跨站请求伪造(CSRF)

漏洞级别： 低危或中危

参考：OWASP:OWASP Category

危害：

CSRF 攻击可以在受害者毫不知情的情况下以受害者名义伪造请求发送给受攻击站点，从而在并未授权的情况下执行在权限保护之下的操作。

描述：

CSRF 攻击是黑客借助受害者的 cookie 骗取服务器的信任，但是黑客并不能拿到 cookie，也看不到 cookie 的内容。另外，对于服务器返回的结果，由于浏览器同源策略的限制，黑客也无法进行解析。因此，黑客无法从返回的结果中得到任何东西，他所能做的就是给服务器发送请求，以执行请求中所描述的命令，在服务器端直接改变数据的值，而非窃取服务器中的数据。

解决方法：

验证 HTTP Referer 字段；在请求地址中添加 token 并验证；在 HTTP 头中自定义属性并验证。

备注：

暂无相关信息

命令执行漏洞

漏洞级别： 高危

参考：OWASP:OWASP Category

危害：

黑客可在服务器上执行任意命令，从而入侵服务器，从而获取服务器的管理员权限。

描述：

黑客可在服务器上执行任意命令，从而入侵服务器，从而获取服务器的管理员权限。

解决方法：

严格过滤用户输入的数据。

备注：

暂无相关信息

命令执行漏洞

漏洞级别： 高危

参考：OWASP:OWASP Category

危害:

黑客可在服务器上执行任意命令，从而入侵服务器，从而获取服务器的管理员权限。

描述:

黑客可在服务器上执行任意命令，从而入侵服务器，从而获取服务器的管理员权限。

解决方法:

严格过滤用户输入的数据。

备注:

暂无相关信息

Struts2 Execute命令执行

漏洞级别： 高危

参考：暂无相关信息

危害:

黑客可在服务器上执行任意命令，从而入侵服务器，从而获取服务器的管理员权限。

描述:

黑客可在服务器上执行任意命令，从而入侵服务器，从而获取服务器的管理员权限。

解决方法:

升级Struts2至最新版本

备注:

暂无相关信息

PHP Version Vulnerabilities

漏洞级别： 低危

参考：暂无相关信息

危害：

PHP版本过低，可能存在一些已知漏洞

描述：

PHP版本过低，可能存在一些已知漏洞

解决方法：

建议升级PHP版本至5.6.30

备注：

暂无相关信息

发现JetBrains .idea.idea/workspace.xml

漏洞级别： 低危

参考：暂无相关信息

危害：

由于开发人员使用JetBrains系列开发工具开发web应用，上传代码至服务器时，未排除web开发目录下的.idea文件夹导致该目录被上传至服务器web目录。

描述：

发现JetBrains .idea.idea/workspace.xml,攻击者可通过泄露的JetBrains .idea.idea/workspace.xml 文件获得部分web应用脚本信息

解决方法：

删除.idea文件夹，并且注意以后上传web应用禁止上传该目录

备注：

暂无相关信息

系统/网站弱口令/可预测的登录凭证

漏洞级别： 高危

参考：OWASP:Brute_force_attack WASC:蛮力 CVE:不适用 CWE:340

危害:

发现系统弱口令，可被黑客直接获得系统控制权限。

描述:

发现系统弱口令，可被黑客直接获得系统控制权限。

解决方法:

修改密码为复杂密码并加密保存，建议密码包含大小写字母，数据和特殊符号，密码长度不低于八位，如果网站存在数据泄漏漏洞（如sql注入漏洞），务必修复漏洞。

备注:

暂无相关信息

Mysql身份认证漏洞(CVE-2012-2122)

漏洞级别： 高危

参考：OWASP:不适用 WASC:不适用 CVE:CVE-2012-2122 CWE:不适用

危害:

该版本Mysql允许攻击者穷举256次用户密码，便能成功登录Mysql服务器。

描述:

影响版本:MySQL版本低于 5.0.96 、5.1.63 、5.5.25。

当连接MySQL时，输入的密码会与期望的正确密码相比较，即使memcmp()返回一个非零值，也会使MySQL认为两个密码是相同。也就是说，只要知道用户名，不断尝试就能直接登入数据库，穷举256次就能猜对一次，目前网络上关于此漏洞的利用工具已流出。

解决方法:

