漏洞扫描服务白皮书

1.1. 服务内容

1.1.1. 服务定义

根据客户提供的目标系统信息通过漏洞扫描器丰富的漏洞规则库进行全面深入的检测扫描 web 应用系统、主机操作系统中存在的安全漏洞；提供专业全面的漏洞评估报告和修复建议。

1.1.2. 服务范围说明

主要针对面向外网的 web 系统、主机服务器等

面向内网的需架设 vpn 通道进入本地内网扫描

1.1.3. 服务内容说明

服务进度	服务内容	方式
漏扫前	确认漏扫目标情况 确认漏扫时间 确认漏扫线程频率 确认漏扫授权	客户提供
漏扫中	漏扫开始通知 监测漏扫状态	人工添加、漏扫工具扫描
漏扫后	输出漏扫报告	邮箱或其他联系方式

1.1.4. 服务流程

项目启动

1、同业主确认漏扫目标情况

应用系统信息：域名或地址

服务器信息：IP 地址

目前防护手段：是否有 WAF、防火墙等

附件一 Xxx 系统漏扫调研表

2、同业主确认漏扫时间

根据目标用户覆盖情况，沟通漏扫时间，在不影响业务情况下进行扫描操作

附件一 Xxx 系统漏扫调研表

3、同业主确认漏扫线程频率

根据目标环境配置情况，沟通漏扫线程频率，在不影响业务情况下进行设置

附件一 Xxx 系统漏扫调研表

4、同业主签订漏扫授权书

签订漏扫授权书，维护各方正常法律权益

附件二 Xxx 系统漏扫授权书

项目中

漏扫开始前及时通知业主，实时监测扫描状态；

漏扫中业主反映业务可用性受到影响及时终止扫描。

业务漏扫

可选随机时间段，7*24 业务漏扫

报告输出

在漏洞扫描结束后，项目服务人员根据漏扫结果编写《安全漏扫报告》，报告内容包括资产风险列表、详情以及修复建议等内容。

1.1.5. 服务实施方

本服务由卓见云实施并提供技术支持和质量管理。

1.1.6. 服务形式

经客户授权采用远程互联网方式提供服务

说明：针对部分内网情况，可通过本地 vpn 通道方式进行。

1.1.7. 服务输出

- 《安全漏扫报告》

1.2. 风险控制

类别	风险控制项	风险管理办法
人员组织安全	组织要求	由卓见云交付服务团队提供服务。
	人员要求	所有服务人员均经过卓见云交付团队能力评估。
保密要求	保密协议	根据业主目标协定是否需签署保密协议。
过程安全	操作安全	漏扫前双方协定扫描时间及力度。 漏扫中实时监测系统正常运行情况。

1.3. 职责与分工

项目方	职责分工
业主	提供详细的目标对象情况和相应的测试授权。 指派一名负责人对接服务工作。

	漏扫中实时监测系统运行情况，存在异常及时反馈。
实施方	完成对目标的相关服务工作。 编写服务报告。

1.4. 结束标志

本服务以服务报告通过验收作为结束标志。