学习周记（三）

原创

極品一═☆宏 于 2019-01-13 10:23:55 发布 1046 收藏

分类专栏： CTF_web

本文链接：https://blog.csdn.net/qq_43214809/article/details/85860619

CTF_Web 周练习（一）

练习还是本着提高自己的目的吧，毕竟时间不等人。在考试周抽了一些时间，进行个人的CTF_Web练习，算上之前的GXNNCTF和圣诞欢乐赛，这也是第三次了。题目虽然不多，但对于我自己一个新手而言，也算是一种提高了。写完这一次，就该去复习了。

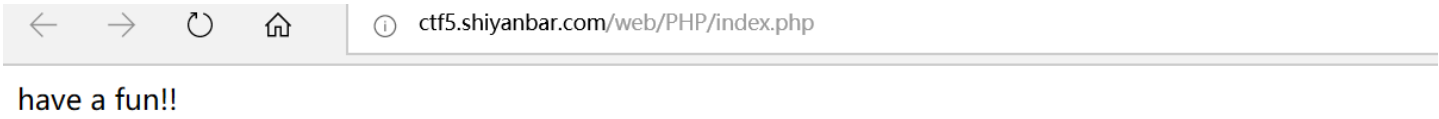
时间:2019年1月6日至2019年1月13日

一、实验吧有关PHP的练习：

1.绕过：

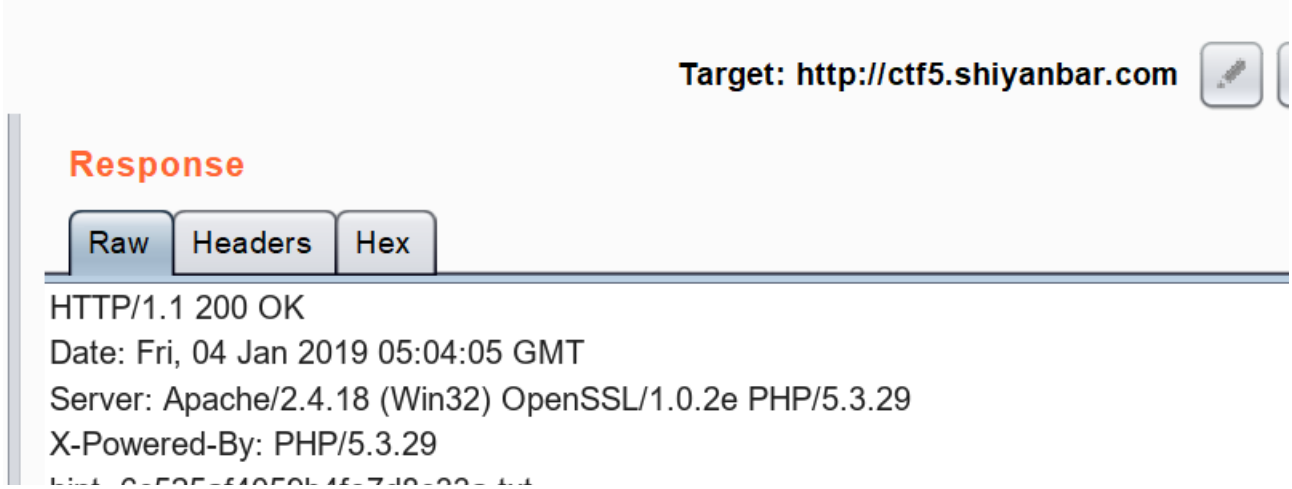
题目链接:http://ctf5.shiyanbar.com/web/PHP/index.php