Linux/Unix解决方案:(1)使用防火墙禁止访问Mysql端口。(2)如果原来MySQL是5.0.x，需要升级到 5.0.96 版本。如果原来MySQL是5.1.x，需要升级到 5.1.63 版本。如果原来MySQL是5.5.x，需要升级到 5.5.25 版本。
Windows解决方案:(1)使用防火墙禁止访问Mysql端口。(2)如果原来MySQL是5.0.x，需要升级到 5.0.96 版本。如果原来MySQL是5.1.x，需要升级到 5.1.63 版本。如果原来MySQL是5.5.x，需要升级到 5.5.25 版本。

备注:

暂无相关信息

Serv-U权限绕过漏洞(CVE-2011-4800)

漏洞级别： 高危

参考：OWASP:不适用 WASC:不适用 CVE:CVE-2011-4800 CWE:不适用 OSVDB-ID:77422

危害:

RhinoSoft Serv-U FTP Server实现上存在目录遍历漏洞，通过输入特定的路径串可以实现目录遍历，攻击者可以下载、上传、删除FTP根目录外的文件。

描述:

影响版本:Serv-U FTP Server 版本号 低于 11.1.0.5。

RhinoSoft Serv-U FTP Server实现上存在目录遍历漏洞，通过输入特定的路径串可以实现目录遍历，攻击者可以下载、上传、删除FTP根目录外的文件。

解决方法:

Linux/Unix解决方案:Linux不存在该软件。
Windows解决方案:升级Serv-U FTP Server到最新版本。

备注:

暂无相关信息

CRLF injection/HTTP response splitting

漏洞级别： 中危

参考：暂无相关信息

危害:

攻击者一旦我们能够控制HTTP 消息头中的字符，注入一些恶意的换行，这样我们就能注入一些会话Cookie或者HTML代码

描述:

攻击者一旦我们能够控制HTTP 消息头中的字符，注入一些恶意的换行，这样我们就能注入一些会话Cookie或者HTML代码

解决方法:

接收请求时过滤\r 、\n之类的换行符，避免输入的数据污染到其他HTTP头

备注:

暂无相关信息

不安全的文件上传功能

漏洞级别： 中危或高危

参考：OWASP:OWASP Category

危害：

文件上传功能没有设置权限限制，容易被黑客利用。攻击者可以上传可执行的WebShell（如php、jsp、asp类型的木马病毒），或者利用目录跳转上传gif、html、xml、config文件，覆盖原有的系统文件，到达获取系统权限的目的。

描述：

文件上传功能没有设置权限限制，容易被黑客利用。攻击者可以上传可执行的WebShell（如php、jsp、asp类型的木马病毒），或者利用目录跳转上传gif、html、、config文件，覆盖原有的系统文件，到达获取系统权限的目的。

解决方法：

1.设置权限限制，只允许管理员访问该文件。
2.严格限制可上传的文件类型。
3.严格限制上传的文件路径。

备注：

暂无相关信息

Unicode编码转换漏洞

漏洞级别： 中危或高危

参考：OWASP:OWASP Category

危害：

在实现Unicode编码转换时存在漏洞。黑客可通过构造特殊编码实现XSS、SQL注入等Web攻击；黑客可通过该漏洞绕过系统的防护体系（如防火墙）实现攻击。

描述：

在实现Unicode编码转换时存在漏洞。黑客可通过构造特殊编码实现XSS、SQL注入等Web攻击；黑客可通过该漏洞绕过系统的防护体系（如防火墙）实现攻击。

解决方法：

正确使用及转换系统编码。

备注：

暂无相关信息

未过滤HTML标签及HTML代码 (或跨站脚本漏洞:Cross Site Scripting)

漏洞级别： 中危或高危

参考：OWASP:XSS WASC:跨站点脚本编制 CVE:不适用 CWE:79

危害：

本页面未过滤HTML代码，攻击者可能可以通过精心构造XSS代码（或绕过防火墙防护策略），实现跨站脚本攻击。恶意用户可以使用JavaScript、VBScript、ActiveX、HTML语言甚至Flash利用应用的漏洞，从而获取其他用户信息。攻击者能盗取会话cookie、获取账户、模拟其他用户身份，甚至可以修改网页呈现给其他用户的内容。

描述：

本页面未过滤HTML代码，攻击者可能可以通过精心构造XSS代码（或绕过防火墙防护策略），实现跨站脚本攻击。

跨站脚本漏洞，即XSS，通常用Javascript语言描述，它允许攻击者发送恶意代码给另一个用户。因为浏览器无法识别脚本是否可信，跨站漏洞脚本便运行并让攻击者获取其他用户的cookie或session。

