# [Web系统安全性攻击与防护总结报告]信息安全课程设计

来源：网络 作者：静谧旋律 更新时间：2025-02-14

*第一篇：[Web系统安全性攻击与防护总结报告]信息安全课程设计郑州轻工业学院本科Web系统安全性攻击与防护总结报告设计题目：学生姓名：系别：国际教育学院专业：互联网班级：学号：指导教师：Web系统安全性攻击与防护(SQL注入与防护)XXX...*

**第一篇：[Web系统安全性攻击与防护总结报告]信息安全课程设计**

郑州轻工业学院本科

Web系统安全性攻击与防护总结报告

设计题目：学生姓名：系

别：国际教育学院专

业：互联网班

级：学

号：指导教师：

Web系统安全性攻击与防护(SQL注入与防护)XX

XX XX XX

2025 年

07 月 日

目录

一、课程设计的目的和意义........................................................................................3

二、sql注入分析........................................................................................................3 2.1 sql注入的原理.................................................................................................3 2.2 sql注入攻击的方式.........................................................................................3 2.2.1构造参数攻击.........................................................................................3 2.2.2转义字符类型的攻击.............................................................................4 2.2.3Union查询攻击.......................................................................................4 2.2.4注释符攻击.............................................................................................5

三、sql注入实例分析................................................................................................5 3.1系统核心代码...................................................................................................5 3.2注入测试和分析...............................................................................................6 3.2.1注入测试.................................................................................................6 3.2.2注入攻击过程及分析.............................................................................8

四、sql注入的防范措施............................................................................................10 4.1 防范措施1(对参数进行强制类型转换)......................................................10 4.2 防范措施2（类型判断）.............................................................................12

五、密码用MD5加密存储和验证...........................................................................14 5.1加密的必要性分析.........................................................................................14 5.2加密核心代码，登录验证核心代码.............................................................14 5.2.1加密核心代码.......................................................................................14 5.2.2登录验证核心代码...............................................................................15

六、服务器目录权限配置..........................................................................................16 6.1、权限分配原则分析......................................................................................16 6.2、具体权限分配过程......................................................................................16

七、总结......................................................................................................................18

一、课程设计的目的和意义

网络技术随着信息化技术的发展，网络技术得到了广泛的应用，其中Web成为主流的网络和应用技术，但随之而来的就是网络安全问题的出现。网络安全问题目前已成为世界范围内不容忽视的问题。在研究与实践的基础上，详细总结网络攻击方法的原理及其有针对性的防护技术，对加强网络安全，实现web服务器安全有重要意义。

二、sql注入分析

2.1 sql注入的原理

SQL 注入是一种攻击方式，在这种攻击方式中，恶意代码被插入到字符串中,然后将该字符串传递到程序执行的SQL 语句中构成攻击者想执行的任意SQL语句，分析服务器返回的信息获得有关网站或服务器的敏感信息，进一步获得非法的信息和权限。

利用WEB应用对用户输入验证设计上的疏忽，或验证的不严格，从而使用户输入的数据中包含对某些数据库系统有特殊意义的符号或命令，让WEB应用用户有机会直接对后台数据库系统下达指令，实施入侵行为。SQL注入的产生主要是由动态字符串构建和不安全的数据库配置产生，其中动态字符串构建主要是由不正确的处理转义字符、不正确的处理类型、不正确的处理联合查询、不正确的处理错误和不正确的处理多次提交构成。不安全的数据库配置产生主要是由默认预先安装的用户、以root，SYSTEM或者Administrator权限系统用户来运行和默认允许很多系统函数（如xp\_cmdshell，OPENROWSET等）构成。

2.2 sql注入攻击的方式

2.2.1构造参数攻击

如果一个恶意用户提供的字段并非一个强制类型,或者没有实施类型强制,就会发生这种形式的攻击。当在一个SQL语句中使用一个数字字段时,如果程序员没有检查用户输入的合法性(是否为数字型)就会发生这种攻击。例如: Statement:=“SELECT\*FROM data WHERE id=”+a\_variable+“;”

从这个语句可以看出,作者希望a\_variable是一个与“id”字段有关的数字。不过,如果终端用户选择一个字符串,就绕过了对转义字符的需要。

2.2.2转义字符类型的攻击

Web应用程序开发时没有对用户的输入进行转义字符过滤时,就会发生这种形式的注入式攻击,它会被传递给一个SQL语句.这样就会导致恶意用户对数据库上的语句实施操纵。例如,下面的这行代码就会演示这种漏洞:

Statement:=“SELECT\*FROM users WHERE name=\'”+userName+“\';”

此段代码的设计目的是将一个特定的用户从其用户表中取出,但是,如果用户名被一个恶意的用户用一种特定的方式伪造,这个语句所执行的操作可能就不仅仅是应用程序开发者所期望的那样例如,将用户名变量(即username)设置为:

a′or′1′=1′,此时原始语句发生了变化:

SELECT\*FROM users WHERE name=′a′OR′1′=′1′;

如果这种代码被用于一个认证过程,那么这个例子就能够强迫选择一个合法的用户名,因为赋值

′1′=′1永远是真。

在一些特定的SQL服务器上,如在SQL Server中,任何一个SQL命令都可以通过这种方法被注入,包括执行多个语句。

2.2.3Union查询攻击

Union查询动机是绕过验证或者提取数据。攻击者在查询语句中注入Union SELECT语句,并且因为用户控制“SELECT语句”的内容,攻击者可以得到想要的信息。Union查询SQL注入测试。

假设我们有如下的查询:

SELEC Name,Psw,Tel FROM Users WHERE Id=$id然后我们设置id的值为:

$id=1UNION ALL SELECT bank CardNumber,1,1 FROM BankCardTable

那么整体的查询就变为:

SELECT Name,Psw,Tel FROM Users WHERE Id=1 UNION ALL SELECT bankCardNumber,1,FROM BankCarTable

显然这样就能得到所有银行卡用户的信息。

2.2.4注释符攻击

使用注释通常可以使攻击者绕过验证。SQL在查询中支持注释,如,--、#等。通过注入注释符,恶意用户或者攻击者可以毫不费力的截断SQL查询语句。例如,对于查询语句SELECT\*FROM users WHERE usermame=uname and Password=psw,如果恶意用户输入参数uname的值为admin--,Password的值为空,那么查询语句变为SELECT\*FROM users WHERE usermame=admin and Password=,也就SELECT\*FROM users WHERE usermame=admin。这就使得恶意用户不用提供密码就可以通过验证。

三、sql注入实例分析

3.1系统核心代码

显示文章内容的主要代码：

《%\'

#####查询数据模块开始

###%> 《%function query()id=request.QueryString(“id”)\'为了测试此处没有对参数进行任何过滤和合法性分析 set rs=conn.execute(“select \* from news where id=”&id)while not rs.eof response.Write(“发布者：”&rs(“adder”)&“

发布时间：”&rs(“time”)&“

标题：”&rs(“title”)&“

[内容：]

”&rs(“content”))rs.movenext wend call first()end function%> 《%\'

#####查询数据模块结束

###%>

3.2注入测试和分析

3.2.1注入测试

现在进行注入测试： 首先看正常显示文章截图：

图（1）

1、在地址后面加一个单引号 \' 看返回结果是否正常

图（2）

返回系统查询报错，说明可能存在注入漏洞。

2、继续测试以确认是否真正存在注入漏洞，在地址后面加上and 1=1 查看返回结果是正常。

图（3）

显示正常没有异常。再接着把and 1=1 改为 and 1=2 看返回结果是否异常。

图（4）

返回空白出现异常。

3、通过上面的注入测试，可以确定该网站一定存在SQL注入漏洞。

3.2.2注入攻击过程及分析

下面使用构造参数攻击：

构造语句：

?action=query&id=54 and exists(select \* from \_admin)发现返回正常，那么可以确定数据库一定存在表 \_admin

下面构造：（猜测字段）

?action=query&id=54 and exists(select un,pw from \_admin)返回结果造成说明sql执行正确,那么数据表\_admin里一定存在 un pw 两个字段

下面继续构造语句：(猜测字用户名)?action=query&id=54 and exists(select \* from \_admin where un =\'admin\')返回结果正常,至此已经获得了一个管理员用户名admin

下面构造：(猜测密码)?action=query&id=54 and exists(select \* from \_admin where pw=\'admin\')返回结果正常,至此经获得了一个管理员用户名admin 密码是 admin 下面点击首页的登录：