打开网址，只发现了这个：

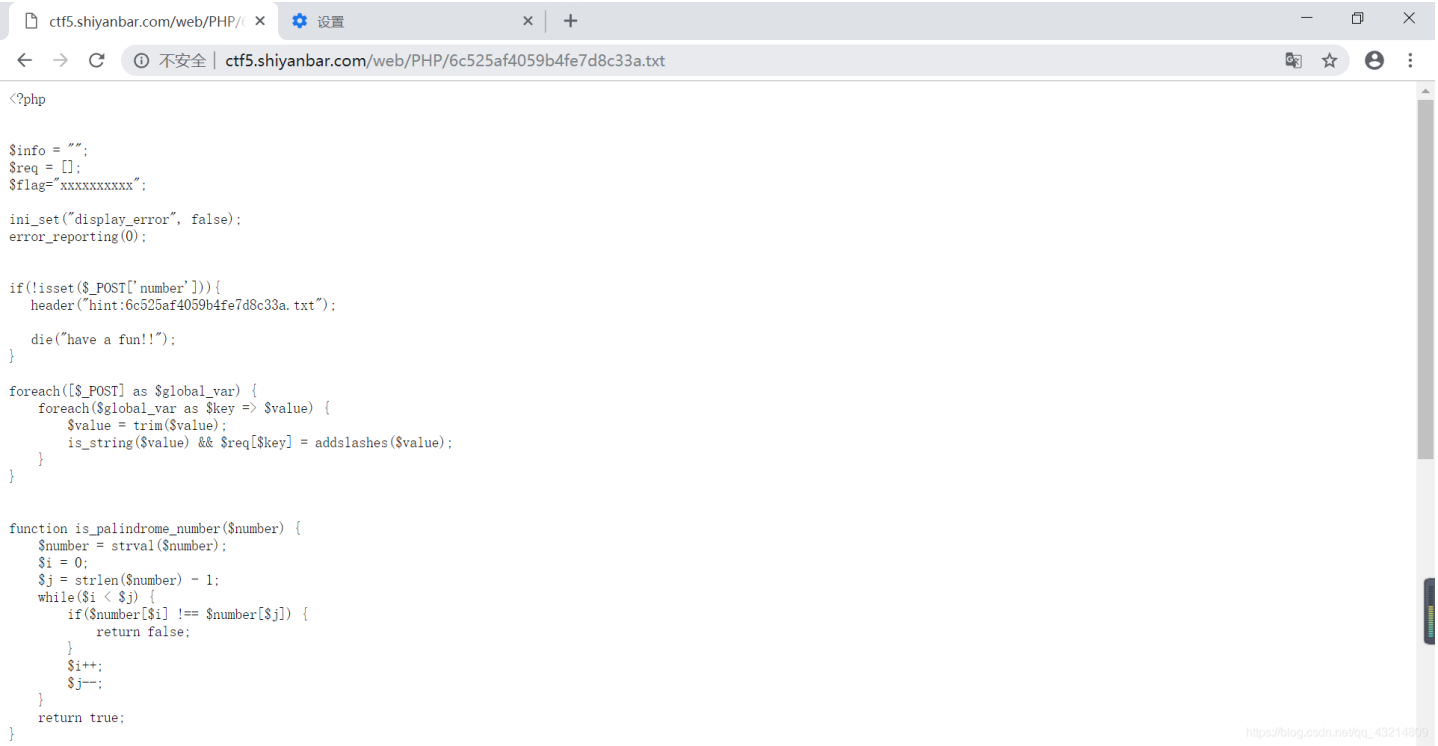


have a fun!!

在现有的页面上好像没发现什么有用的东西，那么打开burpsuite抓包看一下，出现了一个hint：



貌似是个txt文件，将hint放到浏览器里打开，一个我们想要的php代码就出现了：




```php
<?php


$info = "";
$req = [];
$flag="xxxxxxxxxx";

ini_set("display_error", false);
error_reporting(0);


if(!isset($_POST['number'])){
   header("hint:6c525af4059b4fe7d8c33a.txt");

   die("have a fun!!");
}

foreach([$_POST] as $global_var) {
    foreach($global_var as $key => $value) {
        $value = trim($value);
        is_string($value) && $req[$key] = addslashes($value);
    }
}


function is_palindrome_number($number) {
    $number = strval($number);
    $i = 0;
    $j = strlen($number) - 1;
    while($i < $j) {
        if($number[$i] !== $number[$j]) {
            return false;
        }
        $i++;
        $j--;
    }
    return true;
}
```

```php
if(is_numeric($_REQUEST['number'])){
    $info="sorry, you cann't input a number!";
}elseif($req['number']!=strval(intval($req['number']))){
     $info = "number must be equal to it's integer!! ";

}else{

     $value1 = intval($req["number"]);
     $value2 = intval(strrev($req["number"]));
     if($value1!=$value2){
          $info="no, this is not a palindrome number!";
     }else{

          if(is_palindrome_number($req["number"])){
              $info = "nice! {$value1} is a palindrome number!";
```

```
        }else{
            $info=$flag;
        }
    }
}

echo $info;
```


下面进行我们熟悉的代码审计工作。从foreach开始分析，foreach在这里的作用是数组遍历和读值，键为key，值为value；之后对value进行trim移除操作，接下来如果value是字符串，会存入req，并用addslashes函数对预定义字符加''处理。

