SQL 注入攻击

SQL 注入攻击

SQL 注入是一种安全漏洞。它是对数据库驱动的应用程序攻击的一个特定类型。在这种攻击中，攻击者操纵网站基于 Web 的界面，迫使数据库执行不良 SQL 代码。攻击者可以利用这个安全漏洞向网络表格输入框中添加 SQL 代码以获得访问权。而今天的 SQL 注入攻击者查找漏洞的技术更加先进。他们使用各种工具加快开发进程。

SQL 注入攻击最新动态

最近几个月，安全专家发现大量的网站受到一系列的数量众多的 SQL 注入攻击，这种攻击利用脆弱的 Web 应用程序，使用这些站点作一个平台，使访问者的 PC 感染恶意软件。而且数据库安全专家 David Litchfield 正在研究利用多种不需要输入的 PL/SQL 程序的新方法，也就是侧面 SQl 注入。它可以对 Oracle 数据可进行远程攻击。通过用户的 SQL 注入对 Web 站点发动大规模攻击的趋势正在继续。

- 新一轮 SQl 注入攻击敲响警钟
- 新 SQL 注入蠕虫出现
- 新 SQL 注入技术威胁 Oracle 数据
- 为什么侧面 SQL 注入和 NULL 指示器攻击那么重要

SQl 注入攻击测试的实施

手工测试 SQL 注入的方法过去一直是确定数据库是否存在安全漏洞的惟一方法。挖掘返回的错误信息、增加省略符号并且设法猜测数据库结构信息是一项长期的和艰苦的过程。而且，这并不能保证你发现所有的 SQL 注入安全漏洞，很少能够查看或者提取数据。现在，有一些工具能够实施 AQL 注入攻击。一些免费的和商业性的黑客工具都能够实施这种攻击。

- 实施自动的 SQL 注入攻击测试

SQl 注入攻击的应对措施

今天的 SQL 注入攻击在查找漏洞方面的技术更加的先进。在预防 SQl 注入攻击时，我们需要知道网站何时可能受到什么样的漏洞的攻击，而一个好的网络漏洞扫描器将发现您网站上的所有目前已知的 SQL 注入漏洞。而面对数据库的 SQl 注入攻击，也可以采取避免使用单引号标志、限制那些执行 Web 应用程序代码的帐户权限、减少或消除调试信息等方法进行防御，此外，微软也提供了一些简单的工具，例如 Scrawlr 和 UrlScan version 3.0 Beta，来应对 SQL 注入攻击。

- 防止 SQL 注入
- 自动式 SQL 注入攻击的新型防御
- 微软工具应对 SQL 注入攻击

新一轮 SQl 注入攻击敲响警钟

黑客正在寻找快捷键便的方法攻击大量的计算机，他们越来越多的依靠一种重新获得喜爱的旧的可信任的方式：SQL 注入。

最近几个月，安全专家发现大量的网站受到一系列的数量众多的 SQL 注入攻击，这种攻击利用脆弱的 Web 应用程序，然后使用这些站点作一个平台，使访问者的 PC 感染恶意软件。研究人员说这种趋势令人担忧，原因有多个，但是最大的关注点是 Web 上的大量站点都容易受到这种攻击，而且黑客很容易找到并攻击新目标。

甚至相关地基础站点任何时候都可以有几个应用程序运行　它所利用的知识一个编程过程中的小小的错误代码，黑客就得到了一个开口。

“它不需要花费多少精力”惠普实验室 Web 安全研究小组的安全研究员和 Web 应用安全专家 Billy Hoffman 说，“有这么多的面向 Web 的应用程序，它们很多都是几年前写的，都没有经过任何形式的代码检查。”

新一轮的 SQl 注入攻击好像今年很早就开始了，并且一直持续不衰退，研究人员不断发现越来越多拥有一个或多个攻击点的域。这种攻击可以采用几种不同的形式之一，但是公分母是他们试图在不同的合法网页注入恶意 SQL 命令行。这会引发在后门应用程序的上运行的数据库错误。

最近发现的工具包是 Asprox 特洛伊，最近几周研究人员发现它被垃圾邮件 botnet 所分散。SecureWorks 的高级安全研究人员 Joe Stewart 作了 Asprox 特洛伊分析，而 Asprox 特洛伊是有关于窃取密码的特洛伊，比如 Danmc。一旦这种恶意软件感染了一台个人电脑，它就会下载一个二进位，当这个二进位制运行的时候，就会用 Google 搜索包含特别术语的站点。然后就会在这些站点发动 SQL 注入攻击。结果就会是这些站点的访问者

