Web


1. Are you from Europe?

头铁的可以直接抽出来 hhh，我抽了 8 分钟出了两次

正确方法：群里学长早说了，没有后端，那就直接 f12 或者 ctrl+u，拉到最下面有个函数

直接看看不出来，随便找一个代码美化的网站扔进去


Ok。

2. special number

没写出来，正则是看懂 key 长度大于 7 包含数字字母

然后是弱类型里的 0==string，所以让 json_decode 出来的结果是 0

3 can u find me

没写出来，过 8 点后学长给了个 hint: robots.txt

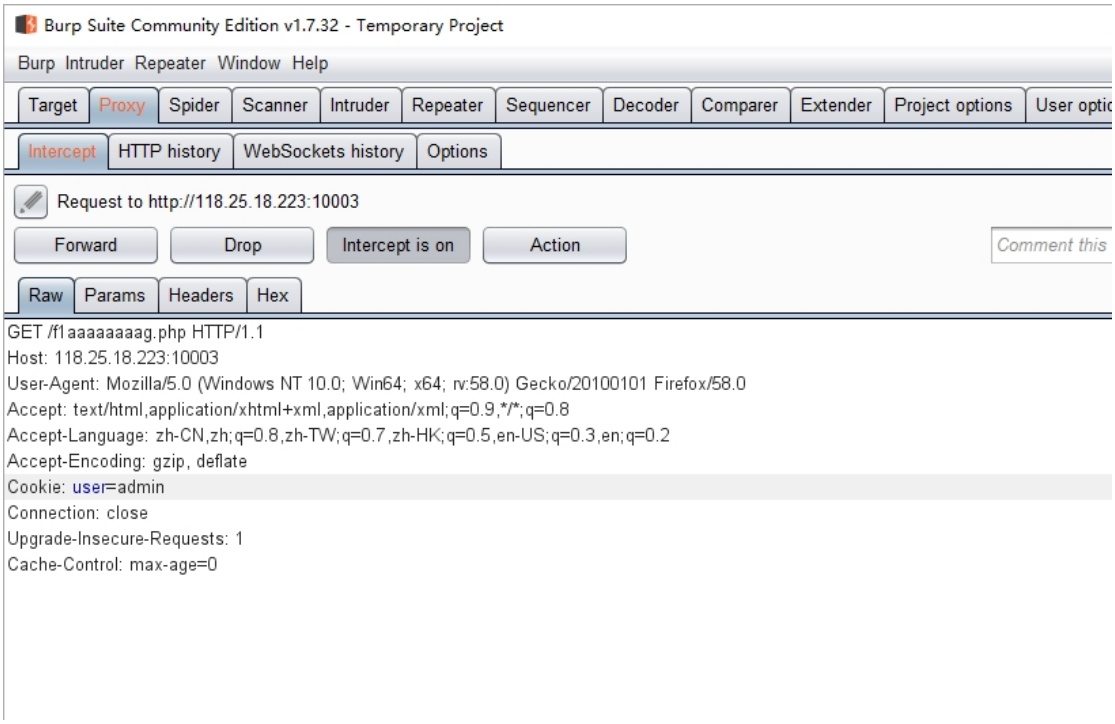
然后 emmm

进下面的 php

然后看到这个 admin

抓包看看

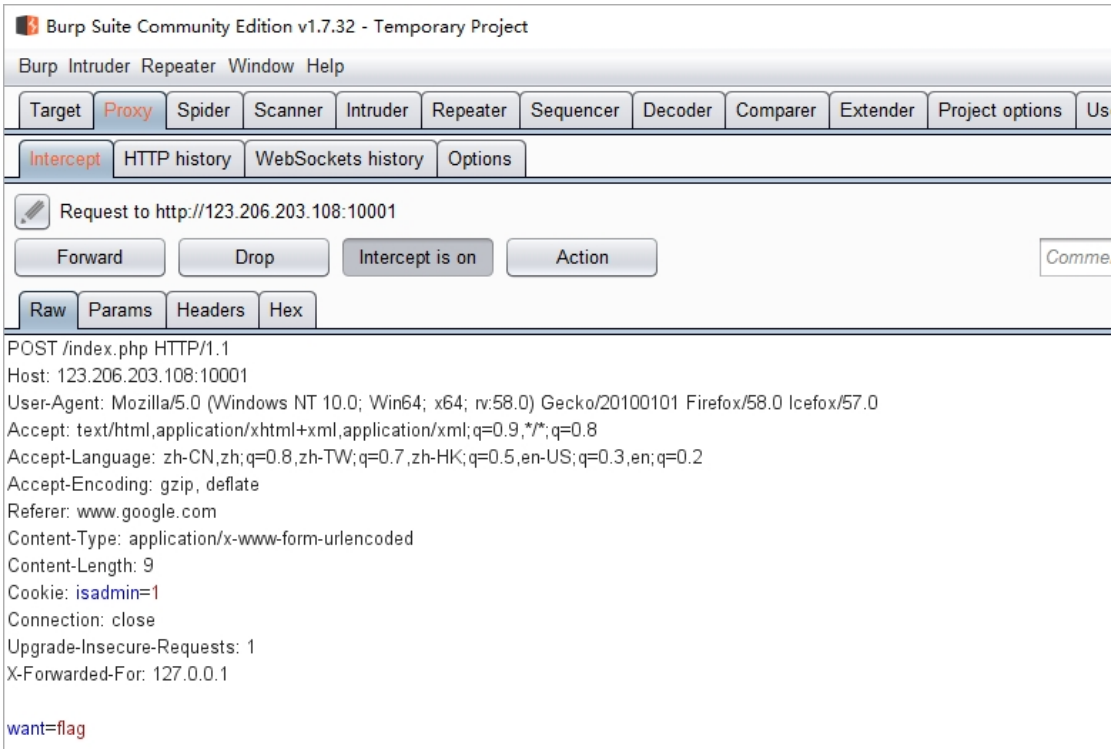
把 user 改成 admin

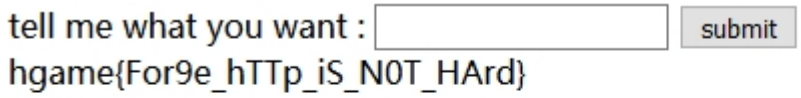

然后 flag 就出来了


4. tell me what you want

根据提示改 header 即可，最后改成这样




然后 flag 就有了




5．我们不一样

源码已经给了

```
include_once("flag.php");
if(isset($_POST['str1'])&&isset($_POST['str2'])){

