AoDun 远程安全评估服务

技术白皮书

文档版本 18-03
发布日期 2018-3-1

北京傲盾软件有限责任公司承诺为客户提供全方位的技术支持

用户可与当地傲盾办事处联系，或直接与公司总部联系。

北京傲盾软件有限责任公司

地址： 中国北京市海淀区上地四街一号院三号楼五层 邮编：100085

网址： http://www.aodun.com.cn

客户服务电话： 800-990-5568

010-82728052-880

商标声明

傲盾® 以及其他傲盾商标均为北京傲盾软件有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

前 言

版本说明

本手册适用于傲盾远程安全评估服务。

内容介绍

本手册主要介绍了傲盾远程安全评估服务的主要功能特点。

文档修改记录

文档版本	修改说明	发布时间	作者
18-03	首次撰写发布	2018-03-06	AD 技术

目　录

1 概述

每年都有数以千计的网络安全漏洞被发现和公布，再加上攻击者手段的不断变化，用户的网络安全状况也随着被公布安全漏洞的增加而日益严峻。因此，安全评估对于绝大多数用户都是不容忽视的，用户必须比攻击者更早掌握自己网络安全漏洞并且做好适当的修补，才能够有效地预防入侵事件的发生。

事实证明，99%的攻击事件都是利用未修补的漏洞。许多已经部署防火墙、入侵检测系统和防病毒软件的企业仍然饱受漏洞入侵之苦，其中有更多受到蠕虫及其变种的破坏，造成巨大的经济损失。归根结底，其原因是用户缺乏一套完整的漏洞管理体系，未能落实定期评估与漏洞修补工作，忽视了漏洞的管理，最终漏洞成为攻击者实施攻击的有效途径，甚至成为蠕虫攻击的目标。

依托国内权威中文漏洞知识库和已在国际上享有盛名的安全小组，傲盾远程安全评估服务能够定期和持续地给用户提供全面可靠的安全评估服务，满足多种应用需求，并且提供完整的漏洞管理机制，有效降低用户网络和主机风险，更大限度地保证用户网络和系统的安全性和稳定性。

2 安全评估的定义

信息系统的安全风险，是由人为的、自然的威胁利用系统脆弱性所造成安全事件的可能性及其可能造成的影响组成。信息安全风险评估（本文以下简称“风险评估”），则是指依据国家有关信息技术标准，对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行科学、公正的综合评估的活动过程，它要评估信息系统的脆弱性、信息系统面临的威胁以及脆弱性被威胁源利用后所产生的实际负面影响，并根据安全事件发生的可能性和负面影响的程度来识别信息系统的安全风险。

信息安全是一个动态的复杂过程，它贯穿于信息资产和信息系统的整个生命周期。信息安全的威胁来自于内部破坏、外部攻击、内外勾结进行的破坏以及自然危害。必须按照风险管理的思想，对可能的威胁、脆弱性和需要保护的信息资源进行分析，依据风险评估的结果为信息系统选择适当的安全措施，妥善应对可能发生的风险。

