网站漏洞模板

1 高危

1.1 Struts2 命令执行漏洞

漏洞等级	高危	**漏洞类型**	Struts2 命令执行漏洞
漏洞信息			
漏洞危害	Struts2 远程命令执行漏洞可导致如下后果： 1.攻击者篡改服务器端对象； 2.攻击者通过修改一些值能够调用被保护的 Java 代码，并且执行任意的 Java 代码。		
漏洞描述	Apache Struts 2.0.0-2.3.16 版本的默认上传机制是基于 Commons FileUpload 1.3 版本，其附加的 ParametersInterceptor 允许访问'class' 参数（该参数直接映射到 getClass()方法），并允许控制 ClassLoader。在具体的 Web 容器部署环境下（如：Tomcat），攻击者利用 Web 容器下的 Java Class 对象及其属性参数（如：日志存储参数），可向服务器发起远程代码执行攻击，进而植入网站后门控制网站服务器主机。		
解决方案	升级到最新版本。		

1.2 后台登录弱口令

漏洞等级	高危	**漏洞类型**	后台登录弱口令
漏洞信息			
漏洞危害	后台登陆弱口令漏洞可导致如下后果： 1、弱口令很 容易被别人破解，从而使用户的计算机面临风险。 2、攻击者获取弱口令直接进入后台管理系统，控制和破坏网站系统。		
漏洞描述	弱口令指的是仅包含简单数字和字母的口令，例如“123”、“abc”等		
解决方案	一般性的建议： 1.不使用空口令或系统缺省的口令，因为这些口令众所周之，为典型的弱口 令。 2.口令长度不小于 8 个字符。 3.口令不应该为连续的某个字符（例如：AAAAAAAA）或重复某些字符的组合 （例如：tzf.tzf.）。 4.口令应该为以下四类字符的组合，大写字母(A-Z)、小写字母(a-z)、数字 (0-9)和特殊字符。每类字符至少包含一个。如果某类字符只包含一个，那 么该字符不应 为首字符或尾字符。 5.口令中不应包含本人、父母、子女和配偶的姓名和出生日期、纪念日期、 登 录 名 、E-mail 地址等等与本人有关的信息，以及字典中的单词。 6.口令不应该为用数字或符号代替某些字母的单词。 7.口令应该易记且可以快速输入，防止他人从你身后很容易看到你的输入。 8.至少 90 天内更换一次口令，防止未被发现的入侵者继续使用该口令。		

1.3 WebShell 木马

漏洞等级	高危	**漏洞类型**	WebShell 木马
漏洞信息			
漏洞危害	WebShell 木马可导致如下后果： 后门控制网站服务器，包括上传下载文件、查看数据库、执行任意程序命令等。 再通过 dos 命令 或者植入后门 木马 通过服务器漏洞等~达到提权的目的 从而旁注同服务器其他的网站。		
漏洞描述	WebShell 就是以 asp、php、jsp 或者 cgi 等网页文件形式存在的一种命令执行环境，也可以将其称做为一种网页后门。黑客在入侵了一个网站后，通常会将这些 asp 或 php 后门文件与网站服务器 WEB 目录下正常的网页文件混在一起，然后就可以使用浏览器来访问这些 asp 或者 php 后门，得到一个命令执行环境，以达到控制网站服务器的目的。		
解决方案	删除木马文件，日常要多维护，并注意空间中是否有来历不明的文件； 不在白名单内的一律禁止上传，上传目录权限遵循最小权限原则；		

1.4 Cookie SQL 注入

漏洞等级	高危	漏洞类型	Cookie SQL 注入
漏洞信息			
漏洞危害	Cookie SQL 注入漏洞可导致如下后果：机密数据被窃取、核心业务数据被篡改、网页被篡改、数据库所在服务器被攻击变为傀儡主机，甚至企业网被入侵。		
漏洞描述	cookie sql 注入是一种特别的注入，Web 应用程序通常与后端的数据库进行交互。Web 应用程序提供相关的接口，以便将它并入 SQL 查询中，然后发送到后端数据库，接着应用程序处理查询结果，反馈给访问者。如果应用程序对访问者的输入处理未做检查或者检查的不完善，访问者便可以构造恶意的数据，当该数据并入 SQL 查询中时，就将得到访问者期望的结果。		
解决方案	过滤客户端提交的危险字符，客户端提交方式包含 GET、POST、COOKIE、User_Agent、Referer、Accept_Language 等。		