解决方法：

严格过滤用户输入的数据。对输入的数据进行特殊字符（<、>、” 等）进行转义。

备注：

暂无相关信息

可直接通过IP访问Web服务器

漏洞级别： 提示或低危

参考：OWASP:OWASP Category WASC:空字符注入 CVE:不适用 CWE:626

危害：

攻击者可直接通过IP访问Web服务器。攻击者可能可以通过该方法（包括变化使用不同的IP、域名访问Web服务器），从而绕过防火墙。

描述：

攻击者可直接通过IP访问Web服务器。攻击者可能可以通过该方法（包括变化使用不同的IP、域名访问Web服务器），从而绕过防火墙。

解决方法：

取消IP访问的功能。

备注：

暂无相关信息

跨站脚本漏洞(Cross Site Scripting)

漏洞级别： 中危或高危

参考：OWASP:XSS WASC:跨站点脚本编制 CVE:不适用 CWE:79

危害：

恶意用户可以使用JavaScript、VBScript、ActiveX、HTML语言甚至Flash利用应用的漏洞，从而获取其他用户信息。攻击者能盗取会话cookie、获取账户、模拟其他用户身份，甚至可以修改网页呈现给其他用户的内容。

描述：

本页面存在跨站脚本攻击。

跨站脚本漏洞，即XSS，通常用Javascript语言描述，它允许攻击者发送恶意代码给另一个用户。因为浏览器无法识别脚本是否可信，跨站漏洞脚本便运行并让攻击者获取其他用户的cookie或session。

解决方法：

严格限制传入参数输入值的格式，过滤特殊字符（ <、>、' 、" 等）。

备注：

暂无相关信息

数据泄漏-SQL注入漏洞

漏洞级别： 高危

参考：OWASP:SQL Injection　WASC:SQL Injection　CVE:不适用　CWE:89

危害：

数据泄漏-SQL注入漏洞可导致如下后果：
1.机密数据被窃取
2.核心业务数据被篡改
3.网页被篡改
4.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。

描述：

SQL注入漏洞是一种可能被攻击者通过经过精心构造的请求数据来修改后台SQL查询语句的一种安全威胁。当Web应用程序未对用户输入的数据进行任何处理（如危险字符过滤或者语句过滤），而直接作为SQL语句执行时，SQL注入就发生了。

SQL注入漏洞是目前互联网最常见也是影响非常广泛的漏洞。从2007年下半年开始，很多网站被篡改。攻击者利用SQL注入漏洞修改了用于生成动态网页的数据库中的文本，从而注入了恶意的HTML script标签。这样的攻击在2008年第一季度开始加速传播，并且持续影响有漏洞的Web程序。

解决方法：

如下一些方法能够防止注入攻击：
1.在网页代码中需要对用户输入的数据进行严格过滤。
2.使用预处理执行SQL语句，对所有传入SQL语句中的变量做绑定。
3.部署Web应用防火墙
4.对数据库操作进行监控

备注：

暂无相关信息

Nginx远程缓冲区溢出漏洞

漏洞级别：　高危

参考：OWASP:OWASP Category

危害：

黑客可在服务器上执行任意命令，从而入侵服务器，从而获取服务器的管理员权限。

描述：

Nginx远程缓冲区溢出漏洞允许黑客在您的服务器上执行任意命令。

Nginx版本号从 0.1.0 到 0.5.37, 0.6.x 到 0.6.39, 0.7.x 到 0.7.62, 0.8.x 到 0.8.15 都受该漏洞的影响。

参考：http://www.exploit-db.com/exploits/9901/

解决方法：

把Nginx程序升级到最新版本。

备注：

扫描器一般通过Web服务器的banner推测您的服务器存在该漏洞，如果您手工修改过服务器的banner，可能会导致误报。

Nginx任意文件执行漏洞

漏洞级别： 高危

参考：OWASP:OWASP Category

危害：

恶意用户只要有办法把带有PHP代码的图片或doc文档上传到您的服务器上，便能入侵您的服务器。

描述：

"Nginx任意文件执行漏洞" 允许您的网站的任何文件（如gif、txt）以PHP、CGI的方式运行。
恶意用户只要有办法把带有PHP代码的图片或doc文档上传到您的服务器上，便能入侵您的服务器。

