

电子商务网站建设中的安全问题研究电子商务考试 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/534/2021_2022__E7_94_B5_E5_AD_90_E5_95_86_E5_c40_534057.htm

随着互联网的不断发展.作为一个企业，在互联网上建立自己的网站，最显而易见的就是可以向世界展示自己的企业风采，让更多人了解自己的企业.使企业能够在公众知名度上有一定的提升，并通过网站进行企业的内部管理和开展电子商务活动。因此，电子商务网站成为企业活动的一个重要组成部分，而如何提高网站的安全，抵抗黑客非法入侵，避免企业信息泄漏给企业带来的损失是目前电子商务网站建设中的重要一环.本文分析了目前对国内电子商务网站安全的常见问题.希望能引起相关企业的重视。

一、服务器安全问题及对策

电子商务网站建设中首要的问题是网站WEB服务器的使用，通常情况下，开展电子商务的企业会采用自建服务器方案来完成电子商务的各项功能，因此为了电子商务网站的特殊需要企业会自己租用通信专线，架设WEB服务器。

1、WEB服务器上的安全漏洞。

WEB服务器上的漏洞可以从以下几方面考虑：(1)、在WEB服务器上你不让人访问的秘密文件、目录或重要数据。(2)、从远程用户向服务器发送信息时，特别是信用卡之类东西时.中途遭不法分子非法拦截。(3)、WEB服务器本身存在一些漏洞使得一些人能侵入到主机系统.破坏一些重要的数据.甚至造成系统瘫痪。(4)、WEB服务器的一些扩展组件存在漏洞，/百考试题/收集/可能导致网络安全和信息泄漏。(5)、还有一些简单的从网上下载的WEB服务器.没有过多考虑到一些安全因素.不能用作商业应用。因此，不管是配置服务

器.还是在编写网站程序时都要注意系统的安全性。尽量堵住任何存在的漏洞.创造安全的环境。

二、网站程序安全问题及对策

电子商务网站程序的安全是许多企业忽视的问题，也是严重导致企业信息泄漏的最主要的途径之一。

1、代码漏洞安全问题。

产生这种漏洞的主要原因是网站程序代码编写的不完善造成的.而这种不完善的代码极有可能会暴露网站的数据库或后台管理等重要的安全信息(下文均以ASP为例)。

- (1)、数据库连接字串的某些错误导致WEB服务器错误提示，而这些错误提示中可能会含有数据库或表等重要信息。
- (2)、企业后台管理程序中只有主程序要求管理员的身份信息，而其它管理页面却忽视了身份验证信息，这种疏忽使非法用户可能通过直接输入后台的某个管理页面的形式进入到后台管理中去，如果正好有管理员密码修改的页面出现此问题，/百考试题/收集/则会导致网站后台的完全暴露。
- (3)、对页面参数不作任何判定导致所谓的SQLInjection，即SQL注入从而泄漏用户信息。这种安全漏洞是2004年以来网站信息安全的最大隐患，而国内许多电子商务网站并没有采取相应的安全措施，导致电子商务网站很容易被攻破。

2、后台管理程序文件的安全问题。

现在大多数企业采用后台管理的方式对电子商务网站进行管理，电子商务网站后台的入口安全是很多企业忽视的问题。比如许多电子商务网站后台入口通常会采用Admin.asplogin.asp、logout.asp等常见形式.也有的网站竟然在网面上链接出管理入口，这样，非法用户很容易就能找到网站的后台管理入口，成为电子商务网站安全的重大隐患对于以上安全问题的解决方法是更改网站的后台入口路径.最好是设定一个不易被猜解到的目录和文件名，同时尽可能不要

在前台页面上暴露出后台的管理入口。/百考试题/收集/弱口令和口令加密安全问题。尽管大多数企业认识到了口令的安全问题，但还是有不少的企业忽视了这个问题。(1)、网站管理口令安全问题。弱口令问题。有些管理员为了记忆方便，会以Admin、Admin888managerwebmaster等作为管理员的用户名。同样，也有用AdminAdmin88812345888888等来作为管理员密码，数据库以sA为用户名，留空密码等，这些弱口令是很容易被黑客猜测到的。明文密码问题。很多企业的管理员密码都采用明文来保存，这样的明文密码是最不安全的因素之一，通过SQL注入很容易就能猎取数据库中的明文密码。简单口令加密问题。一些网站设计人员有时只是对口令进行简单的对称加密，这种经过简单的对称加密密文用现在的Pc机器可以在较短的时间内解密成明文，因此也是不可取的。(2)、网站管理口令安全策略。杜绝使用弱口令，以避免安全隐患，可以采用字母数字符号字符，并超过8位以上的密码。强制对所有用户密码加密，最好采用非对称加密或采用不可逆的运算，如使用32位的MD5码。F8F8" 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