“SQL 注入防护”资料

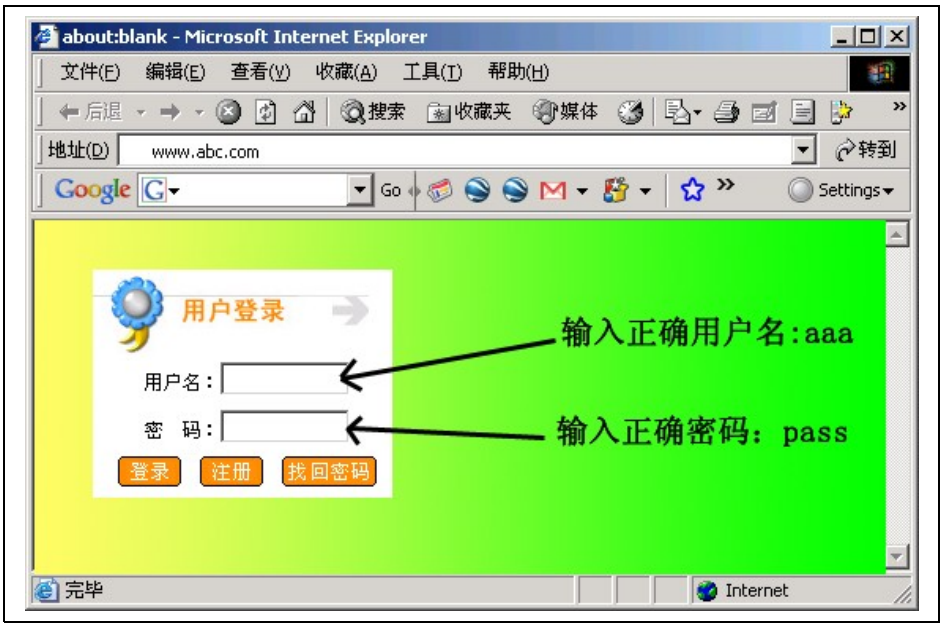
1、什么是 SQL 注入攻击？

在 B/S 模式的应用中，由于网站代码没有对用户输入的信息做合法性检查或者检查存在漏洞，导致用户可以提交一段数据库查询代码，根据程序返回的结果，获得某些他想得知的数据并进而发起更进一步的攻击，直至获取管理员帐号密码、进入系统窃取或者篡改文件、数据，这就是所谓的 SQL Injection，即ＳＱＬ注入。

举个简单例子吧：

某网站 www.abc.com，提供了用户交互的内容，用户使用该网站时需要输入帐号密码进行登录。

正常情况下如下图：



如上图，输入了正确的用户名和密码以后，点击“登录”，就进入系统了。但是，这是一个正常的用户，假设一个怀有其他企图的用户呢？他会对网站代码的行为进行分析，并不断的测试，比如他在应该输入密码的地方输入的是”aa’ or ‘1’=’1”， 而不是”pass”，那么，如果网站代码没有对用户输入作任何检查而仅仅是把用户输入的内容组装成一个数据库查询语句的话，他的这个输入就有可能已经让他能登录到这个系统中！因为当用户点击了“登录”以后，网站代码把用户输入组装成一条语句，然后上数据库里面查询用户输入的帐号密码是否正确，正常情况下这条语句看起来象这样：

Select * from UserTbl where name=’aaa’ and pwd=’pass’

而当在密码取中输入”aa or 1=1”时，网站代码还是照常组装这些用户输入，结果就成了这样：

Select * from UserTbl where name=’aaa’ and pwd=’ aa’ or ‘1’=’1’

这样的一条 SQL 语句是永远成立的，不管他输入的用户名或者密码是否正确！如果网站代码

没有正确的处理话，那么这个居心叵测的操作者在不知道正确密码的情况已经登录进来了！

当然，实际上象这么容易注入攻破的网站可能很少，但是对于存在 SQL 注入漏洞的网站，攻击者还有如此之多的手段和辅助工具，他可以逐步对网站进行分析，来发现其中的漏洞并且进行攻击。

2、安装了杀毒软件和防火墙，还会有 SQL 注入吗？

SQL 注入是从正常的 WWW 端口访问，而且表面看起来跟一般的 Web 页面访问没什么区别，所以目前市面的防火墙都不会对 SQL 注入发出警报，如果管理员没查看 IIS 日志的习惯，可能被入侵很长时间都不会发觉。

3、如果网站程序员有经验，在代码中作了检查，能阻止 SQL 注入吗？

有经验的网站程序员在编写网站代码的时候，一般会对用户的输入作合法性检查，但是这种检查存在的全面性会存在一定的问题；另外，由于采用的是针对 SQL 语法的关键词作检查，就难免会有误判的情况；此外如果检查过于复杂，网站效率会受到较大影响。也就是说，仅仅在网站代码中进行 SQL 注入的检查，其效果不理想。对于初级的攻击者可能能有效防范，但是对于有经验的注入攻击者，则最终还是会被发现漏洞所在，何况从互联网上获得 SQL 注入检查器[实际上很多人用它来发现网站的 SQL 注入漏洞然后再发起攻击]是一件非常容易的事情，这些辅助工具里面集成了很多注入攻击的经验代码，一般的防范对于他们而言很容易发现漏洞。

4、如何才能有效的阻止 SQL 注入攻击？

我们提供的 SQL 注入攻击防护模块，与 IIS 集成在一起，对于用户输入进行检查，能有效的防范 SQL 注入攻击。

SQL 注入攻击防护模块采用高效 C++编码，通过对用户输入按照 SQL 语法进行词法和语法分析，还包括进行表达式的提取计算，而不是简单的通过关键词过滤，能有效的发现用户提交内容中的 SQL 注入攻击企图，能处理的攻击包括：Blind SQL 注入攻击、SQL 注入攻击、XSS 攻击【跨站代码攻击】、文件注入攻击、SSI 注入攻击、PHP 注入攻击等 10 余种攻击类型。可以有效的提高网站防范 SQL 注入攻击的能力。

5、其他能力

除了能防范以上所说的注入攻击以外，系统能支持对注入攻击者进行 IP 锁定；还允许用户设置过滤关键词，用来防止用户向网站提交反动、黄色、政治、宗教等等方面的内容。