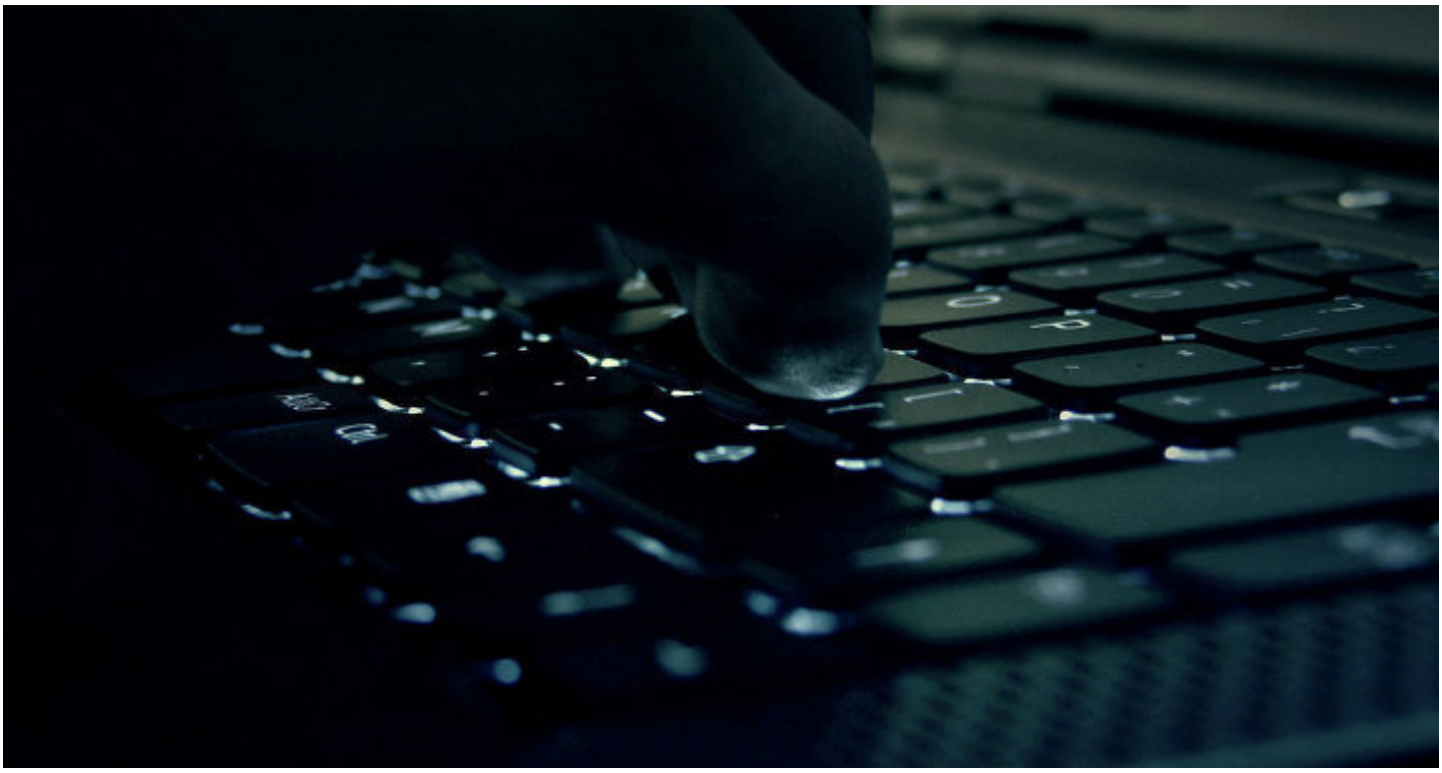


分块传输绕过WAF进行SQL注入


破壳野生喵
公众号——【破壳学院】

0x00最近看到许多师父在玩分块传输，据说能绕过所有WAF?

利用分块传输吊打所有WAF - 安全客,安全资讯平台
2019年1月16日 - 在看了bypassword的《在HTTP协议层面绕过WAF》之后,想起了之前做过的一些研究,所以写个简单的短文来补充一下文章里"分块传输"部分没提到的两个技巧...
安全客 - 百度快照

抱着学习的心态，复现了一波，扩展了很多知识面。

Transfer-Encoding: chunked 表示输出的内容长度不能确定，普通的静态页面、图片之类的基本上都用不到这个。

0x01 什么是分块传输?

