2022 年最佳SQL 注入檢測工具

網絡安全編程與黑客程序員 2022-03-23 23:11

> **文章來源： https://www.wljslmz.cn/1109.html**

SQL 注入(SQLi) 是一種可以訪問敏感或私有數據的隱蔽攻擊形式，它們最早是在上世紀末被發現的，儘管它們的年齡很大，但它們經常被用作黑客工具包中的一種有效技術。今天，給大家介紹一下頂級SQLi 檢測工具。

頂級SQLi 檢測工具

有很多SQLi 檢測工具，其中許多是開源的，可在GitHub 上找到，除了專門的SQLi 檢測工具外，還有更大的套件和專有軟件包將SQLi 作為其整體漏洞檢測功能的一部分。

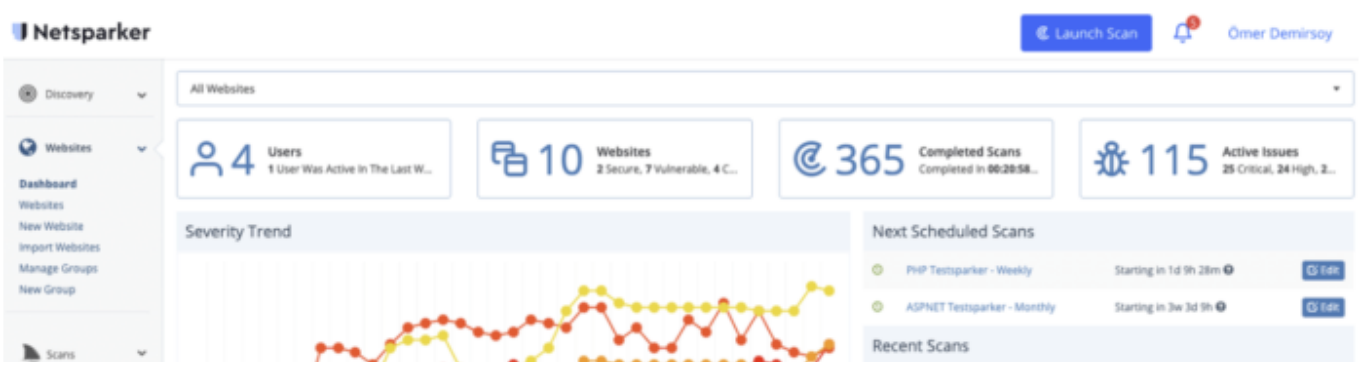
Netsparker

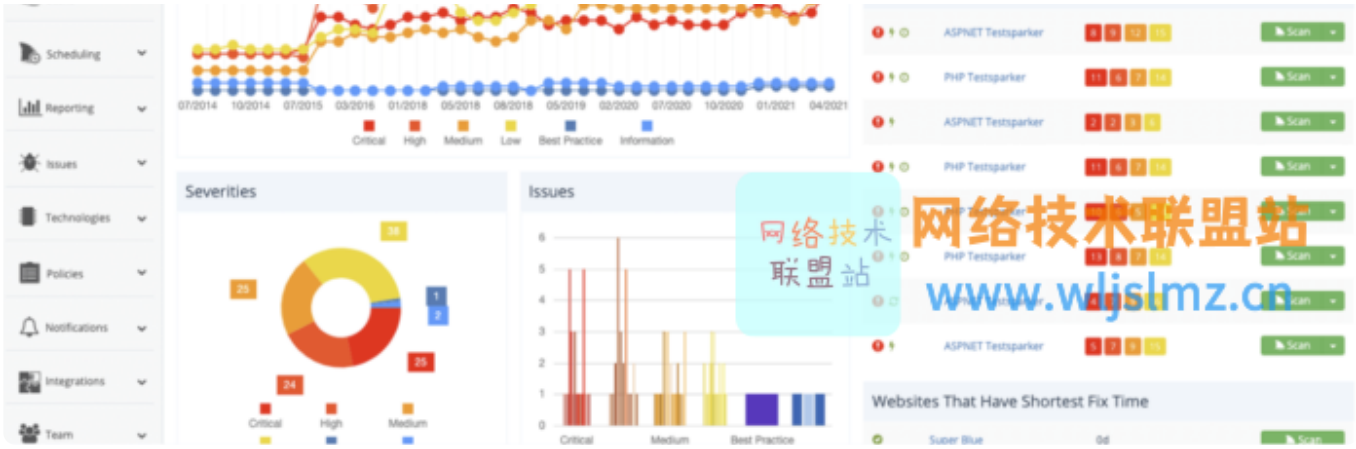
Netsparker是一個Web 漏洞管理解決方案，其中包括SQLi 檢測作為其眾多功能之一，還專注於可擴展性、自動化和集成。

