

Week1—fzlyp

Web

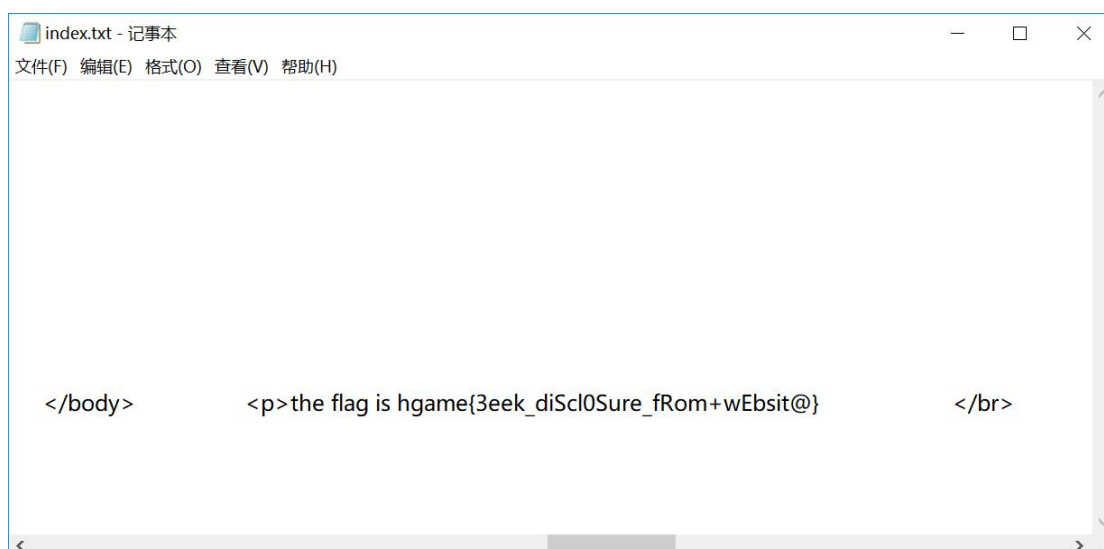
一.谁吃了我的 flag

据当提示当事人用的是 vim 编写题目页面，vim 是有临时文件的，vim 中的 swp 即 swap 文件，在编辑文件时产生，它是隐藏文件，如果原文件名是 vidar，则它的临时文件 Vidart.swp。如果文件正常退出，则此文件自动删除。

题目说非正常退出，所以应该此文件存在，原目录为 <http://118.25.111.31:10086/index.html>，那么访问他的临时文件目录 <http://118.25.111.31:10086/index.html.swp> 出现如下提示，



下载并用记事本打开后，就看到了 flag



另外，实验吧有一题类似但比这个难，各位做了这题后有兴趣可以去试试，也是要用到

相同的思路的: <http://www.shiyanbar.com/ctf/1808>

二.换头大作战

打开网页, 显示如下,

想要flag嘛:

那么就先随便填写一个试试看楼, 如下截图

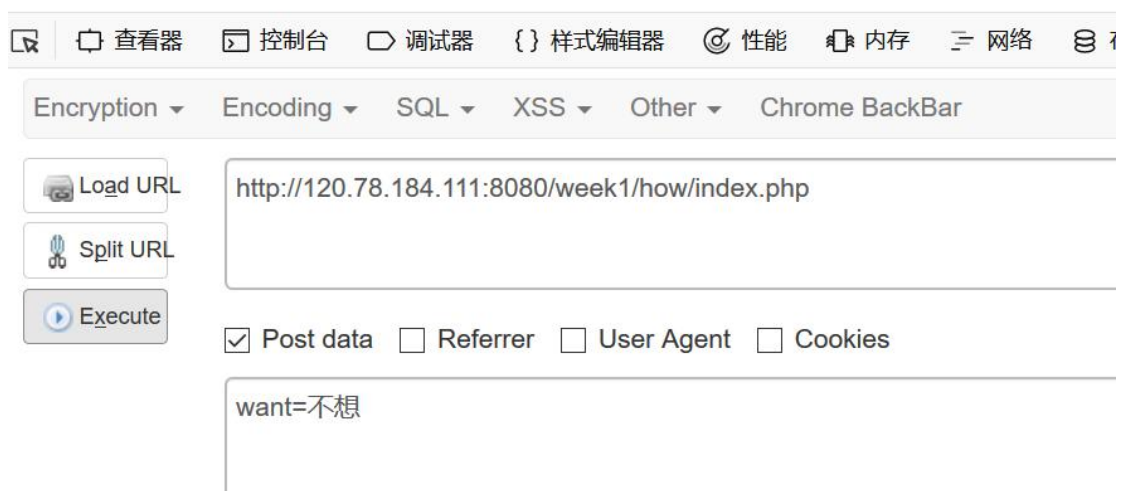


request method is error.I think POST is better

Post 方法提交, ok, 找到 12 姑娘请来了 hackbar 兄弟, 由于观察到上图 url 中出现了 want=不想, 所以知道 post 提交的变量名称为 want

想要flag嘛:

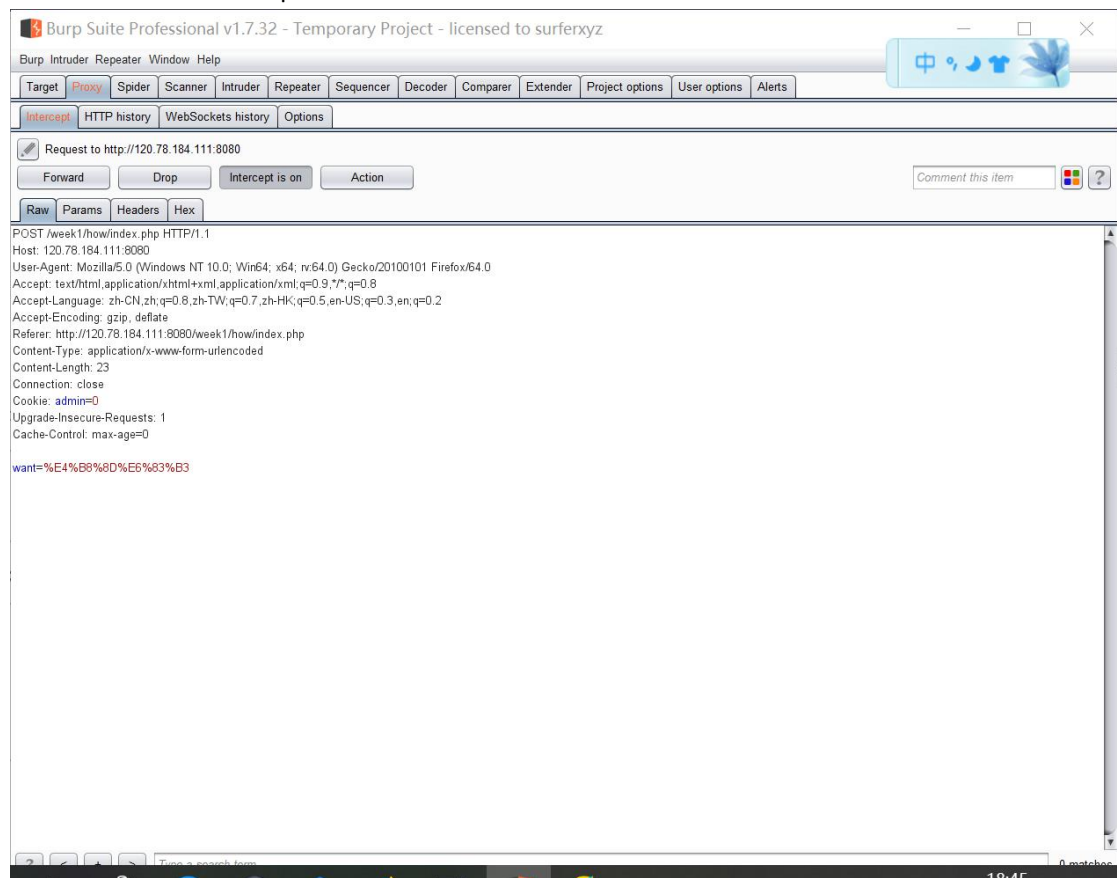
<https://www.wikiwand.com/en/X-Forwarded-For>
only localhost can get flag



