

实战型电子商务系列 “十二五” 规划教材

电子商务网站建设与维护

电子商务网站

后期维护

项目 7



项目三 静态网站开发基础

项目概述

建立电子商务网站并不是最终目的，而仅仅是电子商务网站运营的开端。首先，从安全角度来讲，没有安全就没有交易，没有交易也就没有电子商务。其次，网站运营初期，由于在客户群体中的知名度较低，需要对网站进行宣传推广和营销管理以及综合维护和信息更新。本项目将结合具体案例介绍如何做好电子商务网站安全管理以及企业网站信息的维护。

学习目标

能力目标

- 了解电子商务网站面临的安全隐患；
- 了解ASP网站的常见漏洞及其防范对策；
- 熟悉网站运营与管理的内容。

知识目标

- 了解常见流量统计系统；
- 掌握网站流量指标含义；
- 了解可信网站的验证步骤。

目录

Contents

案例一 北方虹光商贸网站安全管理

案例二 企业网站的维护与管理



案例1 北方虹光商贸网站安全管理

(一) 案例详解

以下是北方虹光商贸企业网站人才频道的后台，由于网站没有进行非法字符过滤，存在漏洞，所以很容易被人用SQL注入的方法进入后台管理页面。如图7-1所示，在管理员和密码文本框中分别输入一串字符 “'or'” ，点击 “登录” 按钮，轻松进入了系统后台，如图7-2所示。

=== 人才招聘管理员登录 ===

管理员:

密 码:

招聘信息管理
应聘人员管理
更改密码
退出登录



共有[6]条招聘信息 以下是[1~6]条

NewsID	标 题	发布日期	- 删除 -
44	大学毕业生	[2012-2-2 12:19:16]	[删除]
43	工程技术人员	[2012-2-2 12:18:19]	[删除]
42	高管人员	[2012-2-2 12:09:33]	[删除]
39	保安	[2006-2-17 17:42:30]	[删除]
38	微机操作人员	[2006-2-17 17:42:06]	[删除]
37	网络维护人员	[2006-2-17 17:41:37]	[删除]

[发布招聘信息]

案例1 北京博导前程信息技术有限公司官方网站

(一) 案例详解

本案例通过介绍北京博导前程信息技术有限公司官方网站的建设过程，包含网站策划、样式规划、内容添加、优化等层面，剖析动态网站建设全过程。



任务一 防止SQL注入

1. 常见ASP网站漏洞

用户名 密码

一般程序在验证中会用到类似以下的SQL语句：

```
username=request.form("username")
```

```
pass=request.form("password")
```

```
sql="select * from users where username='"&username&"'and pass='"&pass &"'"
```

```
If not rs.bof and not rs.eof then
```

```
    ' 查找到记录，表示这是合法用户，允许其进入系统
```

```
Else
```

```
    ' 没有查找到记录，表示用户名或密码有误，不允许进入系统。
```

```
End if
```

此时，只要构造一个特殊的用户名和密码，如：' or '，就可以进入本来没有特权的页面。把username=' or '和pass=' or '代入上面那个语句，结果如下：

```
sql="select * from users where username=' 'or' ' and pass=' ' or ' '"
```

2. 非法字符过滤

【例7-1】字符过滤函数。

该函数用来处理客户提交的文本，将其中的特殊字符替换为实体字符，从而达到防范SQL注入的目的。

```
Function myReplace(myString)
    myString=Replace(myString,"&","&amp;")      ' 替换&为字符实体
    &amp;
    myString=Replace(myString,"<","&lt;")        ' 替换<
    myString=Replace(myString,">","&gt;")        ' 替换>
    myString=Replace(myString,chr(13),"<br>")    ' 替换回车符
    myString=Replace(myString,chr(32),"&nbsp;")    ' 替换空格符
    myString=Replace(myString,chr(9)," &nbsp; &nbsp; &nbsp; &nbsp;")
    ' 替换Tab符
    myString=Replace(myString,chr(39),"&acute;")  ' 替换单引号
    myString=Replace(myString,chr(34),"&quot;")    ' 替换双引号
    myReplace=myString                          ' 返回函数值
End Function
```