該套件圍繞Web 漏洞掃描器構建，並且可以與第三方工具集成，操作員不需要熟悉源代碼。該公司還提供了一個SQL 注入備忘單來幫助緩解工作。

Netsparker 平台使用基於證明的掃描技術來識別和確認漏洞，指示絕對不是誤報的結果，除了SQL 注入之外，它還可以識別Web 應用程序、Web 服務和Web API 中的跨站點腳本(XSS)和其他漏洞。

該平台還具有安全測試工具和報告生成器，並且可以集成到DevOps 環境中，它檢查Apache、Nginx 和IIS 等Web 服務器，並支持基於AJAX 和JavaScript 的應用程序。





SQLMap

SQLMap是GitHub 上提供的自動SQLi 和數據庫接管工具，這個開源滲透測試工具可以自動檢測和利用SQLi 漏洞或其他接管數據庫服務器的攻擊。

它包括一个检测引擎；进行渗透测试的几种方法；以及用于数据库指纹识别、数据提取、访问底层文件系统以及通过带外连接在操作系统 (OS) 上执行命令的工具。

jSQL Injection

jSQL Injection是一种基于 Java 的工具，可帮助 IT 团队从远程服务器中查找数据库信息，它是解决 SQLi 的众多免费、开源方法中的另一种。它支持 Windows、Linux 和 Mac 操作系统以及 Java 版本 11-17。

它是如此有效的 SQLi 威慑，以至于它包含在许多其他漏洞扫描和渗透测试产品和发行版中。这包括Kali Linux、Pentest Box、Parrot Security OS、ArchStrike和BlackArch Linux。

它还提供 33 个数据库引擎的自动注入，包括 Access、DB2、Hana、Ingres、MySQL、Oracle、PostgreSQL、SQL Server、Sybase 和 Teradata。它为用户提供了解决多种注入策略和流程的方法，并提供了用于 SQL 和篡改的脚本沙箱。

Havij

Havij是由一家伊朗安全公司开发的，它提供了一个图形用户界面 (GUI)，并且是一个自动化的 SQLi 工具，支持多种 SQLi 技术，它在支持渗透测试人员发现网页漏洞方面具有特殊价值，虽然它主要适用于 Windows，但也有一些变通方法可以让它在 Linux 上运行。

Burp

Burp Suite中的 Web 漏洞扫描器使用 PortSwigger 的研究来帮助用户自动发现 Web 应用程序中的各种漏洞，例如，Burp Collaborator 识别其目标和外部服务器之间的交互，以检查传统扫描程序不可见的错误，例如异步 SQL 注入和盲目的服务器端请求伪造 (SSRF)。

Burp Scanner 中的爬网引擎位于 Burp Suite Enterprise Edition 和 Burp Suite Professional 等大型套件的核心，可消除跨站点请求伪造 (CSRF) 令牌、有状态功能以及过载或易变 URL 等障碍。其嵌入式 Chromium 浏览器呈现和抓取 JavaScript。爬行算法以与测试人员类似的方式建立其目标的配置文件。

Burp 还旨在处理动态内容、不稳定的互联网连接、API 定义和 Web 应用程序。此外，可以单独或按组选择扫描检查，并且可以保存自定义配置 - 例如仅报告出现在 OWASP Top 10 中的漏洞的扫描配置。

BBQSQL

BBQSQL是一个基于 Python 的注入利用工具，它消除了编写自定义代码和脚本以解决 SQLi 问题的大量乏味。它主要用于处理更复杂的 SQL 注入漏洞。由于它是半自动的且与数据库无关，因此它简化了定制并且相对易于使用。

它还利用基于 Python 的工具来提高性能。用户提供数据，例如受影响的 URL、HTTP 方法和其他输入作为设置的一部分。他们还必须指定注入的去向，以及注入的语法。

Blisqy

Blisqy处理 HTTP 标头上基于时间的盲 SQL 注入。这种漏洞利用可通过盲 SQL 注入，对可打印的 ASCII 字符进行按位运算，从而从数据库中抽取慢速数据。它支持 MySQL 和 MariaDB 数据库。

由于它是用 Python 编写的，因此可以将其导入其他基于 Python 的脚本中。Blisqy 是一种快速有效的补偿网络延迟和其他延迟的方法，因为它的时间比较是动态的，并且在每次测试的运行时计算。

Acunetix Web 漏洞扫描程序

Invicti 的Acunetix将 SQL 注入测试作为其整体功能的一部分，即扫描基于 Web 的应用程序。它的多线程扫描程序可以在 Windows 和 Linux 上快速爬取数十万页。它识别常见的 Web 服务器配置问题，并且特别擅长扫描 WordPress。

它会自动创建所有网站、应用程序和 API 的列表，并使其保持最新状态。该工具还可以扫描 SPA、脚本繁重的网站以及使用 HTML5 和 JavaScript 构建的应用程序，并提供宏来自动扫描受密码保护和难以到达的区域。