会被强制从另外一个站点下载一段恶意 JavaScript 代码。Stewart 说，这些代码会把用户指引到第三个网站上，这里有更多的恶意软件，可能是 Asprox 或 Danmec 的副本。

“Asprox 代码和被中国域名感染，而安装游戏密码窃取特洛伊的代码很相似。”Stewart 说，“我不知道它们是不是从中国取得的副本还是只是一个复制机，但是它们在一定程度上成功了。看起来好像是有人拿了代码，并把它放进了一个大型的程序中，尽可能广泛的传播。”

“暂时驱使黑客的是复制机和扫描和感染工具的全面的实用性，它们和上千个合适的过时 Web 应用程序结合起来，结果就是现在的状况---超过 150 万的网页受到感染。”Dancho Danchev 说。他是一位独立的安全咨询专家和研究人员，他一直在跟踪 SQl 注入攻击。他说：“单独的复制机几乎就是带有 Asprox 的僵尸网络大师，以及它不断努力地参与攻击。此外，被注入的恶意域名被放在 fast-flux，也就是说，它们对被感染恶意软件的主机上的 10 个不同的 IP 作出回应，而这些主机是网络的一部分，那些 IP 也再不断的变化。目前的攻击可以被简单的描述为抵达 Web 最深处的 SQL 注入攻击的长尾巴。它们简单地做些侦察，然后攻击脆弱的目标。”

研究人员说，实际上它不可能以这种方式知道有多少站点受到攻击，虽然 Stewart 估计 Asprox 恶意软件到目前已经感染了 35000 个站点，这是基于 Google 搜索的结果。但是有一点很明显，黑客进行内容攻击的地方知识为了强行进入数据库，而获得有趣的‘天然金块’现在它们正关注于获取尽可能多的 PC，兵士用这些 PC 作为它们活动的平台。

“我们看到的是展开的 Web 威胁，好像桌面威胁，” Hoffman 说，“这些人习惯于只对他们可以从这些站点得到的东西感兴趣。现在，这些站点是他们窃取数据和实行攻击的平台。他们认识到他们可以利用这些机器作为资源。为什么只是在我可以用它安装恶意软件和跳到其它机器上的时候拥有这台机器呢？”

最近的大量 SQl 注入行为看来是来自中国，全世界的研究人员一直都在跟踪这些攻击。Shadowserver Foundation 公布了一份包含了所有把恶意代码注入到其他站点的域名列表，他们中的大部分是中国域名，其他的多是.com 或 .info 的地址。

处于一些原因，SQl 注入已经在黑客中重新流行起来，特别是因为它可以自动化的简易程度。但是它也是令人发狂的执行简单的攻击，其潜在的目标群很大，使它不但吸引了低级的脚本小后生，而且吸引了寻找大目标的专业人士。

“这些站点中没有平民站点，他们只是含有程序错误的站点，这些人取得了尽肯能最广泛的攻击界面，这就是 SQl 的注入点。” Stewart 说，“他们甚至不需要做任何工作来找到目标。他们所做的是到 Google 搜索含有特殊术语的 Active Server Pages（ASP）。他们知道页面可以在后门运行 MS SQL，然后他们只是在这些页面中寻找特殊的证据，这样就完成了。”

中国的 SQl 注入攻击在三月份就开始了，而且还在继续，按照设计它们主要是安装窃取 World of Warcraft 等在线游戏密码的特洛伊。但是，正如 Stewart 所指出的，他们可以短时间内从窃取游戏密码过渡到窃取在线银行密码。

“这根本不需要话很多的精力。可以阻止他们的是这在中国是很严重的犯罪。中国为此已经给一些人判刑了。” Stewart 说，“所以可能是人们不再愿意再冒险。”

