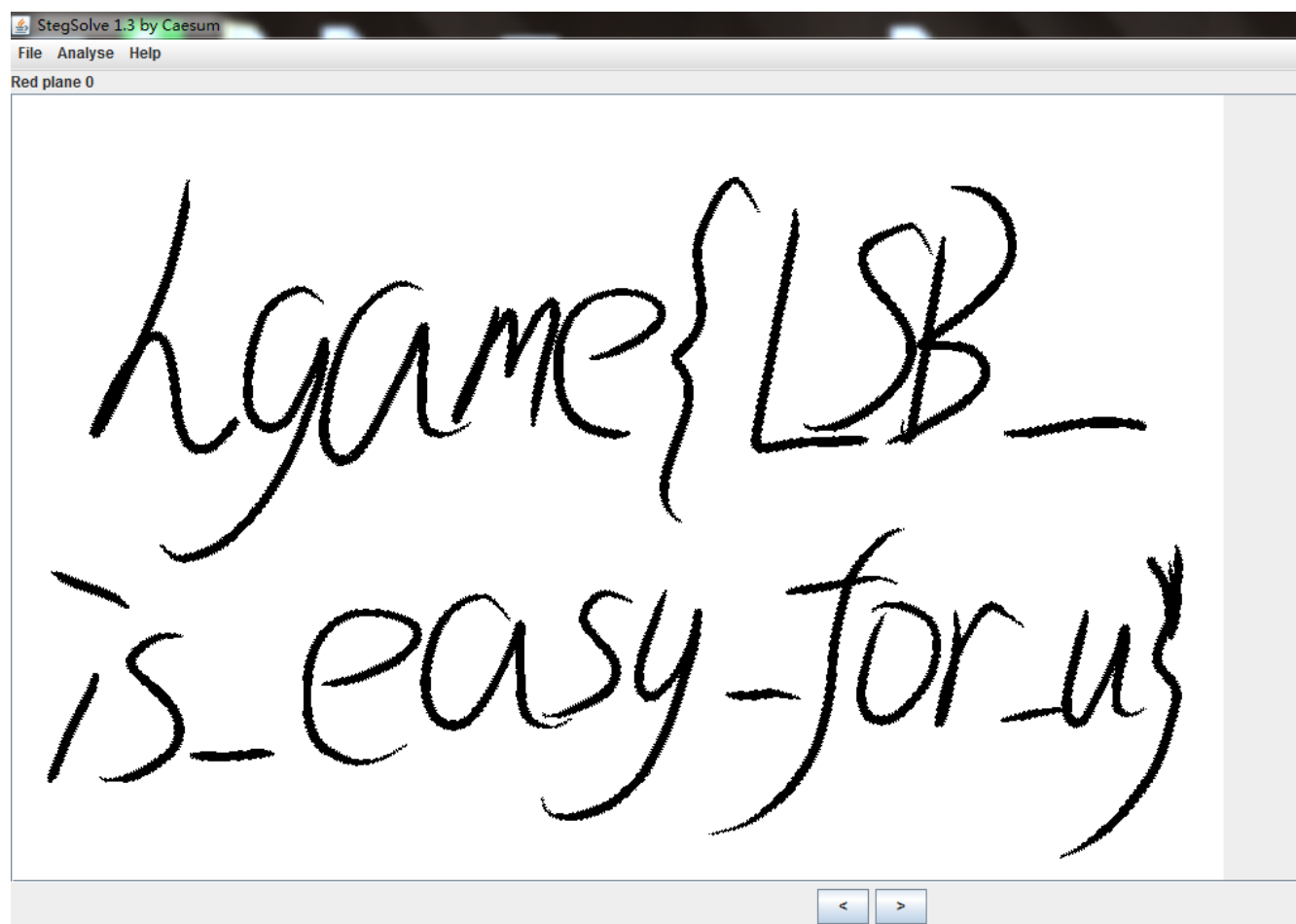


#HGAME Week 1 WriteUp

##MISC

###Hidden Image in LSB

也是根据提示用了stegsolve才做出来的

