

Sophos 咨询服务

Web Application Security Assessment

Web 应用程序安全性评估

在攻击敌手出手之前，识别可被利用的漏洞与未知风险

保护您的外部与内部 Web 应用程序 - 通过识别暴露点和潜在风险，来强化您的网络防御，保障敏感数据安全，并展示合规性。

确保 Web 应用安全，让您高枕无忧

Web 应用是关键的业务载体，负责处理、传输和存储有价值的数据，帮助企业实现运营与声誉目标。保护 Web 应用程序对于构建稳健的安全状态至关重要。通过由安全专家识别漏洞，以评估 Web 应用程序安全性，可主动提升组织的安全韧性。

Sophos Web 应用程序安全性评估服务

Sophos 的 Web 应用程序安全性评估服务可识别访问控制破缺、安全配置错误及应用设计问题等漏洞。我们结合我们对全球威胁形势和攻击者战术、以及对攻击者策略、技术与程序 (TTP) 的深入理解，评估应用程序遭受攻击的可能性，从而确保其安全性。

Sophos Web 应用程序安全性评估主要聚焦两个方面：

- **外部应用程序：**您的 Web 应用程序是您与互联网、潜在客户、现有客户、合作伙伴和供应商的连接桥梁。它们是推动客户品牌认知、营收和销售活动的关键资产，也常常成为吸引攻击者的目标。对外部应用程序的测试模拟匿名攻击者，或那些注册获得身份验证访问权限、甚至付费订阅的攻击敌手行为。
- **内部应用程序：**攻击敌手同样会针对组织内部网络可访问的应用程序，这些系统支撑着企业业务流程和核心数据，如知识产权、客户信息、员工资料及销售数据。内部应用的测试则模拟内部心怀不满的员工，或是使用从数据泄露或钓鱼攻击中窃取的凭据的攻击敌手。

Sophos 将每项评估视为每个组织专属的独特任务。我们采用以目标为导向的方法论，由业界顶尖的安全测试人员执行，并利用我们的专利战术及 Sophos X-Ops 威胁情报团队的情报。该团队包括反威胁小组 (CTU)，以对进阶持续性威胁 (APT) 和国家级攻击者的情报及研究而闻名。

优势

- 增强对 Web 应用程序安全性的信心。
- 获得可执行的安全强化建议。
- 降低安全风险，提升运营效率。
- 维护客户、员工及业务伙伴的信心。
- 满足合规要求（如 PCI-DSS）。

测试您的 Web 应用，降低安全风险

Sophos 测试人员将结合自动化与手动测试技术，对 Web 应用程序进行全面评估，以便在攻击者利用漏洞之前辨识出来。测试人员模拟外部攻击敌手及恶意用户，从匿名和已验证身份两种视角发起攻击。此方法确保涵盖从大规模攻击活动，到针对受保护资源的复杂业务逻辑攻击的各类威胁场景。

在专案结束后，Sophos 将提供详细的修复建议，帮助您解决配置问题、已知及潜在漏洞、访问控制风险等可能被攻击敌手利用的安全缺陷。

报告内容包含



管理摘要：面向高层管理、审计人员、董事会等非技术相关方。



详细发现：为技术人员提供深入的测试结果与修复建议。



评估方法说明：定义评估范围及所执行的评估活动内容。



建议措施：包含详细发现内容、延伸阅读链接以及修复或风险缓解建议。测试人员在适用情况下附上发现的左证资料，并尽可能提供足够信息，让使用公开工具的情况下能重现问题。

更多网络安全测试服务

没有任何单一的测试或技术手法能全面描绘出组织的整体安全防护现况。每种对抗测试方式均有其特定目标及可接受风险水平。Sophos 可和您协作，以判断应采用哪些评估项目与技术组合，来评估您的安全防护现况与控制机制，从而找出您的漏洞。

服务特点

- 对 Web 应用程序进行评估，识别漏洞。
- 借助专家指导和建议，以提升安全状态。
- 采用包括，但不限于 OWASP 十大关键应用安全缺陷的测试。
- 支持几乎所有 Web 开发框架、平台或基础设施。
- 不仅评估应用程序本身，还检查黑客是否有可能藉由该应用程序进一步存取其背后的网络或数据。

了解更多：
sophos.com/advisory-services

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com