1.5 SQL 盲注

漏洞等级	高危	漏洞类型	SQL 盲注
漏洞信息			
漏洞危害	数据泄漏-SQL 注入漏洞可导致如下后果： 机密数据被窃取、核心业务数据被篡改、网页被篡改、数据库所在服务器被攻击变为傀儡主机，甚至企业网被入侵。		
漏洞描述	Web 应用程序通常与后端的数据库进行交互。Web 应用程序提供相关的接口，以便将它并入 SQL 查询中，然后发送到后端数据库，接着应用程序处理查询结果，反馈给访问者。如果应用程序对访问者的输入处理未做检查或者检查的不完善，访问者便可以构造恶意的数据，当该数据并入 SQL 查询中时，就将得到访问者期望的结果。		
解决方案	限定访问者提交数据的类型。 过滤危险的 QL 语句关键字，比如：select、from、update、delete 等。 升级 web 服务器运行平台软件补丁		

1.6 文件上传漏洞

漏洞等级	高危	**漏洞类型**	文件上传漏洞
漏洞信息			
漏洞危害	文件上传漏洞可导致如下后果： 网站或者系统被上传木马文件，导致整个网站或者系统被控制。		
漏洞描述	文件上传漏洞是指用户上传了一个可执行的脚本文件，并通过此脚本文件获得了执行服务器端命令的能力。		
解决方案	1.客户端检测，使用 js 对上传图片进行检测，包括文件大小、文件扩展名、文件类型等； 2.服务端检测，对文件大小、文件路径、文件扩展名、文件类型、文件内容进行检测，对文件重命名； 3.其他限制，服务器端上传目录设置不可执行权限。		

1.7 FckEditor 编辑器漏洞

漏洞等级	高危	**漏洞类型**	FckEditor 编辑器漏洞
漏洞信息			
漏洞危害	写入任意代码，如 Webshell。 写入 Webshell 后可数据篡改，可以修改后台数据库中的敏感用户数据以及系统数据。 上传木马等恶意程序，以便黑客下次稳定的连接。 可进行网页挂马，造成访问该站点的大量用户的损害。 可执行操作系统命令。		
漏洞描述	攻击者能够利用该编辑器的任意文件上传漏洞上传 Webshell，从而控制整个网站。		
解决方案	升级编辑器版本到最新版。		

1.8 SVN 源代码泄漏

漏洞等级	高危	**漏洞类型**	1.9 SVN 源代码泄漏
漏洞信息			
漏洞危害	可以利用.svn/entries 文件，获取到服务器源码、svn 服务器账号密码等信息。		
漏洞描述	SVN（subversion）是源代码版本管理软件，造成 SVN 源代码漏洞的主要原因是管理员操作不规范。“在使用 SVN 管理本地代码过程中，会自动生成一个名为.svn 的隐藏文件夹，其中包含重要的源代码信息。但一些网站管理员在发布代码时，不愿意使用‘导出’功能，而是直接复制代码文件夹到 WEB 服务器上，这就使.svn 隐藏文件夹被暴露于外网环境，攻击者可以借助其中包含的用于版本信息追踪的‘entries’文件，逐步摸清站点结构。”		
解决方案	1.查找服务器上所有.svn 隐藏文件夹，删除； 2.开发人员在使用 SVN 时，严格使用导出功能。禁止直接复制代码。		

1.9 用户验证信息使用 GET 请求提交

漏洞等级	高危	**漏洞类型**	用户验证信息使用 GET 请求提交
漏洞信息			
漏洞危害	用户密码泄漏。		
漏洞描述	用户的凭证信息使用 GET 方式提交，帐号信息会直接暴漏在 URL 地址栏中。		
解决方案	建议改为 POST 请求提交。		

