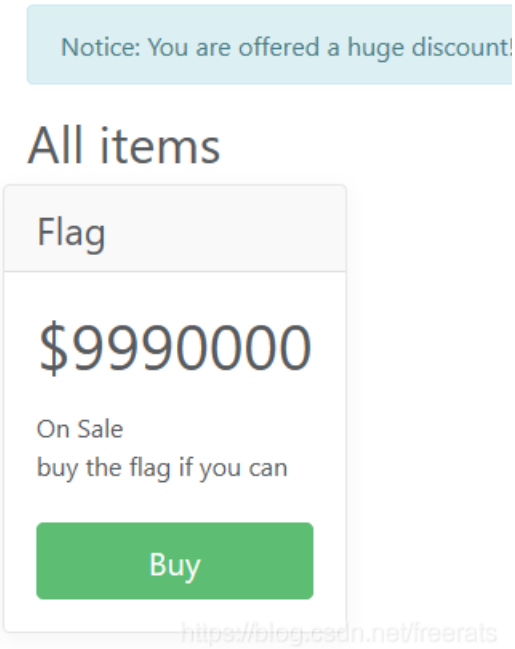
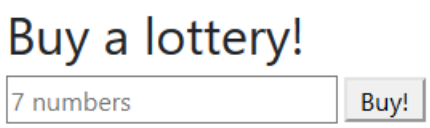
攻防世界 lottery（彩票） writeup

