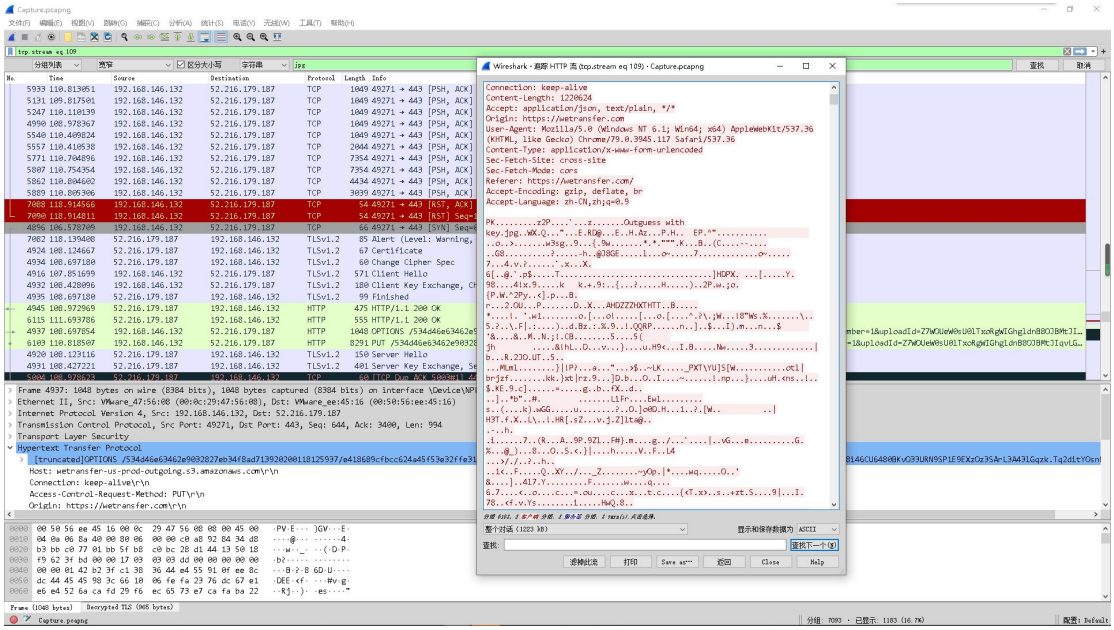
开局一个文档加捕获文件，文档打开全是加密后的对话，把捕获文件丢进鲨鱼扫一扫



发现很多 TLS 流，显然是用文档去解密 SSL 流了，打开首选项，



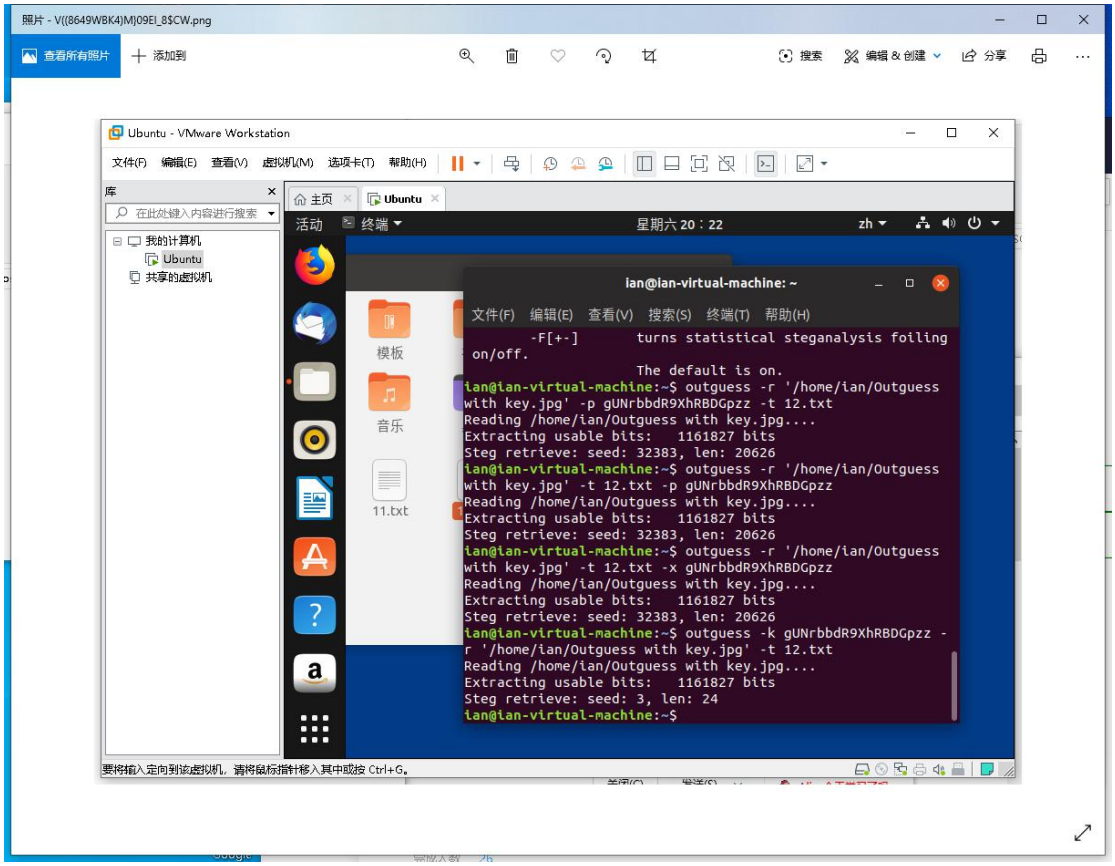
然后会出现很多 HTTP 和 HTTP2 流，开始一个一个追踪过去，其中在一个 HTTP 流中发现可疑选项



