环宇数通
sotote.com

云安全评估服务

2019年12月

服务简介

环宇数通 sotote.com

云安全评估：使用云端专业的安全扫描工具，根据用户真实的业务场景需求和国家网络安全法规及标准，在获得用户充分授权后，模拟黑客攻击方式，通过互联网对用户授权的网站、手机APP等应用进行全面的web安全漏洞检查，最终交付《云安全评估报告》，并提供必要的“等保合规性”安全建设建议。

- **早发现：探测web网站客观安全漏洞，分析漏洞危害；**
- **早修复：基于评估报告，确定修复方案并实施，规避风险；**
- **常态化：安全是动态的，应该像“体检”一样每年至少进行一次。**

“云安全评估”就好像医院中的B超、核磁以及CT扫描一样

服务价值

环宇数通 sotote.com

安全漏洞早发现

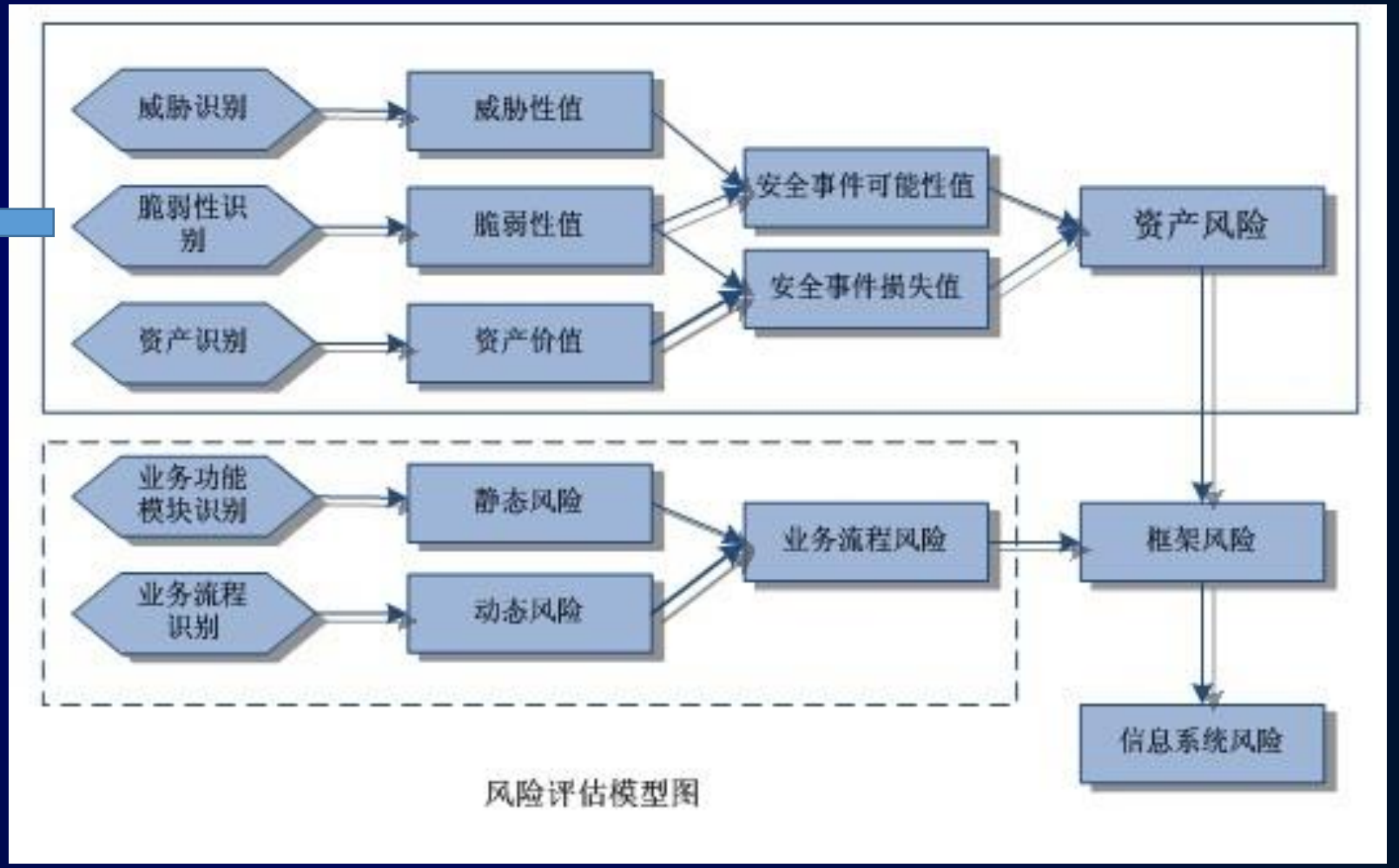
TOP1-注入	注入攻击漏洞，例如SQL，OS以及LDAP注入，这些攻击发生在不可信的数据作为命令或者查询语句的一部分，被发送给解释器的时候，攻击者发送的恶意数据可以欺骗解释器，以执行计划外的命令或者在未被恰当授权时访问数据。
TOP2-失效的身份验证和会话管理	与身份认证和会话管理相关的应用程序功能往往得下到正确的实现，这就导致了攻击者破坏密码、密钥、会话令牌或攻击其他的漏洞去冒充其他用户的身份（暂时的或者永久的）
TOP3-跨站脚本（XSS）	每当应用程序在新网页中包含不受信任的数据而无需正确的验证或转义时，或者使用可以创建JavaScript的浏览器API并使用用户提供的数据更新现有网页就会发生XSS缺陷。XSS允许攻击者在受害者的浏览器上执行脚本，从而劫持用户会话，危害网站，或者将用户转向至恶意网站。
TOP4-失效的访问控制	仅允许通过身份验证的用户的限制没有得到适当的强制执行。攻击者可以利用这些缺陷来访问未经授权的功能和或数据，例如访问其他的用户的账户，查看敏感文件，修改其他用户的数据，更改访问权限等。
