# CTF条件竞争

原创

夏日 の blog 于 2020-02-10 14:15:08 发布 1393 收藏 7
分类专栏： CTF-WEB

本文链接：https://blog.csdn.net/zss192/article/details/104247428



## 目录

简介
个人理解
实例
漏洞修复
参考

## 简介

条件竞争是指一个系统的运行结果依赖于不受控制的事件的先后顺序。当这些不受控制的事件并没有按照开发者想要的方式运行时，就可能会出现 bug。尤其在当前我们的系统中大量对资源进行共享，如果处理不当的话，就会产生条件竞争漏洞。

## 个人理解

通俗的来讲就是假设程序同时处理存钱和取钱，当取钱"速度"大于存钱时，可能就会出现取钱后程序还未来得及将金额减少，程序又立马处理存钱，由此产生非预期的结果。

> 竞争条件”发生在多个线程同时访问同一个共享代码、变量、文件等没有进行锁操作或者同步操作的场景中。 ——Wikipedia-computer_science

## 实例

**1.文件上传+条件竞争**

一般是上传文件，绕过防护之后，小马又会被立马删除。但是由于文件存在过，我们可以利用python脚本不断访问shell，这样就形成了python脚本和web删除程序之间的竞争，一定的测试量后，可以竞争到资源，执行shell，从而得到flag。

**2.Session+条件竞争**

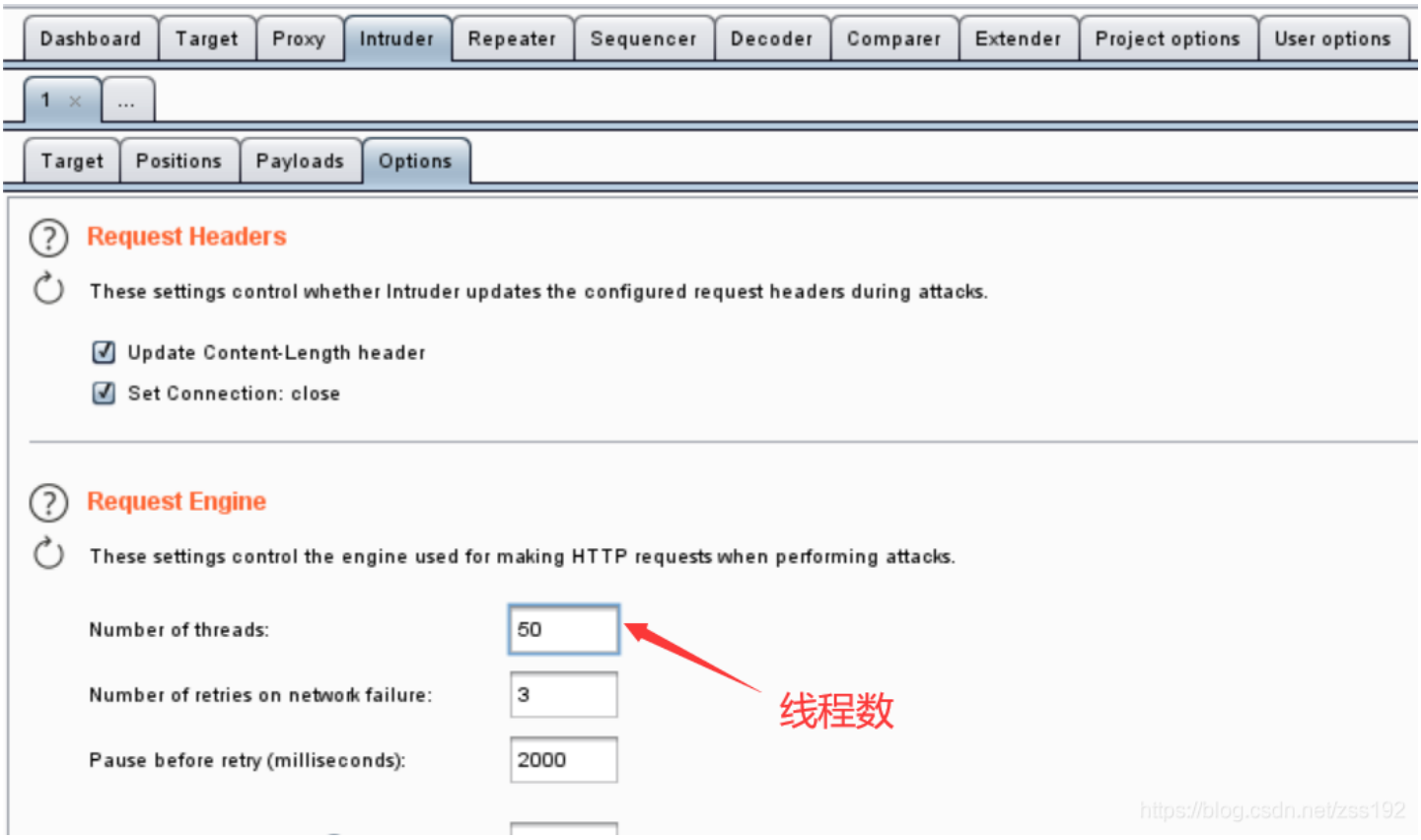
服务器通过session对请求顺序建立了锁，因此我们需要多个session，使用两个浏览器登录同一个账户即可。在将IP改为8.8.8.8时，有短时间的网络请求堵塞，我们在这个时间段，使用另一个session提交请求，即可通过验证，成功将IP改8.8.8.8，然后获得flag。