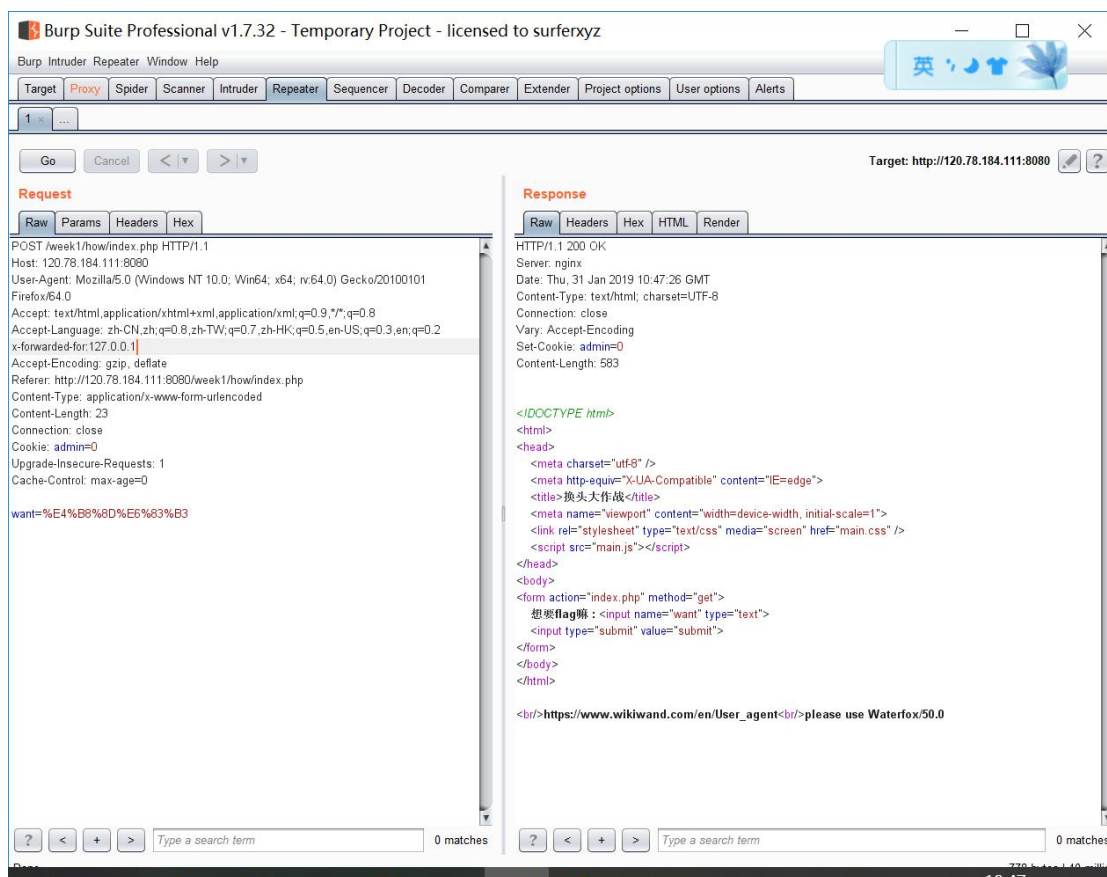
这里吐槽一下提示, www.wikiwand.com 居然是资料网址, 我一开始打不开这个网站, 然后又看到下面的 localhost 以为要修改 localhost ip 才能访问, 然后在这个网站中找 flag,

