Hgame week1 write up --Yuahwg

Web 部分：

1. 谁吃了我的 flag

一开始没有 hint 的时候，看着题目一脸懵逼（完全对不上 mki 学长的脑电波之后题目给了提示

Description

呜呜呜，Mki一起床发现写好的题目变成这样了，是因为昨天没有好好关机吗T_T hint: 据当事人回忆，那个夜晚他正在用vim编写题目页面，似乎没有保存就关机睡觉去了,现在就是后悔，十分的后悔。

百度了下 vim 不正常退出之类的，知道了有一个.swp 文件，于是下载 swp 文件后用 vscode 打开得到了 flag hgame{3eek_diScl0Sure_fRom+wEbsit@}

2. 换头大作战

进入题目后先输入一个 flag 得到如下提示

想要flag嘛： submit

request method is error.I think POST is better

于是 F12 将 get 改为 post 后靠诉我们需要 localhost

想要flag嘛： submit

https://www.wikiwand.com/en/X-Forwarded-For
only localhost can get flag

然后用 burpsuite 抓包改头，百度到可以用 X-Forwarded-For 伪造 ip，修改之后又

有其他一些提示，按照要求修改

```
X-Forwarded-For:127.0.0.1
Referer:www.bilibili.com
```

以及 admin 改为 1 和神奇的 waterfox 后得到 flag hgame{hTTp_HeaDeR_iS_Ez}

3. very easy web

一道初级的 php 代码审计（题目说明了），（但是自己对 php 了解很少，希望下面自己对题目的理解没有错误，也等着 wp 出了后看看大佬们的思路）

首先输入的 id 要满足

```
if(strpos("vidar",$_GET['id'])!==FALSE)
    die("<p>干巴爹</p>");
```

这里即函数返回值应该是 false。

```
$_GET['id'] = urldecode($_GET['id']);
```

然后题目中还需要有一次 url 解码，解码后的值应该和”vidar”相等，在百度的时候找到了一道也和

urldecode 有关的题
https://blog.csdn.net/LJFYYJ/article/details/81047013
参考了下方法，首先知道了 v 的 url 加密是%76，使用?id=%76idar 时，发现会自动 url 解码一次，所以按照博客中使用%的 url 加密%25，如下操作

```
?id=%2576idar
```

得到 flag　hgame{urlDecode_Is_GoOd}

RE 部分：

1. Pro 的 Python 教室

Hgame 的第一道 Python 有关的题？（虽然自己不会 python 但也大致可以做(meng)出来）

```
print 'Plz input the first part:'
first = raw_input()
if first == enc1:
    pass
else:
    print 'Sorry , You\'re so vegatable!'
    exit()
```

第一部分对输入没有改变就是 enc1 的值 hgame{

```
print 'Plz input the secend part:'
secend = raw_input()
secend = base64.b64encode(secend)
if secend == enc2:
    pass
else:
    print 'Sorry , You\'re so vegatable!'
    exit()
```

第二部分对输入进行 base64 加密后等于 enc2 即可，所以把 enc2 进行 base64 解密得到第二部分 Here_1s_3asy_

```
print 'Plz input the third part:'
third = raw_input()
third = base64.b32decode(third)
if third == enc3:
    pass
else:
    print 'Sorry , You\'re so vegatable!'
    exit()
```

Emmm 第三部分其实自己不懂为什么因为自己直接用的 enc3 的值 PythOn}然后提交的　hgame{ Here_1s_3asy_ PythOn}结果通过了。。。
等看看大佬的 wp 理解下吧。。