3 安全评估的目的

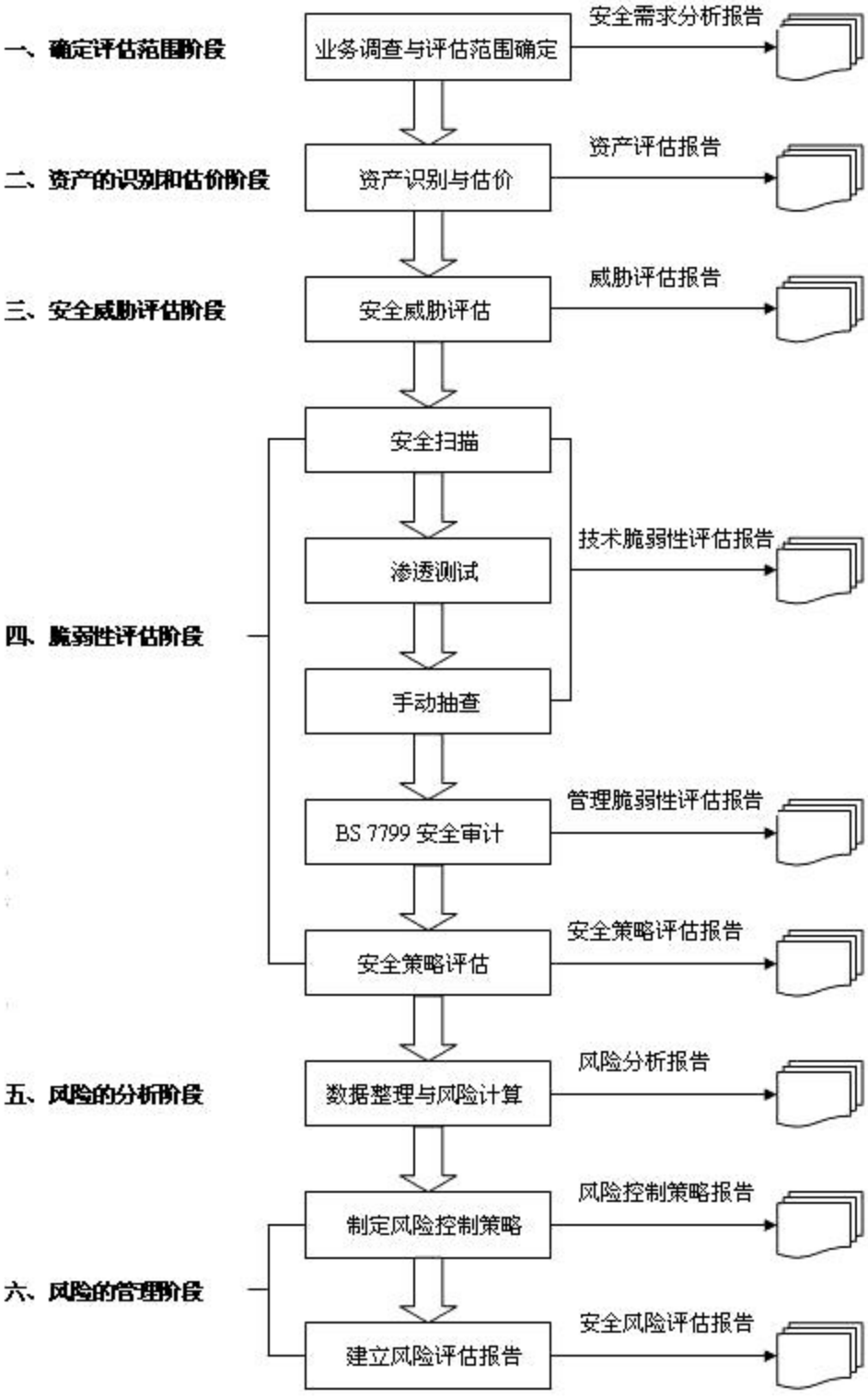
风险评估的目的是全面、准确的了解组织机构的网络安全现状，发现系统的安全问题及其可能的危害，为系统最终安全需求的提出提供依据。分析网络信息系统的安全需求，找出目前的安全策略和实际需求的差距，为保护信息系统的安全提供科学依据。通过合理步骤制定适合系统具体情况的安全策略及其管理和实施规范，为安全体系的设计提供参考。

风险评估是一个组织机构实现信息系统安全的重要步骤，可以使决策者对其业务信息系统的安全建设或安全改造思路有更深刻的认识。通过风险评估，可以清楚地了解业务信息系统包含的重要资产、面临的主要威胁及本身的弱点；评估哪些威胁出现的可能性较大，造成的影响也较大，哪些威胁出现的可能性较小，造成的影响可以忽略不计；搞清楚通过保护哪些资产，防止哪些威胁出现，如何保护和防止才能保证系统达到一定的安全级别；计算安全方案需要多少技术和费用的消耗；还要更进一步分析出信息系统的风险是如何随时间变化的，将来应如何面对这些风险。

风险评估为后期进一步安全防护措施的实施提供了严谨的安全理论依据，为决策者制定网络安全策略、构架安全体系以及确定有效的安全措施、选择可靠的安全产品、建立全面的安全防护层次提供了一套完整、规范的指导模型。

漏洞扫描是系统工作，并非检查某一项程序有没有漏洞，需要包括系统漏洞扫描、安全配置合规检查、应用程序漏洞扫描、web站点漏洞扫描等立体的系统安全评估。另外，漏洞扫描基于事先预防，而非事后分析。提前把安全漏洞补上，避免网络入侵等安全事件发生。