图（5）

用得到的用户名 admin 和密码 admin登录

图（6）

图（7）

成功进入网站后台管理：

图（8）

到这里一个成功的注入过程就完成了，成功的到了网站管理员的用户名和密码。

四、sql注入的防范措施

4.1 防范措施1(对参数进行强制类型转换)核心代码：

《%\'

#####查询数据模块开始

###%> 《%function query()id=cint(request.QueryString(“id”))\'使用cint函数把接收的值强制转为整型 set rs=conn.execute(“select \* from news where id=”&id)while not rs.eof 下面通过再次注入检测看效果： 1.在链接后加单引号 \'

图（9）

提示类型转换失败。

2.在链接后面加 and 1=1

图（10）

仍然提示类型转换失败。3.在链接后面加 and 1=2

图（11）

还是提示类型转换失败。

从此看来是不能注入的。说明实施强制类型转换成功的防治了SQL注入。

4.2 防范措施2（类型判断）

核心代码：

《%\'

#####查询数据模块开始

###%> 《%function query()if isnumeric(request.QueryString(“id”))then \'这里判断参数是否是一个数字如果不是提示非法 id=request.QueryString(“id”)else response.write(“参数非法”)response.end()end if set rs=conn.execute(“select \* from news where id=”&id)while not rs.eof 下面通过再次注入检测看效果： 1.在链接后加单引号 \'

图（12）

提示参数非法。

4.在链接后面加 and 1=1

图（13）

仍然提示参数非法。5.在链接后面加 and 1=2

图（14）

还是提示参数非法。

从此看来是不能注入的。说明实施强类型判断成功的防治了SQL注入。

五、密码用MD5加密存储和验证

5.1加密的必要性分析

从上面可以看到通过SQL注入攻击者很容易就得到用户的密码，如果密码没有经过加密那么攻击者就可以使用该密码登录，如果密码是加密保存在数据库的，而且登录验证是也是加密验证，那么攻击者得到的就是加密的字符串，如果攻击者不能破解该字符串那么攻击者是无法登陆的。这样给网站安全又加上了一道防护。

5.2加密核心代码，登录验证核心代码

5.2.1加密核心代码

《%\'

######添加用户模块开始

######%> 《%function adduser()if request.QueryString(“level”)=“\" then exit function username=request.Form(”username“)password=md5(trim(request.Form(”password“)))\'添加用户时将用户的密码md5加密后保存到数据库

level=cint(request.QueryString(”level“))if level=0 then set rs=conn.execute(”select username from \_user where username=\'“&username&”\'“)set rs2=conn.execute(”select un from \_admin where un=\'“&username&”\'“)if(rs.eof and rs.bof)and(rs2.eof and rs2.bof)then conn.execute(”insert into \_user(username,password)values(\'“&username&”\' ,\'“&password&”\')“)response.Write(”alert(\'添加成功！\');window.close();“)rs.close else

5.2.2登录验证核心代码

《%\'

#####验证登录据模块开始

###%> 《%function checklogon()username=request.Form(”username“)password=md5(trim(request.Form(”password“)))\'登录时先将用户的密码md5加密后与数据库里面的对比 set rs=conn.execute(”select \* from \_user where username=\'“&username&”\' and password=\'“&password&”\'“)set rs2=conn.execute(”select \* from \_admin where un=\'“&username&”\' and pw=\'“&password&”\'“)if(rs.eof and rs.bof)and(rs2.eof and rs2.bof)then

response.Write(”alert(\'用户名或密码错误\');window.location=\'?action=showlogon\';\")rs.close rs2.close else

六、服务器目录权限配置

6.1、权限分配原则分析

对一个网站来说除了上传文件的目录能写入文件以外其它的所有目录均不能写入文件，而且上传文件的目录不能有网页程序的执行权限，这样可以保证即使黑客成功上传程序到上传目录那么也是不执行的。

6.2、具体权限分配过程

利用NTFS文件系统的权限分配功能：

1、首先在文件夹安全选项里面把iis帐号加到网站根目录中。然后指定其只能读取，不能写入文件，那么整个网站里面的所有目录都不能写入文件了。

2、下面接着给上传文件目录加上写人的权限。

至此已经完成了除了上传文件目录可以写入文件其它目录均不能写入文件。

3、接着配置上传目录的运行权限使其不能运行网页程序。

至此完成了权限分析中的所有需求。

七、总结

本次课程设计对网站SQL注入攻击及网站安全技术进行了比较详细地分析，通过本次课程设计使我掌握了对SQL注入攻击漏洞的检测技术和预防SQL注入的手段，而且学会了在IIS和NTFS文件系统环境下安全配置网站的目录权限的技能，了解到信息系统网站中存在的普遍安全漏洞。网站的安全稳定运行，应侧重于预防，不断增强安全意识，采取各种预防措施，才能及时有效地排除安全隐患。