下一个是定义回文串判断函数，紧接着进入至关重要的if条件句。首先是is_numeric判断函数，如果REQUEST['number']是数字或数字字符串，返回true,显然true不是我们想要的。当返回false后，进入下层if判断，继续往下走的条件是'req['number']=strval(intval(req['number'])'。

上网查询得知：intval函数的作用是获取变量的整数值，数字即返回数值，非数字返回0，对于字符串，返回字符串中第一个不是数字的字符之前的数字串所代表的整数值；strval函数的作用是获取变量的字符串值。再往下看，对value2的操作中出现了strrev,即字符串反转。当value1=value2时，进入最后的条件，即req['number']是非回文串，info获得flag，然后输出。

总结一下，出flag的条件是：

1.必须有POST['number']；

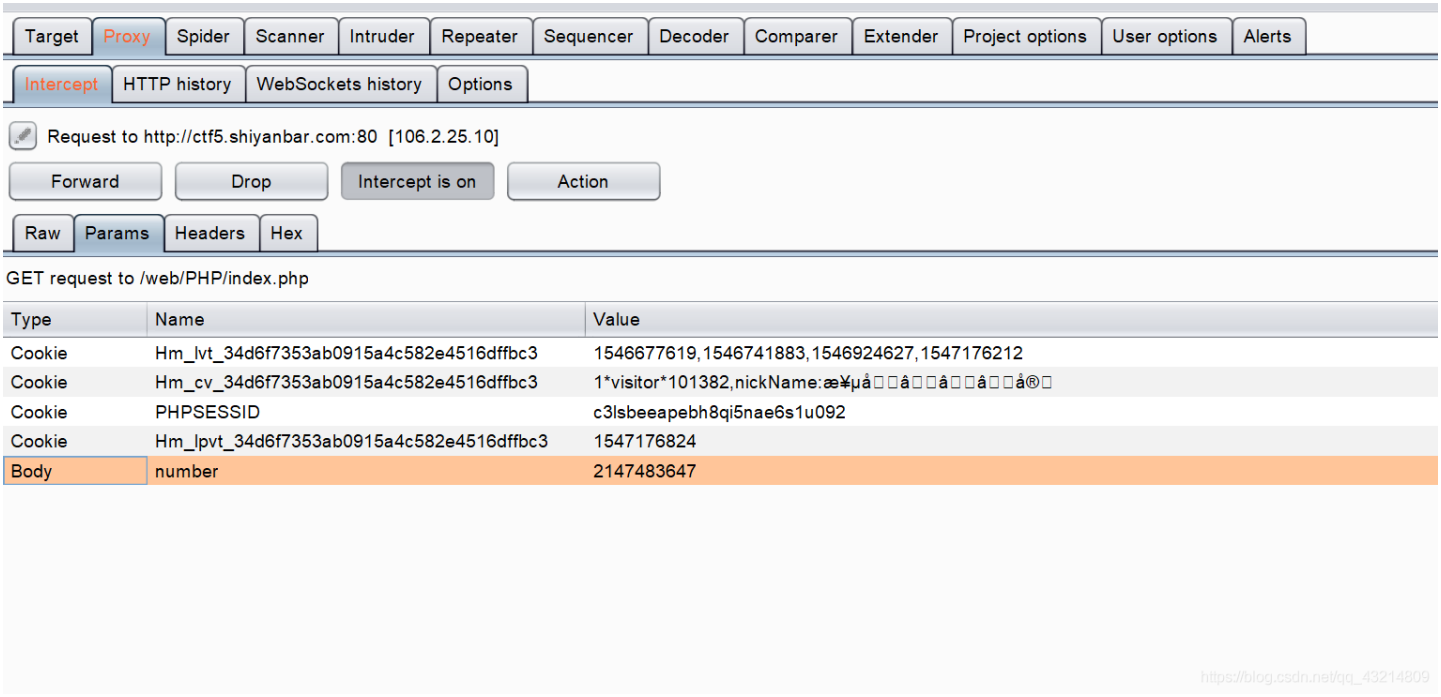
2.'number'的值必须为字符串;存入req的值要和req经过两次转换得到的值相同；

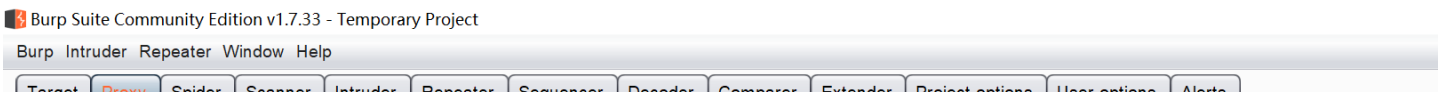
3.'number'的原字符串和反转后的相同，但是'number'不能为回文串。