1.10 允许新建任意文件

漏洞等级	高危	**漏洞类型**	允许新建任意文件
漏洞信息			
漏洞危害	服务器被非法入侵。		
漏洞描述	允许新建任意文件，攻击者能够新建木马文件控制整个网站，或者是服务器，拿下服务器最高管理权限。		
解决方案	限制新建文件的类型，例如禁止掉 jsp、asp、php 等脚本文件的创建。		

1.11 任意文件下载

漏洞等级	高危	**漏洞类型**	任意文件下载漏洞
漏洞信息			
漏洞危害	服务器上的任意敏感文件能够被下载，进一步导致服务器被控制。		
漏洞描述	攻击者能够通过漏洞下载任意文件，包括存在数据库连接密码的配置文件等，从而实现进一步攻击。		
解决方案	限制允许下载的文件类型以及目录。		

1.12 跨站脚本

漏洞等级	高危	漏洞类型	跨站脚本
漏洞信息			
漏洞危害	跨站脚本-XSS 漏洞可导致如下后果： 1.获取其他用户 Cookie 中的敏感数据。 2.屏蔽页面特定信息。 3.伪造页面信息。 4.拒绝服务攻击。 5.突破外网内网不同安全设置。 6.与其它漏洞结合，修改系统设置，查看系统文件，执行系统命令等。		
漏洞描述	跨站脚本攻击是指攻击者利用网站程序对用户输入过滤不足，输入可以显示在页面上对其他用户造成影响的 HTML 代码，从而盗取用户资料、利用用户身份进行某种动作或者对访问者进行病毒侵害的一种攻击方式。		
解决方案	过滤客户端提交的危险字符，客户端提交方式包含 GET、POST、COOKIE、User_Agent、Referer、Accept_Language 等。 开发者角度： 某个数据被接受之前，必须使用一定的验证机制来验证所有输入数据，如长度、格式、类型、语法等；常见的方法，比如黑名单验证，将一些常见的字符，如“<”、“>”或类似“script”的关键字进行过滤。 对于任意的输出数据，要进行适当的编码，防止任何已成功注入的脚本在浏览器端运行；数据输出前，确保用户提交的数据已被正确进行编码；可在代码中明确指定输出的编码方式（如 ISO-8859-1），而不是让攻击者发送一个由他自己编码的脚本给用户。 用户角度： 打开一些 Email 或附件、浏览论坛帖子时，一定要特别谨慎，否则有可能导致恶意脚本执行，也可以在浏览器设置中关闭 JavaScript。 增强安全意识，只信任值得信任的站点或内容，不要信任别的网站发到自己信任的网站中的内容。		

常见的危险关键字如下：

"eval\\(","expression","view-source","location","union","open\\(","document","and","insert","select","delete","update","or","truncate","declare","join","alert","<\\s*vbscript","<\\s*javascript","<\\s*script","oncontrolselect","oncopy","oncut","ondataavailable","ondatasetchanged","ondatasetcomplete","ondblclick","ondeactivate","ondrag","ondragend","ondragenter","ondragleave","ondragover","ondragstart","ondrop","onerror" ,"ondrop","onerror","onerroupdate","onfilterchange","onfinish","onfocus","onfocusin","onfocusout","onhelp","onkeydown","onkeypress","onkeyup","onlayoutcomplete","onload","onlosecapture","onmousedown","onmouseenter","onmouseleave","onmousemove","onmousout","onmouseover","onmouseup","onmousewheel","onmove","onmoveend","onmovestart","onabort","onactivate","onafterprint","onafterupdate","onbefore","onbeforeactivate","onbeforecopy","onbeforecut","onbeforedeactivate" ,"onbefore","onbeforeactivate","onbeforecopy","onbeforecut","onbeforedeactivate","onbeforeeditocus","onbeforepaste","onbeforeprint","onbeforeunload","onbeforeupdate","onblur","onbounce","oncellchange","onchange","onclick","oncontextmenu","onpaste","onpropertychange","onreadystatechange","

onreset","onresize","onresizend","onresizestart","onrowenter","onrowexit","onrowsdelete","onrowsinserted","on scroll","onselect","onselectionchange","onselectstart","onstart","onstop","onsubmit","onunload"。

