网站安全评估 服务白皮书V1.0

网世界 心归宿

网宿科技 全球领先的互联网基础设施平台

关注公众号，及时了解网宿产品与服务动态

400-010-0617 | www.wangsu.com

Content 目录

网宿安全评估服务是“网宿网盾”安全品牌旗下专为各类网站遇到的安全防护问题难提出的服务，主要通过对网站进行漏洞扫描、渗透测试、安全审计、漏洞预警等操作及时发现网站系统中存在的安全隐患，并提出相应的安全解决方案.同时提供远程或现场技术指导服务，帮助网站有效地预防入侵事件的发生。“网宿网盾”是网宿科技发布的云安全全新品牌，其业务全景主要覆盖网络安全、业务安全、内容安全、DNS 安全、源站可用性、传输安全、安全管理和安全评估等八大领域，“网宿网盾”依托高容量节点和自主研发的安全技术，构建出一套云端智能安全体系。

1.行业现状和挑战

随着计算机和互联网技术的飞速发展，信息网络已经成为社会发展和人类生活的重要工具。然而由此带来的网络信息安全问题也日益突出。

1.1 漏洞频发，系统存在安全隐患

随着漏洞挖掘技术的不断发展，攻击工具日益专业化、易用化，漏洞爆发频率越来越高；而网站管理者对网络系统的安全漏洞无法及时发现和修补，可能导致漏洞被不法分子利用进行网络攻击，从而达到非法谋取私利的目的，影响企业正常运作。网络信息安全保障迫在眉睫，漏洞成为了网络世界中隐形的定时炸弹。

1.2 国家立法，重视网络安全

《网络安全法》于 2017 年 6 月 1 日起施行，这是我国第一部全面规范网络空间安全的基础性法律。其中规定网络运营者需履行“采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的

技术措施”、“制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险”等安全义务。

1.3 提前预知风险，防患于未然

在如此严峻的网络安全环境下，如何保障企业数据安全、业务安全已成为网络管理者的重大责任，因此，采用主动方式的安全管理是不容忽视的，网站管理者必须比攻击者更早掌握自己网络安全脆弱性并且做好适当的修补，才能够有效地预防入侵事件的发生，保证业务顺利的开展，维护企业信息的安全。

2.服务介绍

2.1 服务简介

网宿“安全评估服务”主要提供漏洞扫描、渗透测试、安全审计、漏洞预警等服务，帮助网站管理者及时发现系统中存在的安全隐患并提出相应的安全解决方案，有效地预防入侵事件的发生；并且当网站业务系统出现紧急安全问题时，网宿可提供远程或现场的安全技术支持，协助处理安全事件。

2.2 服务适用行业

网宿“安全评估服务”主要适用于政府网站、等级保护测评机构、公安系统网站、运营商网站、金融行业、能源行业、教育行业、医疗行业及互联网行业等各类网站。

3.提供的服务

网宿的“安全评估服务”主要包括：漏洞扫描、渗透测试、安全运维三个部分。

3.1 漏洞扫描

网宿安全团队通过自主挖掘与行业共享相结合的方式搜集漏洞信息并持续更新漏洞库，使用自主研发的漏洞扫描器对网站的主机、网络设备、Web 站点等资产进行综合性安全扫描；发现能被黑客利用的各种弱点，输出详细的扫描报告，帮助网站及时发现系统脆弱性并提供相应的修补建议，在黑客攻击前进行修补，保障服务器和网站的安全。

网宿提供全方位漏洞扫描服务，包括：主机系统安全扫描、Web 站点安全扫描、组件 POC 扫描等。

3.1.1 主机系统安全扫描

网宿主机系统安全扫描服务，检测主机系统中存在的安全隐患，如操作系统漏洞、错误安全配置问题、应用组件安全漏洞、系统弱口令(收集不必要开放的账号、服务、端口等)、主机运行状态等，帮助网站管理人员先于攻击者发现主机安全问题。