Blind SQL Injection via Bit Shifting

Blind SQL Injection via Bit Shifting通过使用位移方法计算字符而不是猜测字符来执行 SQL 盲注入。位移位将位的位置向左或向右移动。例如，00010111 可以转换为 00101110。盲 SQL 模块每个字符需要七个或八个请求，具体取决于配置。

Damn Small SQLi Scanner

Damn Small SQLi Scanner (DSSS) 由 SQLMap 的创建者之一组成，是一个紧凑的 SQLi 漏洞扫描器，由不到 100 行代码组成。除了用作漏洞扫描器之外，该工具还强调其执行某些与占用大量代码的工具相同的任务的能力。

但是，正如其大小所预期的那样，它具有一定的局限性。例如，它只支持 GET 参数而不支持 POST 参数。

Leviathan

Leviathan的特点是工具的大规模审计集合。因此，它包含一系列用于服务发现、暴力破解、SQL 注入检测和运行自定义漏洞利用功能的功能。它内部包含了几个开源工具，包括 masscan、ncrack和DSSS，可以单独使用，也可以组合使用。

此外，它还可以发现在特定国家或 IP 范围内运行的 FTP、SSH、Telnet、RDP 和 MySQL 服务。然后可以通过 ncrack 对发现的服务进行暴力破解。命令可以在受感染的设备上远程运行。针对 SQLi 漏洞，它可以在带有国家扩展名的网站上检测到它们。

NoSQLMap

NoSQLMap是一个可用于审计的 Python 工具。它通常用于 SQL 注入攻击的自动化，并用于发现NoSQL 数据库和使用 NoSQL 从数据库中披露或克隆数据的 Web 应用程序中的默认配置漏洞。

这个开源工具维护得很好，可以看作是 SQLMap 的表亲。顾名思义，NoSQL 解决了与关系数据库中使用的表格方法不同的数据模型。但是 NoSQL 数据库确实支持类似 SQL 的查询语言，因此受制于 SQLi。NoSQLMap 主要关注 MongoDB 和 CouchDB。未来的版本将扩大其曲目。

Tyrant SQL

Tyrant SQL是一个基于 Python 的 GUI SQL 注入工具，类似于 SQLMap。它的 GUI 允许更大的简单性。这使得初学者更容易分析易受攻击的链接并确定弱点所在。

Whitewidow

Whitewidow是另一个开源 SQL 漏洞扫描程序。由于它是自动化的，它可以快速运行一个长文件列表或从谷歌搜索潜在易受攻击的网站。

Whitewidow 还提供其他功能，例如自动文件格式化、随机用户代理、IP 地址、服务器信息和多 SQL 注入语法。该工具还提供了从其中启动 SQLMap 的能力。

然而，Whitewidow 与其说是一种补救工具，不如说是一种教育工具。它可以帮助用户了解漏洞是什么样的，但它依赖于 SQLMap 来获得更强大的 SQLi 检测功能。

Explo

Explo是一个基本工具，旨在以人类和机器可读的格式描述 Web 安全问题。它定义了一个请求/条件工作流，允许它在无需编写脚本的情况下利用安全问题。

因此，它可以解决复杂的漏洞，并以简单的可读和可执行格式共享它们。

什么是 SQL 注入？

结构化查询语言或 SQL 是一种在Microsoft SQL Server、Oracle、IBM DB2 和 MySQL 等关系数据库中大量使用的语言。由于数据库倾向于为企业托管敏感信息，恶意 SQL 注入可能导致敏感信息泄露、Web 内容修改和数据删除。

然后，SQLi 会利用基于 SQL 的应用程序中存在的漏洞。黑客将代码注入 SQL 查询，使他们能够添加、修改和删除数据库项目。

但受影响的不仅仅是数据库。SQLi 可以传播到连接到 SQL 数据库的 Web 应用程序和网站。根据开放 Web 应用程序安全项目 (OWASP)，注入是 Web 应用程序最普遍的威胁。

如何防止 SQL 注入？

SQLi 攻击执行恶意 SQL 查询，可用于绕过应用程序安全性，避免授权和身份验证登录和系统。攻击因数据库引擎的类型而异。最常见的变体包括基于用户输入的 SQLi、基于 cookie 的 SQLi、基于 HTTP 标头的 SQLi 和二阶 SQLi。

SQLi 的缓解和预防最初都是为了了解哪些应用程序可能易受攻击——这意味着任何与 SQL 数据库交互的网站。漏洞扫描是评估您可能面临风险的好方法。另一种方法是进行渗透测试。这本质上是试图闯入您的系统并找到任何可以利用的缺陷。

MarkerHub

實戰滲透|一次巧合偶然的sql注入

HACK之道