3.1 安全评估流程图


一、确定评估范围阶段
业务调查与评估范围确定
安全需求分析报告
二、资产的识别和估价阶段
资产识别与估价
资产评估报告
三、安全威胁评估阶段
安全威胁评估
威胁评估报告
四、脆弱性评估阶段
安全扫描
渗透测试
手动抽查
技术脆弱性评估报告
BS 7799 安全审计
管理脆弱性评估报告
安全策略评估
安全策略评估报告
五、风险的分析阶段
数据整理与风险计算
风险分析报告
六、风险的管理阶段
制定风险控制策略
风险控制策略报告
建立风险评估报告
安全风险评估报告

4 傲盾远程安全评估服务

傲盾软件结合多年的安全服务实践经验，推出漏洞管理服务，可以高效、全方位的检测网络中的各类脆弱性风险，提供专业、有效的安全分析和修补建议，并贴合安全管理流程对修补效果进行审计，最大程度减小受攻击面，是您身边专业的“漏洞管理专家”。

全面发现信息系统存在的安全漏洞、安全配置问题、应用系统安全漏洞，检查系统存在的弱口令，收集系统不必要开放的账号、服务、端口，形成整体安全风险报告。

提供报告分析方式，在大规模安全检查后，快速定位风险类型、区域、严重程度，根据重要性进行排序，可以从报告直接定位到具体主机具体漏洞。

安全管理不只是技术，更重要的是通过流程制度对安全脆弱性风险进行控制，服务结合安全管理制度，支持安全风险预警、检查、分级管理、修复、审计流程，并监督流程的执行。

4.1 服务特性

傲盾漏洞扫描服务能够为信息系统安全脆弱性评估提供有力依据，该服务产品具备以下功能特性：

能够全面发现信息系统存在的各种脆弱性问题，包括安全漏洞、安全配置问题、应 用系统安全漏洞，检查系统存在的弱口令，收集系统不必要开放的账号、服务、端口，形成整体安全风险报告

能够快速定位风险类型、区域、严重程度，直观展示安全风险

能够在虚拟化环境、IPv6环境中进行脆弱性检测

4.2 多种检查能力合一，全面系统脆弱性发现

对于攻击者来说，IT系统的方方面面都存在脆弱性，这些方面包括常见的操作系统漏洞、应用系统漏洞、弱口令，也包括容易被忽略的错误安全配置问题，以及违反最小化原则开放的不必要的账号、服务、端口等。

傲盾远程安全评估系统能够全方位检测IT系统存在的脆弱性，发现信息系统存在的安全漏洞、安全配置问题、应用系统安全漏洞，检查系统存在的弱口令，收集系统不必要开

放的账号、服务、端口，形成整体安全风险报告，帮助安全管理人员先于攻击者发现安全问题，及时进行修补。

傲盾远程安全评估服务支持全方位的安全漏洞、安全配置、应用系统安全漏洞扫描，对网络系统中多个方面的安全脆弱性统一进行分析和风险评估，给出总体安全状态评价，全面掌握信息系统安全风险。

4.3 识别非标准端口，准确扫描服务漏洞

在IT系统安全管理中，经常会遇到由于业务需要而改变默认应用服务端口的情况，改变协议默认端口能够规避业务冲突、减少设备投入、充分利用资源，但某种协议在非标准端口上如何识别和扫描也成为安全管理产品需要解决的问题。

傲盾远程安全评估服务应用先进的非标准端口识别技术、以及丰富的协议指纹库，能够快速准确的识别非标准端口上的应用服务类型，并进一步进行漏洞检测，极大的避免了扫描过程中的漏报和误报。

4.4 服务内容

评估服务通过远程扫描任务对在线的目标主机进行漏洞（系统漏洞和Web应用漏洞）、配置和脆弱帐号检查，可以对扫描目标进行漏洞扫描和主机的配置扫描，能够发现扫描目标中存在的漏洞（系统漏洞）以及主机配置不合规信息。包含主机发现、操作系统识别、服务识别、弱口令检测、漏洞扫描、配置核查、漏洞验证等。

