# 信息泄漏篇

白帽技术与网络安全 昨天

以下文章来源于Ms08067安全实验室 ， 作者徐哥

**Ms08067安全实验室**
www.ms08067.com

作者：实验室核心 cong1984

1、robots.txt泄漏敏感信息
漏洞情况信息：
搜索引擎可以通过robots文件可以获知哪些页面可以爬取，哪些页面不可以爬取。
Robots协议是网站国际互联网界通行的道德规范，其目的是保护网站数据和敏感信息、确保用户个人信息和隐私不被侵犯，如果robots.txt文件编辑的太过详细，反而会泄露网站的敏感目录或者文件，比如网站后台路径，从而得知其使用的系统类型，从而有针对性地进行利用。
检测手段：
1、检测形式多样，工具爬虫扫描得到敏感文件的路径，从而找到robots文件；
2、手工挖掘，直接在域名后输入/robots.txt进行查看。
造成的后果：
攻击者可通过发现robots.txt文件，收集网站的敏感目录或文件，从而有针对性的进行利用。
漏洞威胁等级：
低危：robots.txt中存在allow和disallow的具体内容泄露敏感目录信息。

2、敏感文件信息泄漏
漏洞情况信息：
敏感数据包括但不限于：口令、密钥、证书、会话标识、License、隐私数据（如短消息的内容）、授权凭据、个人数据（如姓名、住址、电话等）等，在程序文件、配置文件、日志文件、备份文件及数据库中都有可能包含敏感数据。
检测手段：
1、 检测形式多样，工具爬虫扫描得到敏感文件的路径，从而找到敏感数据，
2、 手工挖掘，根据web容器或者网页源代码的查看，找到敏感信息。
造成的后果：
攻击者可通过上述方式获取网站敏感文件，收集网站敏感信息，从而有针对性的进行利用。

漏洞威胁等级：
高危：返回含有重要的敏感信息的文件，比如数据库文件、代码的备份文件或svn、git版本控制文件等。

3、历史文件残留
漏洞情况信息：
应用遗留的过时文件、备份页面、渗透测试遗留文件、开发文件残留的测试文件等。
检测手段：
1、 常见检测方法是通过对网站进行web漏洞扫描，直接利用爬虫来爬取网站可能存在的路径以及链接，如果存在备份文件，则可通过web直接进行下载。
2、 也可以通过自行构造字典，对网站某一目录下，指定字典进行爆破，常见的扫描工具有wwwscan、御剑后台扫描工具等。
造成的后果：
攻击者可通过上述方式获取网站备份文件、过时文件、遗留文件等内容，收集网站敏感信息，从而有针对性的进行利用。
漏洞威胁等级：
高危：泄露重要敏感信息，或能够进行核心业务操作。
中危：泄露一般重要信息，做只能进行一般功能操作。
低危：页面泄露非重要信息，不能进行相关功能操作。

4、报错页面敏感信息泄漏
漏洞情况信息：
错误页面由服务器产生403、404、500等错误时，返回详细错误信息。报错信息中可能会包含服务器代码信息、数据库连接信息、SQL语句或者敏感文件的路径，为攻击者收集信息提供了方便。
检测手段：
1. 通过目录扫描或手工输入不存在的文件或路径，触发服务器产生404错误并返回404页面；
2. 通过目录扫描或手工输入一个无权限查看的文件或路径，触发服务器产生403错误并返回403页面；
3. 手工输入不存在的参数或特殊构造的字符串，如单引号，尖括号等，触发服务器产生500错误并返回500页面或异常信息。
造成的后果：
攻击者可通过上述几种方式触发Web应用程序报错，提取报错信息泄露的敏感信息，如Web中间件的版本信息、数据库连接信息。
漏洞威胁等级：
高危：开启调试模式，泄露大量应用的敏感信息如代码、报错信息等；
低危：未开启调试模式，泄露部分中间件版本、少量代码信息等。

5、物理路径泄漏
漏洞情况信息：
应用中泄露出应用在主机中的绝对地址路径。
检测手段：
1. 打开网页源代码，查看图片等媒体的链接及超链接；
2. 通过报错信息获取
造成的后果：
攻击者可通过获取网站物理路径，为下一步攻击做准备。
漏洞威胁等级：
低危：泄露应用绝对路径。