分块传输编码（Chunked transfer encoding）是超文本传输协议（HTTP）中的一种数据传输机制，允许HTTP由应用服务器发送给客户端应用（通常是网页浏览器）的数据可以分成多个部分。分块传输编码只在HTTP协议1.1版本（HTTP/1.1）中提供。 通常，HTTP应答消息中发送的数据是整个发送的，Content-Length消息头字段表示数据的长度。数据的长度很重要，因为客户端需要知道哪里是应答消息的结束，以及后续应答消息的开始。然而，使用分块传输编码，数据分解成一系列数据块，并以一个或多个块发送，这样服务器可以发送数据而不需要预先知道发送内容的总大小。通常数据块的大小是一致的，但也不总是这种情况。
作者：席飞剑、来源：CSDN、原文blog.csdn.net/xifeijian...

面的请求，这时用需要实时生成消息长度，服务器一般使用chunked编码。

在进行Chunked编码传输时，在回复消息的Headers有Transfer-Encoding域值为chunked，表示将用chunked编码传输内容。

这在http协议中也是个常见的字段，用于http传送过程的分块技术，原因是http服务器响应的报文长度经常是不可预测的，使用Content-length的实体搜捕并不是总是管用。

分块技术的意思是说，实体被分成许多的块，也就是应用层的数据，TCP在传送的过程中，不对它们做任何的解释，而是把应用层产生数据全部理解成二进制流，然后按照MSS的长度切成一分一分的，一股脑塞到tcp协议栈里面去，而具体这些二进制的数据如何做解释，需要应用层来完成。