4.4.1 操作系统漏洞扫描

购买漏洞扫描服务后，安全管理员将定期对用户网络进行安全检测，安全检测可帮助客户最大可能的消除安全隐患，尽可能早地发现安全漏洞并进行修补，有效的利用已有系

统，优化资源，提高网络的运行效率。

由于漏洞和安全隐患的形式多种多样，安装新软件和启动新服务都有可能使原来隐藏的漏洞暴露出来，因此进行这些操作之后应该重新扫描系统，才能使安全得到保障。

新的网络建设和网络改造后的安全成效检验；

网络承担重要任务前的安全性测试；

网络安全事故后的分析调查；

重大网络安全事件前的准备；

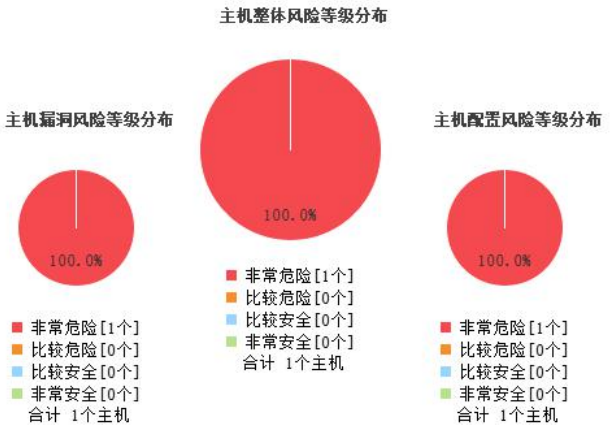
公安、保密部门组织的安全性检查。

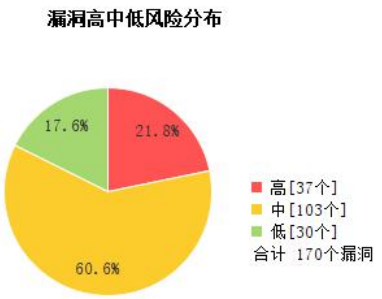
等多种应用场景。

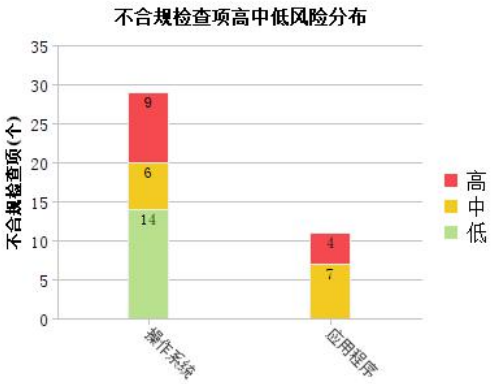
网络风险	非常危险(10.0分)

任务名称	扫描【
任务类型	漏洞配置扫描
漏洞扫描模板	自动匹配扫描
配置检查模板列表	Linux 配置规范 Nginx 配置规范 (Linux)
系统版本信息	V6.0R02F03SP06

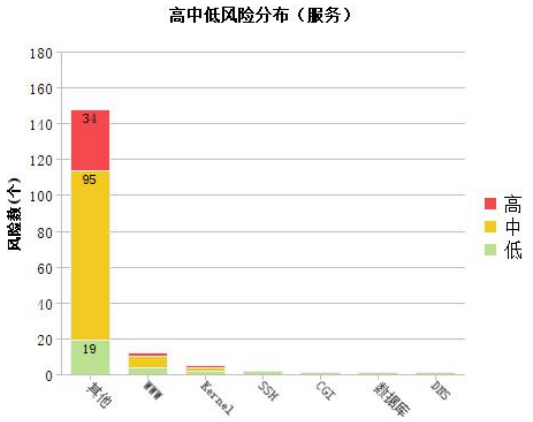
时间统计	开始：2018-03-02 15:50:25 结束：2018-03-02 15:54:45 历时：4分20秒
主机统计	存活主机：1 成功扫描主机：1 失败扫描主机：0 未扫描主机：0







服务 应用 系统 威胁 时间 CVE年份 全部



服务	高风险	中风险	低风险	总计
其他	34	95	19	148
WWW	2	6	4	12
Kernel	1	2	2	5
SSH	0	0	2	2
CGI	0	0	1	1
数据库	0	0	1	1
DNS	0	0	1	1
合计	**37**	**103**	**30**	**170**

服务	高风险	中风险	低风险	总计
其他	34	95	19	148
WWW	2	6	4	12
Kernel	1	2	2	5
SSH	0	0	2	2
CGI	0	0	1	1
数据库	0	0	1	1
DNS	0	0	1	1
合计	**37**	**103**	**30**	**170**