**第二篇：网络信息安全的攻击与防护**

目录

一网络攻击技术.....................................................错误！未定义书签。1.背景介绍...............................................................错误！未定义书签。2.常见的网络攻击技术..........................................错误！未定义书签。1.网络监听.........................................................错误！未定义书签。2.拒绝服务攻击...................................................................................2 3.缓冲区溢出.......................................................................................3

二、网络防御技术................................................................................4 1.常见的网络防御技术..........................................................................4 1.防火墙技术.......................................................................................4 2.访问控制技术...................................................................................4

三、总结...............................................................5错误！未定义书签。一.生活中黑客常用的攻击技术

黑客攻击其实质就是指利用被攻击方信息系统自身存在安全漏洞，通过使用网络命令和专用软件进入对方网络系统的攻击。目前总结出黑客网络攻击的类型主要有以下几种：

1.对应用层攻击。

应用层攻击能够使用多种不同的方法来实现，最常见的方法是使用服务器上通常可找到的应用软件（如SQL Server、PostScript和FTP）缺陷，通过使用这些缺陷，攻击者能够获得计算机的访问权，以及在该计算机上运行相应应用程序所需账户的许可权。

应用层攻击的一种最新形式是使用许多公开化的新技术，如HTML规范、Web浏览器的操作性和HTTP协议等。这些攻击通过网络传送有害的程序，包括Java applet和Active X控件等，并通过用户的浏览器调用它们，很容易达到入侵、攻击的目的。

2.拒绝服务攻击

拒绝服务（Denial of Service, DoS）攻击是目前最常见的一种攻击类型。从网络攻击的各种方法和所产生的破坏情况来看，DoS算是一种很简单，但又很有效的进攻方式。它的目的就是拒绝服务访问，破坏组织的正常运行，最终使网络连接堵塞，或者服务器因疲于处理攻击者发送的数据包而使服务器系统的相关服务崩溃、系统资源耗尽。

攻击的基本过程如下：首先攻击者向服务器发送众多的带有虚假地址的请求，服务器发送回复信息后等待回传信息。由于地址是伪造的，所以服务器一直等不到回传的消息，然而服务器中分配给这次请求的资源就始终没有被释放。当服务器等待一定的时间后，连接会因超时而被切断，攻击者会再度传送新的一批请求，在这种反复发送伪地址请求的情况下，服务器资源最终会被耗尽。

被DDoS攻击时出现的现象主要有如下几种。被攻击主机上有大量等待的TCP连接。网络中充斥着大量的无用的数据包，源地址为假。制造高流量无 用数据，造成网络拥塞，使受害主机无法正常和外界通信。利用受害主机提供的服务或传输协议上的缺陷，反复高速地发出特定的服务请求，使受害主机无法及时处理所有正常请求。严重时会造成系统死机。要避免系统遭受Do S攻击，网络管理员要积极谨慎地维护整个系统，确保无安全隐患和漏洞，而针对更加恶意的攻击方式则需要安装防火墙等安全设备过滤DOS攻击，同时建议网络管理员定期查看安全设备的日志，及时发现对系统构成安全威胁的行为。

3.缓冲区溢出

通过往程序的缓冲区写超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其他的指令。如果这些指令是放在有Root权限的内存中，那么一旦这些指令得到了运行，黑客就以Root权限控制了系统，达到入侵的目的；缓冲区攻击的目的在于扰乱某些以特权身份运行的程序的功能，使攻击者获得程序的控制权。