3.1.2 Web 站点安全扫描

网宿 Web 站点安全扫描服务，可以自动获取站点所包含的所有资源，并模拟站点所有可能的访问行为，对 Web 站点的脆弱性进行检测，提前发现 Web 应用系统中隐蔽的漏洞，并为网站管理人员提供详细的漏洞描述和修补方案，指导进行安全加固，能够有效解决 Web 应用面临的挑战。

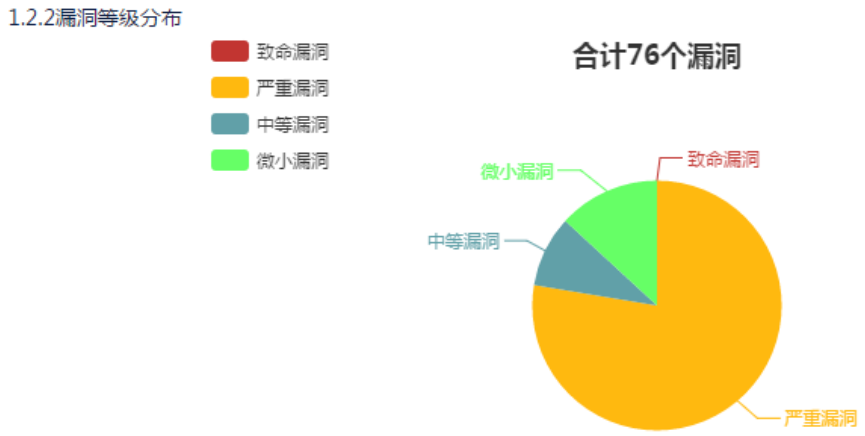
网宿 Web 站点安全扫描的漏洞覆盖了 OWASP Top10、WASC 及各类常见 Web 应用漏洞，主要包括 SQL 注入、XSS、CSRF、命令执行、文件包含、文件上传等漏洞。

3.1.3 组件 POC 扫描

由于漏洞层出不穷，经常在各安全平台(如：Freebuf 等；)爆出最新漏洞及其漏洞验证程序(POC)，针对最新出现的漏洞 POC，网宿安全团队能够在第一时间集成相关 POC 的检测到扫描器中，及时发现问题并解决问题。

Web 站点安全漏洞扫描部分报告如下所示：

1) 漏洞等级图分布如下：



2) 风险等级及漏洞详情图如下：

3.目标信息

3.1目标风险等级列表

序号	IP地址	漏洞风险（个）				目标风险
		致命	严重	中等	微小	
1	http://	0	59	7	10	严重

4.漏洞信息

4.1漏洞分布

序号	漏洞名称	影响目标个数	影响目标百分比	出现次数
1	sql_injection【cookie】漏洞	1/1	100%	1
	受影响目标	http://		
	详细描述	请求方式：get cookie参数：{"name":"IJamnKA\"'--"}		
	风险等级	严重		
2	xss【cookie】漏洞	1/1	100%	1

3.2 渗透测试

3.2.1 渗透测试服务简介

除了通过自研的漏洞扫描工具对网络系统进行脆弱性评估外，“安全评估服务”还包括渗透测试服务。渗透测试服务是在网站管理者授权许可的情况下，通过经验丰富的安全顾问/资深安全专家尽可能完整地模拟黑客使用的漏洞发现技术和攻击技术，对目标系统的安全作深入探测，发现网络系统的脆弱性。能够在漏洞扫描的基础上发现系统、应用、Web 隐蔽性的安全漏洞，避免黑客渗透入侵客户的网络系统，窃取敏感信息。

虽然渗透测试与黑客入侵的整个思路、过程和入侵一致，但是其本质区别在于渗透测试选择不影响业务系统正常运行的方法进行攻击，帮助网站管理者发现网络系统所面临的漏洞和系统缺陷，并提出相应的安全解决方案。