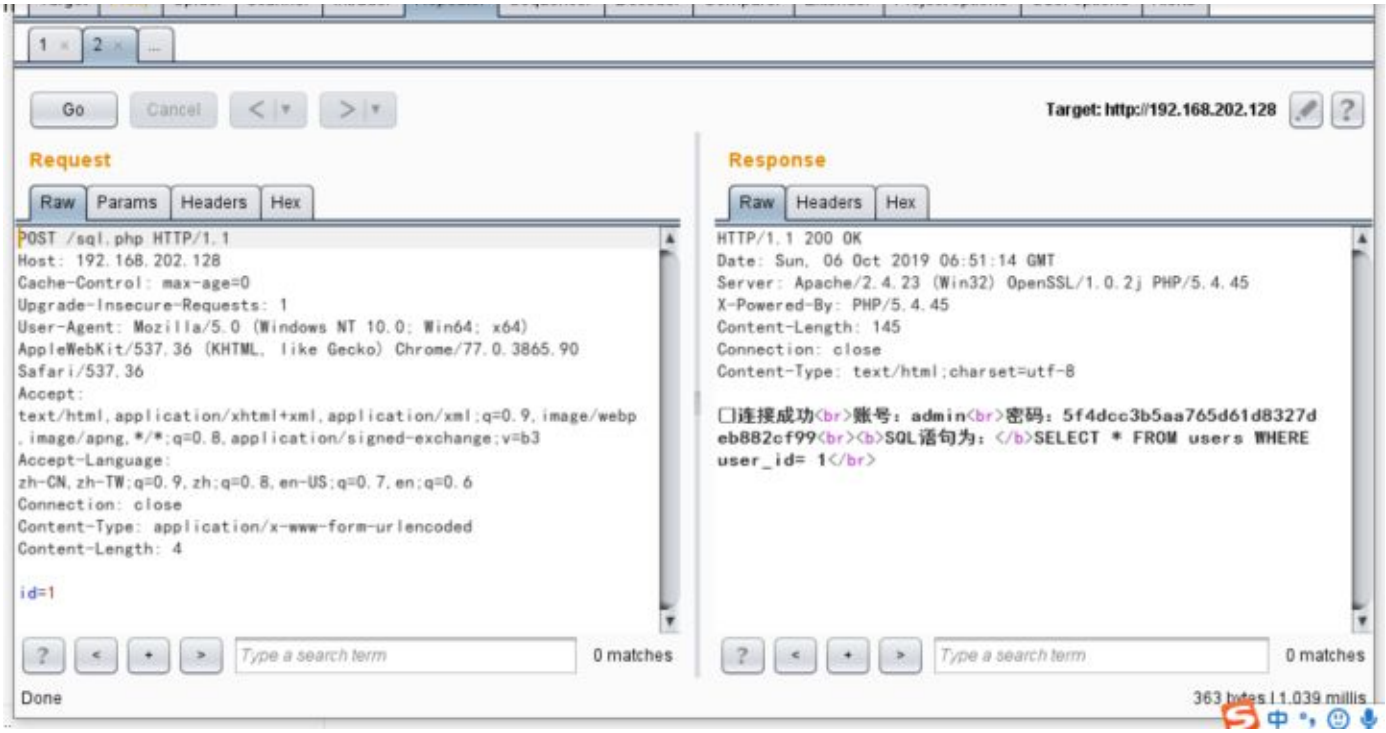
0x02复现

首先准备靶场，可以用DVWA，也可以用sqli。我只用过前者，没用过后者。

前者不会显示你调用的SQL语句，我觉得不大方便，所以我自己自学了一小点PHP，和请教了一下其他师傅，写了最简单的一个SQL注入靶场。

Github地址：github.com/ThestaRY7/SQ...