1.13 WebLogic JAVA 反序列化漏洞

漏洞等级	高危	**漏洞类型**	WebLogic JAVA 反序列化漏洞
漏洞信息			
漏洞危害	能够导致远程命令执行，攻击者能够远程执行服务器系统命令。		
漏洞描述	Java 应用对用户输入的不可信数据做了反序列化处理，攻击者可以通过构造恶意输入，让反序列化产生非预期的对象，非预期的对象在产生过程中就有可能带来任意代码执行。		
解决方案	1.使用 SerialKiller 替换进行序列化操作的 ObjectInputStream 类； 2.在不影响业务的情况下，临时删除掉项目里的“org/apache/commons/collections/functors/InvokerTransformer.class” 文件；		

2 中危

2.1 敏感文件

漏洞等级	中危	**漏洞类型**	敏感文件
漏洞信息			
漏洞危害	敏感文件可导致如下后果： 1、获取其他敏感数据。 2、截取页面特定信息。 5、突破外网内网不同安全设置。 6、与其它漏洞结合，修改系统设置，查看系统文件，执行系统命令等。		
漏洞描述	如 user.txt、password.txt 等这些文件中有可能包含了大量的敏感信息，如服务器的帐号、密码等，攻击者通过利用这些信息有可能控制目标服务器或实施进一步的攻击		
解决方案	如果这些文件中包含了敏感内容，请删除这些文件。禁止对外访问		

2.2 未授权访问漏洞

漏洞等级	中危	**漏洞类型**	未授权访问漏洞
漏洞信息			
漏洞危害	未授权访问可导致如下后果： 1、后台存在未授权访问 导致信息暴露 可直接传脚本文件 导致挂马 2、导致拿 shell 进行进一步的渗透 3、机密数据被窃取 4、核心业务数据被篡改，网页被篡改		
漏洞描述	非授权访问指未经授权使用网络资源或以未授权的方式使用网络资源 主要包括非法用户进入网站管理或系统进行以未授权的方式进行操作。		
解决方案	严格配置安全网站访问控制权限。		

2.3 目录遍历漏洞

漏洞等级	低危	**漏洞类型**	目录遍历漏洞
漏洞信息			
漏洞危害	目录遍历可导致如下后果： 黑客可获得服务器上的文件目录，从而下载敏感文件。		
漏洞描述	服务器开启了相关的目录浏览选项，攻击者访问网站目录能够直接查看目录下的文件。		
解决方案	通过修改配置文件，去除 Web 容器（如 apache、nginx、tomcat）的文件目录索引功能。		

2.4 允许 TRACE 方法

漏洞等级	中危	**漏洞类型**	允许 TRACE 方法
漏洞信息			
漏洞危害	需要目标 web 服务器允许 TRACE 参数； 需要一个用来插入 XST 代码的地方； 目标站点存在跨域漏洞		
漏洞描述	TRACE 是一种 HTTP 方法，允许 TRACE 方法的 web 服务器存在跨站脚本漏洞。		
解决方案	禁用 TRACE 方法，IIS 可使用 URLScan 禁用，而 Apache 则可使用 mod_rewrite 模块禁用。		

2.5 登陆界面密码明文显示

漏洞等级	中危	**漏洞类型**	登陆界面密码明文显示
漏洞信息			
漏洞危害	用户密码泄漏。		
漏洞描述	登陆界面密码明文显示，用户在输入密码时，存在密码泄漏的风险。		
解决方案			

