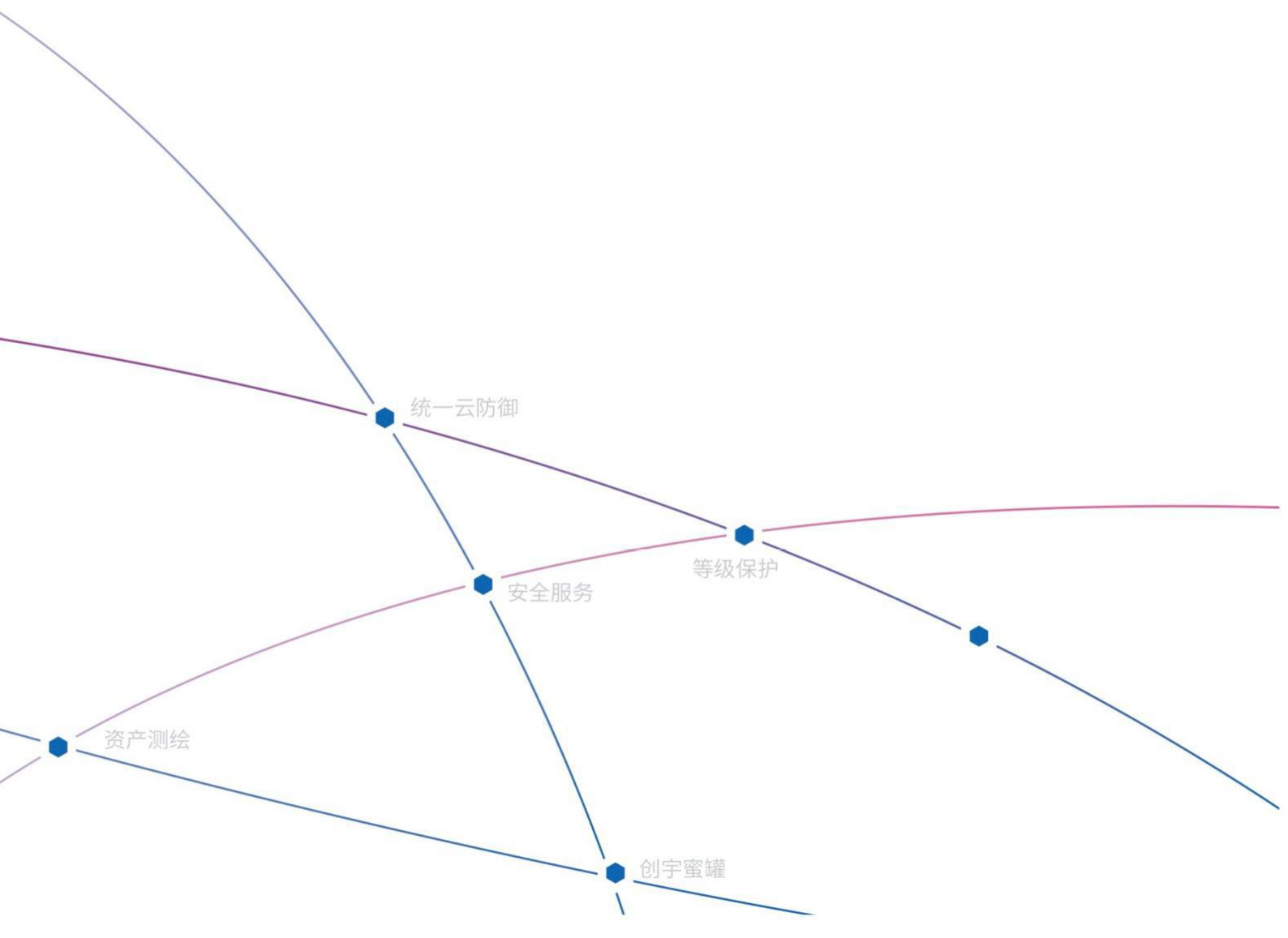
www.yunaq.com

知道创宇

漏洞扫描白皮书



文档信息

文档名称	版本号	保密级别
漏洞扫描白皮书	1.0	内部公开

版本说明

修订人	修订内容	修订时间	版本号	审阅人
田子伊	漏洞扫描白皮书	2022.3.15	1.0	裴文成

版权说明

目录

1. 国内信息安全情况概述

1.1. 信息安全环境简述

随着我国经济发展和社会信息化进程加快，网络信息技术在国家政治、经济、文化等领域的应用日益广泛，保障网络安全已经成为关系国家经济发展、社会稳定乃至国家安全的重要战略任务。近年来信息技术系统的广泛应用，网络的广域连接，针对漏洞的攻击也越来越多，利用漏洞的病毒、木马技术进行网络盗窃和诈骗的网络犯罪活动呈快速上升趋势。产生了大范围的危害，由此给企业造成了重大经济损失。大数据分析显示，SQL 注入类漏洞、信息泄露漏洞、权限问题的漏洞这三类占了较大比例，针对详细信息和数据的攻击正逐成为主流，这些漏洞必须隔离于重要系统之外。漏洞情况越来越严峻，攻击者直接瞄准目标信息，整体攻击体系正在不断成型。因此，对于企业及组织来说，如何及时发现漏洞，修复漏洞，避免安全脆弱性被黑客恶意利用就成为企业安全必不可少的工作。