3.2.2 渗透测试服务内容

- **安全漏洞挖掘**

安全团队可针对网站服务器、Web 站点等网络设备进行安全渗透，发现潜在的安全漏洞，包括服务器安全渗透(检测服务器是否存在系统漏洞、远程命令执行、任意文件读取、提权漏洞等风险)、Web 站点安全渗透(检测 Web 站点是否存在 SQL 注入、XSS 跨站、文件上传、命令执行、账户越权、逻辑漏洞等风险)等。

- **修补建议及协助**

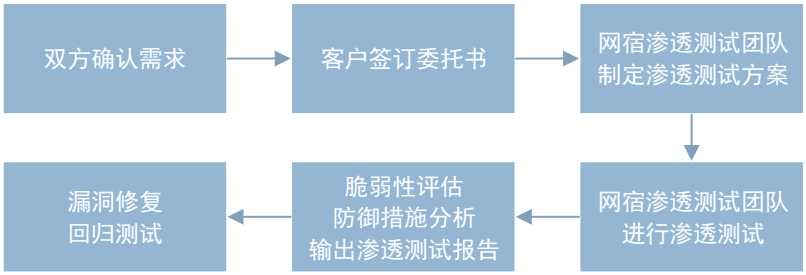
安全团队在对网站服务器、Web 站点等网络设备进行安全渗透后，评估系统的脆弱性以及分析相应的防御措施，为网站管理者提供专业的渗透测试报告、修补建议和必要的协助，从根本上修复漏洞，防止攻击者的攻击。

◆ **回归测试**

漏洞修复后，安全团队针对修复结果进行有效的评估，验证漏洞修复结果。

3.2.3 服务流程

网宿安全渗透测试的服务流程如下：



1. 网站管理者提出渗透测试需求后，由网宿安全团队与客户详细确认需求，包括渗透目标、渗透时间、渗透范围、测试要求等细节；
2. 签订渗透测试委托协议；
3. 网宿安全团队制定渗透测试方案；
4. 由网宿安全团队对 Web 服务器、数据库服务器、应用服务器、Web 站点等进行深入渗透测试；此外，网宿支持在现场对客户的内网办公环境进行渗透测试；
5. 网宿安全团队针对测试结果进行系统脆弱性评估、防御措施分析，并输出渗透测试报告；
6. 网站管理者可以根据报告中的修复建议进行漏洞修复，网宿安全团队可提供必要的协助并验证漏洞修复结果。

3.3 安全运维

网宿“安全评估服务”的安全运维服务包括：配置审查、漏洞预警、安全应急响应，能够帮助网站运维人员更好的保障网络系统的安全。

3.2.4 配置审查

错误的安全配置可能发生在 Web 服务器、应用服务器、第三方应用等的任何一个地方，而黑客可能会利用它们进行攻击，例如：Web 开发所依赖的第三方应用组件(例如 Struts、Spring、ASP.NET 等)的安全配置并未配置恰当而被黑客所利用。因此，管理者必须执行正确的安全配置才能保障服务器和应用程序的安全。

“安全评估服务”提供配置审查服务，对网站主机和主流的第三方应用等核心安全配置进行安全审计，并根据审查结果输出配置审查报告，帮助网站管理者了解系统中配置的安全隐患并提供相应的配置建议，避免不安全的配置被黑客所利用攻击。

3.2.5 漏洞预警

由于漏洞层出不穷，随时可能爆发新型漏洞威胁客户网络系统的安全；“安全评估服务”包括的漏洞预警服务会及时通知网站运营方最新的安全资讯，帮助提前防范最新攻击威胁。

需要网站管理者配合收集所有服务资产的应用组件信息，并反馈给网宿安全团队，网宿安全团队会针对这部分资产的安全信息进行安全资讯追踪(例如：实时跟踪客户所使用的第三方应用组件 struts 是否出现新漏洞)。若在 CVE 等平台发现新型漏洞攻击后由安全人员进行评估是否会对客户资产造成威胁，并在第一时间通过邮件/短信方式告知客户。

