被划分出来的具有不同信任级别的区域，我们成为**信任域**，划分两个不同信任域之间的边界，我们称之为**信任边界**。

2011年12月，[CSDN](https://baike.baidu.com/item/CSDN)的安全系统遭到黑客攻击，600万用户的登录名、密码及邮箱遭到泄漏。随后，CSDN"密码外泄门"持续发酵，多玩、世纪佳缘、走秀等网站相继被曝用户数据遭泄密。

https://blog.csdn.net/stpeace/article/details/78073288?locationNum=8&fps=1

**安全的三要素**

安全的三要素是安全的基本组成元素，分别为**机密性（Confidentiality）**，**完整性（Integrity）**，**可用性（Availability）**。

**如何实施安全评估**

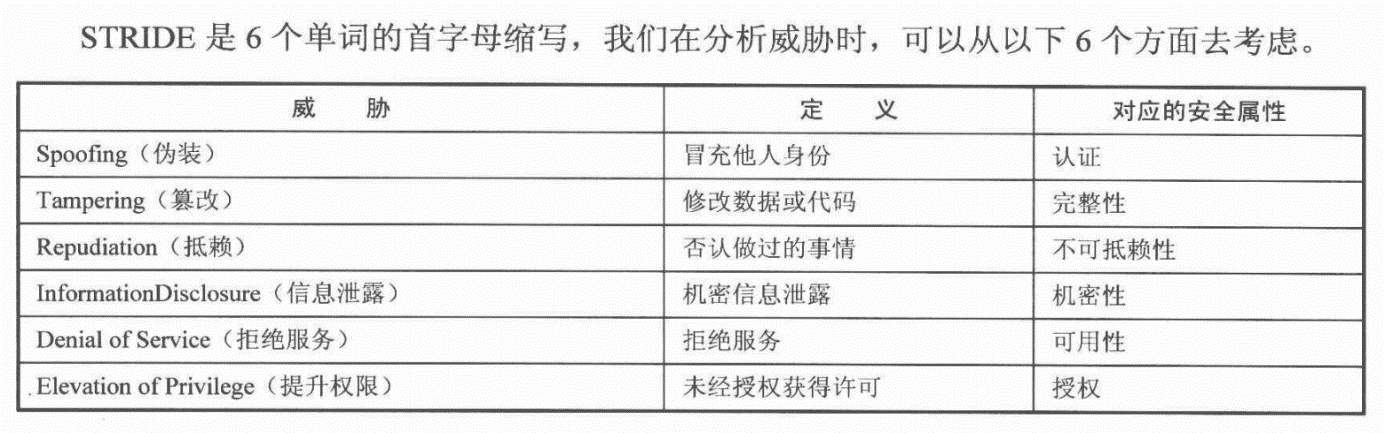
1. 资产等级划分，2.威胁分析，3.风险分析，4.确认解决方案。

资产等级划分

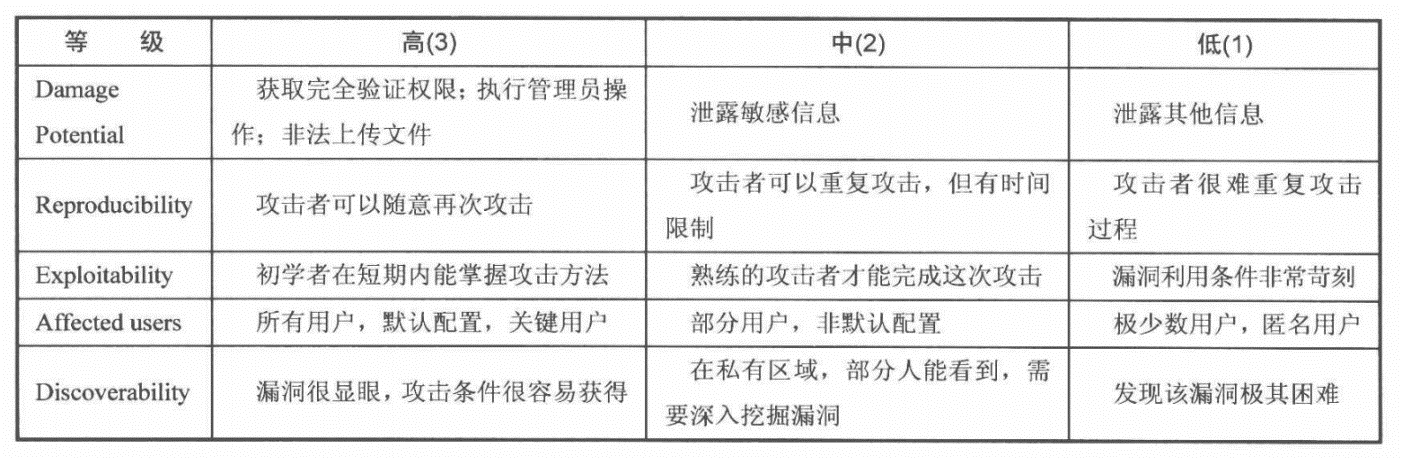
资产等级划分是所有工作的基础，这项工作能够帮助我们明确目标是什么，要保护什么。

威胁分析

STRIDE模型，最早由微软提出



风险分析



**最小权限原则**

最小原则要求系统只授予主体必要的权限，而**不要过度授权**，这样能有效地减少系统，网络，应用，数据库出错的机会。

**纵深防御原则**

纵深防御原则包含**两层含义**：

1.要在各个不同层面，不同方面实施安全方案，避免出现疏漏，不同安全方案之间需要相互配合，构成一个整体；

2.要在正确的地方做正确的事情，即：在解决根本问题的地方实施针对性的安全方案。

**数据与代码分离原则**

这一原则适用于各种由于“注入”而引发安全问题的场景。

实际上，缓冲区溢出，也可以认为是程序违背了这一原则的后果——程序在栈或者堆中，将用户数据当做代码执行，混淆了代码与数据的边界，从而导致安全问题的发生。

**不可预测性原则**

微软使用的ASLR技术，在较新版本的Linux内核中也支持。在ASLR的控制下，一个程序每次启动时，其进程的栈基址都不相同，具有一定的随机性，对于攻击者来说，这就是“不可预测性”。

不可预测性，能有效地对抗基于篡改，伪造的攻击。

不可预测性的实现往往需要用到加密算法，随机数算法，哈希算法，好好利用这条规则，在设计安全方案时往往会事半功倍。

假设一个内容管理系统中的文章序号，是按照数字升序排列的，id=1000, id=1002, id=1003

For（i=0;i<100000;i++）{

Delete(url + ”?id” = i);

}