（作者：Dennis Fisher 译者：Tina Guo 来源：TechTarget 中国）

新 SQL 注入蠕虫出现

通过用户的 SQL 注入对 Web 站点发动大规模攻击的趋势正在继续，SANS Internet Storm Center 和 Shadowserver Foundation 的专家们正在跟踪新近发现的 SQL 注入蠕虫，这种蠕虫表现为攻击 RealPlayer 漏洞，并在脆弱的站点安插恶意软件。这些攻击主要集中在 ASP 页，他们使用常见的 iFrame 攻击方法，这种方法包含在最近的大量 SQL 注入攻击中。在成功攻击一个脆弱的 PC 后，受到感染的站点就会在用户的 PC 上面安装二进制。Shadowserver 的研究演员对这种攻击的分析表明，该二进制被命名为“test.exe”，而它只是一长串的下载器和恶意软件中的一环。

Shadowserver 的分析是说：“在攻击中，被下载的二进制看起来是，我们一段时间以来在中国的恶意软件家族中看到的工具包中的一部分。安装后，这种恶意软件要做的第一件事情就是下载配置文件。配置文件中包含一些命令，指挥系统下一步怎么做。在我们的例子中，它（命令它）下载另外一个文件，并汇报进入到一个 URL 中。”

整个家族的玩笑。Shadowserver 也有一个不错的恶意站点和提供恶意软件的 IP 地址列表，供大家过滤使用。

（作者：Dennis Fisher 译者：Tina Guo 来源：TechTarget 中国）

新 SQL 注入技术威胁 Oracle 数据库

数据库安全专家 David Litchfield 正在研究利用多种不需要输入的 PL/SQL 程序的新方法。他把这型技术描述为侧面 SQl 注入，可以对 Oracle 数据可进行远程攻击。

这种攻击利用一些普通的数据类型，包括 DATE 和 NUMBER，它们不需要使用用户的输入，所以通常不被认为可以攻击。但是，Litchfield 在他关于侧面注入攻击的新文章中写道，使用一点创造性译码和一些 Oracle 数据可管理系统工作方式的知识，黑客就可以操作一些一般的功能。

Litchfield 是英国 NGS Software 公司的创始人之一，他说这个问题可能不会那么容易的攻击，但是特殊情况下，它可以被用于向数据库传输任意 SQL 命令。

PL/SQL 是 Oracle 公司的 SQL（structured query language）的延伸。

“总之，如果使用 SYSDATE，那些不需要用户输入的功能和程序就有可能受到攻击。这里的教训总是会得到验证，防止这类攻击进入你的代码。第二个教训是 DATE 或者 NUMBER 不应该再被认为是安全的，也不会和注入携带者一样有用：这篇文章证明，他们是。”他写道。

这类攻击工作模式如下：使用 SYSDATE 功能，黑客可以使用 ALTER SESSION 权限欺骗 SQl 编译器，接受任意的 SQL 数据作为 DATE 数据类型的输入。DATE_PROC 使用变量 V_DATE 在调用 SYSDATE 功能后，设置数据。尽管如此，通过改变讨论（altering the session）和插入 SQL 命令，黑客可以迫使数据库执行他的命令。

黑客的攻击不需要本地访问数据库。

“可以通过远程完成，例如，借助一个 Web 应用程序，通过 SQL 注入漏洞，但是不是直接进入。” Litchfield 在邮件采访中，如此说。“首先，我们攻击注入点来执行促进功能，这允许我们运行任意 SQL，然后在这里可以使用这项技术。”

Litchfield 的文章中有意思的一点是 DATE 和 NUMBER 等数据类型被认为是“安全”的事实，意味着他们还没有受到攻击。最近几个月中，这类攻击越来越多，研究人员已经开始深入研究流形的应用程序，在有些情况下发现了严重的新型攻击携带者。

去年夏天，Watchfire 公司的研究人员，现在是 IBM 的一部分，他们发现攻击摇摆指示器的方法，这是一个被认为不能攻击的平常的程序失误。IBM 的 ISS 部门的研究人员 Mark Dowd 发表了一篇论文，详细指出了攻击 NULL 指示器解除参照。

对他来说，Litchfield 的新方法不是通过长时间的脑子里的工作，而是通过看电视产生的。

他说：“同时，观看‘Bones’的一段情节，里面发生的一些事情让我想到不要接受默写认为真实东西，比如，在这种情况下，通过 DATE 和 NUMBER 数据类型进行 SQL 注入是不可能的。所以坐下来，想一想我在文章中提出的一些技术。”