正常请求POST包：



分块传输POST包：

服务器能正常接收到数据并返回了正常

Transfer-Encoding:Chunked

而post的数据是这种格式

```
2
id
2
=3
0
```

2 #这个2表示下面数据的个数 可以在这个后面加入分号添加注释 比如 2;hello world 可以利用这个特性添加随机字符来干扰waf

id #参数 接收参数就是id一共就两个字母 所以上面的个数是2

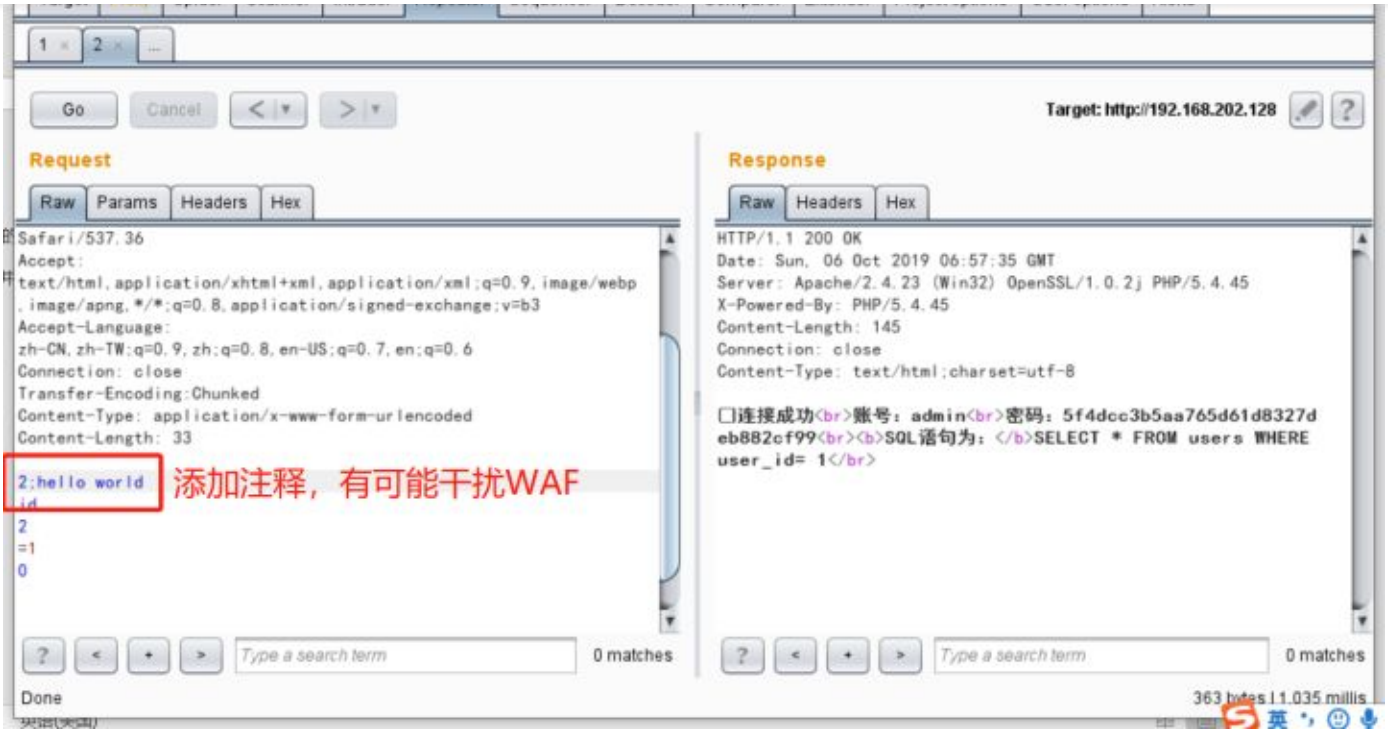
2 #同理 表示下面的数据的个数

=1 #这个也是同理 和前面的id连起来 post的数据就是 id=1

0 #分块传输表示结束的方式 一个0和两个换号

#换行

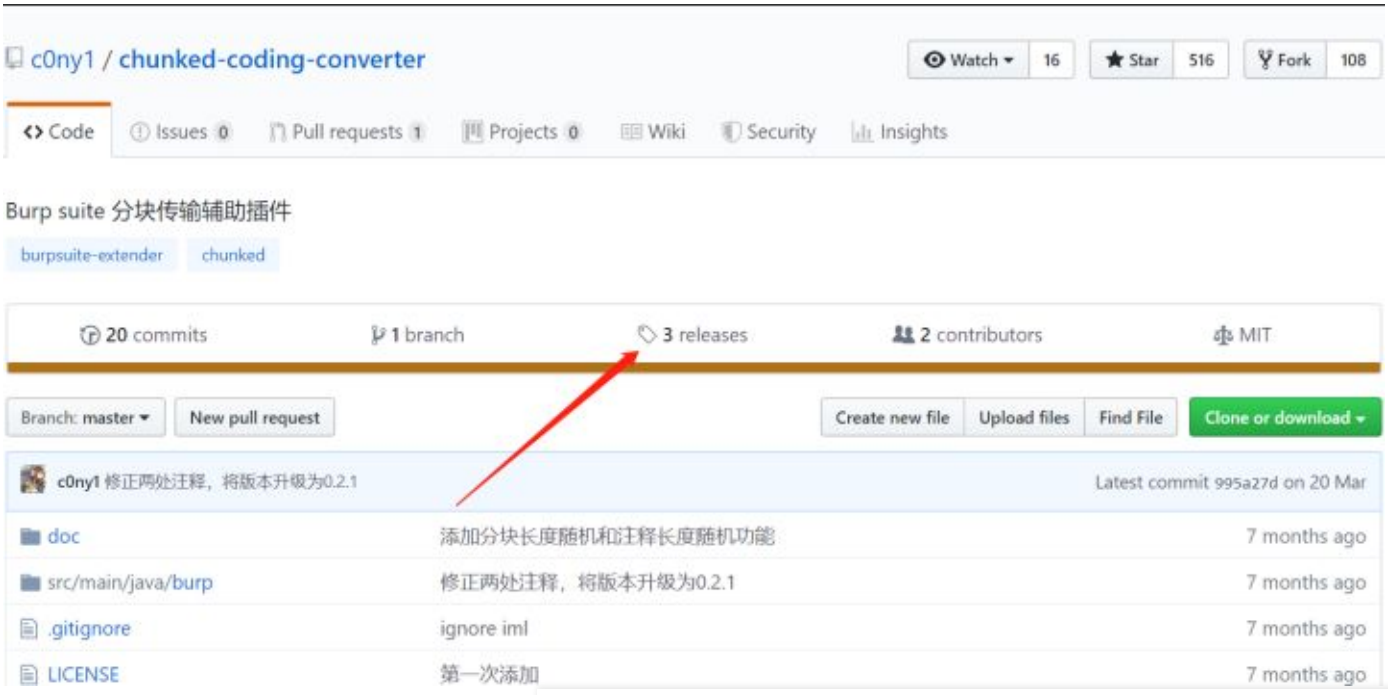
#换行



至此，复现结束。

0x03 插件

经 师傅提醒，github已有大佬写出Burp插件，分块传输。
github.com/c0ny1/chunke...