缓冲区溢出的一般攻击步骤为：在程序的地址空间里安排适当的代码——通过适当的地址初始化寄存器和存储器，让程序跳到黑客安排的地址空间中执行。缓冲区溢出对系统带来了巨大的危害，要有效地防止这种攻击，应该做到以下几点。必须及时发现缓冲区溢出这类漏洞：在一个系统中，比如UNIX操作系统，这类漏洞是非常多的，系统管理员应经常和系统供应商联系，及时对系统升级以堵塞缓冲区溢出漏洞。程序指针完整性检查：在程序指针被引用之前检测它是否改变。即便一个攻击者成功地改变了程序的指针，由于系统事先检测到了指针的改变，因此这个指针将不会被使用。数组边界检查：所有的对数组的读写操作都应当被检查以确保对数组的操作在正确的范围内。最直接的方法是检查所有的数组操作，通常可以采用一些优化的技术来减少检查的次数。目前主要有以下的几种检查方法：Compaq C编译器、Purify存储器存取检查等。

二． 生活中常见的网络防御技术

1.常见的网络防御技术

1.防火墙技术 网络安全中使用最广泛的技术就是防火墙技术，对于其网络用户来说，如果决定使用防火墙，那么首先需要由专家领导和网络系统管理员共同设定本网络的安全策略，即确定什么类型的信息允许通过防火墙，什么类型的信息不允许通过防火墙。防火墙的职责就是根据本馆的安全策略，对外部网络与内部网络之间交流的数据进行检查，符合的予以放行，不符合的拒之门外。该技术主要完成以下具体任务：

通过源地址过滤，拒绝外部非法IP地址，有效的避免了与本馆信息服务无关的外部网络主机越权访问；防火墙可以只保留有用的服务，将其他不需要的服务关闭，这样做可以将系统受攻击的可能性降到最低限度，使黑客无机可乘；同样，防火墙可以制定访问策略，只有被授权的外部主机才可以访问内部网络上的有限IP地址，从而保证外部网络只能访问内部网络中的必要资源，使得与本馆信息服务无关的操作将被拒绝；由于外部网络对内部网络的所有访问都要经过防火墙，所以防火墙可以全面监视外部网络对内部网络的访问活动，并进行详细的记录，通过分析可以得出可疑的攻击行为。

防火墙可以进行地址转换工作，使外部网络用户不能看到内部网络的结构，使黑客失去攻击目标。

虽然防火墙技术是在内部网与外部网之间实施安全防范的最佳选择，但也存在一定的局限性：不能完全防范外部刻意的人为攻击；不能防范内部用户攻击；不能防止内部用户因误操作而造成口令失密受到的攻击；很难防止病毒或者受病毒感染的文件的传输。

2.访问控制技术

访问控制是网络安全防范和保护的主要技术，它的主要任务是保证网络资源不被非法使用和非法访问。

入网访问控制为网络访问提供了第一层访问控制。它控制哪些用户能够登录到服务器并获取网络资源，控制准许用户入网的时间和准许他们在哪台工作站入网。用户的入网访问控制可分为三个步骤：用户名的识别与验证、用户口令的识别与验证、用户账号的缺省限制检查。三道关卡中只要任何一关未过，该用户便不能进入该网络。对网络用户的用户名和口令进行验证是防止非法访问的第一道防线。用户注册时首先输入用户名和口令，服务器将验证所输入的用户名是否合法。如果验证合法，才继续验证用户输入的口令，否则，用户将被拒之网络外。用户的口令是用户入网的关键所在。为保证口令的安全性，用户口令不能显示在显示屏上，口令长度应不少于6个字符，口令字符最好是数字、字母和其他字符的混合。

网络的权限控制是针对网络非法操作所提出的一种安全保护措施。用户和用户组被赋予一定的权限。网络控制用户和用户组可以访问哪些目录、子目录、文件和其他资源。可以指定用户对这些文件、目录、设备能够执行哪些操作。我们可以根据访问权限将用户分为以下几类：（1）特殊用户（即系统管理员）；（2）一般用户，系统管理员根据他们的实际需要为他们分配操作权限；（3）审计用户，负责网络的安全控制与资源使用情况的审计。用户对网络资源的访问权限可以用一个访问控制表来描述。

网络应允许控制用户对目录、文件、设备的访问。用户在目录一级指定的权限对所有文件和子目录有效，用户还可进一步指定对目录下的子目录和文件的权限。对目录和文件的访问权限一般有八种：系统管理员权限（Supervisor）、读权限（Read）、写权限（Write）、创建权限（Create）、删除权限（Erase）、修改权限（Modify）、文件查找权限、存取控制权限。一个网络系统管理员应当为用户指定适当的访问权限，这些访问权限控制着用户对服务器的访问。八种访问权限的有效组合可以让用户有效地完成工作，同时又能有效地控制用户对服务器资源的访问，从而加强了网络和服务器的安全性。