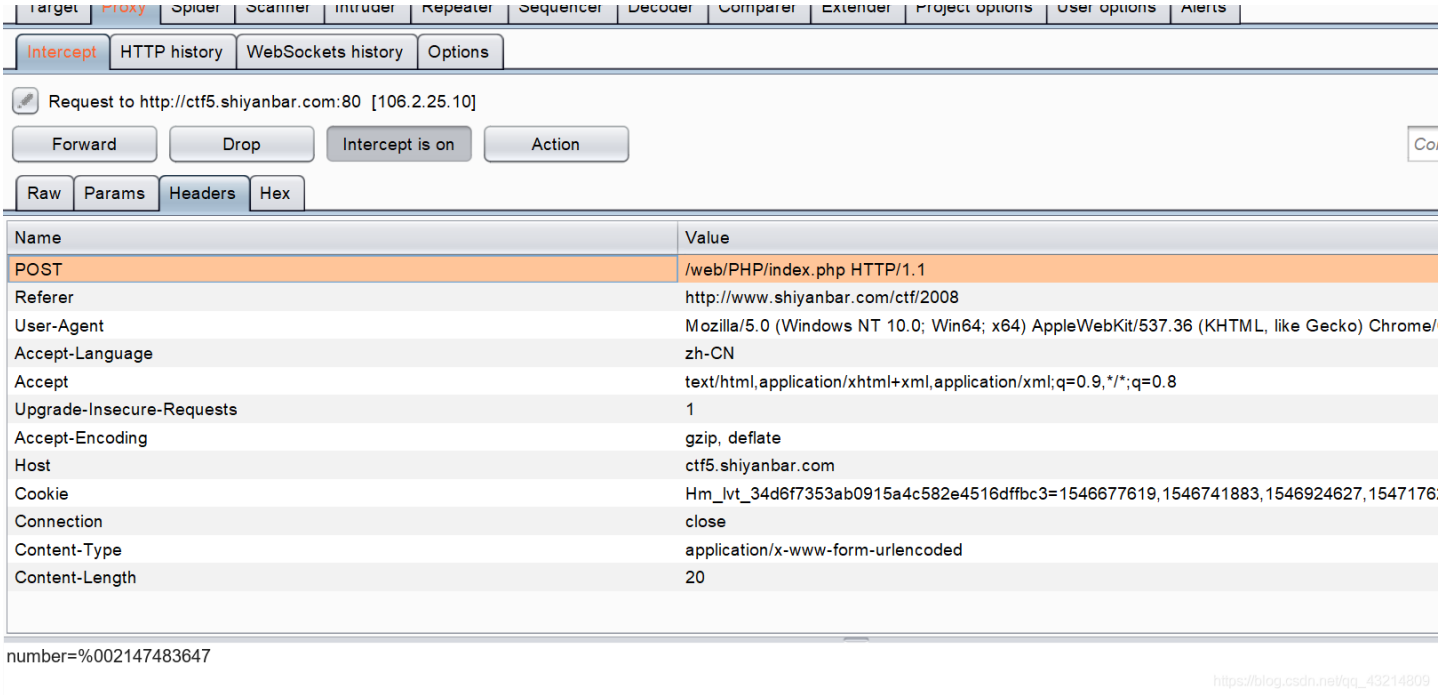
这样一看，似乎条件之间存在矛盾，因为当经过intval和strval后，得到的值一定与原值不同，不是回文串却在反转后要和原串相同。