案例1 企业网站新闻模块开发

任务二 防止 mdb数据库可能被下载的漏洞

在用Access做后台数据库时，如果有人通过各种方法知道或者猜到了服务器的Access数据库的路径和数据库名称，那么他就能够下载这个Access数据库文件，这是非常危险的。

例如，如果你的Access数据库user.mdb放在虚拟目录下的database目录下，那么有人在浏览器地址栏中输入http://网站url/database/ user.mdb，即可下载user.mdb。解决方法:是为数据库文件名称起个复杂的非常规的名字，并把它放在几层目录下。例如2012d34ksfsl718f.mdb，把它放在如./rhghf/i67/的几层目录下，这样黑客要想通过猜的方式得到你的Access数据库文件就难上加难了。

(二) 相关术语

所谓SQL注入，就是通过把SQL命令插入到Web表单递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令。

(三) 案例分析

由于针对网站的网络访问控制措施被广泛采用，且一般只开放HTTP等必要的服务端口，因此黑客已经难以通过传统网络层攻击方式（查找并攻击操作系统漏洞、数据库漏洞）攻击网站。然而，Web应用程序漏洞的存在更加普遍，随着Web应用技术的深入普及，Web应用程序漏洞发掘和攻击速度越来越快，基于Web漏洞的攻击更容易被利用，已经成为黑客首选。据统计，现在对网站成功的攻击中，超过7成都是基于Web应用层，而非网络层。如上面的网站被SQL注入的例子就是一个很好的说明。

目录

Contents

案例一 北方虹光商贸网站安全管理

案例二 企业网站的维护与管理



案例2 企业网站的维护与管理

(一) 案例详解

【例7-2】系统出错——卓越上千元图书只要25元。

“昨晚卓越网上的书25元随便买，有谁买了吗？”“快抢啊，几千块的书只要25元”……昨日凌晨，包括重庆、上海、北京在内的网友不断在泡泡网、开心网等论坛上发出上述帖子。一套全19册《宋元明清书目题跋丛刊》的商品说明中显示，其市场价为4600元，卓越网当晚价格标为25元，后面还提示“为您节省4575元”，而超级VIP价则仅为23.75元。据悉，当晚有大量来自上海、北京、天津等地的网友抓住了“机会”。

大量上千元的图书只卖25元，难到天上会掉馅饼？天亮后正等着收货的网友，却等来了卓越方面退单的通知。（资料转自新浪网2009-12-25）

案例1 企业网站新闻模块开发

任务一 网站信息的维护

网站的更新包括以下三个方面：

第一，维护新闻栏目。网站的新闻栏目是客户了解企业的门户，其应将企业的重大活动、产品的最新动态、企业的发展趋势、客户服务措施及时、真实地呈现给客户，让新闻栏目成为网站的亮点，以此吸引更多的客户前来浏览、交易。

第二，维护商品信息。商品信息是电子商务网站的主体，随着外在条件的变化，商品的信息(如商品的价格、种类、功能等)也在不断地变化，网站必须追随其变化，不断地对商品信息进行维护更新，反映商品的真实状态。

第三，为保证网站中的链接通畅，网站的维护人员要经常对网站所有的**网页链接进行测试**，保证各链接正确无误。

案例1 企业网站新闻模块开发

任务二 网站的在线交易管理

在线交易管理可以分为购物车管理、订单管理等多个方面。

在线购物车管理:应对用户正在进行的购买活动进行实时跟踪,从而使管理员能够看到消费者的购买、挑选和退货的全部过程,并实时监测用户的购买行为,纠正一些错误或不当事件的发生。

订单信息管理:也是网上销售管理的一个不可缺少的部分,要对网上全部交易产生的订单进行跟踪管理。管理员可以浏览、查询、修改订单,对订单/合同进行分析,追踪从订单发生到订单完成的全过程,比如目前的各订单处理状态如何,有多少新订单进来,要不要打印出订货单,订单出货有没有设定,以及进行在线清款与顾客退货等相关交易的处理等等。

案例1 企业网站新闻模块开发

任务三 网站统计管理

电子商务网站访问量统计是电子商务网站的一个重要组成部分。

- 通过对访问量数据的统计与分析，可以找出网站的优势与不足，从而对网站进行相应的修改，更好地实现网站的建设目标；
- 可以根据数据变化规律和趋势随时调整网站的发展方向；
- 有助于选择更合适的网站宣传推广手段。