三．总结

计算机网络技术的日新月异，为现代人的生活提供了很大的方便。但网络安全威胁依然存在，网上经常报道一些明星的照片泄露，12306账号和密码泄露，一些邮箱的密码泄露，以及经常发生的QQ号被盗等等……这些都会给我们的生活带来麻烦，甚至让我们付出经济代价。因此现在人们对于网络安全的认识也越来越重视，在整体概念上了解黑客的攻击技术和常用工具方法，对于我们防范黑客攻击提供了基本的知识储备。而具体到平时的学习工作中，我们应该养成良好的上网习惯和培养良好的网络安全意识，在平时的工作中应该注意，不要运行陌生人发过来的不明文件，即使是非可执行文件，也要十分小心，不要在不安全的网站上登录一些重要账号，或者不要在网站上记录账号密码。以免造成密码泄露。只要我们在平时上网时多注意，就可以有效地防范网络攻击。

此外，经常使用杀毒软件扫描，及时发现木马的存在。我们应该时刻警惕黑客的网络攻击，从自我做起，构建起网络安全坚实防线，尽可能让网络黑客无孔可入。

**第三篇：信息安全课程设计**

信息系统安全课程设计报告

课题名称：OpenSSL 非对称加密

提交文档学生姓名：提交文档学生学号：

同组 成 员 名 单：指导 教 师 姓 名：

指导教师评阅成绩：指导教师评阅意见：

提交报告时间： 2025年 6 月 10日

1.课程设计目标

了解OpenSSL非对称加密算法的背景知识，并实现加密解密。

2.分析与设计

（1）实现方法：

编程语言为C++语言。

编程方法：根据算法要求编写代码。

（2）利用OpenSSL命令制作生成密钥：

#include

#include

#include

#include

#include

int main()

{

char plain[256]=“啦啦啦啦啦”;

char encrypted[1024];

char decrypted[1024];

const char\* pub\_key=“public.pem”;

const char\* priv\_key=“private.pem”;

printf(“%sn”,plain);int len=strlen(plain);BIO \*pBio = BIO\_new\_file(pub\_key,“r”);if(pBio==NULL){

printf(“failed to open pub\_key file %s!n”, pub\_key);

return-1;

}

RSA\* rsa1= PEM\_read\_bio\_RSA\_PUBKEY(pBio, NULL, NULL, NULL);

if(rsa1==NULL){

printf(“unable to read public key!n”);

return-1;

}

BIO\_free\_all(pBio);int outlen=RSA\_public\_encrypt(len,(unsigned char \*)plain,(unsigned char \*)encrypted, rsa1,RSA\_PKCS1\_PADDING);

printf(“%dn”,outlen);encrypted[outlen]=\'\';printf(“%sn”,encrypted);FILE\* fp=fopen(“out.txt”,“w”);fwrite(encrypted,1,outlen,fp);fclose(fp);pBio = BIO\_new\_file(priv\_key,“r”);if(pBio==NULL){

printf(“failed to open priv\_key file %s!n”, pub\_key);

return-1;

}

RSA \*rsa2 = PEM\_read\_bio\_RSAPrivateKey(pBio, NULL, NULL, NULL);

if(rsa2==NULL){

printf(“unable to read private key!n”);

return-1;

}

BIO\_free\_all(pBio);

outlen=RSA\_private\_decrypt(outlen,(unsigned char \*)encrypted,(unsigned char \*)decrypted, rsa2,RSA\_PKCS1\_PADDING);

}

（3）手动产生公钥：

#include

#include

#include

#include

#include

int main()

{

char plain[256]=“rtre”;

char encrypted[1024];

decrypted[outlen]=\'\';printf(“%sn”,decrypted);return 0;

char decrypted[1024];

const char\* pub\_key=“public2.pem”;

const char\* priv\_key=“private2.pem”;

const int g\_nBits = 1024;

printf(“%sn”,plain);

int len=strlen(plain);RSA \*rsa1 = RSA\_generate\_key(g\_nBits,RSA\_F4,NULL,NULL);

if(rsa1 == NULL)

{

printf(“rsa\_generate\_key errorn”);

return-1;