2.6 用户凭证信息以明文发送

漏洞等级	中危	**漏洞类型**	凭证信息明文传输
漏洞信息			
漏洞危害	用户的凭证信息在传输过程中被窃取。		
漏洞描述	用户的身份验证信息使用明文的形式发送给服务器，如果数据报文被攻击者截获，能够导致用户账号密码泄露。		
解决方案	1.为了数据传输的安全，建议使用 HTTPS 协议，HTTPS 在 HTTP 的基础上加入了 SSL 协议，SSL 依靠证书来验证服务器的身份，并为浏览器和服务器之间的通信加密。 2.密码在发送给服务器验证之前，在前端采用 js 脚本对敏感信息进行加密之后，再传给服务器。		

2.7 允许任何域的 Flash 文件访问资源

漏洞等级	中危	漏洞类型	允许任何域的 Flash 文件访问资源
漏洞信息			
漏洞危害	可能会导致“跨站点伪造请求”或“跨站点跟踪”（“跨站点脚本编制”的变体）之类的攻击。		
漏洞描述	crossdomain.xml 是一个策略文件，定义 Web 页面资源是否能从不同域的 Flash 应用程序进行访问。当 Web 站点的 crossdomain.xml 策略太宽容（例如，允许任何域的 Flash 文件访问站点资源）时，可能会导致“跨站点伪造请求”或“跨站点跟踪”（“跨站点脚本编制”的变体）之类的攻击。		
解决方案	确保 crossdomain.xml 中 domain 的值为特定的域名，例如：allow-access-from domain="*.test.com"。		

3 低危

3.1 Web 应用程序错误

漏洞等级	低危	**漏洞类型**	Web 应用程序错误
漏洞信息			
漏洞危害	Web 应用程序错误可导致如下后果： 攻击者向服务器提交精心构造的恶意数据后，有可能导致服务器出现内部错误、服务器宕机或数据库错乱。		
漏洞描述	web 应用程序在处理访问者的请求时，如果符合 web 应用程序的逻辑或者 web 应用程序本身没有异常，那么将结果直接反馈给访问者。往往 web 应用程序在处理这些请求的时候未做相应的处理，直接把网站错误反馈给访问者。		
解决方案	过滤客户端提交的危险字符，客户端提交方式包含 GET、POST、COOKIE、User-Agent、Referer、Accept-Language 等。		

3.2 网站管理后台

漏洞等级	低危	**漏洞类型**	网站管理后台
漏洞信息			
漏洞危害	网站管理后台漏洞可导致如下后果： 1、攻击者可能通过使用常用的地址尝试访问目标站点，获取站点的后台管理地址。通过破解用户名和密码等方法进入网站后台管理系统。		
漏洞描述	站点信息的更新通常通过后台管理来实现的，web 应用程序开发者或者站点维护者可能使用常用的后台地址名称来管理，比如 admin、manager 等。		
解决方案	1、使用非常规的后台管理地址名称。 2、网站前端程序和后台管理程序分离，比如为后台管理地址设置一个二级域名。		

3.3 robots.txt 文件的检测

漏洞等级	低危	**漏洞类型**	robots.txt 文件
漏洞信息			
漏洞危害	robots.txt 文件可导致如下后果： 发现 robots.txt 文件 robots.txt 文件有可能泄露系统中的敏感信息，如后台地址或者不愿意对外公开的地址等，恶意攻击者有可能利用这些信息实施进一步的攻击。		
漏洞描述	黑客可获得服务器上的文件目录，从而下载敏感文件		
解决方案	禁止访问		

3.4 发现内部 IP 泄露模式

漏洞等级	低危	**漏洞类型**	发现内部 IP 泄露模式
漏洞信息			
漏洞危害	内部 IP 泄漏可导致如下后果： 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 恶意攻击者有可能利用这些信息实施进一步的攻击。		
漏洞描述	对攻击者而言，泄露内部 IP 非常有价值，因为它显示了内部网络的 IP 地址方案。知道内部网络的 IP 地址方案，可以辅助攻击者策划出对内部网络进一步的攻击。		
解决方案	除去 Web 站点中的内部 IP 地址		