6、明文密码本地保存
漏洞情况信息：
明文密码保存在本地客户端
检测手段：
1. 查看网页源代码
2. 查看网站在本地客户端的缓存文件
造成的后果：
攻击者可通过嗅探或直接查看源代码的方式获取传输到前端的账号及密码，登录他人账号。
漏洞威胁等级：
高危：全部账号的明文密码保存在本地客户端
低危：只有本账号的明文密码保存在本地客户端

7、入侵痕迹残留
漏洞情况信息：
在渗透过程中发现应用中存在曾经的入侵痕迹，如存在的webshell文件。
检测手段：
通常使用Web应用安全漏洞扫描工具或目录扫描工具发现入侵痕迹。
造成的后果：
残留的入侵痕迹可被其他攻击者用于二次攻击，对网站造成一定的影响。
漏洞威胁等级：
高危：发现存在入侵痕迹，比如存在Webshell或者网页被篡改。

8、HTTP头信息泄漏
漏洞情况信息：
在服务器返回的HTTP头中泄露服务器信息

检测手段：
1. 在浏览器的调试窗口中查看HTTP响应头
2. 使用代理软件如burpsuite、fiddler，拦截HTTP响应头
造成的后果：
攻击者可通过获取服务器banner信息，针对某个版本存在的漏洞进行定向攻击。
漏洞威胁等级：
低危：泄露服务器版本等信息

9、目录浏览
漏洞情况信息：
目录浏览漏洞是由于网站存在配置缺陷，存在目录可浏览漏洞，这会导致网站很多隐私文件与目录泄露，比如数据库备份文件、配置文件等，攻击者利用该信息可以更容易得到网站权限，导致网站被黑。
检测手段：
可以利用web漏洞扫描器扫描web应用进行检测，也可通过搜索，网站标题包含“index of”关键词的网站进行访问。
造成的后果：
攻击者通过访问网站某一目录时，该目录没有默认首页文件或没有正确设置默认首页文件，将会把整个目录结构列出来，将网站结构完全暴露给攻击者；攻击者可能通过浏览目录结构，访问到某些隐秘文件（如PHPINFO文件、服务器探针文件、网站管理员后台访问地址、数据库连接文件等）。
漏洞威胁等级：
高危：目录可以浏览，泄露包含密码、个人信息等敏感文件。
低危：目录可以浏览，未泄露包含密码、个人信息等敏感文件。

10、默认页面泄漏
漏洞情况信息：
存在默认安装中间件、插件、框架等会携带示例页面及说明文档。
检测手段：
1. 可以利用web漏洞扫描器或目录扫描器扫描web应用进行检测
2. 根据网站使用的第三方组件和框架手工输入对应的示例页面。
造成的后果：
攻击者可利用默认页面提供的功能和信息对服务器进行攻击。
漏洞威胁等级：
高危：存在可访问默认页面，泄露高风险敏感信息（如：tomcat 的 examples 目录）。
中危：存在可访问默认页面，泄露于业务、操作和配置相关的敏感信息。
低危：存在可访问的默认页面，但未泄露敏感信息。

11、存在可访问的管理后台入口
漏洞情况信息：
应用存在未限制访问的后台，或者能直接登录管理后台。
检测手段：
1. 可以利用web漏洞扫描器或目录扫描器扫描web应用进行检测
2. 识别网站使用的cms框架，判断其默认的管理后台地址。
3. 在网站中寻找管理后台超链接。
造成的后果：
攻击者可通过登录网站管理后台篡改页面，或利用上传功能上传webshell，导致服务器被控制。
漏洞威胁等级：
高危：可访问默认管理后台，通过后台获取 shell。
中危：可访问默认管理后台，并成功登录，但无法获取 shell。
低危：可访问默认管理后台，但无法登录或执行危险操作。

