

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

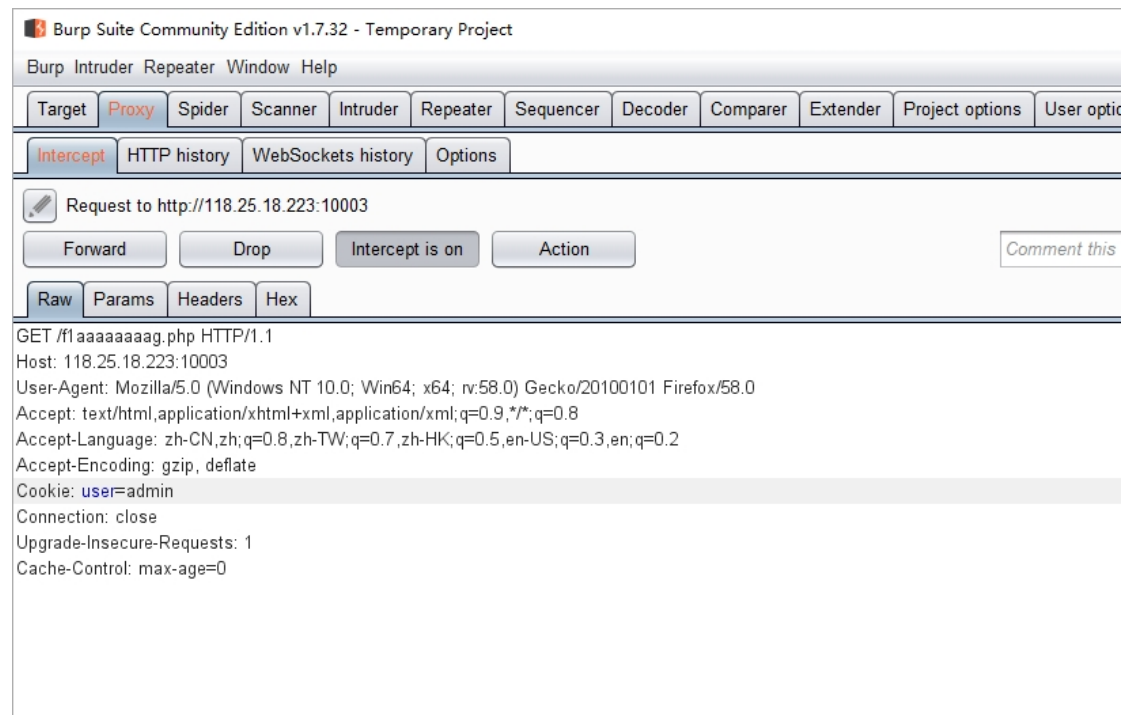
然后看到这个 admin

抓包看看

把 user 改成 admin



only admin can get flag



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

Burp Suite Community Edition v1.7.32 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options Us

Intercept HTTP history WebSockets history Options

Request to http://123.206.203.108:10001

Forward Drop Intercept is on Action

Raw Params Headers Hex

POST /index.php HTTP/1.1
Host: 123.206.203.108:10001
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0 Icefox/57.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: www.google.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 9
Cookie: isadmin=1
Connection: close
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 127.0.0.1

want=flag

然后 flag 就有了

tell me what you want :

hgame{For9e_hTtp_iS_N0T_HArD}

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

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

3. Pacp1

```

550 17.535130 192.168.11... 192.168.11... TCP 550 30616 + 30616 [ACK] Seq=174536 Ack=6153 Win=31304 Len=0
559 17.535130 192.168.11... 192.168.11... HTTP 359 HTTP/1.1 200 OK (text/html)
560 17.576299 192.168.11... 192.168.11... TCP 54 30616 + 80 [ACK] Seq=6153 Ack=174835 Win=64512 Len=0
<
Data: 1f8b08000000000003cb484fcc4dad4e4a4b4d4a4eb334...
[Length: 59]
Chunk boundary: 0d0a
> End of chunked encoding
\r\n
Content-encoded entity body (gzip): 59 bytes -> 39 bytes
File Data: 39 bytes
v Line-based text data: text/html
hgame{bfebcf95972871907c89893aa3096ec6}

0000 68 67 61 6d 65 7b 62 66 65 62 63 66 39 35 39 37 hgame{bf ebcf9597
0010 32 38 37 31 39 30 37 63 38 39 38 39 33 61 61 33 2871907c 89893aa3
0020 30 39 36 65 63 36 7d 096ec6}

```

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。