(1) 统计网站使用率

(2) 统计新会员购物比率、会员总数、所有会员购物比率、复购率、转化率。概括性分析会员购物状态，重点在于本周新增了多少会员，新增会员购物比率是否高于总体水平。如果你的注册会员购物比率很高，那引导新会员注册不失为提高销售额的好方法。

(3) 比对每日运营数据。

案例1 企业网站新闻模块开发

(二) 相关术语

1. 网站使用率

网站使用率包括IP、PV、平均浏览页数、在线时间、跳出率、回访者比率、访问时间比率。实际上，这些最基本的每项数据提高起来都不容易，意味着要不断改进每一个发现问题的细节，不断去完善购物体验。

2. 每日运营数据

每日运营数据包括总订单、订单有效率、总销售额、毛利润、毛利率、下单转化率、付款转化率、退货率。通过每日、每周的数据汇总，重点指导运营内部的工作，如产品引导、定价策略、促销策略、包邮策略等。所有的问题，在运营数据中都能够找到答案。

3. 会员复购率

会员复购率包括1次购物比例、2次购物比例、3次购物比例、4次购物比例、5次购物比例、6次购物比例；转化率体现的是B2C的购物流程、用户体验是否友好，可以称为外功，复购率则体现B2C整体的竞争力，绝对是内功，这包括知名度、口碑、客户服务、包装、发货单等每个细节，好的电子商务网站复购率能做到90%，没有复购率的网站没有前途

一、电子商务网站的安全隐患与安全需求

二、电子商务网站安全措施及分析

三、网站安全面临的主要问题及解决

四、网站防范对策

五、电子商务网站运营与维护

六、网站流量数据统计与分析

模块二 相关知识

一、电子商务网站的安全隐患与安全需求

1. 电子商务网站面临的安全隐患

(1) **信息的截获和窃取**。如果采用加密措施不够，攻击者通过互联网、公共电话网在电磁波辐射范围内安装截获装置或在数据包通过网关和路由器上截获数据，获取机密信息或通过对信息流量、流向、通信频度和长度分析，推测出有用信息如消费者的银行账号、密码以及企业的商业机密等，从而破坏信息的机密性。

(2) **信息的篡改**。当攻击者熟悉网络信息格式后，通过技术手段对网络传输信息中途修改并发往目的地，破坏信息完整性。

(3) **信息假冒**。当攻击者掌握网络信息数据规律或解密商务信息后，假冒合法用户或发送假冒信息欺骗其他用户。如钓鱼网站就是指不法分子利用各种手段，假冒真实网站的URL地址以及页面内容，以此来骗取用户银行或信用卡账号、密码等私人资料。

(4) **交易抵赖**。交易抵赖包括多方面，如发信者事后否认曾发送信息、收信者事后否认曾收到消息、购买者下了订货单不承认、商家卖出的商品因价格差而不承认原有的交易等。

模块二 相关知识

一、电子商务网站的安全隐患与安全需求

2. 电子商务网站安全需求

(1) **保密性**。传统贸易是通过可靠的通信渠道发送商业报文来达到保守机密的目的，而电子商务网站如果没有采取相应的安全措施，就很有可能导致一些敏感的商业信息被泄露。

(2) **隐私性**。因为想在不提供个人信息的前提下参与电子商务活动几乎是不可能的事。而这些个人信息如果被泄露，就必然会破坏到个人隐私。

(3) **正确性和完整性**。

(4) **不可抵赖性**。

模块二 相关知识

二、电子商务网站安全措施及分析

(1) 防病毒技术。反病毒技术主要包括预防病毒、检测病毒和消毒等3种技术：

①预防病毒技术，它通过自身常驻系统内存优先获得系统的控制权，监视和判断系统中是否有病毒存在，进而阻止计算机病毒进入计算机系统和对系统进行破坏。这类技术有加密可执行程序、引导区保护、系统监控与读写控制等；