PK 开头显然是个压缩包，解压下来后

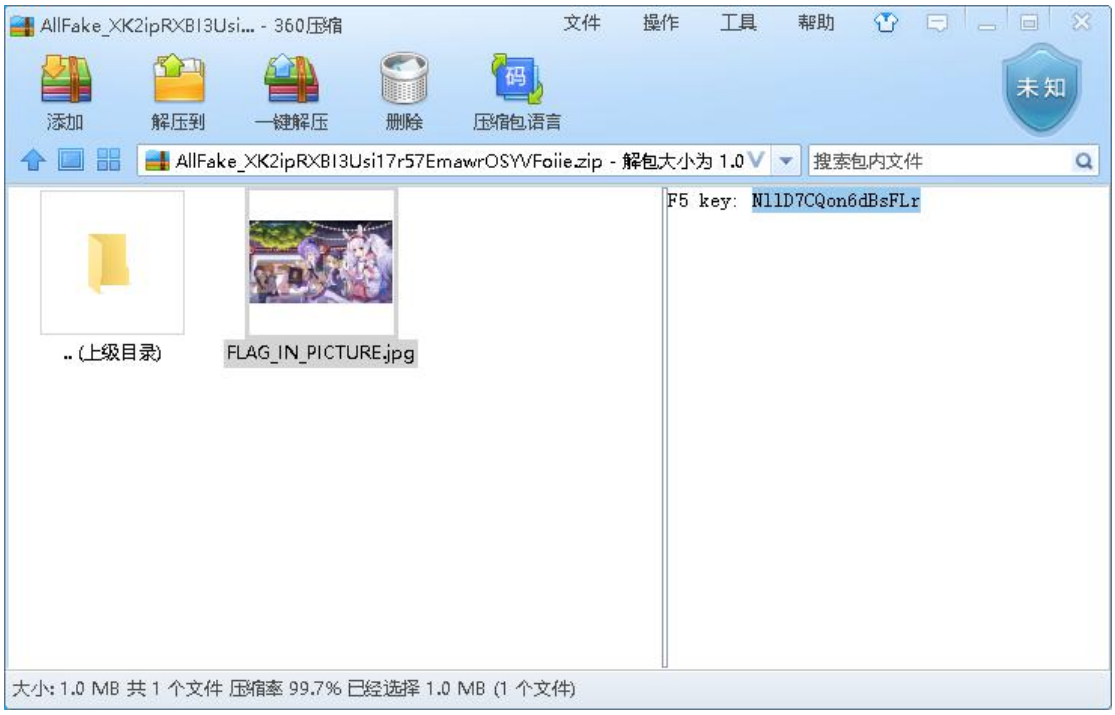
很明显的图片内容和题目介绍吻合了，那就是这个没错了，然后图片名字显示 Outguess，并且在图片备份中发现了 Key,

