安全知识：漏洞的形成和防治 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/454/2021_2022__E5_AE_89_E5_85_A8_E7_9F_A5_E8_c100_454532.htm 软件和系统无法避免会出现漏洞。一说起漏洞，有人就会感到气愤，认为被坑了。其实不然，漏洞的产生是不可避免的。有了漏洞，我们就应该去补救。 漏洞的形成 大型软件、系统的编写，并不是一两个人就能完成的，而是需要许许多多程序员共同完成。那么，他们是怎么工作的呢？他们是将一个软件或系统分成若干板块，分工编写，然后再汇总，测试。最后，修补，发布。 有人或许会问，为什么最后要修补呢？其实，这就是一个重要的环节。前面讲到要讲软件、系统分成若干板块，分工编写。问题就出在分工编写这个环节：世界上总找不到思维一样的人，所以有时不免会出现种种问题，且不说“ 几不管 ”的中间地带，就是在软件汇总时，为了测试方便，程序员总会留有后门；在测试以后再进行修补…… 这些后门，如果一旦疏忽（或是为某种目的故意留下），或是没有发现，软件发布后自然而然就成了漏洞。 还值得一提的就是若干板块之间的空隙，这里很容易出现连程序员的都没想到的漏洞！ 还有，“ 几不管 ”地带，也正是漏洞的温床！如果，在软件发布前没能及时发现，就为不法之徒提供了便利。 漏洞的另一形成温床就是网络协议！网络协议有TCP、UDP、ICMP、IGMP等。其实，他们本来的用途是好的，但却被别人用于不乏的活动：例如，ICMP本来是用于寻找网络相关信息，后来却被用于网络嗅探和攻击；TCP本来是用于网络传输，后来却被用于泄漏用户信息…… 漏洞的温床实在太多了，有时

并不能完全怪程序员，因为有些东西连他们也无能为力啊！漏洞的防治 有了漏洞就要补！否则，日后的受害者可能就是自己。例如，微软就是著名的漏洞王！他同时也是著名的补丁王！有这样一句话：微软的补丁，谁人能及！Windows实在太大，太复杂了，所以漏洞多也是可以原谅的。更何况，全世界最精锐的黑客部队的也喜欢将矛头直指Windows，可悲啊！ 补漏洞方法主要有两类： 一、本身补救。这种补漏洞方法主要是靠厂商的补丁或者是禁用某项服务来补救。也就是说，靠软件或系统本身来补救。 二、借助补救。这种补漏洞方法主要是靠第三者完成，就是靠别的软件来进行补救。我们用得最广泛的就是反病毒软件和网络防火墙。 软件的补救必须要有目的的补救，不能盲目的补。在补救前，我们可以借助别的软件来测试。例如，查找网络漏洞，可以用嗅探器；查找反病毒软件的查毒漏洞，可以通过网络上提供的病毒压缩包等。 漏洞是客观存在的，它是随软件和系统的产生的，是不可避免的。关键就在于补救，补救得好，软件或系统的性能将大大提高！ 