    if ($_POST['str1']!=$_POST['str2']&&strcmp($_POST['str1'],$_POST['str2'])==0) {
        echo "flag is:".$flag;
        exit();
    } else{
        echo "Something wrong..";
    }
}
```

百度了一下就是 php 弱类型里的 strcmp

strcmp 是比较两个字符串，如果 str1<str2 则返回<0 如果 str1 大于 str2 返回>0 如果两者相等 返回 0

我们是不知道$password 的值的，题目要求 strcmp 判断的接受的值和$password 必需相等，strcmp 传入的期望类型是字符串类型，如果传入的是个数组会怎么样呢

我们传入 password[]=xxx 可以绕过 是因为函数接受到了不符合的类型，将发生错误，但是

还是判断其相等

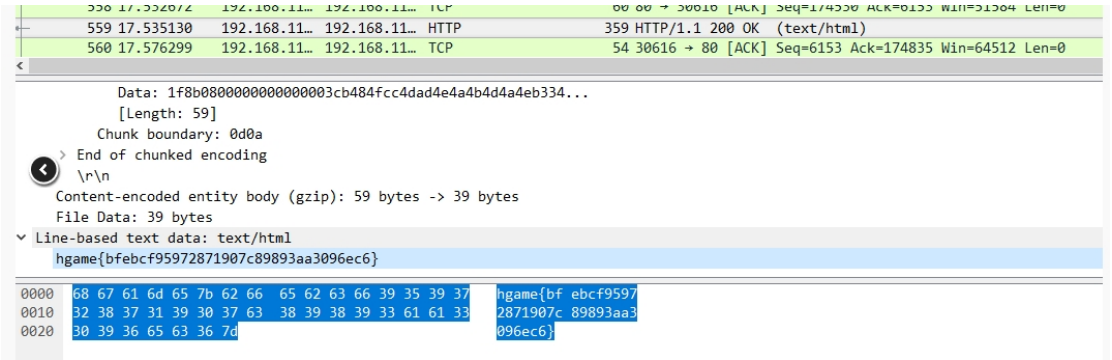
倒是 post 数据如何传入难了我这个菜鸡好久，问学长在 firefox 上下了个 hackbar

flag is:hgame{g3t_f14g_is_so0000_ez}


Misc

3．Pacp1

直接用 wireshark 打开搜 flag 然后点开那个返回 200 的流量包




Crypto

2. Polybius

百度一下没找到工具，直接对着表手解了，然后把 j 换成 i。