呜呜，浪费了半小时。

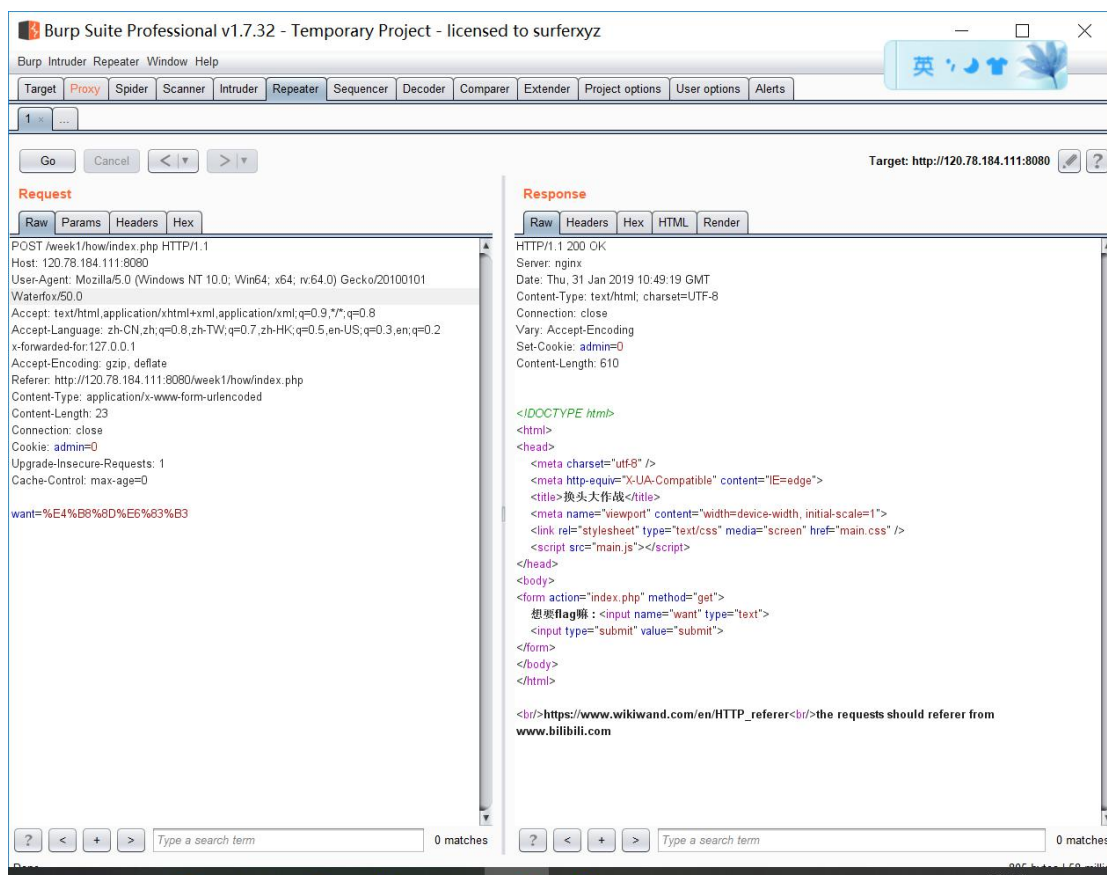
好了，接下来就是 burpsuite 了，抓包并且 ctrl+r



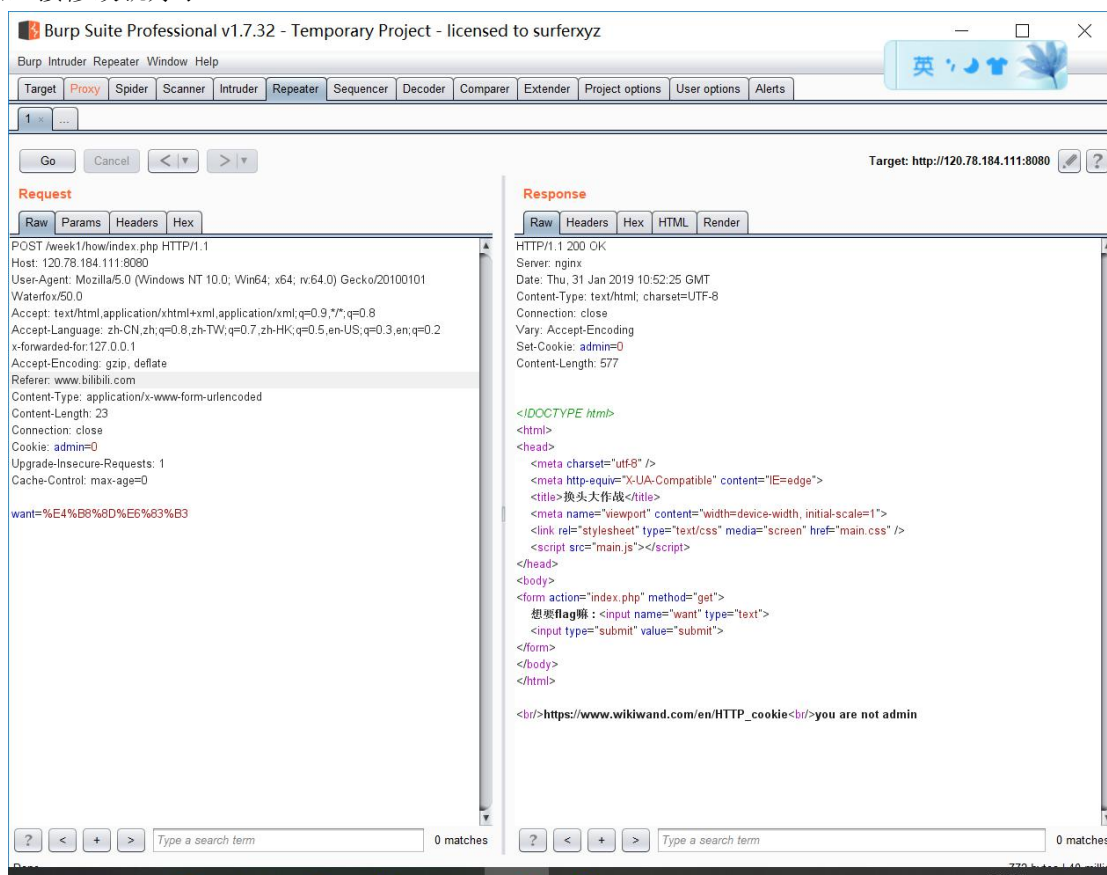
再加入 X-Forwarded-For: 127.0.0.1，冲鸭！GO



Wtf? 水狐，我去百度一下发现居然真有这个浏览器，那么简单，去下载呗，等等，仔细看截图左边第四行，Firefox/64.0，这个似乎就是我的浏览器哦，那么是不是把这个换一下就好了呢，试试先



真的可以了，不过又有了新的条件，应该来自比利比利，再仔细看左边第九行就有 refer，那么直接修改就好了



[illegible]

三.代码审计初♂体验

A screenshot of a web browser window. The address bar shows the URL `120.78.184.111:8080/week1/very_ez/index.php`. Below the address bar is a navigation bar with various icons and text: a star icon, the word "书签" (Bookmarks), a "C" icon, the word "知" (Zhihu), the word "知乎", a "微信" (WeChat) icon, the word "简" (Jian), the word "简书", a "杭电" (Hangzhou Dianzi University) icon, the Google logo, the word "Google", an "邮箱" (Email) icon, the word "邮箱", a "洛谷" (Luogu) icon, the word "洛谷", a "w3" icon, and the word "bilibili". The main content area of the browser displays a PHP script:

```
<?php
error_reporting(0);