995a27d

c0ny1 released this on 20 Mar

修复Bug

- 解决部分计算机下配置窗口显示不全问题
- 解决无法加载默认配置问题

致谢

- 感谢 `longhao` 邮件反馈的配置窗口显示不全问题

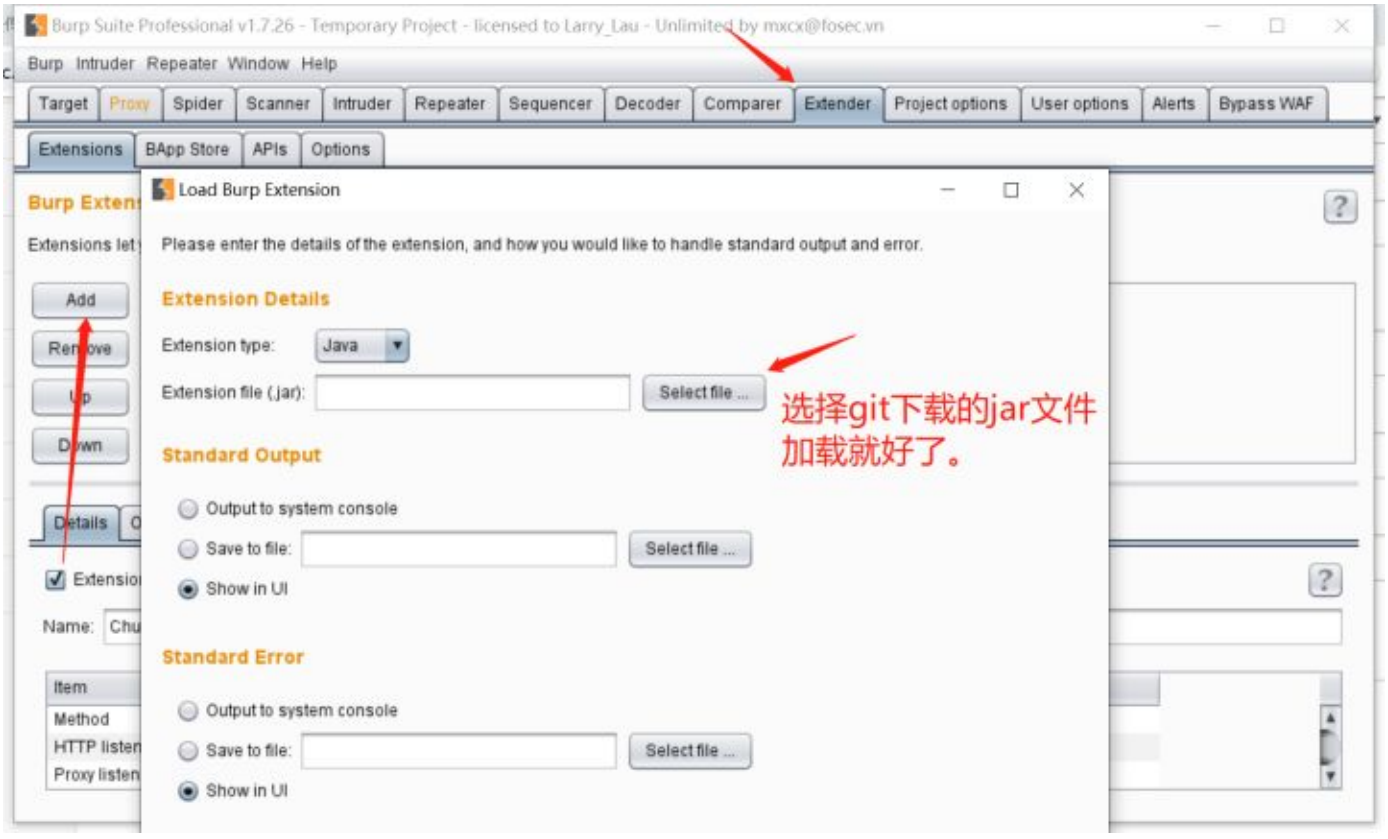
单击下载

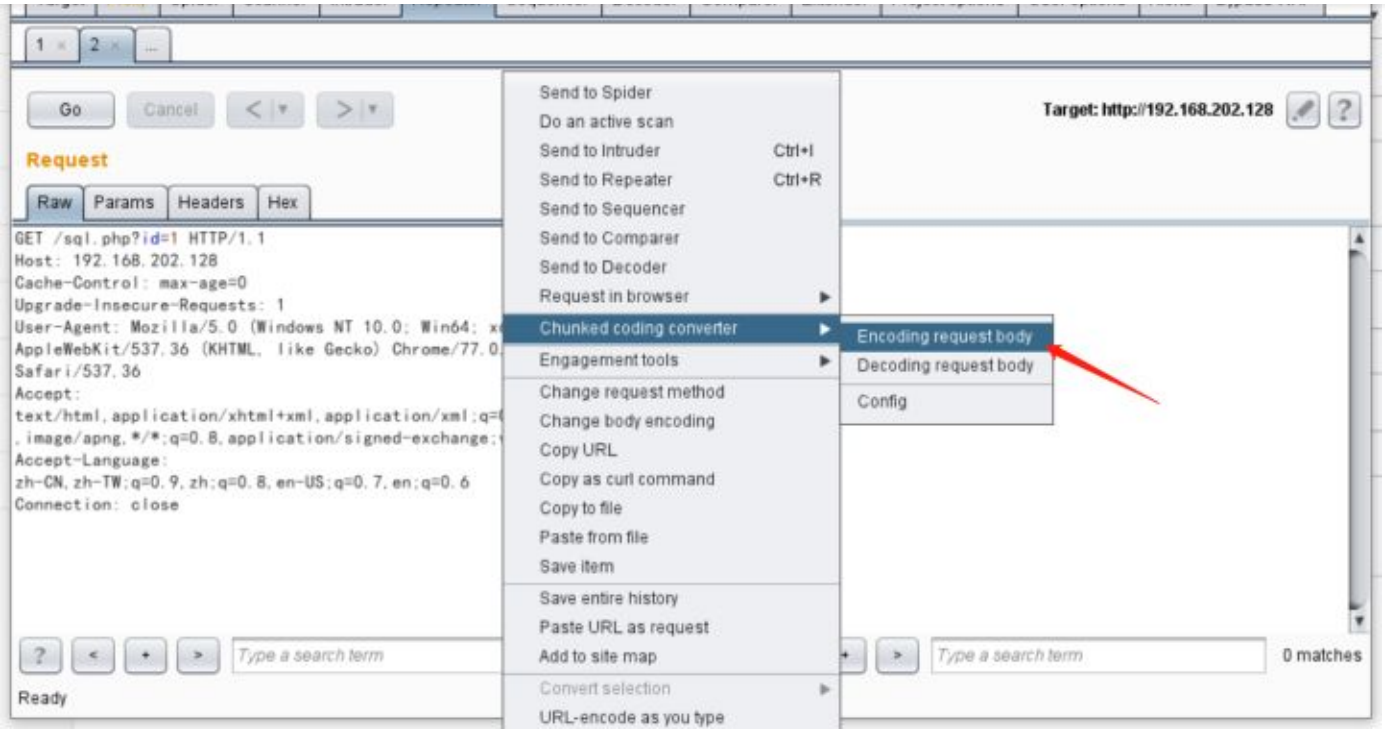
Assets 3

chunked-coding-converter.0.2.1.jar 39.1 KB

Source code (zip)

Source code (tar.gz)





作者初衷用于分享与普及网络知识，若读者因此作出任何危害网络安全行为后果自负，与原作者无关。

发布于 2019-11-22

网络安全　信息安全　数据传输

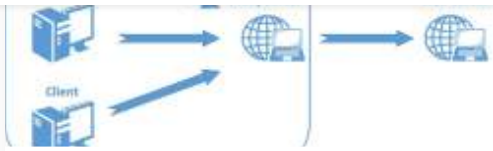
文章被以下专栏收录

Pockr安全喵
网络安全知识技术交流

进入专栏

推荐阅读

倾旋 发表于一叶知安
渗透测试中的Bypass技巧



老欢不慌
使用代理隐藏IP地址的两种方式

倾旋
自动化

4 条评论 ⇌ 切换为时间排序

写下你的评论...

蒙宸辉 5 个月前
我用分块传输post接收不到参数，不使用分块传输正常接收

赞

Demo 回复 蒙宸辉 1 个月前
是不是不是 http1.1呢
赞

蒙宸辉 回复 Demo 1 个月前
之前测试的现在已经忘了，还是很感谢你能回复的[笑哭]
赞

Demo 1 个月前
感谢作者 奇奇怪怪又[好奇]知识加一
赞