CTF Lottery

转载

Azurexuoxi 于 2018-08-11 12:58:43 发布 1791 收藏
分类专栏： 信息安全 文章标签： ctf

首先 访问 `/robots.txt` 或者 `/.git/` 发现 Git 仓库可以 GitHack 拿到源码。
漏洞在 api.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++;
}
}
```

其中 `$numbers` 来自用户json输入 `{"action":"buy","numbers":"1122334"}`，没有检查数据类型。`$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：

```
{"action":"buy","numbers":[true,true,true,true,true,true,true]}
```

当每一位中奖号码都不是0时即可中最高奖，攒钱买flag。

另外比赛过程中发现有的选手用了暴力重复注册然后买彩票的方法。考虑了一下这种方法花费的时间并不比直接审计代码短，为了给广大彩民一点希望，可以留作一种备选的非预期解，就没有改题加验证码或者提高flag价格。