（作者：Dennis Fisher 译者：Tina Guo 来源：TechTarget 中国）

为什么侧面 SQL 注入和 NULL 指示器攻击那么重要

最近在研究领域有很多有趣的工作，主要是关于一些专业而深奥的应用攻击，比如 Mark Dowd 的 NULL 指示器攻击和 David Litchfield 的侧面 SQL 注入技术，这两种攻击有一些共同点，特别是他们都利用那么被认为不可能受到攻击的事物这一事实。两外一个相似之处是，有些人把这两种技术分为理论和纯学术想法的演习，而永远不可能见到光亮。这种想法的支持者说，企业永远也不需要担心这种难理解的疯狂的多步骤攻击。他们说，这有点儿像缓冲器溢出和需要注意的蠕虫。

这有点儿，嗯，应该怎么说呢，可笑。这些新型攻击确实需要你关注，如果你负责保护公司网络的话。黑客在像这样的可信赖的攻击上的投资很大，特别是当它们完全是新的并不太好理解的时候。安全专家知道缓冲器溢出是什么样的，并且有许多产品可以阻止这些攻击。但是像 Mark Dowd 的 NULL 指示器攻击和 David Litchfield 侧面的 SQL 注入技术这样的复杂技术，会使网络防护崩溃，而当被发现时，已经 gameover 了。还有谁说在乌克兰或巴西或者中国还没有长时间地使用相同的技术呢？

当然，蠕虫和病毒以及网络钓鱼仍然威胁网络安全，但是因为新的攻击类型看起来比较困难或复杂就忽视的做法，说好听点儿是愚蠢，说得不好听就是犯了过失罪。

（作者：Dennis Fisher　译者：Tina Guo 来源：TechTarget 中国）

实施自动的 SQL 注入攻击测试

SQL 注入是一种安全漏洞。攻击者可以利用这个安全漏洞向网络表格输入框中添加 SQL 代码以获得访问权。手工测试 SQL 注入的方法过去一直是确定数据库是否存在安全漏洞的惟一方法。挖掘返回的错误信息、增加省略符号并且设法猜测数据库结构信息是一项长期的和艰苦的过程。而且，这并不能保证你发现所有的 SQL 注入安全漏洞，很少能够查看或者提取数据。

现在，有一些工具能够实施 AQL 注入攻击。一些免费的和商业性的黑客工具都能够实施这种攻击。

如果你有一个连接到后端数据库的 Web 前端，允许 ASP、ASP、.NET、CGI 和类似的脚本语言支持的动态用户输入，你就可能遭到 SQL 注入攻击。你能做的就是以道德黑客(ethical hacking)的方式对你自己的系统实施自动的 SQL 注入攻击，以便发现能够在外部攻破什么东西。不要选择这个或者省略那个，让你的工具为你做工作。