原创

冰可乐不加可乐 于 2020-03-12 17:44:33 发布 365 收藏



在最后一个页面看到flag可以进行购买，应该有足够的钱就可获得flag；

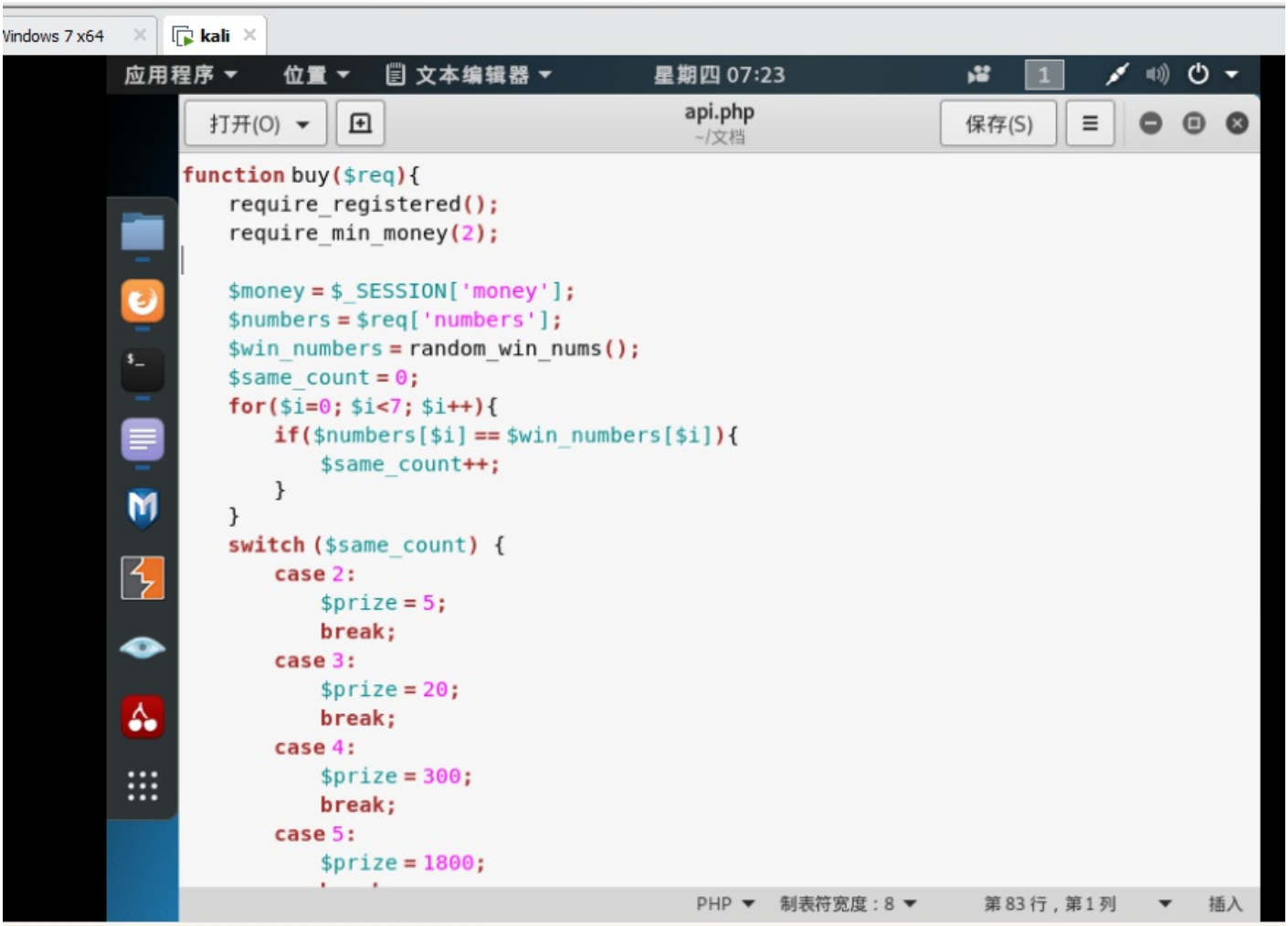


登入后看到一个输入7位数字的框，尝试输入七位数字后就会出现类似买七色球的七位随机数，这里可以赚钱，进行抓包

```
POST /api.php HTTP/1.1
Host: 111.198.29.45:35909
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:73.0) Gecko
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,
Accept-Encoding: gzip, deflate
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Content-Length: 36
Origin: http://111.198.29.45:35909
Connection: close
Referer: http://111.198.29.45:35909/buy.php
Cookie: PHPSESSID=225251afd14565317f13b5751e449d67

{"action":"buy","numbers":"1234567"}
```

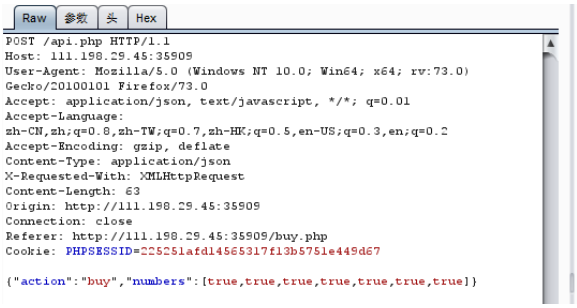

出现参数action，numbers。
使用AWVS进行扫描，发现存在git泄露
打开githack把文件下载下来
在api.php里发现一串主要的php代码
其中关键代码为下图

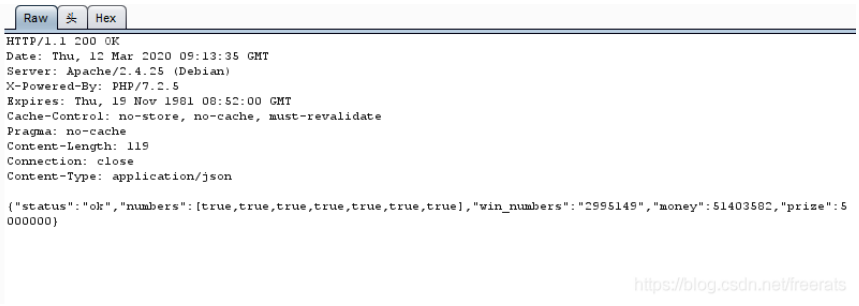


VMware Tools 具有很多功能，能改善鼠标移动性、视频和性能。请登录客户机操作系统，单击"安装 Tools"。

安装 Tools

在图中有number参数，与七位随机数进行比较
漏洞为比较方式为==弱类型比较（若数据类型不同，则会转化为相同类型进行比较），因此只要传入七个true即可匹配成功。
框内限制只能输入七个字符，所以在bp里传入





以数组的方式传入不会报错
接下来多传几次就可以有足够的钱买flag了