include("flag.php");

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

$_GET['id'] = urldecode($_GET['id']);
if($_GET['id'] === "vidar")
{
    echo $flag;
}
highlight_file(__FILE__);
?>
```

大致意思就是要通过 `get` 的方式提交变量 ID 的值，其中如果 `id=vidar` 则发送***



但是，ID 经过 `urldecode` 函数转换，需要等于 “vidar”

我们知道，在浏览器的地址栏进行 `get` 传参时，浏览器会自动进行一次 `UrlDecode()` 的解码，然后才会传给程序使用。

所以，可以想到二次转码，浏览器转码一次，然后 `urldecode` 转码一次，那么我们就可以利用 `%25`，转码之后就是 `%`，那么我们只要找到字母的 `url` 编码就可以成功绕过了。

编码查询网址 http://www.w3school.com.cn/tags/html_ref_urlencode.html

`id=vidar` 可以构造为 `id=v%2569dar`，成功出结果。



```
hgame{urlDecode_Is_GoOd} <?php
error_reporting(0);
include("flag.php");

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

$_GET['id'] = urldecode($_GET['id']);
if($_GET['id'] === "vidar")
{
    echo $flag;
}
highlight_file(__FILE__);
?>
```

到这里，一次性给两个课外拓展题吧

1. 代码审计+换头 <http://www.shiyanbar.com/ctf/32>
2. 代码审计+绕过 <http://123.206.87.240:8002/web7/>

四. Can you find me?

