计算机三级网络技术:网站被黑的10大原因计算机等级考试
PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/584/2021_2022__E8_AE_A1_E7_AE_97_E6_9C_BA_E4_c98_584482.htm 1、跨站脚本(XSS) ■ 问题：XSS漏洞是最普遍和最致命的网络应用软件安全漏洞，当一款应用软件将用户数据发送到不带认证或者不对内容进行编码的网络浏览器时容易发生。黑客可以利用浏览器中的恶意脚本获得用户的数据，破坏网站，插入有害内容，以及展开钓鱼式攻击和恶意攻击。 ■ 真实案例：恶意攻击者去年针对Paypal发起了攻击，他们将Paypal用户重新引导到另一个恶意网站并警告用户，他们的账户已经失窃。用户们被引导到另一个钓鱼式网站上，然后输入自己的Paypal登录信息、社会保险号和信用卡资料。Paypal公司称，它在2006年6月修复了那个漏洞。 ■ 如何保护用户：利用一个白名单来验证接到的所有数据，来自白名单之外的数据一律拦截。另外，还可以对所有接收到的数据进行编码。OWASP说：“ 验证机制可以检测攻击，编码则可以防止其他恶意攻击者在浏览器上运行的内容中插入其他脚本。 ”2、注入漏洞 ■ 问题：当用户提供的数据被作为指令的一部分发送到转换器(将文本指令转换成可执行的机器指令)的时候，黑客会欺骗转换器。攻击者可以利用注入漏洞创建、读取、更新或者删除应用软件上的任意数据。在最坏的情况下，攻击者可以利用这些漏洞完全控制应用软件和底层系统，甚至绕过系统底层的防火墙。 ■ 真实案例：俄罗斯黑客在2006年1月份攻破了美国罗得岛政府网站，窃取了大量信用卡资料。黑客们声称SQL注入攻击窃取了5.3万个信用卡账号，而主机服务供应商则声称只

被窃取了4113个信用卡账号。 ■ 如何保护用户：尽可能不要使用转换器。OWASP组织说：“ 如果你必须使用转换器，那么，避免遭受注入攻击的最好方法是使用安全的API，比如参数化指令和对象关系映射库。 ”3、恶意文件执行 ■ 问题：黑客们可以远程执行代码、远程安装rootkits工具或者完全攻破一个系统。任何一款接受来自用户的文件名或者文件的网络应用软件都是存在漏洞的。漏洞可能是用PHP语言写的，PHP是网络开发过程中应用最普遍的一种脚本语言。 ■ 真实案例：一位青少年程序员在2002年发现了Guess.com网站是存在漏洞的，攻击者可以从Guess数据库中窃取20万个客户的资料，包括用户名、信用卡号和有效期等。Guess公司在次年受到联邦贸易委员会调查之后，同意升级其安全系统。 ■ 如何保护用户：不要将用户提供的任何文件写入基于服务器的资源，比如镜像和脚本等。设定防火墙规则，防止外部网站与内部系统之间建立任何新的连接。 4、不安全的直接对象参照物 ■ 问题：攻击者可以利用直接对象参照物而越权存取其他对象。当网站地址或者其他参数包含了文件、目录、数据库记录或者关键字等参照物对象时就可能发生这种攻击。银行网站通常使用用户的账号作为主关键字，这样就可能在网络接口中暴露用户的账号。 OWASP说：“ 数据库关键字的参照物通常会泄密。攻击者可以通过猜想或者搜索另一个有效关键字的方式攻击这些参数。通常，它们都是连续的。 ” ■ 真实案例：澳大利亚的一个税务网站在2000年被一位用户攻破。那位用户只是在网站地址中更改了税务ID账号就获得了1.7万家企业的详细资料。黑客以电子邮件的方式通知了那1.7万家企业，告知它们的数据已经被破解了。 ■ 如何保护

用户：利用索引，通过间接参照映射或者另一种间接法来避免发生直接对象参照物泄密。如果你不能避免使用直接参照，那么在使用它们之前必须对网站访问者进行授权。 5、跨站指令伪造 ■ 问题：这种攻击简单但破坏性强，它可以控制受害人的浏览器然后发送恶意指令到网络应用软件上。这种网站是很容易被攻击的，部分原因是因为它们是根据会话cookie或者“ 自动记忆 ”功能来授权指令的。各银行就是潜在的被攻击目标。 Williams说：“ 网络上99%的应用软件都是易被跨站指令伪造漏洞感染的。现实中是否发生过某人因此被攻击而损失钱财的事呢?也许连各银行都不知道。对于银行来说，整个攻击看起来就像是用户登录到系统中进行了一次合法的交易。 ” ■ 真实案例：一位名叫Samy的黑客在2005年末利用一个蠕虫在MySpace网站上获得了100万个“ 好友 ”资料，在成千上万个MySpace网页上自动出现了“ Samy是我的英雄 ”的文字。攻击本身也许是无害的，但是据说这个案例证明了将跨站脚本与伪造跨站指令结合在一起所具备的威力。另一个案例发生在一年前，Google网站上出现了一个漏洞，外部网站可以利用那个漏洞改变用户的语言偏好设置。 ■ 如何保护用户：不要依赖浏览器自动提交的凭证或者标识。OWASP说：“ 解决这个问题的唯一方法是使用一种浏览器不会记住的自定义标识。 ”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