}

BIO \*pBio = BIO\_new\_file(pub\_key,“w”);

if(pBio == NULL)

{

printf(“BIO\_new\_file %s errorn”, pub\_key);

return-1;

}

PEM\_write\_bio\_RSAPublicKey(pBio,rsa1);

BIO\_free\_all(pBio);

int outlen=RSA\_public\_encrypt(len,(unsigned char \*)plain,(unsigned char \*)encrypted, rsa1,RSA\_PKCS1\_PADDING);

printf(“%dn”,outlen);

encrypted[outlen]=\'\';

printf(“%sn”,encrypted);

FILE\* fp=fopen(“out.txt”,“w”);

fwrite(encrypted,1,outlen,fp);

fclose(fp);

pBio = BIO\_new\_file(priv\_key,“w”);

if(pBio == NULL)

{

printf(“BIO\_new\_file %s errorn”, priv\_key);

return-1;

}

PEM\_write\_bio\_RSAPrivateKey(pBio,rsa1,NULL,NULL,NULL,NULL,NULL);BIO\_free\_all(pBio);outlen=RSA\_private\_decrypt(outlen,(unsigned char \*)encrypted,(unsigned char \*)decrypted, rsa1,RSA\_PKCS1\_PADDING);

decrypted[outlen]=\'\';

printf(“%sn”,decrypted);

return 0;

}

3.总结

RSA是目前最有影响力的公钥加密算法，它能够抵抗到目前为止已知的绝大多数密码攻击，已被ISO推荐为公钥数据加密标准，学习这个算法让我对加密和解密的知识有了更加深入的理解。同时也提高了我的编程能力。每次实现一个算法，都让我对信息安全相关的技术更加有兴趣，原本枯燥的学习变得非常生动有趣。

感谢老师的耐心指导，这门课真的很有意思，老师讲得也很好，让我受益匪浅。

**第四篇：安全案例：电信骨干网DDoS攻击防护解决方案**

近年来，电信数据业务迎来飞速发展，作为经济大省，某省近年来电信数据业务发展迅速，宽带数据业务用户快速增长。然而，伴随着用户数量的增长，电信网络安全问题也频繁发生，其中DDoS攻击情况尤为严重。

该省电信运营商对2025年7月到12月的网络安全事件统计后发现，几个经常受到网络攻击的地市，每月平均受到的网络攻击多达10次以上，2025年9月，某地市IDC受到严重DDoS攻击，攻击流量达到22G，造成城域网、IDC全阻15分钟，对业务造成严重的影响。尝试了多种解决办法，仍然无法从根本上解决问题。

在这种情况下，该省电信迫切需要引入专业安全合作伙伴，建立一整套抵御DDoS流量攻击的系统。为此，省电信研究院对众多安全厂家的异常流量过滤设备进行了评测对比，联想网御的异常流量过滤设备在众多厂家比拼中脱颖而出，性能和功能卓越。同时，联想网御异常流量管理系统在多个省市电信行业的成功应用也获得信息化主管领导的认可，经过多次深入的技术交流，该省电信最终确定了联想网御作为抵御DDoS流量攻击系统建设的合作伙伴。

结合该省电信的安全需求和现网建设情况，充分考虑宽带互联网络高带宽、大流量、要求可靠性高的网络特点，联想网御的技术专家为电信运营商量身定制了异常流量清洗方案：结合电信IDC客户遭受的DDoS攻击情况和僵尸网络发动攻击的特点，技术专家分析认为攻击流量主要来自国外和国内其他运营商网络，另有少部分来自省网内部。因此，系统建设先期在省干出口位置集中式部署，重点防范经由省干入口向地市城域网的攻击。考虑到省干出口链路带宽大，网络位置十分关键。联想网御又为用户设计、采取了目标保护策略——根据需要可以灵活地定义要保护的目标IP地址或者目标IP网段，进行重点检测分析和过滤攻击流量，实现了较强的针对性，同时有效节省了建设投资，同时，根据该省电信用户的网络使用特点，设计采用了8台设备集群旁路部署方式（如图所示），大流量攻击处理能力达到16G，轻松满足了15G大流量攻击处理能力的设计要求，避免了改变正常网络流量的网络路径，同时保证了网络的高可靠性。