一般我觉得 `web` 题有三部曲，源码抓包扫后台

本题也是一样，直接打开没发现什么特殊的東西，那么就查看源码

the gate has been hidden
can you find it? xixixi

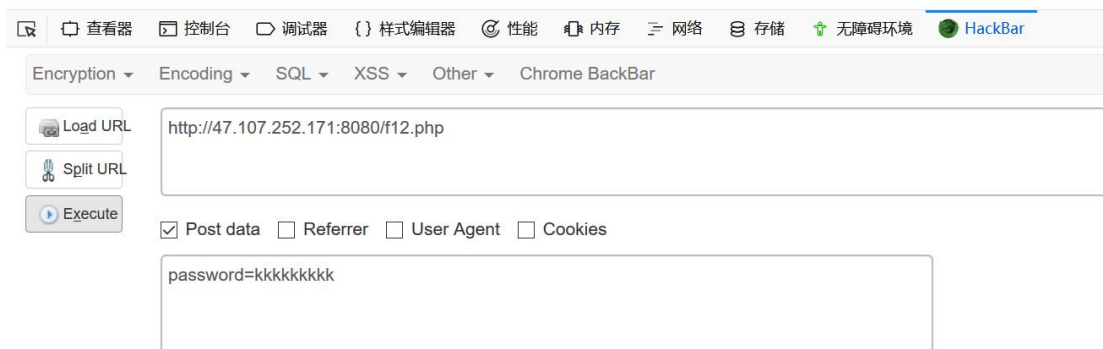
```
47.107.252[1] - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
<!DOCTYPE html>
<html>
<head>
    <title>can u find me? </title>
</head>
<body>
    <p>the gate has been hidden</p>
    <p>can you find it? xixixi</p>
    <a href="f12.php"> </a>
</body>
</html>
```

发现了“f12.php”，打开看看呗

```
<body>
    <p>yeah!you find the gate</p>
    <p>but can you find the password?</p>
    <p>please post password to me! I will open the gate for you!</p>
</body>
```