这是以自动的方式测试你的系统的 AQL 注入安全漏洞的两个步骤。我在这里简单介绍一下这个过程。

第一步:扫描安全漏洞

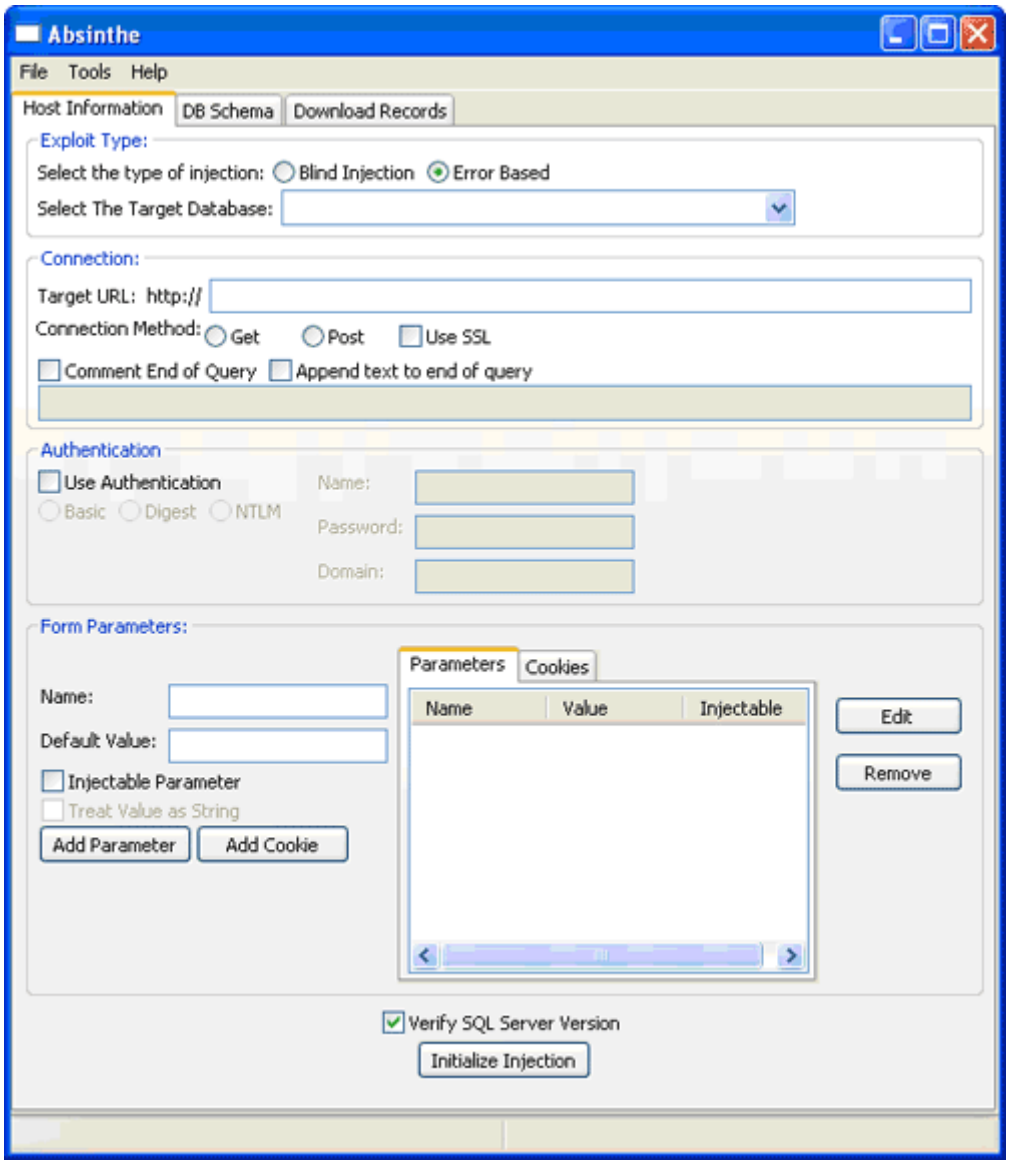
首先，你必须使用一个 Web 应用程序安全漏洞扫描器扫描逆的网站，看看是否存在任何输入过滤或者其它具体的 SQL 注入安全漏洞。由于我的时间总是很紧张并且需要良好的报告功能，我喜欢使用商用工具，如 N-Stealth 安全扫描器、Acunetix 公司的 Web 安全漏洞扫描器和(我最喜欢的)SPI Dynamics WebInspect。Wikto 等免费的工具通常也能发现这些安全漏洞。

图 1 显示的是 WebInspect 发现的两个不同的 SQL 注入安全漏洞的例子。

第二步:开始 SQL 注入

一旦你确定你的目标系统是否存在 SQL 注入安全漏洞，你的下一个步骤就是实施 SQL 注入过程并且确定能够从数据库中搜集到什么。请注意，我不建议注入实际的数据或者试图投放数据库表格，这两种做法对于你的数据库的安全是有害的。发现潜在的 SQL 注入漏洞是一回事，以自动的方式实际实施攻击是另一回事。

我喜欢的自动实施实际的 SQL 注入攻击的工具是 SPI Dynamics 公司的 AQL 注入器(这个工具是 WebInspect 软件的一部分)。你还可以使用图 2 显示的 Absinthe。



实施自动的 SQL 注入攻击测试图 2:Absinthe 工具用于自动实施 SQL 注入分析。

这两种工具能够让你实施基本的和 SQL 盲注攻击。这两种测试都应该实施，特别是如果基本的 SQL 注入攻击没有返回任何结果的情况下。这些工具能够以自动的方式非常快地查询和提取数据，在几分钟之内就可以列印大量的表格。

其它选择包括 Foundstone 公司制作的一种免费的 Web 服务测试框架。这个工具的名称是“WSDigger”，能够实施基本的 SQL 注入攻击。你还可以使用 Automagic SQL 注入器进行一些自动的 SQL 注入查询。你还可以使用配置了 SQL 注入插件的“Sleuth”工具软件。但是，这个软件需要 SA 访问权限。这就消除了匿名外部测试的好处。