id = asldqwfhiioqw, id= aweofaoshklsaf , id=poerafqwofihasd……

id值变得不可预测后，攻击者想再想批量删除文章，只能通过爬虫把所有id抓取下来。

**客户端脚本安全**

**两个页面地址中的协议、域名和端口号一致，则表示同源。**

| **地址** | **同源** | **原因** |
| --- | --- | --- |
| [http://www.google.com](http://www.google.com/) | 否 | 协议不一致 |
| [https://google.com](https://google.com/) | 否 | 域名不一致 |
| [https://www.google.com:81](https://www.google.com:81/) | 否 | 端口号不一致 |
| <https://www.google.com/a/s.html> | 是 | 协议，域名和端口号都一致 |

存储在浏览器中的数据，如localStroage、Cookie和IndexedDB不能通过脚本跨域访问

不能通过脚本操作不同域下的DOM

不能通过ajax请求不同域的数据

同源策略是浏览器的一个安全功能，不同源的客户端脚本在没有明确授权的情况下，不能读写对方资源。所以a.com下的js脚本采用ajax读取b.com里面的文件数据是会报错的。

不受同源策略限制的：

1、页面中的链接，重定向以及表单提交是不会受到同源策略限制的。

2、跨域资源的引入是可以的。但是js不能读写加载的内容。如嵌入到页面中的<script src="..."></script>，<img>，<link>，<iframe>等。

网络攻击类型

ping of death

teardrop

UDP flood

SYN flood

Land攻击

Smurf攻击

电子邮件炸弹

**信息收集型攻击**

访问类攻击

Web攻击

**拒绝服务型攻击**

病毒类攻击

**利用型攻击**

缓冲区溢出攻击

漏洞攻击

木马攻击

将攻击进行分类为：探测攻

击、获取权限攻击、操作攻击、拒绝服务攻击。相应的对漏洞分类为：系统信息泄漏漏洞、权限类漏洞、拒绝服务类漏洞。对攻击工具分类为：信息获取工具、权限提升工具、操作类攻击工具、拒绝服务攻击工具。

又称目的达成攻击，指在一定的权限范围内对目标所进行的直接的目的实现性操作，是攻击实施阶段进行的。其目的如前所述：窃取信息、窃取服务、信息破坏、信息干扰，主要的操作攻击有安装攻击的软件如Sniff、木马等进行窃听， 述了网络攻击的目的和过程。

的攻击分类方法没有对此进行分类。这类攻击没有对应的漏洞，它所利用

的是己经获取的目标系统的权限或安装的相应功能的软件。主要的攻击工参考文献：

具是具有相应功能的软件程序