那显然就是要我们用 Outguess 去解密了，虚拟机跑一下，

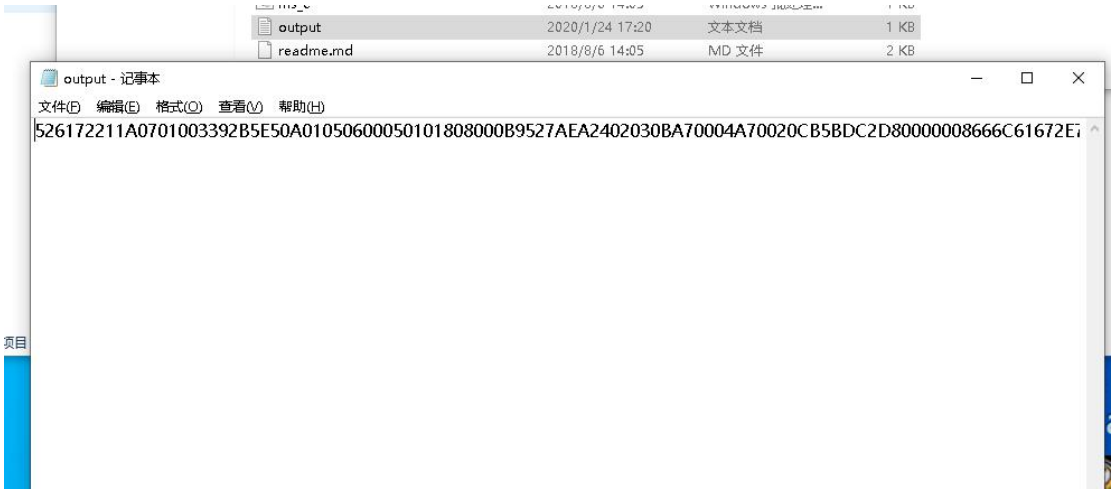


（最后一个格式是对的），然后得出的文本里面是个网址，输入后下载一个二维码扫码后即得到 FLAG。

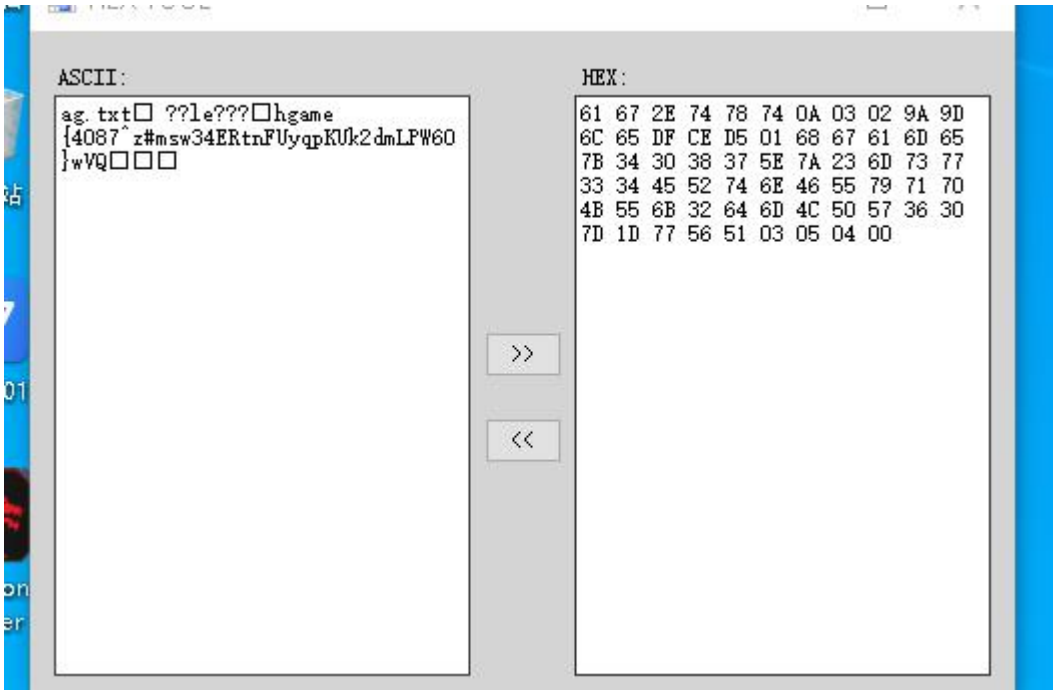
0x02 所见即为假



首先打开压缩包，发现提示，显然是 F5 的 JPG 格式隐写，通过 F5 解密以后