②检测病毒技术，它是通过对计算机病毒的特征来进行判断的技术，如自身校验、关键字、文件长度的变化等；

③消毒技术，它通过对计算机病毒的分析，开发出具有删除病毒程序并恢复原文件的软件。

(2) 防火墙。

(3) 漏洞扫描。

模块二 相关知识

三、网站安全面临的主要问题及解决

具体的解决方法如下。

- (1) 建立主动的安全检测机制。
- (2) 进行有效的入侵防护。
- (3) 针对网站安全问题，建立及时响应机制。

四、网站防范对策

- (1) 天天关注你负责的网站。
- (2) 定期备份数据库和供下载的文档。
- (3) 密码要健壮。后台管理的帐号密码应与管理员个人常用的不同，以防他人从别处得到网站的密码。如果有多个管理员，要保证所有人的密码都是“健壮的”，即不能像“admin, 123456, 生日, 电话”这样容易猜测，必须是数字、字母和符号的组合。

模块二 相关知识

四、网站防范对策

- (4) 网站改版后，如需保留旧版，要记得删除旧版的后台。
- (5) 文件时间一致原则
- (6) 要把数据库扩展名更名为.asa。
- (7) 给用户尽可能少的功能和权限。
- (8) 出错信息越模糊越好，这里的出错信息包括程序的错误信息和对攻击行为的提示信息。
- (9) 访问网站时提示发现病毒，遇到这种情况，首先应该马上替换掉染毒页面，然后按应对非法入侵的方法处理。
- (10) 定期修改密码。

模块二 相关知识

五、电子商务网站运营与维护

1. 网站运营管理内容

在网站运营过程中，根据网站运营以及发展的需要，还要对网站的功能需要进行优化和扩充，如增加客户关系管理模块（CRM）等，这样才能更好地提升企业的管理水平，为客户提供个性化的服务。

- （1）用户反馈信息管理。
- （2）系统权限管理。
- （3）网站数据的备份与恢复。

2. 电子商务网站运营与维护策略

（1）运营与维护策略。

- ①产品的定位。
- ②网络营销和推广。
- ③品牌信用度的建立。
- ④客户关系的维护。
- ⑤售后服务。
- ⑥物流配送。

模块二 相关知识

五、电子商务网站运营与维护

2. 电子商务网站运营与维护策略

(2) 电子商务运营中的角色及岗位职责。

- ①部门经理岗位职责
- ②商品编辑岗位职责
- ③文案编辑岗位职责
- ④外联推广岗位职责
- ⑤程序维护岗位职责
- ⑥美工编辑岗位职责

3. 可信网站的验证

(1) 什么是“可信网站”的验证？

“可信网站”验证服务（站点卫士）是由中国互联网络信息中心（CNNIC）携手北龙中网联合颁发的验证网站真实身份的第三方权威服务。它通过对域名注册信息、网站信息和企业工商或事业单位组织机构信息进行严格交互审核来认证网站真实信息，并利用先进的木马扫描技术帮助网站了解自身安全情况，是中国数百万网站的“可信身份证”。

模块二 相关知识

五、电子商务网站运营与维护

3. 可信网站的验证

(2) 企业为什么需要可信网站的验证服务？

“可信网站”验证服务，将由网站付费安装一个“可信网站”的第三方认证标识，所有网民都可以通过点击网站页面底部的“可信网站”标识确认企业的真实身份。“可信网站”验证服务通过对企业域名注册信息、网站信息和企业工商登记信息进行严格交互审核来验证网站真实身份。通过认证后，企业网站就进入CNNIC运行的国家最高目录数据库中的“可信网站”子数据库中，从而提高网站本身的可信度

NET 中网

首页 Home 产品与服务 Products & Services 帮助与支持 Help 合作伙伴 Partners 会员中心 Member Center 公共事务 Public affairs 关于中网 About Us

掌商搜索2.0版震撼上市!!!

便捷高效的网络商务人士必备神器

网站、域名、网址信息查询 移动搜索 热门站点/软件推荐

高效的商业信息搜索 最全面的域名网址注册信息查询 最靠谱的网站身份信息查询 贴心的手机导航和热门软件推荐

国家网络目录数据库收录信息查询

请输入搜索内容...