CVE年份	高风险	中风险	低风险	总计
CVE-2014	12	47	11	70
CVE-2016	11	15	3	29
CVE-2017	8	5	0	13
CVE-2015	5	16	3	24
CVE-2013	1	15	3	19
CVE-2010	0	2	0	2
CVE-2011	0	2	0	2
CVE-2012	0	1	0	1
Others	0	0	7	7
CVE-1999	0	0	3	3
合计	**37**	**103**	**30**	**170**

时间	高风险	中风险	低风险	总计
2014年	12	49	11	72
2016年	11	15	4	30
2017年	8	5	0	13
2015年	5	16	3	24
2013年	1	15	4	20
2012年	0	2	1	3
2011年	0	1	0	1
1999年	0	0	4	4
2001年	0	0	3	3
合计	**37**	**103**	**30**	**170**

威胁	高风险	中风险	低风险	总计
其他	35	99	21	155
远程拒绝服务	1	1	0	2
远程执行命令	1	0	0	1
远程信息泄露	0	3	9	12
合计	**37**	**103**	**30**	**170**

系统	高风险	中风险	低风险	总计
Linux	28	86	17	131
UNIX通用	7	10	2	19
系统无关	2	7	11	20
合计	**37**	**103**	**30**	**170**

应用	高风险	中风险	低风险	总计
其他	34	93	26	153
Nginx	2	5	0	7
Linux Kernel	1	3	1	5
SSL	0	2	1	3
OpenSSH	0	0	1	1
SSH	0	0	1	1
合计	**37**	**103**	**30**	**170**

4.4.2 主机配置核查

主机配置核查可以大大提高安全检查结果的准确性和合规性，用以在企业的上线安全检查、第三方入网安全检查、合规安全检查（上级检查）、日常安全检查和安全服务任务中，协助查找设备在安全配置中存在的差距，并与安全整改与安全建设相结合，提升各类

业务系统的安全防护能力和达到整体合规要求.

作为对传统漏洞扫描项目的强力补充，能够帮助用户发现网络和应用中存在的配置缺陷、管理漏洞，帮助用户提升网络和应用系统的安全强度。

主要应用于设备入网、工程验收、日常维护、合规检查等方面。通过对目标系统展开合规安全检查，找出不符合的项并选择和实施安全措施来控制安全风险。

配置扫描引擎支持操作系统配置安全检查、数据库配置安全检查、应用程序配置安全检查、网络设备配置安全检查以及虚拟化设备的配置安全检查，等强大的扫描能力。

安全配置检查	操作系统	AIX 配置、HP-UX 配置、Linux 配置、Debian 配置、Oracle Linux 配置、Suse 配置、Solaris 配置、Windows2000 配置、Windows 配置
	数据库	DB2 配置、Informix 配置、MySQL 配置、Oracle 配置、SQL Server 配置、Sybase 配置、
	应用程序	Apache 配置、BIND 配置、Domino 配置、HIS 配置、IIS7.0 配置、IIS6.0 配置、Jboss4,5,6 配置、Nginx 配置、Resin 配置、Tomcat 配置、TongWeb 配置、WebLogic 配置、WebSphere 配置
	网络设备	Cisco 配置、H3C 配置、Huawei 配置、Juniper 配置、ZTE 配置、锐捷交换机配置、等
	虚拟化设备	Hyper-V 配置、OpenStack 配置、VMware ESXi 配置、VMware vCenter 配置、Xen 配置、XenServer 配置

Nginx配置核查

分组	检查配置项		风险值	主机分布 [不合规数/总数]	不合规百分比	不合规主机
日志审计	1	检查是否启用日志功能---记录错误日志	7	1/1	100%	
	2	检查是否启用日志功能---记录访问日志	7	1/1	100%	
协议安全	3	检查是否限制IP访问	4	1/1	100%	
其它安全	11	检查是否隐藏nginx版本信息	7	1/1	100%	
	10	检查是否自定义错误信息	7	1/1	100%	
	5	检查是否控制超时时间---客户端保持活动的超时时间	4	1/1	100%	
	4	检查是否控制超时时间---客户端请求读取超时时间	4	1/1	100%	
	7	检查是否限制客户端下载的并发连接数	4	1/1	100%	
	6	检查是否控制超时时间---响应客户端的超时时间	4	1/1	100%	
	9	检查是否配置防盗链接设置	4	1/1	100%	
	8	检查是否限制客户端的下载速度	4	1/1	100%	