TOP5-安全配置错误	好的安全需要对应用程序、框架、应用程序服务器、web服务器、数据库服务器和平台定义和执行安全配置，由于许多设置的默认值并不是安全的，因此，必须定义，实施和维护这些设置。这包含了对所有的软件保持及时更新，包括所有应用的库文件
TOP6-敏感信息泄露	许多Web应用程序没有正确保护铭感数据，如信用卡，税务ID和身份验证凭据，攻击者可能会窃取或篡改这些弱保护的数据以进行信用卡诈骗、身份窃取，或其他犯罪，敏感数据值需额外的保护，比如在存放或在传输过程中的加密，以及在与浏览器交换在时进行特殊的预防措施。
TOP7-攻击检测与防范不足	大多数应用程序和API缺乏针对手动和自动攻击的检测，预防和相应的基本功能。攻击 保护远远超出了基本输入验证，并且涉及自动检测，记录，影响甚至阻止攻击。应用程序所欲这还需要有快速部署补丁以防止攻击的能力。
TOP8-跨站请求伪造	一个跨站请求伪造攻击迫使登录用户的浏览器将伪造的HTTP请求，包括该用户的会话Cookie和其他的认证信息，发送到一个存在漏洞的web应用程序，这就允许了攻击者迫使用户服务器向存在漏洞的应用程序发送请求，而这些请求会被应用程序认为是用户的合法请求。
TOP9-使用含有已知漏洞的组件	组件，比如：库文件、框架和其他软件模块，几乎总是以全部的权限运行，如果一个带有漏洞的组件被利用，这种攻击可以造成更为严重的数据丢失或服务器接管。应用程序使用带有已知漏洞的组件会破坏应用程序防御系统，并使一系列可能的攻击影响成为可能。
TOP10-未受保护的APIs	现在现代应用程序和API通常涉及丰富的客户端应用程序，例如浏览器中的JavaScript和移动端应用程序，连接到某种API（SOAP/XML ,REST/JSON.RPC,GWT等），这些API通常是不受保护的，并且包含许多漏洞