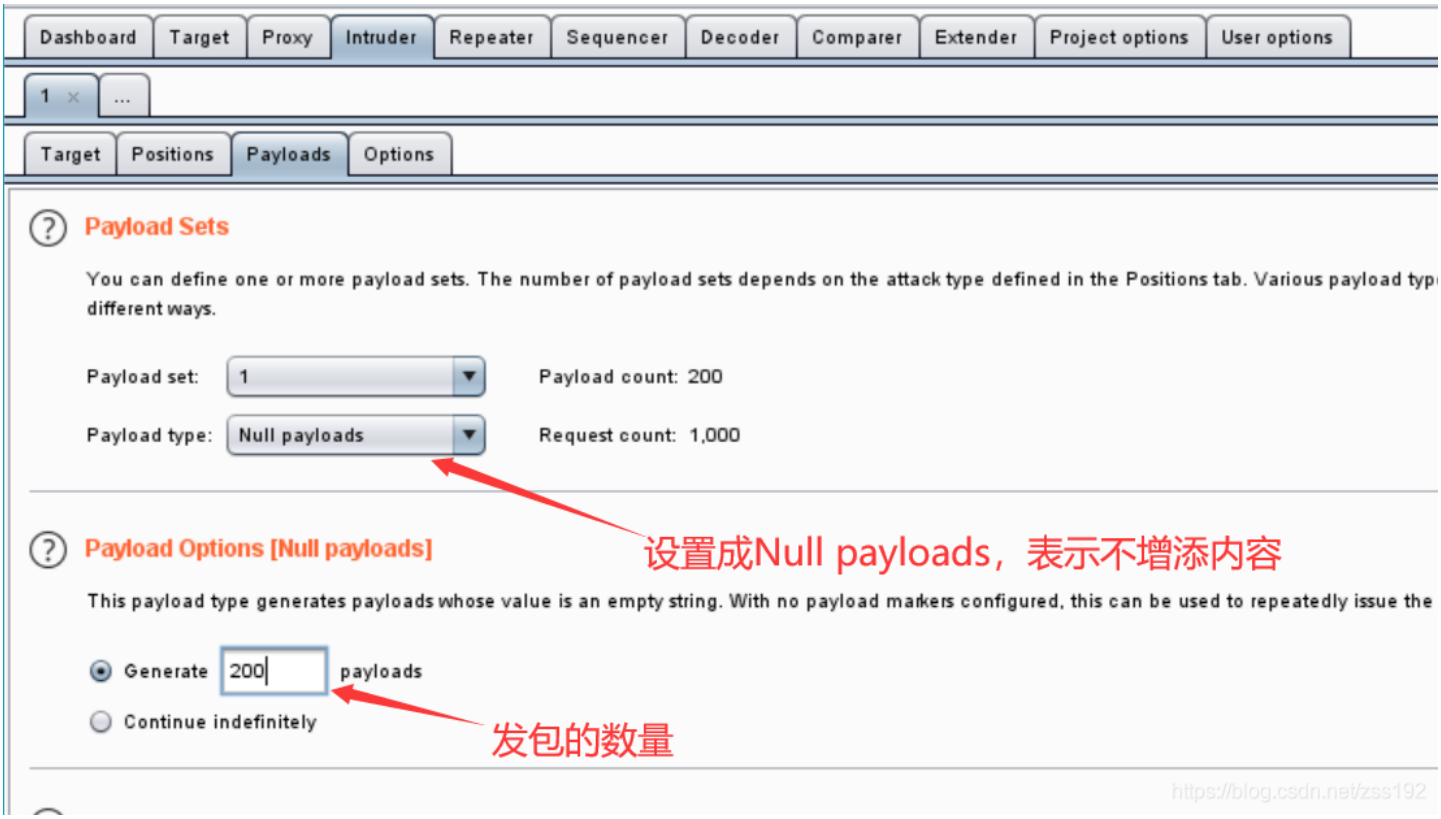
### 3.hgame-2020-Cosmos的二手市场


因为卖东西会收取手续费，正常情况下我们不可能会赚钱。我们可直接利用burpsuite低线程买入,高线程卖出,一次性买入100,卖出200;买入的线程50,卖出的线程100即可。

**那么怎么设置线程数呢？？**

intruder—>Options下，将线程设置成50




## 漏洞修复

1.对于数据库的操作，比较正统的方法是设置锁
2.对于文件上传，“引狼入室”的方法不可取，最好先进行充分的检测，再上传到服务器。

## 参考

条件竞争
测试Web应用程序中的竞争条件