这样一来，我们只能利用其他条件来构造。结合之前GXNNCTF里面的ereg()函数00截断绕过的经历，想到能否在这段代码里也找到可以用00绕过的方法。

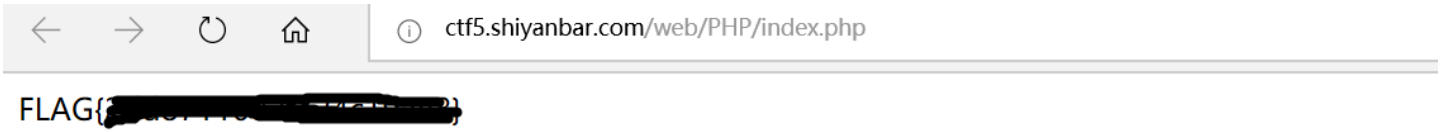
上网查询了一下，对于intval函数，转换的最大值取决于操作系统。 32 位系统最大带符号的 integer 范围是 -2147483648 到 2147483647，64 位系统上，最大带符号的 integer 值是 9223372036854775807。当超过最大值时，intval的值取2147483647，我们可以取2147483647，反转后就是7463847412，这样一来，取intval后仍未原值，而且还不是回文串，第三个条件解决。至于第二个，trim函数会过滤空格以及 \n\r\t\v\0，但不会过滤\f，is_numeric会过滤 \f，但不会过滤 \0 。那么利用trim和is_numeric可以实现绕过，在我们构造的number前面加上一个%00，即%002147483647。通过更改POST请求头，添加Body即可：







点击'Intercept is on'，即可看到Flag：



FLAG{[redacted]}

2.编码：

题目链接：http://ctf5.shiyanbar.com/DUTCTF/index.php

打开网址，出现下图：

Notice: Use of undefined constant id - assumed 'id' in **C:\h43a1W3\phpstudy\WWW\DUTCTF\index.php** on line **2**

Notice: Undefined index: id in **C:\h43a1W3\phpstudy\WWW\DUTCTF\index.php** on line **2**

Deprecated: Function eregi() is deprecated in **C:\h43a1W3\phpstudy\WWW\DUTCTF\index.php** on line **2**

Notice: Use of undefined constant id - assumed 'id' in **C:\h43a1W3\phpstudy\WWW\DUTCTF\index.php** on line **7**

Notice: Use of undefined constant id - assumed 'id' in **C:\h43a1W3\phpstudy\WWW\DUTCTF\index.php** on line **7**

Notice: Undefined index: id in **C:\h43a1W3\phpstudy\WWW\DUTCTF\index.php** on line **7**

Notice: Use of undefined constant id - assumed 'id' in **C:\h43a1W3\phpstudy\WWW\DUTCTF\index.php** on line **8**

Can you authenticate to this website? index.php.txt

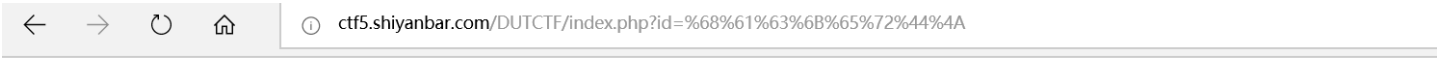
发现最后一句话里有.txt，试着打开一下，出现了我们想要的代码：


```
<?php
if(eregi("hackerDJ",$_GET[id])) {
  echo("<p>not allowed!</p>");
  exit();
}

$_GET[id] = urldecode($_GET[id]);
if($_GET[id] == "hackerDJ")
{
  echo "<p>Access granted!</p>";
  echo "<p>flag: **********} </p>";
}
?>


<br><br>
Can you authenticate to this website?
```


这段代码还是比较短的，而且很容易就可以找到得到flag的条件，对'hackerDJ'进行URL编码，得到%68%61%63%6B%65%72%44%4A，输入后得到下面的界面：