最后，如果你要在你现用的系统部外进行实际练习，并且学习更多的有关 SQL 注入和其它能够导致数据库被攻破的前端 Web 应用程序安全漏洞的知识，你可以查看 Foundstone 公司的“Hacme Bank”，或者参考一下 Web 安全演示工具“WebGoat”。

你使用什么工具自动实施 SQL 注入攻击测试都没有关系，只要你能够了解它们是如何工作的并且得到预期的结果就行了。就做黑客要做的事情就行了。

(作者：Kevin Beaver 来源：TechTarget 中国)

防止 SQL 注入

负责公共易访问的互联网服务器的安全的专业技术人员，常常（理直气壮地）关注维护从厂商那里购买的操作系统和服务器软件。确实，这些软件包常常包含重大的安全漏洞，而且对于每一个安全管理员来说，确保使用厂商的最新安全补丁和修复程序，来修补他们的服务器是义不容辞的。

然而，这并不是管理者的责任范围。您可能知道，您机构开发的、用来强化动态网站功能的自定义代码存在在网站服务其中开放重大漏洞的潜在可能。当你正在使用 Web 应用程序向后端数据库提供界面时，这些漏洞是特别危险的。对数据库驱动的应用程序攻击的一个特定类型是 SQL 注入。在这种攻击中，入侵者操纵网站基于 Web 的界面，迫使数据库执行不良 SQL 代码。

最好通过实例来了解 SQL 注入攻击。试想一个包裹递送公司建立的简单网站，它向知道与某个包裹相连的追踪号码的任何人，提供递送状态信息。该应用程序可能会简单地向用户要追踪号码，然后使用下面的 SQL 代码，在数据库表里查找它。

```
select *

FROM Shipments

where TrackingID=’ @tracking’
```

这里，@tracking 是一个从 Web 应用程序传递过来的变量。在正常情况下，这个应用程序可能会完全正常地工作。例如，如果用户输入追踪号码 1A2123ZC2，相应的查询将是：

```
select *
```

```
FROM Shipments

where TrackingID=’1A2123ZC2’
```

理想的情况——用户将仅仅输入一个有效的追踪号码——造成一个有缺陷的假设。怀有恶意的个人用户不太可能这么合作。假设用户输入如下所示的，在追踪号码区域里的字符串：

```
1A2123ZC2’ or true
```

相应的查询将是：

```
select *

FROM Shipments

where TrackingID=’1A2123ZC2’ or true
```

这将有意想不到的结果，可以得到存储在数据库里的所有的追踪信息。现在假设，我们遇到一个更有恶意的用户，输入下面的字符串：

```
1A2123ZC2’; delete FROM Shipments
```

这将导致数据库执行下面的查询：

```
select *

FROM Shipments

where TrackingID=’1A2123ZC2’;

delete FROM Shipments
```

这将会有明确的不良结果，那就是从数据库中删除所有的追踪信息。

你可以采取一些步骤，以减少针对您的数据库的 SQL 注入攻击的可能性：

- **避免使用单引号标志。** 包括您的 Web 应用程序中的代码，用双引号代替单引号。这将强迫数据库服务器把引号作为一个字符，而不是字符串定界符。
- **限制那些执行 Web 应用程序代码的帐户权限。** 在上面的例子中，如果该帐户仅有执行预期的行为（从运送表检索记录）的许可，就不可能将其删除。
- **减少或消除调试信息。**当您的服务器发生错误情况时，Web 用户不应该查看错误的技术细节。这种类型的信息可以帮助入侵者寻求利用您的数据库结构。
- **培训您的开发人员。**确保在您的机构中，负责开发代码的人员知道这种威胁的严重性，以及他们可以采取的、帮助维护您的服务器的简单步骤。
- **测试您的 Web 应用程序。**抽查您的开发人员的工作。您可以做一个简单的检查，即把单引号放进发往您的服务器的数据中。如果您收到一个任何形式的错误回应，表明您可能容易受到 SQL 注入攻击。

如果您花时间去实施这些简单的步骤，您将在保护您的网络/数据库互动的路上走得很好。

（作者：Mike Chapple 译者：李娜娜 来源：TT 中国）

自动式 SQL 注入攻击的新型防御

最近，SANS 协会互联网风暴中心(Internet Storm Center)的分析家们发现了一种工具：可以将易受 SQL 注入攻击网站的搜索和开发过程自动化。自动操作阐明了使用部分合法网站来主办和传播恶意软件，这一技术正日益流行。