Linux配置核查

分组	检查配置项		风险值	主机分布 [不合规数/总数]	不合规百分比	不合规主机
账号口令	22	检查设备密码复杂度策略	7	1/1	100%	
	1	检查是否设置口令生存周期	7	1/1	100%	
	3	检查口令最小长度	7	1/1	100%	
	2	检查是否设置口令更改最小间隔天数	7	1/1	100%	
	4	检查是否设置口令过期前警告天数	7	1/1	100%	
认证授权	23	检查用户目录缺省访问权限设置	7	1/1	100%	
	11	检查重要目录或文件权限设置	5	1/1	100%	
	10	检查用户umask设置	5	1/1	100%	
	19	检查重要文件属性设置	5	1/1	100%	
日志审计	27	检查是否配置远程日志功能	1	1/1	100%	
	38	检查安全事件日志配置	1	1/1	100%	
	37	检查是否记录用户对设备的操作	1	1/1	100%	
协议安全	13	检查是否禁止root用户远程登录	7	1/1	100%	
其它安全	21	检查是否使用PAM认证模块禁止wheel组之外的用户su为root	7	1/1	100%	

4.4.3 Web 站点漏洞扫描

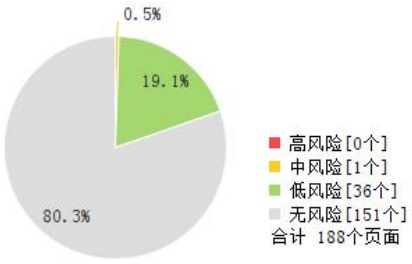
Web站点漏洞扫描服务，支持对web服务器进行全面的多种扫描，包含超过3000多种有潜在危险的网页文件的检测，支持HTTP/HTTPS协议站点的检查，支持多种web应用脚本、web插件的检查，支持大小写敏感，会话重组，密码猜测等先进的漏洞扫描技术，支持文件上传检查，日志文件检查，默认配置检查，信息泄漏检查，隐私泄露检查，远程注射（XSS/Script/HTML）检查，远程文件检索（Web 目录中），拒绝服务漏洞检查，远程文件检索（服务器），代码远程支持执行检查，SQL注入检查，跨站脚本检查，认证绕过验证，软件关联检查，文件属性检查，banner信息检查等。

网络风险	比较安全(4.3分)

任务名称	扫描[http://[redacted].aodun.com.cn:7789/j[redacted]
任务类型	WEB应用扫描
漏洞扫描模板	自动匹配扫描
信息统计	已爬取文件数：188 有漏洞文件数：37 已扫描链接数：137 已爬取链接数：303

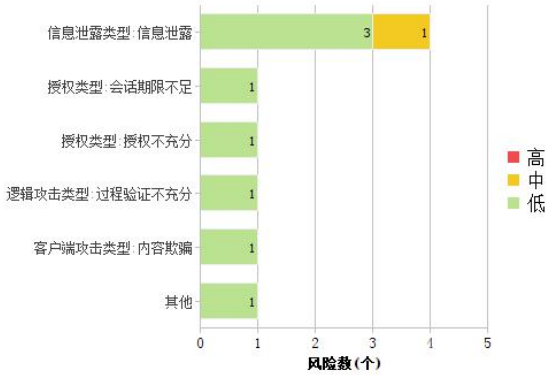
域名统计	已扫描域名数：1 非常危险域名数：0
时间统计	开始：2018-02-02 18:31:56 结束：2018-02-02 19:36:36 历时：1小时4分40秒
版本信息	系统版本：V6.0R02F03SP06 Web插件版本：V6.0R02F00.0802

页面风险级别分布



漏洞高中低风险分布

高中低风险分布（威胁）



威胁分类	高风险	中风险	低风险	总计
授权类型:会话期限不足	0	0	1	1
授权类型:授权不充分	0	0	1	1
信息泄露类型:信息泄露	0	1	3	4
逻辑攻击类型:过程验证不充分	0	0	1	1
客户端攻击类型:内容欺骗	0	0	1	1
其他	0	0	1	1
合计	**0**	**1**	**8**	**9**