1.2. 云平台和大数据的安全防护能力将是关注重点

云计算、大数据等新技术、新业务的快速应用与发展，更多政府和企业将业务系统部署到云平台，大量涉及国计民生、企业运营的数据和用户个人信息存储在云上，吸引了攻击者的目光。攻击者不断挖掘云平台自身可能存在的安全漏洞，一旦发现漏洞并加以利用，可能导致严重的大规模信息泄露事件发生。此外，攻击者也可以利用云平台特有脆弱性实施网络攻击。因此，云平台和大数据的安全防护将成为行业重点关注的问题。

2. 漏洞扫描简介

漏洞扫描是指基于漏洞数据库，通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用漏洞的一种安全检测行为。

漏洞扫描器包括网络漏扫、主机漏扫、数据库漏扫等不同种类。

2.1. 概述

在不影响用户各业务系统正常运行的情况下，使用专业的安全漏洞扫描工具对用户的信息系统进行漏洞扫描，并结合人工对漏洞信息进行验证以及编写安全报告，以发现系统中的安全漏洞和风险点并及时汇报。

2.2. 服务流程

◆ **信息收集**

信息收集主要是指收集目标系统暴露于环境中，不需要额外的授权便可获取到的信息，例如目标的子域名、端口等信息。

◆ **安全检测**

（1）专业安全工具扫描：

使用专业的安全工具进行扫描、嗅探等操作，对系统的网络和应用程序进行安全检测。

（2）漏洞信息人工验证：

安排专业的安全工程师对漏洞扫描的结果进行分析，并对部分漏洞进行人工验证。

◆ **报告编写**

漏洞扫描服务报告包括整体服务流程描述，会对发现问题的验证手法进行必要的说明，并且结合目标系统环境，出具针对性的解决方案。

2.3. 服务特点

◆ **专业、完善的漏洞扫描报告**

通过知道创宇自主研发的漏洞扫描工具，为客户提供专业的漏洞扫描报告，包括详细的漏洞风险说明、影响的系统类型和版本、安全解决建议等，及时发现风险，及时修补加固；

◆ **闭环处理漏洞生命周期**

帮助客户实现闭环处理漏洞管理，从资产发现，漏洞扫描，漏洞检查报告，漏洞修补，修补效果验证；

◆ **定期监测，实时更新**

完全贴合客户需求，针对目标系统的扫描周期可以随时调整，并保证扫描设备的特征库随时处于最新版本状态；

2.4. 服务对象

主要针对 WEB 应用系统、主机、服务器、终端等资产。

2.5. 工作成果

漏洞扫描报告，包含扫描情况综述、统计、漏洞名称、漏洞评级、漏洞位置、漏洞类型、漏洞描述、修复建议，以及由专业的安全工程师对漏洞验证的过程和结果截图等内容。

2.6. 漏洞扫描示例

漏洞扫描报告的示例文件：

修复方案示例：

漏洞名称	使用了存在漏洞的 Javascript 库（新增）
漏洞等级	中危
漏洞类型	web 漏洞
漏洞描述	正在使用一个存在漏洞的 Javascript 库。此版本的 Javascript 库存在一个或多个漏洞。有关受影响的库和所报告的漏洞的详细信息，请参阅攻击详细信息和其他网页。
修复建议	升级至最新版本。
提交时间	2018 年 12 月 28 日 22 时 12 分 50 秒

漏洞位置与验证结果: 第 1 处

端口	【443/ -】
URL	https://www.manutouch.com.cn/bws/Scripts/jquery-1.10.2.min.js
Header	GET /bws/Scripts/jquery-1.10.2.min.js HTTP/1.1 Cookie: ASP.NET_SessionId=wdzacrxmew3wlgzcpyebfnix;.ASPXAUTH=;Staf

【邮　箱】：bfjfzx@knownsec.com

【网　址】：https://www.knownsec.com

【地　址】：北京市朝阳区望京 SOHO T3 A 座 15 层

知道创宇云安全