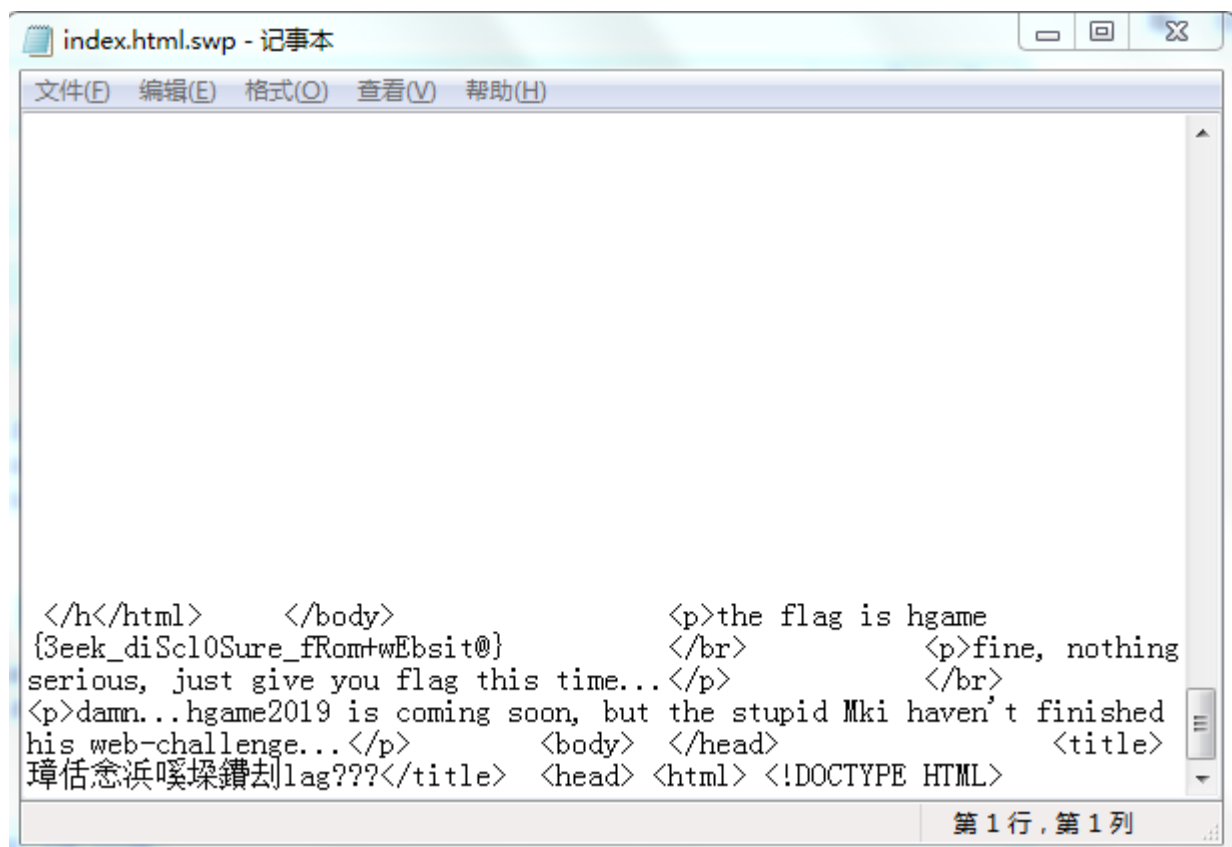


##WEB

###谁吃了我的flag

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submit，则它的临时文件为.submit.swp。如果文件正常退出，则此文件自动删除。