解决方法：

正确配置nginx。在Nginx配置文件中添加以下代码：if ($fastcgi_script_name ~ \..*\/.*php) {return 403;}。或者修改php.ini文件，将cgi.fix_pathinfo的值设置为0;

备注：

暂无相关信息

DNS域传送漏洞

漏洞级别： 高危

参考：暂无相关信息

危害：

DNS服务器配置不当，导致所有域名DNS泄露，从而引起进一步的入侵。

描述：

DNS服务器配置不当，导致所有域名DNS泄露，从而引起进一步的入侵。

解决方法：

正确配置DNS服务器

备注:

暂无相关信息

Possible vul file —可能是带有漏洞的(开源)脚本/程序

漏洞级别： 高危

参考：OWASP:OWASP Category

危害:

当前文件可能存在严重的漏洞，黑客可以通过该文件的漏洞直接入侵您的系统。

描述:

"Possible vul file" 属于高危漏洞。该漏洞意味着当前文件可能存在严重的漏洞，黑客可以通过该文件的漏洞入侵您的系统。

解决方法:

升级当前的(开源)脚本/程序

备注:

扫描器一般对该漏洞的准确率是95%，如果您升级过该脚本，而且没有修改版本信息，则有可能误报。

SVN文件源代码泄漏漏洞

漏洞级别： 高危

参考：OWASP:OWASP Category

危害:

黑客可以利用该漏洞下载网站的源代码，再从源代码里获得数据库的连接密码；或者通过源代码分析出新的系统漏洞，从而进一步入侵您的系统。

描述:

黑客可以利用该漏洞下载网站的源代码，再从源代码里获得数据库的连接密码；或者通过源代码分析出新的系统漏洞，从而进一步入侵您的系统。

解决方法：

删除指定SVN生成的各种文件，如“/.svn/entries”等。

备注：

暂无相关信息

Flash 安全配置缺陷

漏洞级别： 低危或中危

参考：OWASP:OWASP Category

危害：

"Flash 安全配置缺陷" 是指网站的flash配置文件 crossdomain.xml 配置不当，形成Flash跨域攻击安全隐患。

描述：

"Flash 安全配置缺陷" 是指网站的flash配置文件 crossdomain.xml 配置不当，形成Flash跨域攻击安全隐患。
当您发现检测报表提示该漏洞时，请检查crossdomain.xml是否存在以下代码:
<allow-access-from domain="*" />。

解决方法：

去掉以下代码"<allow-access-from domain="*" />"，并严格控制flash的可信任域。

备注：

暂无相关信息

发现robots.txt文件/不存在robots.txt标注的文件

漏洞级别： 中危或低危

参考：OWASP:OWASP Category

危害：

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。

描述：

目标WEB站点上发现了robots.txt文件。
1.robots.txt是搜索引擎访问网站的时候要查看的第一个文件。
2.robots.txt文件会告诉蜘蛛程序在服务器上什么文件是可以被查看的什么文件是不允许查看的。举一个简单的例子：当一个搜索蜘蛛访问一个站点时，它会首先检查该站点根目录下是否存robots.txt，如果存在，搜索机器人就会按照该文件中的内容来确定访问的范围；如果该文件不存在，所有的搜索蜘蛛将能够访问网站上所有没有被口令保护的页面。同时robots.txt是任何人都可公开访问的，恶意攻击者可以通过分析robots.txt的内容，来获取敏感的目录或文件路径等信息。

另外一种情况是：如果robots.txt标准的文件不存在，请确定是不是该文件意外丢失。

解决方法：

确保robots.txt中不包含敏感信息，建议将不希望对外公布的目录或文件请使用权限控制，使得匿名用户无法访问这些信息。

备注：

暂无相关信息

命令执行漏洞

漏洞级别： 高危

参考：OWASP:OWASP Category

危害：

黑客可在服务器上执行任意命令，从而入侵服务器，从而获取服务器的管理员权限。

描述：

黑客可在服务器上执行任意命令，从而入侵服务器，从而获取服务器的管理员权限。

解决方法：

严格过滤用户输入的数据。

备注：

暂无相关信息

发生了内部错误 (500 Internal Server Error)

漏洞级别： 低危或中危

参考：OWASP:OWASP Category

危害:

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。

描述:

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。

解决方法:

针对出现问题的参数，严格过滤用户输入的数据。

备注:

