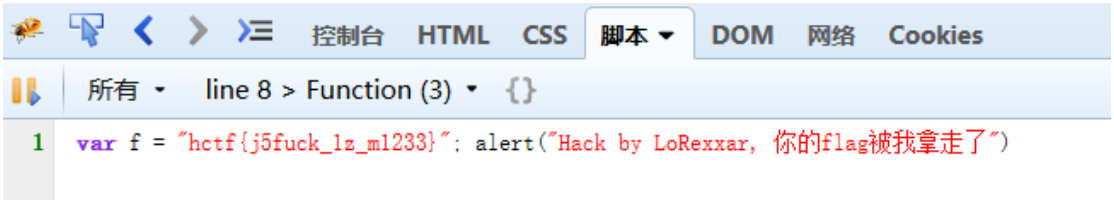
WEB

这 TM 是啥

进入页面首先弹出来一个窗口，打开 firebug 发现了很神奇的东西

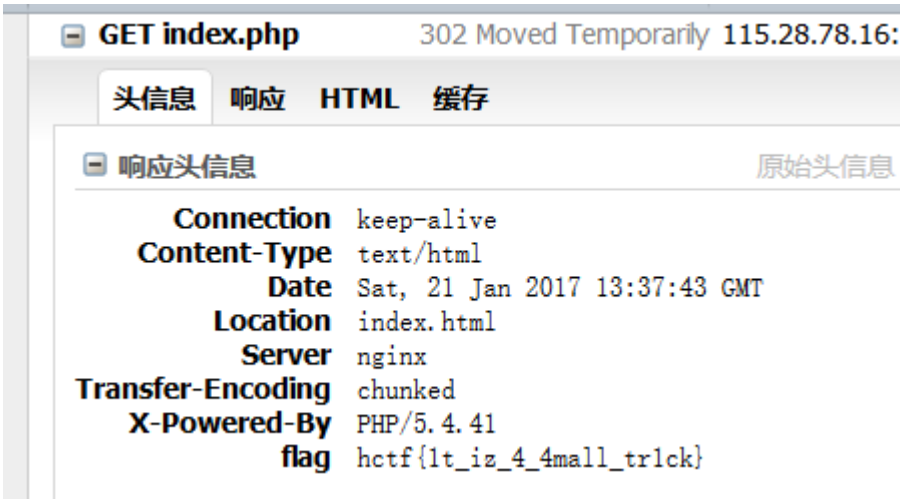
```
<script>
1
2        [][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![
3
</script>
```

之前听说过 JS 这个神奇的功能，所以想到弹出来的窗口和 Flag 都在 JS 代码里



查看脚本，发现 flag

我是谁我在哪？？？



Flag 直接就在响应头文件里。。。

神奇的数字

先看了一下 php 代码，要 POST number，number 的值符合要求，就能得到 flag，
主要符合
开头不能是 + 和 -
intval($req[“number”])= intval(strrev($req[“number”])) 是回文数字
is_palindrome_number($req["number"])为 false 不是回文数字

实际上在得出矛盾的结论之前我试了一些数字，输入 1，121，11111 这些，就会返回

```
"nice! {$n1} is a palindrome number!";
```

而随便输一些数字会返回

```
"no, this is not a palindrome number!";
```

所以发现两个条件矛盾，但当我输入一个很大的数字的时候，却返回

```
"number must be integer!";
```

发现当输入一个很大的数字的时候

```
($req["number"] != intval($req["number"]
```

所以感觉问题在 intval 这个函数这里，然后写了两行 php 测试了一下，当输入很大的数的时候返回的是 2147483647，于是想到 number=02147483647 时，倒叙 74638474120 超出 intval 的限制，便返回 2147483647，但是并没有得到 flag，百度后知道这个数字是 32 位的最大数字，试了一下 64 位的 number = 09223372036854775807,发现了这个奇怪的 dongxi。

不可能拿到的 flag

题目要求 user！=password，但是 sha1 加密后 user=password
一开始智障居然试各种符号- -，然后想到 sha1（）函数本身的问题，百度搜了 php sha1() 发现了这个 http://blog.csdn.net/zhaohansk/article/details/44153141 博客。。。。。。