某省电信运营商骨干网联想网御异常流量管理系统应用方案

联想网御在用户网络中同时部署流量检测分析设备和异常流量过滤系统，组成一套完整的异常流量管理系统。由流量检测分析设备（Leadsec-Detector）进行采样分析，对流经骨干网的数据流进行分析、统计、报警，确定受攻击的目标IP范围；由异常流量过滤系统(Leadsec-Guard)来牵引到达目标IP的网络流量，过滤攻击流量后将正常流量回注到网络中，通过两者的无缝配合，完成了网络攻击的分析、识别，以及自动清理。

LeadSec-Guard还可支持虚拟化，将单台设备或者集群组虚拟为多个逻辑异常流量过滤系统。因此，系统管理员可以为每个逻辑系统分配相应的管理员进行策略配置、安全审计等独立操作。这将有力地支撑宽带网络运营商拓展安全增值服务，推动安全运营。同时，系统中还配置了Leadsec-Manager管理系统，在实现集中设备配置和管理的同时，提供丰富的报表功能，全面帮助管理员深入掌控网络安全运行情况。

项目完成后，该省干出口链路中异常流量所占用带宽降至总拥有带宽的5％以下，网络安全事件发生概率大大降低，轻了异常流量对该省电信省干网络平台造成的压力，提升了带宽利用率，为IDC、网吧等宽带业务大客户提供了一条安全、畅通的互联网链路，提升了品牌价值，为该省电信创造了竞争优势。

**第五篇：教育信息安全与防护培训心得体会**

教育信息安全与防护培训心得体会范文.DOCX

【珍惜当下，不负遇见】

（本文档共

【

】页/【

1008

】字）

单位

姓名

20XX年X月

教育信息安全与防护培训心得体会

——单位

姓名

20XX年X月

20XX年X月，我通过国培智慧云平台学习了《教育信息安全与防护》系列课程，课程有《教育信息安全管理与防护-教育现代化与教育信息化》《中小学教师网络信息安全防护案例分析-网络信息安全防护案例》《常用信息安全防护技术与实践-教育网络安全分析》等。通过聆听专家的精彩讲解，我感触颇深。

通过学习教育信息安全与防护，使我更加深刻的理解网络信息安全的重要性。网络信息安全是保护个人信息的完整性和保密性的重要条件，只有明白了网络信息安全的基础知识，我们才能更加的了解网络信息安全在如今信息化时代的重要性!

如今信息化的时代，我们每个人都需要跟着时代的步伐，那么我们不缺乏使用电脑信息工具，那么我们需要了解网络的好处和风险，利弊都有，我们需要把弊端降到最低，把利处合理利用，使我们在网络时代不会落后;现在我们每个人的信息都会在网络上面，只是看你如何保护自己的信息呢?你的个人电脑会不会被黑客攻击?你注册的会员网站会不会泄露你的信息呢?等等!所有这些，都可视为网络信息安全的一部分。

经过学习我才更加的认识到网络安全的重要性，因为我们每个人都基本在使用电脑，个人电脑有没有被黑客攻击，病毒侵害呢?每个人的个人电脑都会存储好多个人信息和重要文本文件，那么我们为了保障这些文本信息的安全不被篡改，我们就需要更加深刻的认识网络信息安全的重要性，并不断学习和提高自己的网络安全技能，可以保护好自己的网络信息安全。比如我们的个人电脑大家估计在不经意间已经把自己的好多重要文件给共享了，你其实不想让大家知道你的秘密文件的，却不知道怎么都把这些文件给共享给大家了，好多黑客可以很容易侵入到你的个人电脑的，所以我们需要更多的了解网络安全的基本知识。

网络信息安全需要简单的认识到文件的加密解密，病毒的防护，个人网络设置，加密解密技术，个人电脑的安全防护，生活中的网络泄密和不经意间的个人信息泄露，等等;有时候我们个人的信息是自己泄露的，只是我们没有留意，我们的陌生人可以简单的通过你的个人主页，你的网络言论中分析得到你的个人资料，你会不经意间说明你的所在的城市小区等等，这都是不经意间出现的，那么你的不留意有可能就被另外一些人所利用了，所以我们需要注意在网络信息时代的用词和个人信息的保护，提高防护意识!

本DOCX文档由 www.zciku.com/中词库网 生成，海量范文文档任你选，，为你的工作锦上添花,祝你一臂之力！