暂无相关信息

可能是敏感关键字

漏洞级别： 低危或中危

参考：OWASP:OWASP Category

危害:

该网页存在敏感关键字。

描述:

该网页存在敏感关键字。

解决方法:

去除敏感关键字

备注:

暂无相关信息

可能是敏感文件(Possible Sensitive File)

漏洞级别： 低危或中危

参考：OWASP:OWASP Category

危害:

敏感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。

描述：

敏感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。

解决方法：

删除敏感文件，或修改文件名。

备注：

扫描器存在误报的可能，误报的原因可能是:1. 被检测网站使用了随机的自定义404页面
2. 被检测的文件存在大量随机广告
3. 由于网络原因导致读取网页超时，形成误报

Apache+PHP(mod_cgi)命令执行漏洞

漏洞级别： 高危

参考：OWASP:OWASP Category

危害：

黑客可在服务器上执行任意命令，从而入侵服务器，从而获取服务器的管理员权限。

描述：

该漏洞允许攻击者在您的服务器上直接执行系统命令，从而获取系统管理员权限。

PHP以mod_cgi模式运行于Apache环境时，可能导致高危漏洞。
参考:http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/

解决方法：

严格过滤用户输入的数据。

备注：

暂无相关信息

Apache/2.0.x Vulnerabilities(CVE-2011-3192)

漏洞级别： 高危或中危

参考：OWASP:不适用 WASC:不适用 CVE:CVE-2011-3192 CWE:不适用

危害：

发现服务器泄漏了具体的软件版本信息，而且该软件版本可能存在漏洞。

描述：

影响版本: Apache 低于2.2.19的2.2.x版本
发现服务器泄漏了具体的软件版本信息，而且该软件版本可能存在漏洞。黑客可下载针对性的黑客攻击程序，对该服务器进行攻击。

解决方法：

Linux/Unix解决方案:屏蔽软件版本信息，并升级服务器到最新版本。
Windows解决方案:屏蔽软件版本信息，并升级服务器到最新版本。

备注：

扫描器一般通过Web服务器的banner推测您的服务器存在该漏洞，如果您手工修改过服务器的banner，可能会导致误报。

网页被挂马或存在恶意代码

漏洞级别： 高危

参考：暂无相关信息

危害：

当前网页被挂马或存在恶意代码。

描述：

当前网页被挂马或存在恶意代码。

解决方法：

清除恶意代码后，修复网站上漏洞，以防止被黑客再次入侵或篡改。

备注：

暂无相关信息

可能是备份文件

漏洞级别： 高危或中危

参考：OWASP:OWASP Category

危害：

如果备份文件中包含了源码，恶意攻击者可以通过对源码的分析，会更加容易的找到程序的脆弱点。如果备份文件中包含了敏感的信息，则恶意攻击者有可能直接使用这些信息获取对目标服务器的控制。

描述：

如果备份文件中包含了源码，恶意攻击者可以通过对源码的分析，会更加容易的找到程序的脆弱点。如果备份文件中包含了敏感的信息，则恶意攻击者有可能直接使用这些信息获取对目标服务器的控制。

解决方法：

检查服务器WEB路径下的特殊后缀文件，注意一定要同时包含隐藏隐藏属性的文件，删除无用的备份文件，对WEB源码目录建议仅设置可读权限，以免备份文件的写入。

备注：

暂无相关信息

Padding Oracle漏洞

漏洞级别： 高危或中危

参考：OWASP:OWASP Category

危害：

黑客能够使用Padding Oracle攻击方式来解密cookie，加密状态及认证密码等关键信息。

描述：

微软的IIS服务器接收到客户端篡改过的加密内容，会判断是否和发送前的内容符合，如果不符合，就会返回特定的错误码，并给出加密字符串排列（padding）是VALID、INVALID的提示。客户端根据这些提示，反复尝试，经过 128 * b（b为加密内容的字节数）次尝试后，即可破解出machine key，从而伪造出授权的高权限cookie，可以窃取session、viewstate中的内容，可以获取web应用进程涉及到的敏感数据和文件。
参考:“Padding Oracle攻击实战（Practical Padding Oracle Attacks）：http://static.usenix.org/events/woot10/tech/full_papers/Rizzo.pdf

解决方法：

升级补丁修复问题，补丁获取链接http://technet.microsoft.com/en-us/security/bulletin/MS10-070

备注：

暂无相关信息

PHP触发出错信息-Possible PHP Error Message

漏洞级别： 高危或中危

参考：暂无相关信息

危害:

黑客可通过特殊的攻击向量，导致PHP出错并显示出错误信息，信息中有可能泄漏如绝对路径、源代码、sql语句等敏感信息，恶意攻击者很有可能利用这些信息实施进一步的攻击。视实际的web应用场景和攻击者的技术水平，该漏洞风险介于中危和高危之间。

描述:

黑客可通过特殊的攻击向量，导致PHP出错并显示出错误信息，有可能泄漏如绝对路径、源代码、sql语句等敏感信息，恶意攻击者有可能利用这些信息实施进一步的攻击。视实际的web应用场景和攻击者的技术水平，该漏洞风险介于中危和高危之间。

解决方法:

关闭PHP错误回显，修改php.ini配置文件中的display_errors=Off，或修正代码。

备注:

暂无相关信息

文件内容泄漏漏洞（文件包含漏洞）

漏洞级别： 高危

参考：OWASP:OWASP Category WASC:空字符注入 CVE:不适用 CWE:626

危害:

攻击者可以通过文件内容泄漏漏洞（或文件包含漏洞）获取敏感文件的内容，或直接执行其指定的恶意脚本，进得Web服务器的控制权限。

描述:

1.文件内容泄漏漏洞（或文件包含漏洞）允许攻击者读取服务器中的任意文件，或通过特殊的指令将脚本源码文件的内容合并至当前的文件中执行。
2.很多脚本语言允许通过特殊的指令（如PHP 通过require关键字）将其他脚本源码文件的内容合并至当前的文件中执行，如果这些特殊的指令在包含的文件路径中含有用户提交的数据，则恶意攻击

者就有可能通过构造特殊的数据将WEB服务器限制访问的文件内容（如操作系统或某些重要应用的配置文件）包含进来并通过浏览器获取其内容，这种方式通常称为本地文件包含；如果应用程序的配置还允许包含远程的其他服务器上的文件，恶意攻击者就有可能构造特殊的脚本然后通过包含并予以执行，进而获取WEB应用的敏感数据或控制权。

解决方法：

1、如果可能，使用包含指令时显式指定包含的文件名称；
2、如果必须通过用户的输入指定包含的文件，则最好分析用户的输入，然后从文件白名单中显式地选择；
3、请对用户的输入进行严格的过滤，确保其包含的文件在预定的目录中或不能包含URL参数。

备注：

暂无相关信息

Multiviews攻击

漏洞级别： 高危

参考：OWASP:OWASP Category

危害：

攻击者能利用该漏洞发现系统中敏感文件的位置。

描述：

当 Multiviews启用时，远程攻击者通过向索引页提交一个包含"M=D"字符传的请求，可查看目录内容。

解决方法：

更新Apache至最新版本，或正确配置Web容器/Web服务器。

备注：

暂无相关信息

短文件/文件夹泄露漏洞

漏洞级别： 高危

参考：OWASP:OWASP Category

危害：

攻击者可以利用“~”字符猜解或遍历服务器中的文件名，或对IIS服务器中的.Net Framework进行拒绝服务攻击。

描述：

攻击者可以利用“~”字符猜解或遍历服务器中的文件名，或对IIS服务器中的.Net Framework进行拒绝服务攻击。

解决方法：

1）如果你的web环境不需要asp.net的支持，你可以进入Internet 信息服务(IIS)管理器 --- Web 服务扩展 - ASP.NET 选择禁止此功能。
2）升级net framework 至4.0以上版本.
3）如果是虚拟主机空间用户，请联系空间提供商进行修复。

备注：

暂无相关信息

发现FTP服务

漏洞级别： 中危或低危

参考：暂无相关信息

危害：

发现FTP服务运行于该服务器上，如果服务器泄漏了提供FTP服务的软件版本信息，攻击者可能可以针对这个版本发动缓冲区溢出、权限绕过等攻击。

描述：

发现FTP服务运行于该服务器上，如果服务器泄漏了提供FTP服务的软件版本信息，攻击者可能可以针对这个版本发动缓冲区溢出、权限绕过等攻击。

解决方法：

如果FTP不需要对互联网的远程用户开放，请通过防火墙控制FTP的访问权限；如果服务器泄漏了提供FTP服务的软件版本信息，建议屏蔽这些版本信息。

备注：

暂无相关信息

路径污染(Path Pollution)