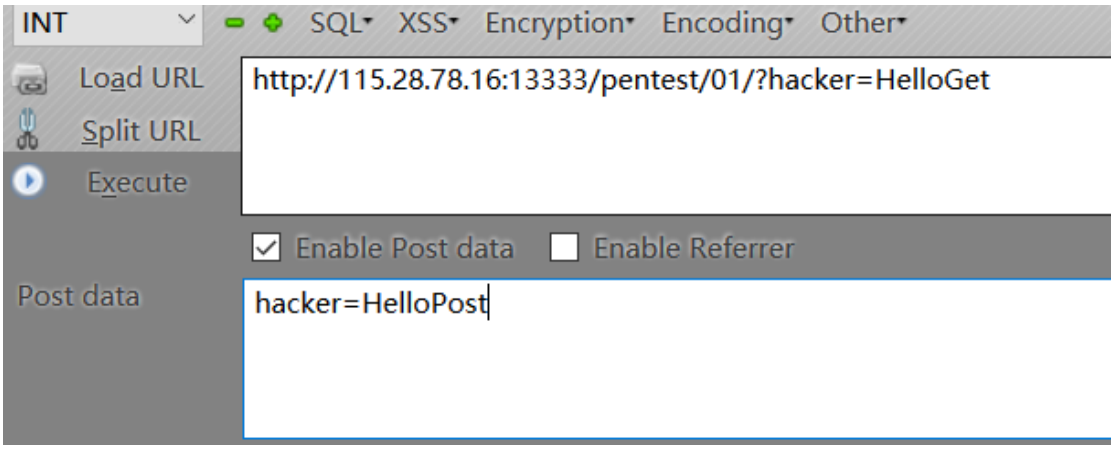
php 真可怕我要回农村

审查 php 代码发现要发送 b 为第 11 位为 0 的字符串并且（+'0.1'）*10 = 8,
于是发送 b="0.70000000000"并不行，PHP 代码下断点发现问题在($b+$a)*10=1
然后毫无理由地试了下 b=0.77"0.7000000000000"，得到 flag

PENTEST

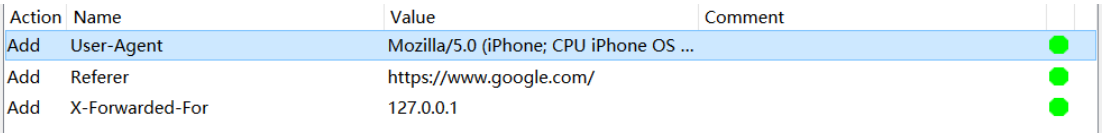
lightless 的渗透教室入门篇（一）

根据要求用 hackbar 同时发送 get 和 post 请求便得到 flag



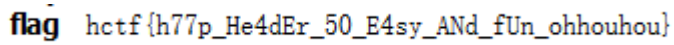
lightless 的渗透教室入门篇（二）

用火狐的一个扩展工具 Modifyheaders 伪造 http 请求报文头

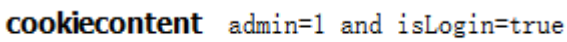


Action	Name	Value	Comment
Add	User-Agent	Mozilla/5.0 (iPhone; CPU iPhone OS ...	
Add	Referer	https://www.google.com/	
Add	X-Forwarded-For	127.0.0.1	

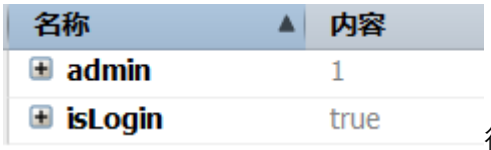
其中找到 ios7 的 ua，对应位置改为 99：
Mozilla/5.0 (iPhone; CPU iPhone OS 99_0 like Mac OS X) AppleWebKit/537.51.1 (KHTML, like Gecko) Version/99.0 Mobile/11A465 Safari/9537.53

最后 flag 在响应头里 

lightless 的渗透教室入门篇（三）



根据提示

伪造 Cookie 

名称	内容
admin	1
isLogin	true

得到 flag

Misc

Explorer 的图库之一

用 winhex 打开文件，直接看到 flag

CRYPTO

密码学教室入门（二）

根据凯撒密码和 flag 开头为 hgame 可以找到字母对应关系，数字略有不同但也轻松猜出