服务流程

环宇数通 sotote.com

云安全评估可以高效快速的识别web网站的安全漏洞（脆弱性），是完整“信息安全风险评估”流程中的重要组成部分。

备注：云安全评估只是完整风险评估的组成部分，不包括全部流程。若需要完整风险评估服务，敬请致电环宇服务人员或拨打热线电话：4006390078



风险评估模型图

实施流程

环宇数通 sotote.com

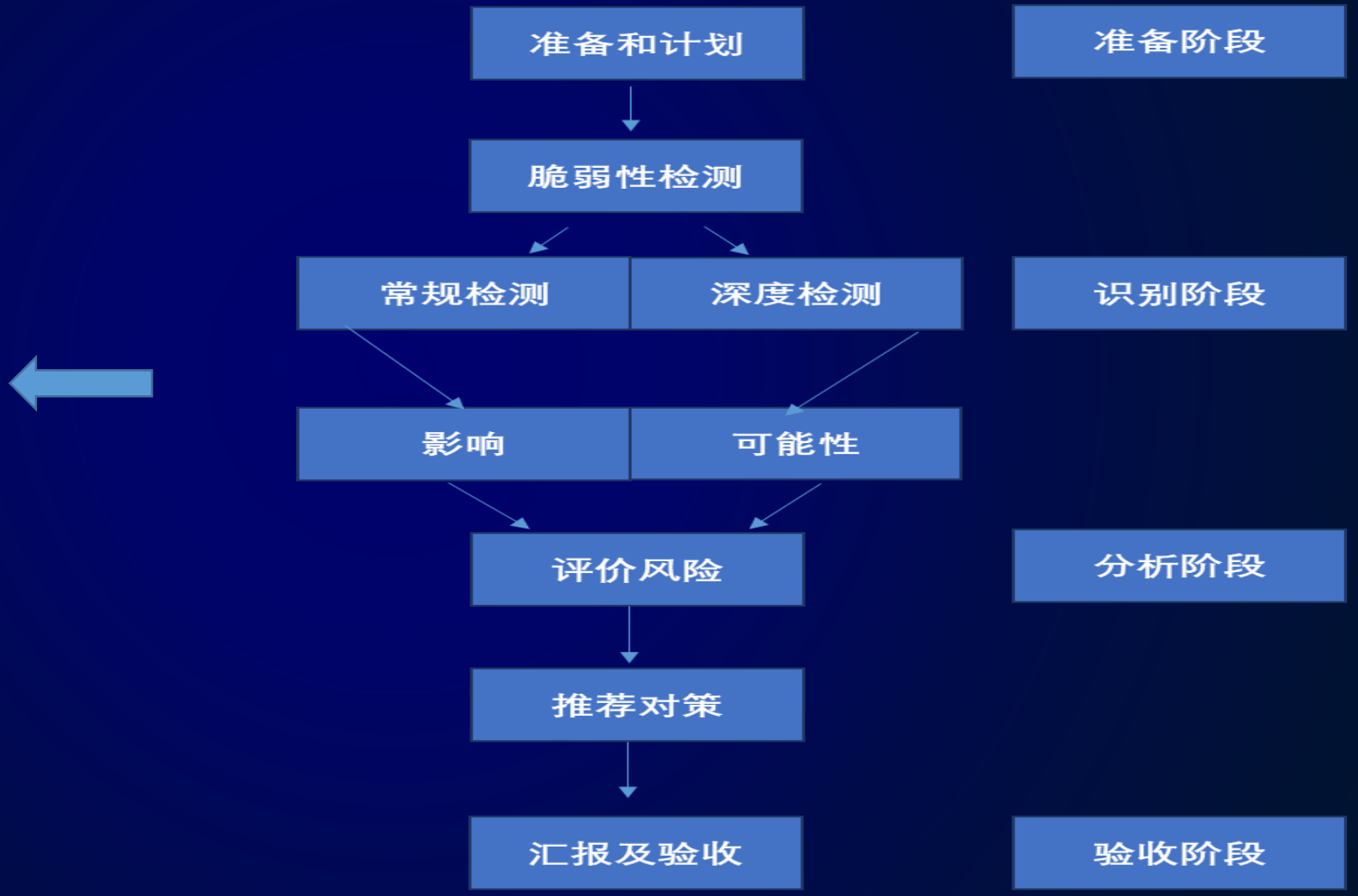
云安全评估脆弱检测一共分为四个阶段

一、准备阶段：准备需要的授权书与调研表

二、识别阶段：通过脆弱性检测工具检测，识别检测出高危漏洞与中危漏洞，第一阶段常规检测，第二阶段深度测试。

三、分析阶段：通过检测结果，进行人工分析，检测。

四、验收阶段：通过人工分析检测，输出一份详细的威胁报告，给客户验收。



服务依据

环宇数通 sotote.com

- 2017年《中华人民共和国网络安全法》
- GB/T 22239-2019 《信息安全技术网络安全等级保护基本要求》
- GB/T 28448-2019 《信息安全技术网络安全等级保护测评要求》
- GB/T 25070-2019 《信息安全技术网络安全等级保护安全设计技术要求》
- GB/T 20984—2007《信息安全技术信息安全风险评估规范》
- GB/Z 24364—2009《信息安全技术信息安全风险管理指南》
- GB/T 31509—2015《信息安全技术信息安全风险评估实施指南》
- GB/T 31722—2015/ISO/IEC 27005:2008《信息安全技术信息安全风险管理》

环宇简介

环宇数通
sotote.com

创立于2009年，团队来自顶级系统集成商和安全厂商

2013年，自主知识产权数通云产品

2015年，正式加入阿里云生态体系

2016年，阿里云全国授权服务中心

2017年，建立完善的环宇云服务体系

2018年，获得ISO27001国际安全资质

2019年，国信安全以及中国招投标服务平台合作伙伴

公司愿景：中国最具竞争力的云服务商

企业宗旨：助力企业云安全数字化转型

企业文化：精益求精、真诚守信、团结一心、勇于创新

环宇数通
sotote.com

北京环宇数通科技有限公司

咨询热线：400-639-0078