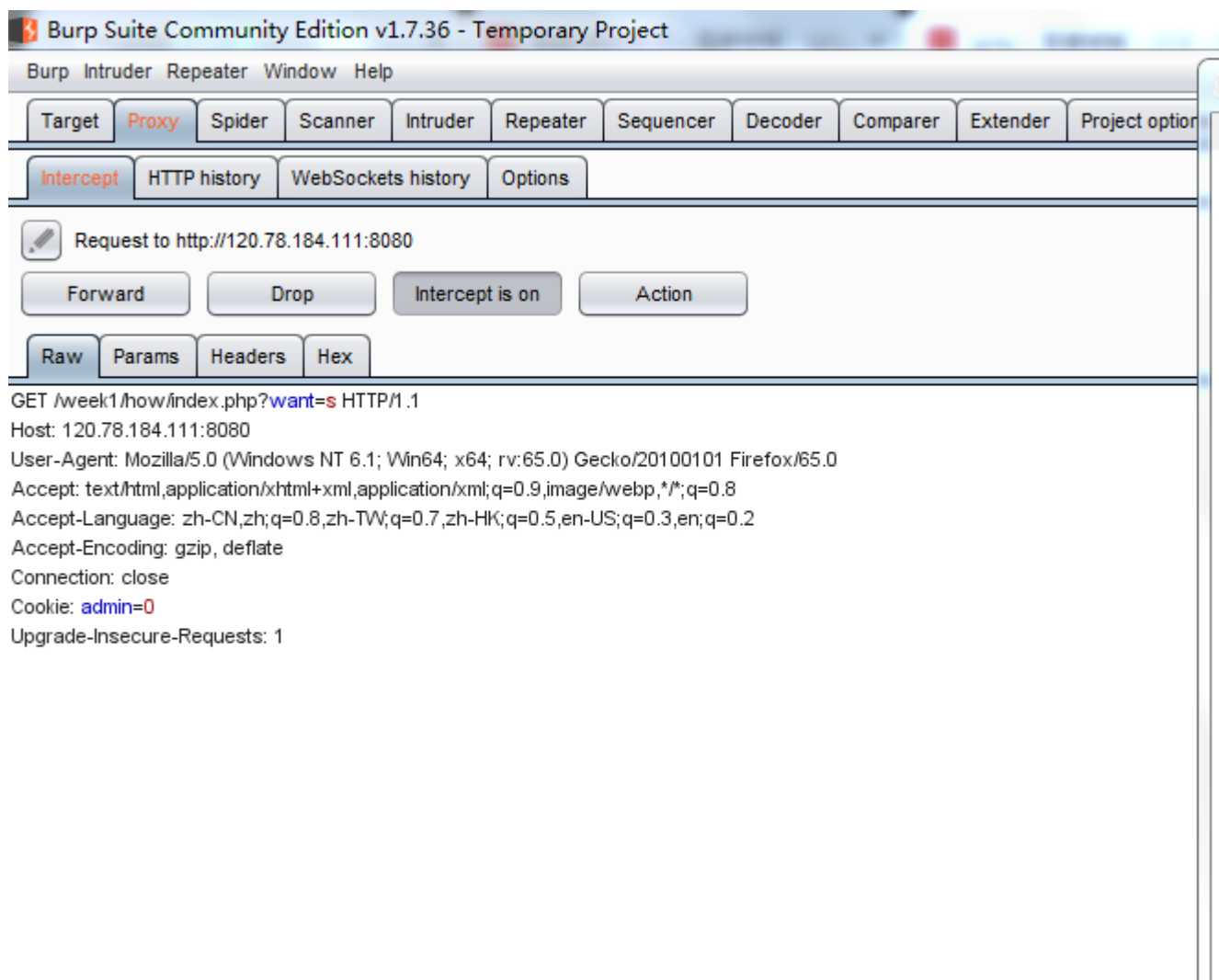
<http://118.25.111.31:10086/index.html.swp>



```
</h</html>      </body>                <p>the flag is hgame
{3eek_diSc10Sure_fRom+WEbsit@}          </br>          <p>fine, nothing
serious, just give you flag this time...</p>          </br>
<p>damn...hgame2019 is coming soon, but the stupid Mki haven't finished
his web-challenge...</p>          <body> </head>          <title>
璋估念浜悝操鏼去lag???
```

###换头大作战

用了burps



uite

右键--选择change request method

根据提示一步一步的改就行，第一次改：X-Forwarded-For:127.0.0.1 第二次：Waterfox/50.0 第三次：referer:www.bilibili.com 第四次：Cookie: admin=1

###very easy web

根据提示百度了相关内容

首先：

if (eregi ("hackerDJ" , \$ _ GET [id])) 不能让他匹配成功

其次

$G_{ET}[id] = urldecode(_GET[id]) ;$

if (\$ _ GET [id] == "hackerDJ")

进行了urldecode解码，解码后为hackerDJ

\$ get进行传参的时候一般都进行了一次解码，下面又进行了一次解码。本题目也提示了

为二次解码

所以我们将hackerDJ中的一个字母进行二次编码即可

用J吧

j=%4a

%=%25

hackerD%254a

有效载荷如下：

第三题：urldecode二次编码绕过 焦点： $G_{ET}[id] = urldecode(_GET[id])$

```
1 | <?php if(ereg("hackerDJ",$_GET[id])) { echo(" not allowed! "); exit(); } $_GET[id] = urldecode($_GET[id])
```

代码一开始使用ereg判断

if(ereg("hackerDJ" ,\$_GET[id])) {

echo("

not allowed!

