山东大学 软件 学院

网络攻防 课堂报告

|  |  |  |
| --- | --- | --- |
| 学号：202200201095 | 姓名： 杨伟康 | 班级： 22网安 |
| 硬件环境：  处理器 11th Gen Intel(R) Core(TM) i5-11400H @ 2.70GHz 2.69 GHz  机带 RAM 16.0 GB (15.9 GB 可用)  设备 ID 9DCDB7C5-EBBA-4C1F-845F-94B127DFAE09  产品 ID 00342-30515-76480-AAOEM  系统类型 64 位操作系统, 基于 x64 的处理器  笔和触控 没有可用于此显示器的笔或触控输入 | | |
| 软件环境：  Window+ ibm appscan | | |
| Blog记录：   1. ibm appscan简介   AppScan是IBM的一款应用程序安全测试工具，旨在帮助组织发现和修复应用程序中的安全漏洞。它提供了全面的功能和工具，用于自动化应用程序安全测试、漏洞扫描和漏洞管理。   1. 主要功能   1. 自动化漏洞扫描：AppScan可以自动扫描Web应用程序和移动应用程序，发现其中的安全漏洞。它支持多种扫描技术和策略，包括黑盒扫描和白盒扫描，帮助用户全面评估应用程序的安全性。  2. 漏洞识别和分类：AppScan能够发现各种常见的应用程序安全漏洞，如跨站脚本攻击（XSS）、SQL注入、命令注入、路径遍历、CSRF等。它能够将漏洞按照严重程度和风险级别进行分类和评估。  3. 安全漏洞修复建议：AppScan提供了详细的修复建议，帮助开发团队快速定位和修复发现的漏洞。它提供了代码示例、漏洞修补建议和最佳实践，以帮助开发人员解决安全问题。  4. 安全测试报告和分析：AppScan生成详细的安全测试报告，包括发现的漏洞、修复建议、风险评估等。报告可以以多种格式导出，如PDF、HTML、CSV等，方便与安全团队和开发人员共享和分析。  5. 集成和自定义：AppScan可以与其他应用程序开发和安全工具集成，如开发环境、CI/CD工具等。它还提供了一些自定义选项和配置，允许用户根据需要调整扫描策略和设置。  6. 移动应用程序安全测试：AppScan支持移动应用程序的安全测试，包括iOS和Android应用程序。它可以发现移动应用程序中的漏洞和风险，并提供修复建议和最佳实践。   1. 使用示例     点击web应用程序，可以进一步具体配置要扫描的网站或服务器，这里以百度为例子    配置完成后开始扫描    可以看到，不到两分钟已经进行了几百次请求    点击数据可以看到具体扫描的网站内容，请求、参数、cookie等    最后就是扫描出的问题，百度作为老牌网站基本的安全防护还是有的，所以并未扫描出    这里进行暂停，可以进行配置的修改    比如某些网站的登录，或者自动填表      还可以进行手动探索    最后，扫一下我们山大的sdu.cn试一下    扫描时把需要登录的界面跳过了，扫一些不太重要的网站    扫了十几分钟大部分网页都因为需要登录跳过了。 | | |
| 结论分析与体会：  总的来说，IBM AppScan是一款非常出色的应用程序安全测试工具。它提供了全面的功能和工具，能够自动化地进行应用程序安全测试、漏洞扫描和漏洞管理。在使用过程中，我深刻体会到了它的高效、便捷和准确性。  同时，AppScan的易用性也非常值得称赞。它的界面设计简洁明了，操作流程也非常直观易懂。即使对于没有太多安全测试经验的人员来说，也能够快速上手并开展测试工作。  此外，AppScan还支持多种扫描技术和策略，包括黑盒扫描和白盒扫描等，能够满足不同场景下的测试需求。同时，它还能够与其他应用程序开发和安全工具集成，提高了测试流程的灵活性和效率。 | | |