通用网址 无线网址 可信网站验证

到期删除列表: 通用网址 无线网址

国家最高层次网络目录数据库，由中国互联网信息中心建立并维护。

中网可信网站权威数据库查询

请输入搜索内容...

按单位名称查询 按网站名称查询 按网站域名查询 按可信编码查询

中国最大、应用最广泛的网站可信身份第三方权威数据库。

动态公告 more

- 必应搜索无缝对接中网“可信网站”验证
- 傲游云浏览器融合中网“可信网站”验证
- 毛伟董事长当选中国互联网协会副理事长
- 中国（上海）知识产权发展高峰论坛...
- 掌商搜索客户端（wap.cn）2.0版已正...

申请 可信网站，被可信网站权威数据库收录 立即申请

模块二 相关知识

五、电子商务网站运营与维护

3. 可信网站的验证

(3) “可信网站”验证服务功能。

验证网站真伪，可有效防范钓鱼、仿冒网站；
权威机构验证，增强中小企业网站可信性；
全天木马扫描，每日及时通知；
享受反钓鱼联盟准成员待遇。

(4) 验证注册。

- “可信网站”验证服务申请者需要提交以下资料：
- 申请者为企业的，需提交营业执照副本复印件；
- 申请者为非企业的，需提供组织机构代码证复印件；
- “可信网站”注册申请书原件；
- 经办人的身份证明复印件。

通过上述审核，申请单位即可以获得“可信网站”验证服务，并获得“可信网站”验证标识。

NET 中网

首页 Home 产品与服务 Products & Services 帮助与支持 Help 合作伙伴 Partners 会员中心 Member Center 公共事务 Public Affairs 关于中网 About Us

掌商搜索2.0版震撼上市!!!

便捷高效的 掌商搜索 网络商务人士必备神器

网站、域名、网址信息查询 移动搜索 热门站点/软件推荐

高效的商业信息搜索 最全面的域名网址注册信息查询 最靠谱的网站身份信息查询 贴心的手机导航和热门软件推荐

国家网络目录数据库收录信息查询 中网可信网站权威数据库查询 动态公告 more

请输入搜索内容 请输入搜索内容

通用网址 无线网址 可信网站验证 按单位名称查询 按网站名称查询 按网站域名查询 按可信编码查询

到期删除列表: 通用网址 无线网址

国家最高层次网络目录数据库, 由中国互联网络信息中心建立并维护。

中国最大、应用最广泛的 网站可信身份第三方权威数据库。

必应搜索无缝对接中网“可信网站”验证 傲游云浏览器融合中网“可信网站”验证 毛伟董事长当选中国互联网协会副理事长 中国(上海)知识产权发展高峰论坛... 掌商搜索客户端(wap.cn)2.0版已正...

申请 可信网站, 被可信网站权威数据库收录 立即申请

模块二 相关知识

六、网站流量数据统计与分析

3. 常见流量统计系统介绍



The image shows the homepage of CNZZ (China Network Zhanzhi) Data Expert. The header features the CNZZ logo and the text '数据专家' (Data Expert) and 'www.cnzz.com'. Below the header, there is a statistics summary: '注册用户 1895270人; 统计站点 3262739家; 每天160万网站使用CNZZ, 日统计量50亿PV, 一周覆盖90%上网用户。' To the right of this summary are links for '统计演示' (Statistics Demo) and '马上注册' (Register Now). Below the summary are four main service buttons: '站长统计' (Website Owner Statistics), '全景统计' (Full View Statistics), 'AD 广告统计' (AD Advertising Statistics), and '数据中心' (Data Center). The main content area features a large orange banner for '新版全景统计盛装发布' (New Version Full View Statistics Grand Release). The banner includes the text '数十亮点更新 玩转网站分析' (Dozens of highlights updated, playing with website analysis), '立即开始60天 免费试用' (Start immediately for 60 days free trial), and '为企业、电商网站提供高级网站流量统计分析' (Provide advanced website traffic analysis for enterprises, e-commerce websites). To the right of the banner is a 'NEW' badge and a screenshot of the CNZZ dashboard. Below the banner is a navigation bar with four tabs: 'CNZZ站长统计', 'CNZZ全景统计' (which is currently selected), 'CNZZ精准广告', and 'CNZZ数据中心'. At the bottom, there is a '申请步骤' (Application Steps) section with a flow: '注册成为CNZZ会员' (Register as a CNZZ member) → '登录获取代码' (Login to get code) → '加载代码' (Load code) → '统计数据' (Statistics data).