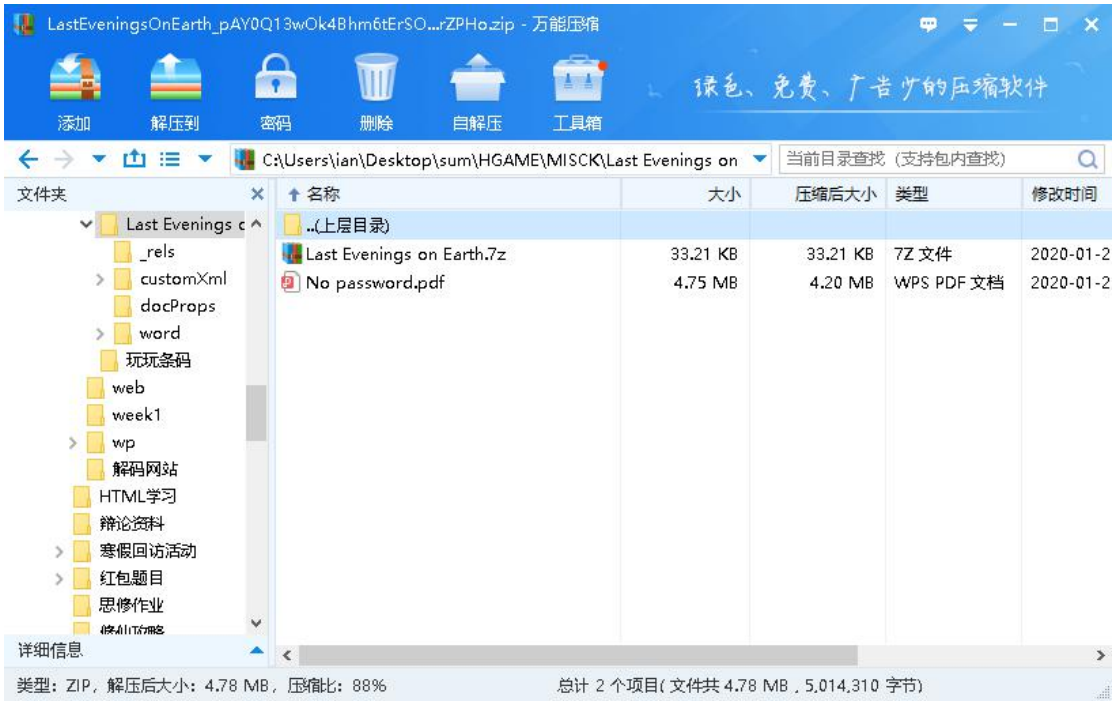


猜测应该是 HEX16 进制，通过 cs_hextoasc 转换后

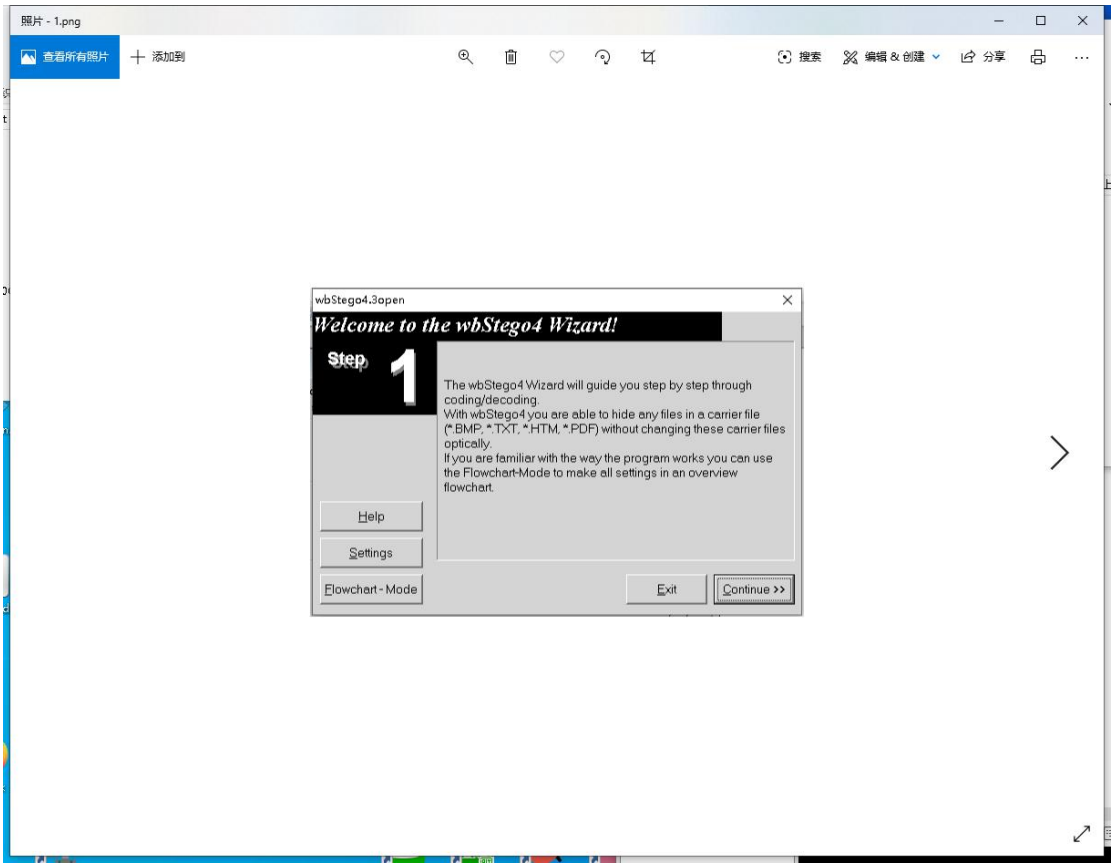


即得到了 Flag。

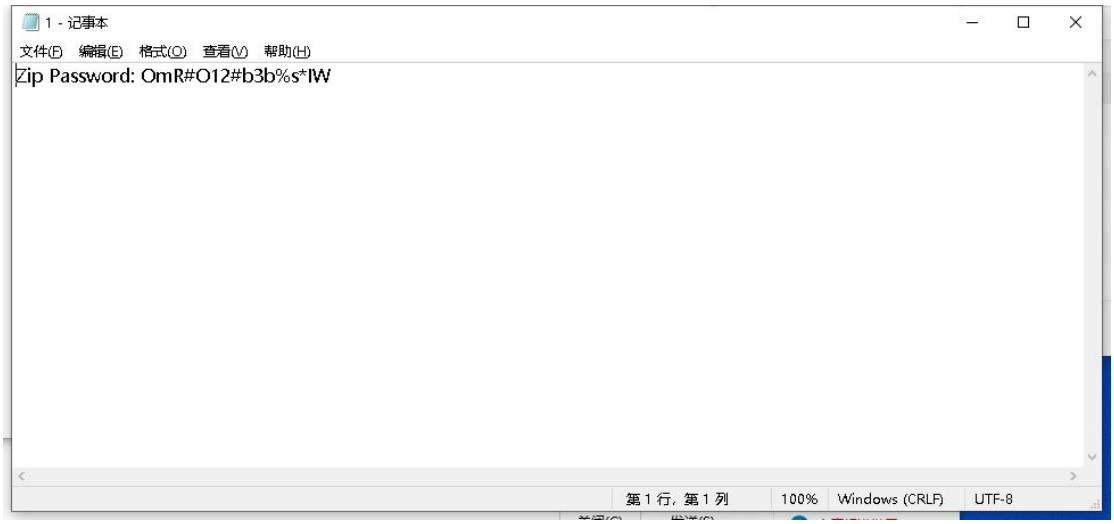
0x03 地球上最后的夜晚



开局一个有密码的压缩包和一个提示为 no password 的 PDF 格式文档，猜测为 PDF 格式的隐写，百度一波后，使用工具 WbStego4 解密



得到 ZIP 密码



打开文档后

发现与隐藏字符和白色字符都无关，那么大胆猜测为 WORD 文档的 XML 转换，分解 WORD（直接选择用 7Z 打开压缩包）然后在 word 目录下发现一个 secret.xml 的目录，打开后得到 flag