3.5 发现数据库错误模式

漏洞等级	低危	**漏洞类型**	发现数据库错误模式
漏洞信息			
漏洞危害	数据库错误可导致如下后果： 可能会查看、修改或删除数据库条目和表。		
漏洞描述	在测试响应中发现数据库错误，该错误可能已被“SQL 注入”以外的攻击所触发。 虽然不确定，但这个错误可能表示应用程序有“SQL 注入”漏洞。 使用受外部影响的输入构造整个 SQL 命令或 SQL 命令的一部分，但是会错误的无害化某些特殊元素，这些元素可在所需 SQL 命令发送到数据库时对其进行修改。如果在用户可控制的输入中没有充分除去或引用 SQL 语法，那么生成的 SQL 查询可能会导致将这些输入解释为 SQL 而不是普通用户数据。这可用于修改查询逻辑以绕过安全性检查，或者插入其他用于修改后端数据库的语句，也可能包括执行系统命令。		
解决方案	过滤客户端提交的危险字符，客户端提交方式包含 GET、POST、COOKIE、User_Agent、Referer、Accept_Language 等。		

3.6 HTML form without CSRF protection

漏洞等级	低危	**漏洞类型**	HTML form without CSRF protection
漏洞信息			
漏洞危害	能够导致个人隐私泄露，危及财产安全。		
漏洞描述	攻击者能够盗用用户的身份，以用户的名义给网站发送恶意请求。		
解决方案	通过 referer、token 或者验证码来检测用户提交； 尽量不要在页面的链接中暴露用户隐私信息； 避免全站通用的 cookie，严格设置 cookie 的域。		

3.7 X-Frame-Options HTTP 未配置

漏洞等级	低危	**漏洞类型**	X-Frame-Options HTTP 未配置
漏洞信息			
漏洞危害	X-Frame-Options HTTP 响应头，可以指示浏览器是否应该加载一个 iframe 中的页面。未配置存在站点内的页面被其他页面嵌入从而进行点击劫持。		
漏洞描述	X-Frame-Options HTTP 响应头可以指示浏览器是否允许当前网页在“frame”或“iframe”标签中显示，以此使网站内容不被其他站点引用和免于点击劫持攻击。		
解决方案	一般性的建议： 给您的网站添加 X-Frame-Options 响应头，赋值有如下三种，1、DENY：无论如何不在框架中显示；2、SAMEORIGIN：仅在同源域名下的框架中显示；3、ALLOW-FROM uri：仅在指定域名下的框架中显示。如 Apache 修改配置文件添加“Header always append X-Frame-Options SAMEORIGIN”；Nginx 修改配置文件“add_header X-Frame-Options SAMEORIGIN;”。		

3.8 Long password denial of service

漏洞等级	低危	**漏洞类型**	Long password denial of service
漏洞信息			
漏洞危害	可能会导致网站暂时变为/无限期不可用或无响应。		
漏洞描述	通过发送一个很长的密码（1000000 字符）有可能导致拒绝服务器上的服务攻击。这可能导致的网站变得不可用或不响应。在很长的密码发送，密码散列过程中会导致 CPU 和内存耗尽。		
解决方案	一般性的建议： 限制接受密码的最大长度。		

3.9 版本信息披露（IIS）

漏洞等级	低危	**漏洞类型**	版本信息披露（IIS）
漏洞信息			
漏洞危害	版本信息披露（IIS）可导致如下后果： 这些信息可以帮助攻击者获得系统在使用中更深入的了解，并有可能开发针对 IIS 的特定版本的进一步攻击。		
漏洞描述	一个版本披露（IIS）在目标 Web 服务器的 HTTP 响应，攻击者可能利用公开的信息，收获特定的安全漏洞确定的版本。		
解决方案	配置 Web 服务器，以防止信息泄漏的 HTTP 响应的服务器头。		