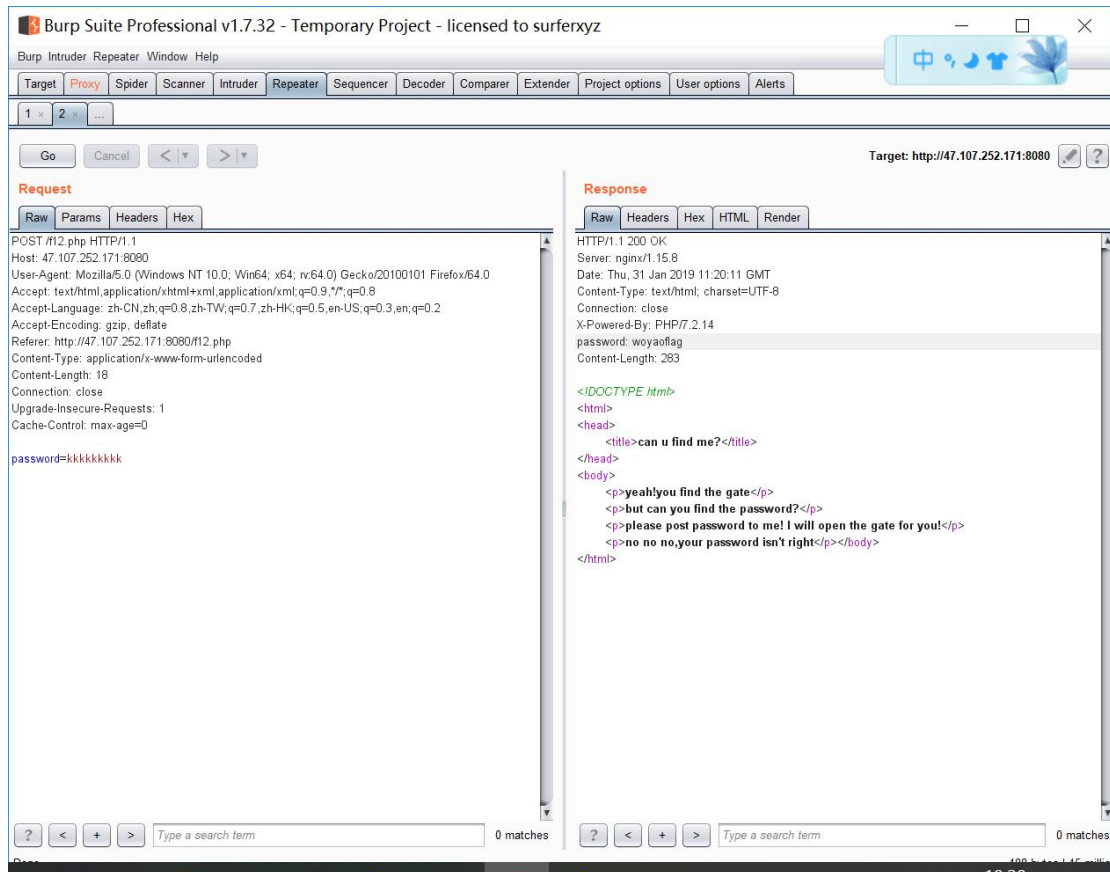
用 post 提交 password 变量是、，先随便提交试试

yeah!you find the gate
but can you find the password?
please post password to me! I will open the gate for you!
no no no,your password isn't right



The screenshot shows the Chrome DevTools Network tab. The selected request is a POST to `http://47.107.252.171:8080/f12.php`. The 'Post data' tab is active, showing a single parameter: `password=kkkkkkkkkk`. The 'Headers' tab shows the 'Content-Type' as `application/x-www-form-urlencoded`. The 'Cookies' tab is empty.

Oh，不正确，难道要抓包暴力破解么，先抓包看看，ctrl+r,然后 go



哈哈，不需要暴力。出现了左边第七行。修改 password=woyaoflag 就可以了。

虽然此题出题学长良心，但是如果没有 password 提示，应该就真的要暴力了，找到了一题用 burpsuite 来暴力破解密码的，有兴趣可以试试。

<http://123.206.87.240:8002/webshell/>

Re

一. Brainfxxker

根据代码逻辑，通过 ptr 来构造两个 for 循环然后根据 ascii 码输出，我改写了一下代码。为了不至于截图太长，做了些缩进。

```

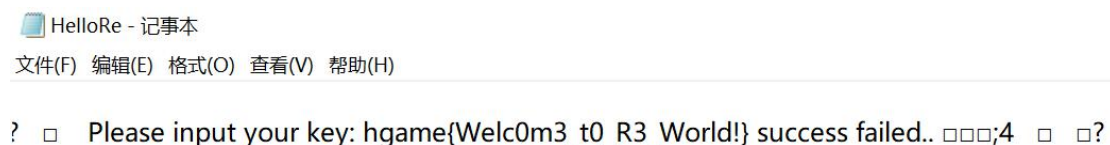
using namespace std;
int main() {
    string a;
    a = ">+++++++[<----->-]<+.[.]";
    int data[100] = { 0 };
    int ptr = 0;
    for (auto i = a.cbegin(); i != a.cend(); ++i) {
        switch (*i) {
            case '>':
                ++ptr; break;
            case '<':
                --ptr; break;
            case '+':
                ++data[ptr]; break;
            case '-':
                --data[ptr]; break;
            case '.':
                cout << data[ptr]; break;
            case '[':
                if (!data[ptr]) { while (*i++ != ']') continue; --i; }
                break;
            case ']':
                if (data[ptr]) { while (*(i - 1) != '[') --i; --i; }
                break;
        }
    }
    system("pause");
}

```

然后因为 uint8_t 是无符号的，[+.] 只为输出，他的+不能算上，所以结果取绝对值后要减一，一个个输入后再对标 ascii 表转换就 ok 了

二. HelloRe

下载文件打开方式记事本



三. Python 教室

enc1 = 'hgame{' enc2 = 'SGVyZV8xc18zYXN5Xw==' enc3 = 'Pyth0n}'
 但是 third = base64.b32decode(third)
 所以查表对照，改一下 enc3 的内容就好了

Misc

这个太简单了 一题是下载 stegsolve
打字机 是根据动漫永恒的紫罗兰

这肯定是 Violet Evergarden。
连蒙带猜出 flag

