深入了解网络安全之安全漏洞杂谈 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/142/2021_2022__E6_B7_B1_E5_85_A5_E4_BA_86_E8_c101_142701.htm 网络安全的核心目标是保障业务系统的可持续性和数据的安全性，而这两点的主要威胁来自于蠕虫的暴发、黑客的攻击、拒绝服务攻击、木马。蠕虫、黑客攻击问题都和漏洞紧密联系在一起，一旦有重大安全漏洞出现，整个互联网就会面临一次重大挑战。虽然传统木马和安全漏洞关系不大，但最近很多木马都巧妙的利用了IE的漏洞，让你在浏览网页时不知不觉的就中了招。 安全漏洞的定义已经有很多了，我这里给出一个通俗的说法就是：能够被利用来干“ 原本以为 ”不能干的事，并且和安全相关的缺陷。这个缺陷可以是设计上的问题、程序代码实现上的问题。 一、不同角度看安全漏洞的分类 对一个特定程序的安全漏洞可以从多方面进行分类。 1. 从用户群体分类：●大众类软件的漏洞。如Windows的漏洞、IE的漏洞等等。●专用软件的漏洞。如Oracle漏洞、Apache漏洞等等。 2. 从数据角度看分为：●能读按理不能读的数据，包括内存中的数据、文件中的数据、用户输入的数据、数据库中的数据、网络上传输的数据等等。●能把指定的内容写入指定的地方（这个地方包括文件、内存、数据库等）●输入的数据能被执行（包括按机器码执行、按Shell代码执行、按SQL代码执行等等） 3.从作用范围角度看分为：●远程漏洞，攻击者可以利用并直接通过网络发起攻击的漏洞。这类漏洞危害极大，攻击者能随心所欲的通过此漏洞操作他人的电脑。并且此类漏洞很容易导致蠕虫攻击，在Windows。●本地漏洞，攻

击者必须在本机拥有访问权限前提下才能发起攻击的漏洞。比较典型的是本地权限提升漏洞，这类漏洞在Unix系统中广泛存在，能让普通用户获得最高管理员权限。 4.从触发条件上看可以分为： ●主动触发漏洞，攻击者可以主动利用该漏洞进行攻击，如直接访问他人计算机。 ●被动触发漏洞，必须要计算机的操作人员配合才能进行攻击利用的漏洞。比如攻击者给管理员发一封邮件，带了一个特殊的jpg图片文件，如果管理员打开图片文件就会导致看图软件的某个漏洞被触发，从而系统被攻击，但如果管理员不看这个图片则不会受攻击。 5.从操作角度看可分为： ●文件操作类型，主要为操作的目标文件路径可被控制（如通过参数、配置文件、环境变量、符号链接灯），这样就可能导致下面两个问题：◇写入内容可被控制，从而可伪造文件内容，导致权限提升或直接修改重要数据（如修改存贷数据），这类漏洞有很多，如历史上Oracle TNS LOG文件可指定漏洞，可导致任何人可控制运行Oracle服务的计算机；◇内容信息可被输出，包含内容被打印到屏幕、记录到可读的日志文件、产生可被用户读的core文件等等，这类漏洞在历史上Unix系统中的crontab子系统中出现过很多次，普通用户能读受保护的shadow文件； ●内存覆盖，主要为内存单元可指定，写入内容可指定，这样就能执行攻击者想执行的代码（缓冲区溢出、格式串漏洞、PTrace漏洞、历史上Windows2000的硬件调试寄存器用户可写漏洞）或直接修改内存中的机密数据。 ●逻辑错误，这类漏洞广泛存在，但很少有范式，所以难以查觉，可细分为：◇条件竞争漏洞（通常为设计问题，典型的有Ptrace漏洞、广泛存在的文件操作时序竞争） ◇策略错误，通常为设计问题

，如历史上FreeBSD的Smart IO漏洞。◇算法问题（通常为设计问题或代码实现问题），如历史上微软的Windows 95/98的共享口令可轻易获取漏洞。◇设计的不完善，如TCP/IP协议中的3步握手导致了SYN FLOOD拒绝服务攻击。◇实现中的错误（通常为设计没有问题，但编码人员出现了逻辑错误，如历史上博彩系统的伪随机算法实现问题）●外部命令执行问题，典型的有外部命令可被控制（通过PATH变量，输入中的SHELL特殊字符等等）和SQL注入问题。 6. 从时序上看可分为：●已发现很久的漏洞：厂商已经发布补丁或修补方法，很多人都已经知道。这类漏洞通常很多人已经进行了修补，宏观上看危害比较小。●刚发现的漏洞：厂商刚发补丁或修补方法，知道的人还不多。相对于上一种漏洞其危害性较大，如果此时出现了蠕虫或傻瓜化的利用程序，那么会导致大批系统受到攻击。●0day：还没有公开的漏洞，在私下交易中的。这类漏洞通常对大众不会有什么影响，但会导致攻击者瞄准的目标受到精确攻击，危害也是非常之大。 二、不同角度看待漏洞利用 如果一个缺陷不能被利用来干“ 原本 ”不能干的事（安全相关的），那么就不能被称为安全漏洞，所以安全漏洞必然和漏洞利用紧密联系在一起。 漏洞利用的视角有：●数据视角：访问本来不可访问的数据，包括读和写。这一条通常是攻击者的核心目的，而且可造成非常严重的灾难（如银行数据可被人写）。●权限视角：主要为权限绕过或权限提升。通常权限提升都是为了获得期望的数据操作能力。●可用性视角：获得对系统某些服务的控制权限，这可能导致某些重要服务被攻击者停止而导致拒绝服务攻击。●认证绕过：通常利用认证系统的漏洞而不用受权就能进

入系统。通常认证绕过都是为权限提升或直接的数据访问服务的。 ●代码执行角度：主要是让程序将输入的内容作为代码来执行，从而获得远程系统的访问权限或本地系统的更高权限。这个角度是SQL注入、内存指针游戏类漏洞（缓冲区溢出、格式串、整形溢出等等）等的主要驱动。这个角度通常为绕过系统认证、权限提升、数据读取作准备的。 100Test下载频道开通，各类考试题目直接下载。详细请访问www.100test.com