如果，传入的id的值为hackerDJ，则返回not allowed

下边使用urldecode对id的值进行解码，所以可以让id得到的值是hackerDJ的url编码，由于浏览器会自行解码一次，所以编码两次就好，因为要对hackerDJ编码，但是hackerDJ不是规则的，我们需要对着ascii码表编码两次。其实没有必要将hackerDJ全部进行二次编码，在这里我们仅对D进行编码，查ascii码表：D对应的ascii码为44，然后再找一个在线URL编码网站，%44 URL编码后为 %2544

参考：?id=hacker%2544J

将r对照ASCII表进行了二次编码

```
HGAME 2019 x 120.78.184.111:8080/week1/ve x +
< > ↻ ⬆ ⓘ 不安全 | 120.78.184.111:8080/week1/very_ez/index.php?id=vida%2572

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

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

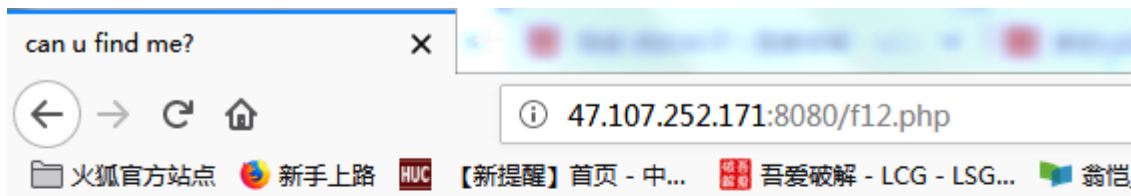
$_GET['id'] = urldecode($_GET['id']);
if($_GET['id'] === "vidar")
{
    echo $flag;
}
highlight_file(__FILE__);
?>
```

###can you find me?

[查看源代码](#)

```
1 <!DOCTYPE html>
2 <html>
3 <head>
4     <title>can u find me?</title>
5 </head>
6 <body>
7     <p>the gate has been hidden</p>
8     <p>can you find it? xixixi</p>
9     <a href="f12.php"></a>
10 </body>
11 </html>
12
```

进行访问

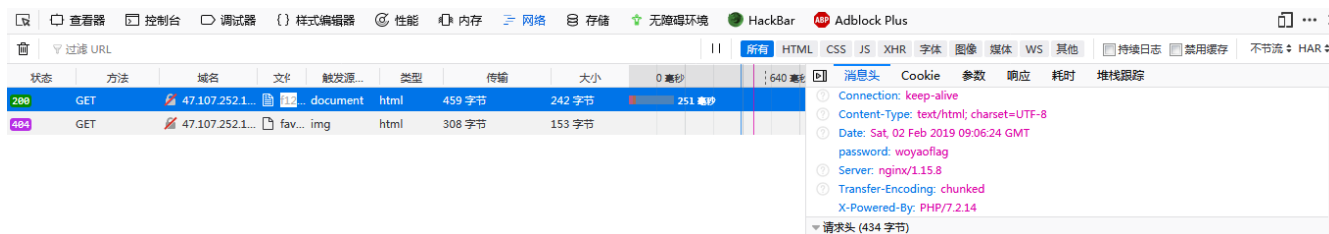


yeah!you find the gate

but can you find the password?

please post password to me! I will open the gate for you!

找到password



用hackbar

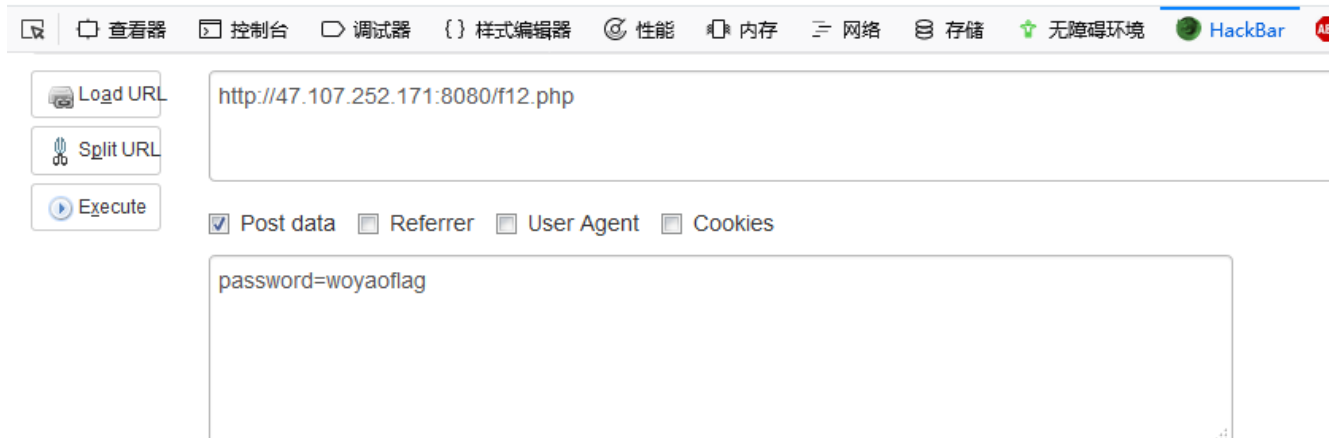
yeah!you find the gate

but can you find the password?

please post password to me! I will open the gate for you!

right! .