3.2.6 安全应急响应

“安全评估服务”包括应急响应服务，能够在网站业务系统出现紧急安全问题时提供快速、专业的应急处理。支持远程或现场的安全技术支持方式，协助处理安全事件，帮助网站快速恢复业务，同时分析黑客入侵行为、入侵原因等信息输出排查报告并给客户提供相应的安全建议。

对于未购买网宿云安全产品(如：云 WAF、高防云清洗 DMS 等)的，当遇到紧急安全事件时：

1. 当网站遭受大量 DDoS、CC 攻击导致源站服务器性能下降，站点无法访问时；可紧急接入网宿抗 D 服务进行 DDoS、CC 攻击安全防护；

2. 当网站遭受黑客入侵，出现服务器被挂后门木马、网页被篡改等安全事件时，网宿安全团队可提供远程或现场安全技术支持，协助处理安全事件，分析黑客入侵原因、入侵行为、被挂的后门木马等信息，帮助网站快速恢复运行，并给网站管理者提供相应的安全建议；同时可紧急接入网宿云 WAF 服务进行安全防护，避免黑客再次入侵。

对于已购买网宿云安全产品(如：云 WAF、高防云清洗 DMS 等)的，当遇到紧急安全事件时:

1. 当出现安全攻击事件，网宿云安全平台能够实时进行安全防护，并提供一对一安全专家服务，保护源站的安全；
2. 当出现新型攻击时，网宿安全团队第一时间对新型攻击的攻击原理、攻击特征、防护措施等进行分析，并生成相应的防护策略同步下发至全网；
3. 对于已经购买 DDoS 防攻击带宽并设定封顶防护值的用户，若出现遭受的 DDoS 攻击带宽超过上限而需要继续防护时，网宿可紧急扩展防护带宽进行防护。

4.服务价值

4.1 定时扫描持续监控

如果要真正做到事先感知网络系统的脆弱性，并采取相应的措施进行修补，每年仅进行一两次网络系统漏洞扫描是远远不够的。网宿“安全评估服务”提供对目标系统进行定时扫描，避免主机或站点的漏洞重复出现被忽略，尤其是如果开放主机的某些端口可能会导致数据泄露，必须对这些端口进行定时扫描，一旦发现未做访问控制需及时处理。

4.2 风险检测横向扩展

随着漏洞挖掘技术的不断发展，攻击工具日益专业化、易用化，漏洞爆发频率越来越高；网宿安全团队紧跟最新安全漏洞，实时更新漏洞库，保障风险检测的及时性和全面性。

4.3 多维度风险分析报告

“安全评估服务”提供安全扫描、渗透测试、配置审查等安全服务后，均会为网站管理者提供一份详细的安全分析报告，从检测目标、漏洞等级、漏洞类型、风险等级等多维度直观地展示网站系统每个漏洞的详细信息及修补建议，使网站管理者更简单直观的了解漏洞风险状态，帮助修补漏洞以及验证修补效果，并可提供必要的协助。

4.4 预知风险，防患于未然

采用网宿“安全评估服务”，能够帮助网站管理者提前掌握网站的网络安全问题并且做好适当的修补，有效地预防入侵事件的发生，从而保证业务顺利的开展，保护企业信息安全。

关于网宿

网宿科技 始创于 2000 年 1 月，主要提供互联网内容分发与加速（CDN）、云计算、云安全、全球分布式数据中心(IDC) 等服务。

2009 年 10 月，网宿科技在深交所上市，股票代码 300017。

网宿科技拥有遍布全球的 1000+ CDN 加速节点，在北京、上海、广州、深圳等地设有分公司，在美国、香港、印度、爱尔兰、马来西亚、济南、南京、杭州等地建有多家全资子公司，并在厦门及美国硅谷设立了研发中心。现有员工 3000 多名，研发以及技术人员占总人数 60% 左右。客户群覆盖各类互联网门户网站、视音频网站、网络游戏公司、电子商务网站、政府网站、企业网站以及运营商等，公司服务的客户超过 3000 家，是市场同类公司中拥有客户数量较多、行业覆盖面较广的公司。