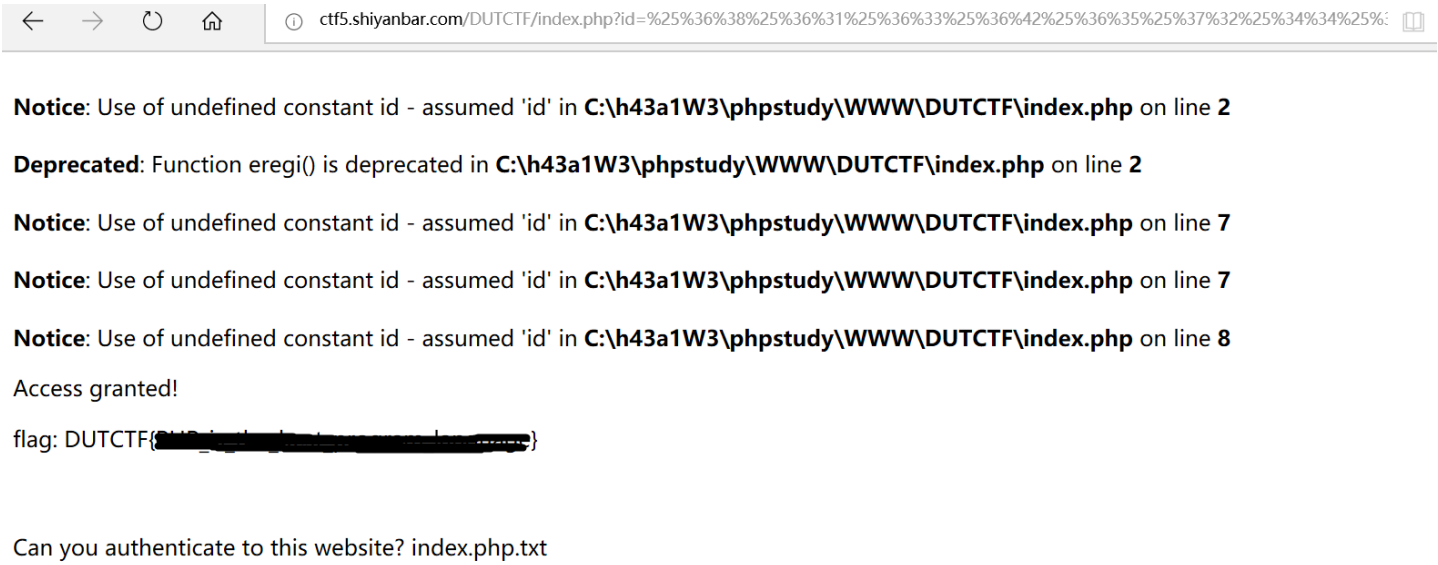


Notice: Use of undefined constant id - assumed 'id' in **C:\h43a1W3\phpstudy\WWW\DUTCTF\index.php** on line **2**

Deprecated: Function eregi() is deprecated in **C:\h43a1W3\phpstudy\WWW\DUTCTF\index.php** on line **2**

not allowed!

好像不可以，再编码一次试试，得到%25%36%38%25%36%31%25%36%33%25%36%42%25%36%35%25%37%32%25%34%34%25%34%41，这次就可以了：



3.两篇有用的文章：

PHP函数漏洞总结：https://blog.csdn.net/qq_31481187/article/details/60968595

CTF中的PHP知识：https://www.restran.net/2016/09/26/php-security-notes/

二、攻防世界WEB新手练习：

由于我个人能力有限，知识储备量不多，再加上个人时间的限制，我只做了前6道题，做完后发现这也确实蛮简单的，重点就是知识储备的够不够。

我谈谈自己通过做题学到的东西吧，可能比较片面，毕竟都是基于题目的。

1.查看开发人员工具算是解题的一个最基本的方法吧，我个人感觉做题的话先看一眼不是什么浪费时间的事，有可能里面会有相关的提示。

2.关于GET和POST的传参方式。GET的话，有许多方法，一些博主总结了有4、5条吧，最直接的应该是直接在url里构造变量及赋值；至于POST,就像上面那部分第一题绕过，我们可以抓包，在Params里添加Body，然后输入变量名和值，最后再改一下头，是GET的话就改成POST。

3.备份文件：在圣诞欢乐赛中Web的第二题是.swp文件的恢复，当时上网查询了一些关于.swp文件的知识，关于vim编辑的。这次的话，也算是了解到其他备份文件，比如说.git/ .svn/ .swp /.svn/ .~/ .bak/ .bash_history/

4.有关robots协议，题目涉及的内容还是比较简单的，直接在网址后面加个内容就行了。但是这一部分内容还是比较重要的，有关robots协议的详解还是有不少的，有必要抽出时间看一看。

三、练习的体会：

首先，讲实话，我到现在对Web相关知识的了解还不是很多，知识盲区真的太多了，就算是PHP代码这一类的题目，看懂是一方面，怎么分析出Flag则是另一方面。我在做题的时候不会去查看别人写的writeup，宁可一道题做好几天，也不会去查看。自己做出来的总归要比别人告诉的好一些，收获的要更多一些。解题完成后可以去看一下别人的wp，看一下别人的思路是怎样的，能不能从别人的解题方法中找到不一样的思路。

其次，这三次练习，包括连续写三次周记都是抽时间完成的，真的是用一些期末复习的时间，要不是自己成绩还好不用担心挂科，我这段时间也不会来搞这些东西，哪怕这是专业学习内容。好在马上考试结束，寒假来了就可以每天把精力放在这上面了，回想起这段时间也确实挺累的，下一篇周总结就要到考试结束后再写了，这段时间应该不会再去练习了，毕竟该好好复习了。

最后，再次感谢一些博主们的经验总结与分享，真的受益匪浅。