[click me to get flag](#)

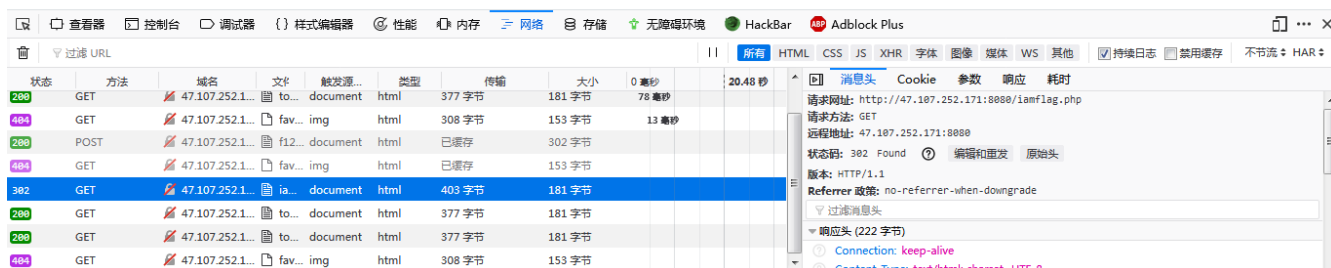




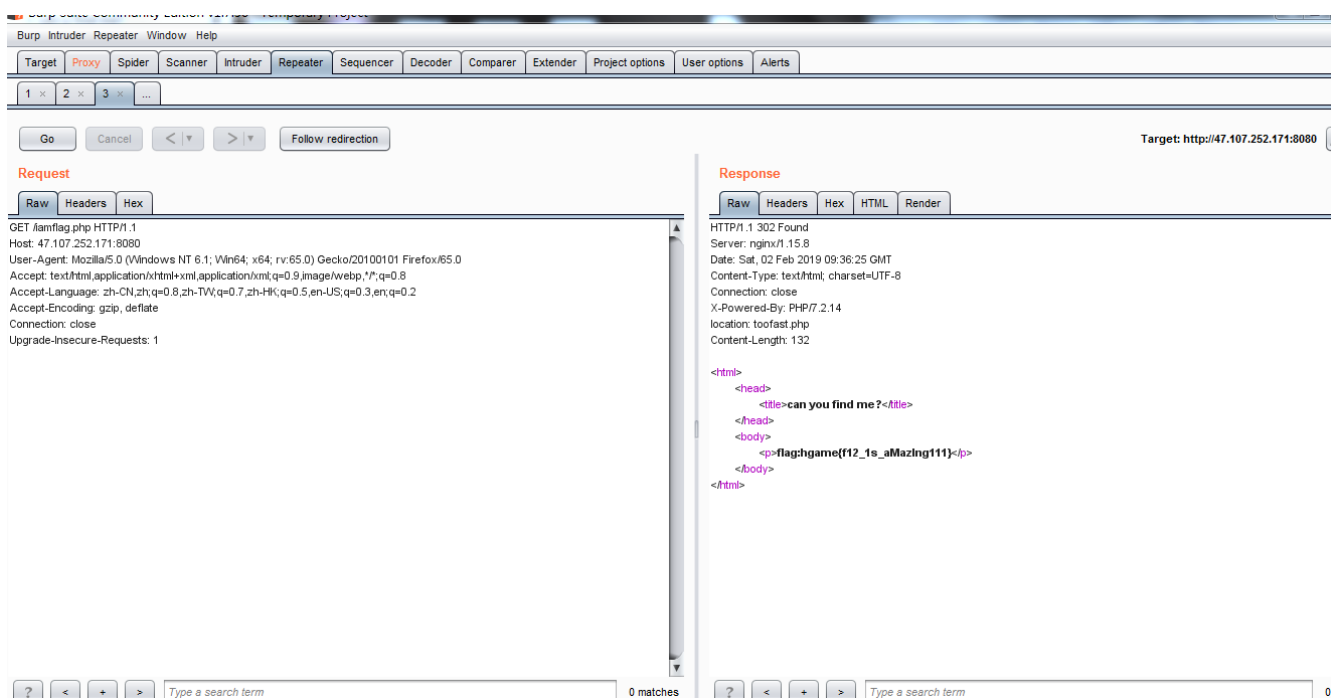
aoh,your speed is sososo fast,the flag must have been left in somewhere

然后根据学长提示，找到304页面

aoh,your speed is sososo fast,the flag must have been left in somewhere



然后用burpsuite对其抓包



找到。