漏洞级别： 低危或中危

参考：OWASP:OWASP Category

危害:

服务器返回了错误信息或“HTTP-500错误”。攻击者向服务器提交精心构造的“Url路径”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。

描述:

服务器返回了错误信息或“HTTP-500错误”。攻击者向服务器提交精心构造的“Url路径”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。

解决方法:

严格过滤用户输入的数据。

备注:

暂无相关信息

URL重定向滥用

漏洞级别： 中高危

参考：OWASP:OWASP Category WASC:URL重定向滥用 CVE:不适用 CWE:601

危害:

Web 应用程序执行指向外部站点的重定向。攻击者可能会使用 Web 服务器攻击其他站点，这将增加他（或她）的匿名性。

描述:

网络钓鱼是一种社会工程技巧，其中攻击者伪装成受害者可能会与其进行业务往来的合法实体，以便提示用户透露某些机密信息（往往是认证凭证），而攻击者以后可以利用这些信息。网络钓鱼在本质上是一种信息收集形式，或者说是对信息的“渔猎”。
某个 HTTP 参数被发现保存有 URL 值，并导致 Web 应用程序将请求重定向至指定的 URL。通过将 URL 值修改为指向恶意站点，攻击者可以成功发起网络钓鱼诈骗并窃取用户凭证。
由于修改的链接中的服务器名称与原始站点完全相同，这样攻击者的网络钓鱼企图就披上了更容易让人轻信的外衣。

解决方法:

如下一些方法能够防止攻击：
1.在网页代码中需要对用户输入的数据进行严格过滤。
2.部署Web应用防火墙

备注:

暂无相关信息

目录遍历漏洞

漏洞级别： 中危或高危

参考：OWASP:OWASP Category

危害：

黑客可获得服务器上的文件目录，从而下载敏感文件。

描述：

黑客可获得服务器上的文件目录，从而下载敏感文件。

解决方法：

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。apache修改配置文件httpd.conf在配置文件中相关配置下给该目录添加Options Indexes；
nginx修改配置文件nginx.conf,在相关配置下给该目录添加autoindex on;
tomcat修改配置文件config/web.xml,添加 listingsfalse

备注：

暂无相关信息

UTF8 Directory Traversal Vulnerability源代码泄漏漏洞

漏洞级别： 高危

参考：OWASP:OWASP Category

危害：

黑客可以利用该漏洞下载网站的源代码，再从源代码里获得数据库的连接密码；或者通过源代码分析出新的系统漏洞，从而进一步入侵您的系统。

描述：

黑客可以利用该漏洞下载网站的源代码，再从源代码里获得数据库的连接密码；或者通过源代码分析出新的系统漏洞，从而进一步入侵您的系统。

解决方法：

升级Web容器至最新版本

备注：

暂无相关信息

Error-ASP.NET error message

漏洞级别： 中危

参考：暂无相关信息

危害:

发现ASP.NET Error错误信息

描述:

黑客可通过特殊的攻击向量，导致应用出错并显示出错误信息，有可能泄漏如绝对路径、源代码、sql语句等敏感信息，恶意攻击者有可能利用这些信息实施进一步的攻击。视实际的web应用场景和攻击者的技术水平，该漏洞风险介于中危和高危之间。

解决方法:

关闭错误信息回显，通过修改web目录下的web.config配置文件，统一报错页面，

CVS File Leak

漏洞级别： 低危

参考：暂无相关信息

危害:

发现cvs代码版本控制的cvs文件泄露，导致攻击者可进一步获取web应用敏感信息

描述:

发现cvs代码版本控制的cvs文件泄露，导致攻击者可进一步获取web应用敏感信息

解决方法:

删除CVS文件夹，并且注意以后上传web应用时禁止上传该文件夹

备注:

暂无相关信息

PHP errors enabled

漏洞级别： 中危

参考：暂无相关信息

危害：

发现php开启错误回显，导致PHP出错并显示出错误信息

描述：

黑客可通过特殊的攻击向量，导致PHP出错并显示出错误信息，有可能泄漏如绝对路径、源代码、sql语句等敏感信息，恶意攻击者有可能利用这些信息实施进一步的攻击。视实际的web应用场景和攻击者的技术水平，该漏洞风险介于中危和高危之间。