CNZZ 数据专家
www.cnzz.com

注册用户 **1895270**人; 统计站点 **3262739**家;
每天**160万**网站使用CNZZ, 日统计量**50亿**PV, 一周覆盖**90%**上网用户。

[统计演示](#) [马上注册](#)

站长统计 **全景统计** **AD 广告统计** **数据中心**

新版全景统计盛装发布

数十亮点更新 玩转网站分析 **立即开始60天 免费试用**

为企业、电商网站提供高级网站流量统计分析

CNZZ站长统计 CNZZ全景统计 CNZZ精准广告 CNZZ数据中心

申请步骤: 注册成为CNZZ会员 → 登录获取代码 → 加载代码 → 统计数据

模块二 相关知识

六、网站流量数据统计与分析

4. 流量统计系统的使用

网站名称:	<input type="text"/>
网站首页:	<input type="text" value="http://"/>
域名列表:	<div><div></div></div>
网站类型:	请选择站点类型 ▼ ▼
网站地区:	请选择地区 ▼ ▼
开通统计:	<input checked="" type="checkbox"/> 打勾表示开通
网站简介:	<div><div></div></div> 添加

注册成功后，添加要统计的站点名称、网址和相关简介

文字样式

<script src="http://s20.cnzz.com/stat.php?id=3189342&web_id=3189342" language="JavaScript"></script>


复制到剪贴板

样例:
[站长统计](#)

图片样式1

<script src="http://s20.cnzz.com/stat.php?id=3189342&web_id=3189342&show=pic"

复制到剪贴板

样例:


登录获取代码

六、网站流量数据统计与分析

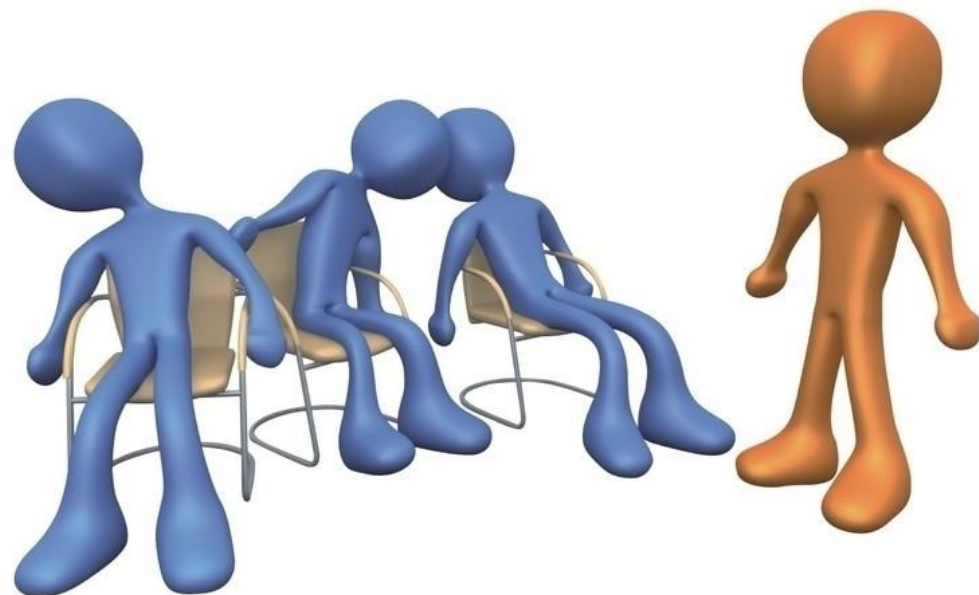
(3) 加载代码。将选择好的样式代码放到网页的结尾部分，即您要跟踪的每个网页标记</body> 之前。

(4) 统计数据。登录后，进入站点列表页，点击“查看统计报表”按钮，即可查看该站点统计数据



结束

End



《《 休息，休息一下

总有一些时候

你需要寻找灵感或者协助