/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

/\* 程序作者：爱的伊苏 \*/

/\* 程序完成时间：2019/1/4 \*/

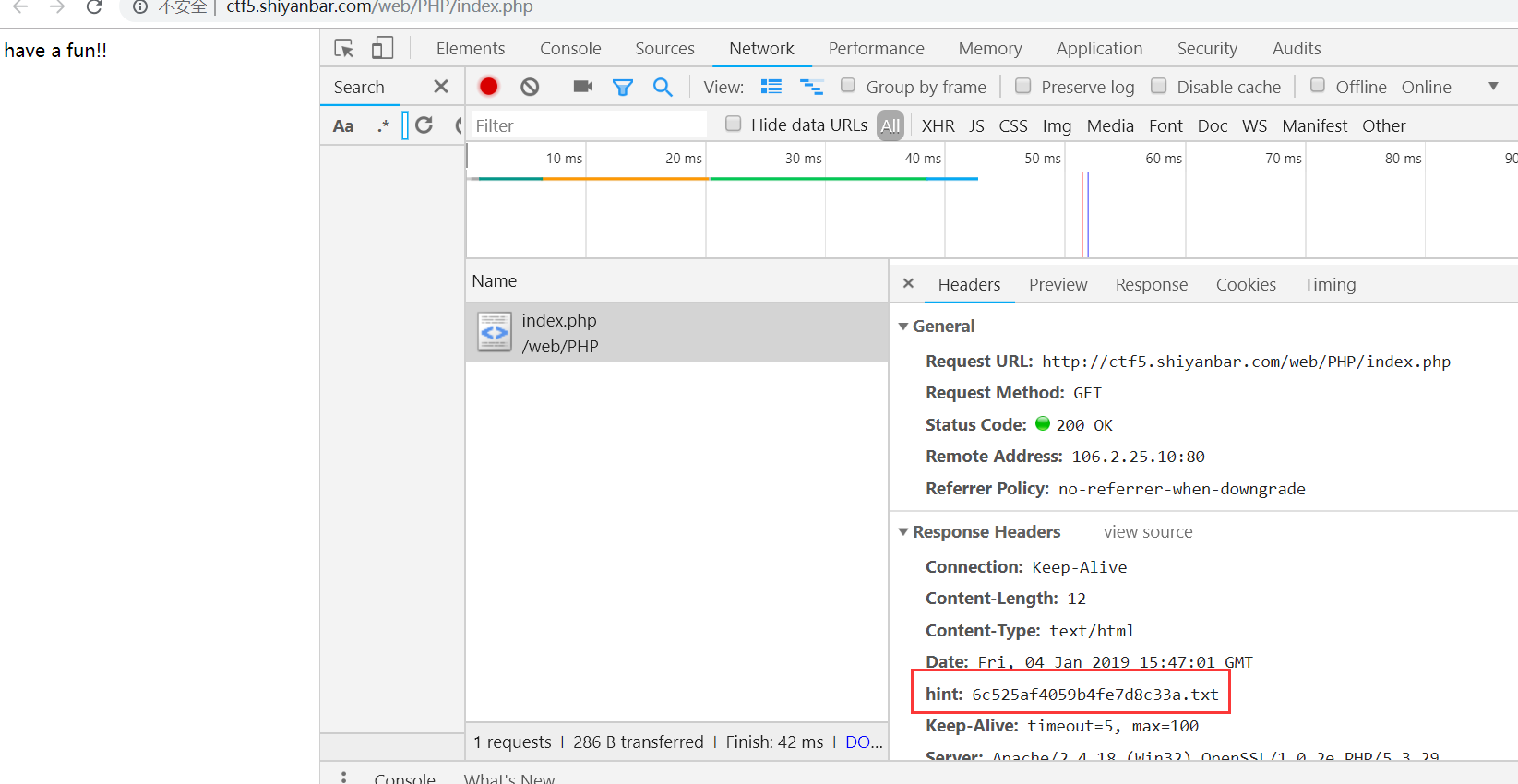
/\* 有任何问题请联系：740531307@qq.com \*/

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

//@永远得意的笑下去

实验吧题目，进去以后看见have a fun！！

直接利用谷歌浏览器开发者模式查看数据包



如图所示

打开对应txt文件以后发现是代码审计。



<?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!!");

} ------------------------------监测点1 输入必须为number

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;

}

if(is\_numeric($\_REQUEST['number'])){-----------监测点2 不能为纯数字

$info="sorry, you cann't input a number!";

}elseif($req['number']!=strval(intval($req['number']))){

----------监测点3对number取整再转化为字符串后要和原提交的字符串相等

$info = "number must be equal to it's integer!! ";

}else{

$value1 = intval($req["number"]);

$value2 = intval(strrev($req["number"]));

if($value1!=$value2){------------监测点4 顺序等于逆序

$info="no, this is not a palindrome number!";

}else{

-----------------监测点5 不是回文数

if(is\_palindrome\_number($req["number"])){

$info = "nice! {$value1} is a palindrome number!";

}else{

$info=$flag;

}

}

}

echo $info;

对上述代码进行代码审计。

有五个监测点

Intval（）最大数值取决于操作系统。

32位 ： -2147483648 到 2147483647

64位-9223372036854775808~9223372036854775807

加上空格%00 （%00可以放在数字前后，%20只能放在后面；这里的%00或者是%20可以将数字解释为字符串）

##### 以便构造 payload （payload 字面意思 **“有效载荷，有效负荷，有效载重”**。）

##### intval(999999999999)=2147483647

##### 以下等式成立：intval(2147483647)=intval(7463847412)=2147483647，而7463847412便是2147483647的逆序文本，而且2147483647不是回文数。

##### 

##### 通过火狐浏览器自带插件HackBar进行发包得到最终结果