在这篇文章中，Techtarget 中国的特约专家会探讨一下 SQL 注入攻击，并研究如何发现、隔离和解决一个不同的安全网站的恶意网页。

以往的 SQL 注入攻击

SQL 注入攻击并不是什么新事物。例如，在 2003 年公开审理的一个案例中，一家服装公司，Guess 公司在其网站上遭受了一次 SQL 注入攻击，结果导致安全破坏以及政府主导的法律解决。当时，法庭文件把 SQL 注入描述为事故“当攻击者在标准网页浏览器的地址栏里键入某些字符，指引应用程序从支持或连接到网站的数据库那里获得信息”。在法庭上，已经发现攻击者操纵应用程序，以明文形式访问 guess.com 数据库里的每一个表格，包括提供买家信用卡信息的那些表格。

如果暴露敏感信息，公司面临的责任并没有改变。然而，关于最近一轮的 SQL 注入攻击的新内容是：攻击自动化的程度和它们所执行的绝对范围。

新型的 SQL 注入攻击

从技术角度来看，在如何寻找有漏洞的网站方面，今天的 SQL 注入攻击者更加彻底。他们使用各种工具加快开发进程。考虑到 Asprox 特洛伊木马病毒，它通过垃圾邮件和僵尸网络四处传播。Joe Stewart 是总部设在亚特兰大的 SecureWorks 公司的高级安全研究员，他介绍了整个过程是如何进行的：

1. 通过垃圾邮件（它通过受到感染的主机互相发送）安装一个特洛伊木马病毒。

2. 受到特洛伊木马病毒感染的电脑下载一个二进制，当启动时，它使用 Google 搜寻潜在的漏洞网站，这些网站使用由微软的 Active Server Pages 建立的窗体。搜寻结果成为 SQL 注入攻击的目标列表。

3. 特洛伊木马病毒发动对那些网站的 SQL 注入攻击，感染它们中的一部分。

4. 访问受感染网站的人们，被蒙骗从另一个网站下载一段恶意 JavaScript 代码。

5. 代码指引用户到第三方站点，那里有更多的恶意软件，比如 Asprox 或 Danmec 的副本。

这些步骤恰好说明，在过去的五年里所发生的变化。以前，网站应用程序开发商被建议测试和修补他们的代码，以防止发现及恶意利用 SQL 注入漏洞这样的微小机会发生。然而，最近的攻击已经表明目前更可能发现和恶意利用漏洞。因此，开发商应在配置前，优先大力地测试代码，一旦报道出新的漏洞，及时进行修补。

了解一个网站何时受到攻击

当然，没有任何一个企业希望在不知情的情况下传播恶意软件。所以你如何知道你的网站受否受到了感染？奇怪的是，答案可能出现在来自 Google 的公告里。在黑客攻击工具两方面如何工作的一个很好的例子中，Google 是 stopbadware.org 项目的一个主要成员，监测网站是否有“恶意软件”：即间谍软件、病毒软件和欺骗性广告软件。事实上，Google 自动向下面域内的电子邮件地址发送恶意软件警报，这些地址中的网页搜寻器存在问题：

* abuse@

* admin@

* administrator@

* contact@

* info@

* postmaster@

* support@

* webmaster@

* abuse@

* admin@

* administrator@

* contact@

* info@

* postmaster@

* support@

* webmaster@

当然，一个企业必须做好准备接收这些消息，即一些听起来很容易受骗的东西。在这些地址里，也许有垃圾邮件过滤器，或者更糟的是，没有指定的收件人，这就意味着这些消息可能不会被阅读。为所有企业的网域，编目和核实联络资料是很好地回应这新一轮攻击的第一步。精明的安全专家也许想利用这些攻击的消息，进而获取额外的资源，对整个网站进行检查。

在过去的五年中，Web 活动的爆炸性速度的增长，已经导致产生了许多“迷失”的网站，随后发起的项目，因没有合理的结果而被摒弃。不幸的是，Google 网络蠕虫将会不懈努力，精确地找到它们，并且如果它们是潜在的攻击目标，最终将会受到攻击。然而，所幸的是，一个企业可以主动地确定它是否有“恶意软件”的问题：免费使用 Google Webmaster Tools，可以检查任何网站。