解决方法：

关闭PHP错误回显，修改php.ini配置文件中的display_errors=Off，或修正代码。

备注：

暂无相关信息

PHP Information Leak

漏洞级别： 中危

参考：暂无相关信息

危害：

发现PHPInfo()信息泄漏漏洞，Web站点的某些测试页面可能会使用到PHP的phpinfo()函数，会输出服务器的关键信息

描述：

发现存在phpinfo()函数返回的页面，泄露web应用及服务器相关敏感信息

解决方法：

如果该文件为测试文件，需立即删除，或者删除该文件中的phpinfo()函数

备注：

暂无相关信息

PHP open_basedir is not set

漏洞级别： 低危

参考：暂无相关信息

危害：

发现PHP配置文件中open_basedir未设置，open_basedir可将用户访问文件的活动范围限制在指定的区域

描述：

发现PHP配置文件中open_basedir未设置，攻击者可能会利用该缺陷进行任意文件读取等攻击手段

解决方法：

修改PHP配置文件，添加open_basedir="指定目录"，open_basedir可将用户访问文件的活动范围限制在指定的区域

备注：

暂无相关信息

Possible .Net Error Message

漏洞级别： 中危

参考：暂无相关信息

危害：

发现ASP.NET Error错误信息

描述：

黑客可通过特殊的攻击向量，导致应用出错并显示出错误信息，有可能泄漏如绝对路径、源代码、sql语句等敏感信息，恶意攻击者有可能利用这些信息实施进一步的攻击。视实际的web应用场景和攻击者的技术水平，该漏洞风险介于中危和高危之间。

解决方法：

关闭错误信息回显，通过修改web目录下的web.config配置文件，统一报错页面，

Vulnerable Version Of JQuery

漏洞级别： 低危

参考：暂无相关信息

危害：

发现web应用程序使用了低版本存在漏洞的JQuery

描述：

该版本的JQuery，存在安全问题，有可能对web应用造成影响

解决方法：

建议升级JQuery至最新版本

备注：

暂无相关信息

XPath Injection

漏洞级别： low

参考：暂无相关信息

危害：

攻击者通过构建特殊的输入，这些输入往往是XPath语法中的一些组合，这些输入将作为参数传入Web 应用程序，通过执行XPath查询而执行攻击者想要的操作

描述：

攻击者通过构建特殊的输入，这些输入往往是XPath语法中的一些组合，这些输入将作为参数传入Web 应用程序，通过执行XPath查询而执行攻击者想要的操作

解决方法：

严格限制传入参数输入值的格式，过滤特殊字符（ <、>、' 、" 等）。

备注：

暂无相关信息

发现敏感服务端口

漏洞级别： 提示

参考：暂无相关信息

危害：

在该服务器上发现敏感服务端口对外开放存在风险，容易引起安全问题

描述：

在该服务器上发现敏感服务端口对外开放存在风险，容易引起安全问题

解决方法：

关闭非必需的服务端口，如是必需开放端口，建议修改其默认端口更改为高位端口；设置白名单访问，限制非法连接请求

备注：

暂无相关信息

发现敏感服务端口

漏洞级别： 提示

参考：暂无相关信息

危害：

在该服务器上发现敏感服务端口对外开放存在风险，容易引起安全问题

描述：

在该服务器上发现敏感服务端口对外开放存在风险，容易引起安全问题

解决方法：

关闭非必需的服务端口，如是必需开放端口，建议修改其默认端口更改为高位端口；设置白名单访问，限制非法连接请求

备注：

暂无相关信息

.htaccess 文件可读

漏洞级别： 低危

参考：暂无相关信息

危害：

黑客可通过分析.htaccess文件中的内容，为进一步攻击提供更详细的信息

描述：

黑客可通过分析.htaccess文件中的内容，为进一步攻击提供更详细的信息

解决方法：

修改nginx配置文件，在server块中添加location ~ /\.ht { deny all; }，禁止访问该文件

备注：

暂无相关信息

Resin Vulnerability

漏洞级别： 中危或高危

参考：暂无相关信息

危害：

远程攻击者可能利用此漏洞读取Web主目录下的任意文件，包括JSP源码或类文件。

描述：

默认下Resin的/webapps目录下/resin-doc中包含有一个扩展war文件，远程攻击者可能利用此漏洞读取Web主目录下的任意文件，包括JSP源码或类文件。

解决方法：

从生产系统中删除resin-doc.war文件，不要使用默认的配置文件部署。

备注：

暂无相关信息