3.10 Apache httpd remote denial of service

漏洞等级	低危	**漏洞类型**	Apache httpd remote denial of service
漏洞信息			
漏洞危害	受影响的 Apache 版本（1.3.x 中，2.0.x 版本通过 2.0.64 和 2.2.x 版通过 2.2.19）针对任意 HTTP Server，建立一个连接，以很低的速度发包，并保持住这个连接不断开。如果客户端持续建立这样的连接，那么服务器上可用的连接池将很快被占满，从而导致拒绝服务攻击。		
漏洞描述	针对任意 HTTP Server，建立一个连接，以很低的速度发包，并保持住这个连接不断开。如果客户端持续建立这样的连接，那么服务器上可用的连接池将很快被占满，从而导致拒绝服务攻击。		
解决方案	限制 web 服务器的 HTTP 头部传输的最大许可时间。		

3.11 Apache HTTP Server "httpOnly" Cookie 信息泄露漏洞

漏洞等级	低危	**漏洞类型**	Apache HTTP Server "httpOnly" Cookie 信息泄露漏洞
漏洞信息			
漏洞危害	Apache HTTP Server 在对状态代码 400 的默认错误响应的实现上存在 Cookie 信息泄露漏洞，成功利用后可允许攻击者获取敏感信息。		
漏洞描述	Apache HTTP Server 是 Apache 软件基金会的一个开放源码的网页服务器，可以在大多数计算机操作系统中运行。Apache HTTP Server 在对状态代码 400 的默认错误响应的实现上存在 Cookie 信息泄露漏洞，成功利用后可允许攻击者获取敏感信息。		
解决方案	受影响系统： Apache Group Apache HTTP Server 2.2.x 不受影响系统： Apache Group Apache HTTP Server 2.2.22-dev。 升级 apache 版本到最新		

3.12 启用了不安全的 HTTP 方法

漏洞等级	低危	**漏洞类型**	启用了不安全的 HTTP 方法
漏洞信息			
漏洞危害	可能会在 Web 服务器上上载、修改或删除 Web 页面、脚本和文件		
漏洞描述	Web 服务器或应用程序服务器是以不安全的方式配置的。		
解决方案	除标准的 GET 和 POST 方法外，HTTP 请求还使用其他各种方法。许多这类方法主要用于完成不常见与特殊的任务。如果低权限用户可以访问这些方法，他们就能够以此向应用程序实施有效攻击。以下是一些值得注意的方法： PUT 向指定的目录上载文件 DELETE 删除指定的资源 COPY 将指定的资源复制到 Destination 消息头指定的位置 MOVE 将指定的资源移动到 Destination 消息头指定的位置 SEARCH 在一个目录路径中搜索资源 PROPFIND 获取与指定资源有关的信息，如作者、大小与内容类型 TRACE 在响应中返回服务器收到的原始请求 其中几个方法属于 HTTP 协议的 WebDAV（Web-based Distributed Authoring and Versioning）扩展，如果服务器不需要支持 WebDAV，请务必禁用它，或禁止不必要的 HTTP 方法。		

3.13 Vulnerable JavaScript library

漏洞等级	低危	**漏洞类型**	Vulnerable Javascript library
漏洞信息			
漏洞危害			
漏洞描述	jQuery 是继 prototype 之后又一个优秀的 Javascript 代码库，jQuery 1.6.3 之前版本中存在跨站脚本漏洞。当使用 location.hash 选择元素时，通过特制的标签，攻击者利用该漏洞可以注入任意 web 脚本或 HTML 代码。		
解决方案	升级到最新版本。		

3.14 HTTP.sys remote code execution vulnerability

漏洞等级	低危	**漏洞类型**	HTTP.sys remote code execution vulnerability
漏洞信息			
漏洞危害	攻击者可以通过向受影响的系统发送特制的 HTTP 请求，在系统帐户的上下文中执行任意代码。		
漏洞描述	当 HTTP.sys 不正确地解析特制的 HTTP 请求时，HTTP 协议栈（HTTP.sys）中存在一个远程代码执行漏洞。		
解决方案	Microsoft 已针对此问题提供了安全更新，建议您尽快应用此更新。 参考：MS15-034 HTTP.sys Remote Code Execution Vulnerability		