那些不方便依赖 Google 的组织，应该着手对他们的网站进行详细的检查。有一些有所帮助的工具，以 Xenu’s Link Sleuth 开始，它是一个免费程序，能检测某一网站上的所有连接，并且报告各种错误。切记要测试生产站点和从公司网络以外的一台机器上运行检查；否则，就可能会漏掉一些问题。

如何应对新型的攻击

向前发展，网络漏洞扫描器中将引入一个积极主动的策略，这些扫描器有：例如 Acunetix 有限公司和 SPI Dynamics（现在为 Hewlett-Packard Co.所有）的那些扫描器。一个好的网络漏洞扫描器——不要与网络扫描器混淆——将发现您网站上的所有目前已知的 SQL 注入漏洞。当新的漏洞为人所知时，一个新式的扫描器就会发现他们。

谨记，防御 SQL 注入攻击也许还不够。攻击者对目标正采取一致和自动的搜寻，并对它们实行攻击。这些技术可以很好应用于除 SQL 以外的，其它 Web 基础架构漏洞。

最后，在 Web 应用程序开发过程和生产前的安全测试的各个阶段，目前安全代码的测试比以往更加重要。它们应该通过配置后的测试进行扩充，这些测试包括漏洞扫描工具和现场监测。

（作者：Michael Cobb　译者：李娜娜 来源：TechTarget 中国）

微软工具应对 SQL 注入攻击

微软提醒用户，有几款工具可以支持应用配置，这是在针对网站中的缺陷代码发起的越来越多的 SQL 注入攻击。

这家软件巨头推荐用户使用周二的安全公告中提到的工具。它通知用户，他们正在跟踪大量攻击。这些攻击发生在使用微软 ASP 和 ASP.NET 技术的网站上。问题存在于一些微小软件代码漏洞，而这样的漏洞很难检测到。

微软安全响应通信(MSRC)经理，Bill Sisk 说： “这些 SQL 注入攻击并不利用特定的软件漏洞，但是，他们以一些网站为目标，这些网站在访问或使用存储在相关的数据库中的数据时，不遵守安全代码实践的。”

在过去的几个月中，研究人员一直在跟踪上千个网站中的大量的 SQL 注入。这种攻击使用一些黑客工具，而这些工具可以在黑市上买得到。基本上这些攻击可以引发 Web 应用服务器上的错误，允许黑客在系统中插入自己的代码并获得访问权。具体被攻击的网站数量还不能确定。

在给用户的公告中，微软把 Scrawlr 确定为漏洞扫描器，这种扫描器是由 Hewlett Packard 和 MSRC 的研究人员共同开发的。在一篇博客中，惠普的应用安全中心的高级产品经理 Erik Peterson 说，这种工具随软不如厂商全力支持的产品，但是它是免费的，并且可以块孙分析网站的潜在问题。这种工具不能确定那一行代码有问题，只能在 1500 个页面中慢慢查找。它不支持网站请求认证，也不能为 SQL 注入测试窗体，此外还有一些其它限制。

UrlScan version 3.0 Beta 是微软开发的一款工具，可以阻止 HTTP 请求。微软说这款工具可以阻止有害的请求到达服务器上的 Web 应用程序。按照设计这种工具可以从

urlscan.ini 文件中读取配置。很多例子证明这款工具可以作为 URL 过滤器安装。管理员可以使用这种工具限制由互联网信心服务处理的请求类型。

微软对 SQl 注入的源码分析也可以用于检测受到 SQL 注入攻击的 ASP 代码。它可以产生一个报告，显示代码问题。微软承认这种工具也有一些限制。他只能解决在 VBScript 上写的 ASP 代码，而且使用它有时会导致一些分析错误。

BigFix 的首席技术官 Amrit Williams 说， 把这种工具交给 Web 开发人员和 IT 管理员，可以帮助他们促进安全意识，特别是对 90 年代中期的质量不太好的产品。Amrit Williams 原来是 Gartner 的分析师。Amrit Williams 警告说，这种工具不能提到更高级的技术，或者经验丰富的全人力分析。

在一封交换邮件中，Williams 说： “不幸的是，总是重大事故驱动人们去做正确的事情。在软件开发生命周期，甚至是 Web 开发中的安全部分，尤其如此。而 Web 开发更快速，并且比传统的软件开发结构少。”

(作者：Robert Westervelt 译者：Tina Guo 来源：TechTarget 中国)