12、存在可访问的管理控制台入口
漏洞情况信息：
Web 控制台是一种基于 Web 的用户界面， 其常常被用于网站后台或者web容器。控制台中，其不仅仅局限于容器或者网站管理后台，还包括一些数据库默认地址等。在web安全中，网站系统在泄漏其web容器（中间件）或者数据库的控制台后，存在增加被入侵的风险。常见的web控制台包括以下多种：tomcat、aria2、weblogic、websphere、oracle 、 jboss 、 等 。 这 些 web 的 容 器 控 制 台 常 见 访 问 形 式 ：http://hostname:port/load/，
例如：http://x.x.x.x:8080/manage/。
检测手段：
常见的web控制台检测方法：整体思路为首先需识别网站容器的指纹，判断其所采用的中间件，然后去扫描其所开放的端口，根据开放端口信息和常见固定的路径，去判断其控制台地址。以下列举常见控制台的检测方法：
1. Apache+tomcat ： tomcat 常 见 的 web 控 制 台 地 址 为 ：http://x.x.x.x/manager/html
或者添加端口：
http://x.x.x.x:8080/manager/html，从TOMCAT5（开始默认/admin后台不存在，tomcat5之前的控制台为/admin。
2. Weblogic控制台：http://[weblogic所在机器IP]:[weblogic端口]/console若没有指定端口，且安装在本机上则为：（weblogic默认端口为7001）
http://localhost:7001/console。
3. Websphere控制台：websphere的控制台常见有两种，一种是基于http，另一种是基于https的，分别为如下：http://localhost:9060/ibm/console和

https://localhost:9043/ibm/console/logon.jsp。
4. Oracle web控制台：一般默认的是http://localhost:5500/em,一般存放于Oracle安装文件夹下的install文件夹下的文本文件，上面有web控制台的地址。
5. Mongodb web控制台：自带了Web控制台：默认和数据服务一同开启。他的端口在Mongodb数据库服务器端口的基础上加1000，如果是默认的Mongodb数据服务端口(Which is 27017)，则相应的Web端口为28017，这个页面可以看到当前Mongodb的所有连接、各个数据库和Collection的访问统计，包括：Reads, Writes, Queries,GetMores ,Inserts, Updates, Removes、写锁的状态、以及日志文件的最后几百行（CentOS+10gen yum 安装的mongodb默认的日志文件位于/var/log/mongo/mongod.log)。
6. HP system managent控制台：该控制台一般默认的端口为2381，可在其后添加路径/cpqlogin.php?errno=100&severity=4，即可访问.
https://localhost:2381/cpqlogin.php?errno=100&severity=4
7. Service Registry 3控制台：在 Web 浏览器中键入以下 URL：
http://hostname:port/soar/例如：http://localhost:6060/soar/如果系统中安装了Registry，则 hostname 为 localhost。如果系统中尚未安装 Registry，请使用安装了Registry的系统的名称。port 的值通常为 6060，除非发生端口冲突。
8. Tomcat控制台URL：
http://www.exmaple.com/manager/html
9. Tomcat控制台默认帐号admin，默认密码admin或空
10. Jboss控制台URL：
http://www.exmaple.com/jmx-console/
11. Jboss控制台URL：
http://www.exmaple.com/web-console/
12. Jboss控制台默认无须登陆，或者admin/admin
13.WebSpher控制台URL：
http://www.exmaple.com/ibm/console/logon.jsp
14. WebSphere默认帐号admin，默认密码admin
15. Apache控制台URL：
http://www.exmaple.com/server-status
16. Axis2控制台URL：
http://www.exmaple.com/axis2-admin/
17. Axis2控制台默认口令帐户：admin/axis2
18. iSAP控制台URL：
http://www.exmaple.com/admin/login.jsp
19. iSAP控制台默认的帐号和密码：admin/admin
20. “普元”管理控制台URL：
http://www.exmaple.com/eosmgr/

21. “普元”管理控制台默认的帐号和密码：sysadmin/000000
造成的后果：
攻击者使用弱口令扫描工具或者直接使用常见的弱口令去尝试登录Web中间件的管理控制后台，然后通过部署war包上传webshell，进而控制整个系统。
漏洞威胁等级：
高危：可访问默认中间件控制台，且能过成功获取 shell。
中危：可访问默认中间件控制台，并成功登录，但无法获取 shell。
低危：可访问默认中间件控制台，但无法登录且无法执行危险操作。