3.15 IIS 短文件名泄露

漏洞等级	低危	漏洞类型	Microsoft IIS tilde directory enumeration
漏洞信息			
漏洞危害	攻击者可利用此漏洞枚举服务器目录中的文件或者文件夹。可惜的是只能列举出文件夹或者文件的名字的前 5 个或者 6 个字符。		
漏洞描述	在 Win3.x 版本的时候，Windows 中的文件名是由不超过 8 个字符的主文件名，和不超过 3 个字符的扩展名组成。到了 Windows 95 的时候，这个长度被扩展成主文件名 + 扩展名，字符长度不超过 255 个字符。为了保证兼容性，Windows 提供了一种转换的方式，用“~”和数字来缩短文件名的长度。这种转换使得一些老的应用程序在新的 Windows 平台上也可以使用。		
解决方案	修复建议： a.关闭 NTFS 8.3 文件格式的支持。该功能默认是开启的，对于大多数用户来说无需开启。关闭的方法：如果在 C 盘上关闭这个功能，则可在命令行中使用以下命令： fsutil 8dot3name set C: 1 1 表示禁用，0 表示启用。如果不写盘符，则是全局设置，这时可选的有 4 个值：0（全部启动），1（全部禁用），2（每个盘符单独设置），3（除系统盘外全部禁用） 。 b. 禁止 url 中使用“~”或它的 Unicode 编码。		

3.16 密码提交使用 GET 方式

漏洞等级	低危	**漏洞类型**	密码提交使用 GET 方式
漏洞信息			
漏洞危害	用户密码泄漏。		
漏洞描述	输入的用户名和登录密码，使用 GET 方式进行传输，输入的信息会直接暴漏在 URL 地址栏当中。		
解决方案	改用 POST 方式进行提交，并且建议传输过程中对密码进行加密。		

3.17 允许使用弱口令创建用户

漏洞等级	低危	**漏洞类型**	允许使用弱口令创建用户
漏洞信息			
漏洞危害	允许用户使用弱口令登陆，弱口令容易被攻击者暴力破解。		
漏洞描述	弱口令容易被攻击者暴力破解。		
解决方案	建议禁止用户使用弱口令登陆，必须设置 6 位以上，数字加上字母大小组合的强壮密码。		

3.18 未设置登陆失败锁定机制

漏洞等级	低危	**漏洞类型**	未设置登陆失败锁定机制
漏洞信息			
漏洞危害	密码被暴力猜解。		
漏洞描述	允许攻击者进行暴力破解，获取密码。		
解决方案	建议设置锁定机制，例如当用户尝试登陆失败 5 次之后，锁定帐号 30min。		

3.19 日志信息可删除

漏洞等级	低危	**漏洞类型**	日志信息可删除
漏洞信息			
漏洞危害	恶意操作无法溯源。		
漏洞描述	恶意操作记录可以被删除，无法通过日志文件溯源。		
解决方案	禁止删除日志文件。		

3.20 允许单个帐号的多重并发会话

漏洞等级	**低危**	**漏洞类型**	允许单个帐号的多重并发会话
漏洞信息			
漏洞危害			
漏洞描述	应能够对单个账户的多重并发会话进行限制。		
解决方案	记录用户登录状态，已登录用户同时在异地登录时采取提示、挤出等措施，确保账户无法同时在异地登录。		

3.21 URL 重定向

漏洞等级	**低危**	**漏洞类型**	URL 重定向
漏洞信息			
漏洞危害	URL 重定向可导致如下后果： 用户发出相关访问请求时，系统将自动跳转到指定位置。如果攻击者能控制跳转的对象，则会用于钓鱼、挂马等。		
漏洞描述	url 重定向是指把一个 URL 重定向到另一个 URL 上。即把目录或文件的访问请求转发到另外的一个目录或者文件，当用户发出相关访问请求时，系统将自动跳转到指定位置。		
解决方案	过滤客户端提交的危险字符，客户端提交方式包含 GET、POST、COOKIE、User_Agent、Referer、Accept_Language 等。		