SQL-иньекция

Первичная защита в QP7

Что это такое

Первичная защита представляет собой удаление некоторых опасных SQL-конструкций, например UPDATE, DELETE, UNION:

Где она поддерживается

- Стандартный функционал фильтрации и сортировки Publishing Container (защита осуществляется в Run-Time, а не на этапе сборки, поэтому работает как для статических параметров Publishing Container, так и для динамических)
- GetContentData (Прямой вызов из DBConnector Cnn.GetContentData не защищен)

Поддерживается в следующих версиях QP:

a. ASP – с версии 7.1
b. ASP.NET – во всех (так как данный тип сборки появился только в версии 7.2)
c. ASP.NET (like ASP) – отсутствует

Также с версии 7.1 появились рекомендуемые для использования в фильтрах функции NumValue и StrValue.

Где она не поддерживается

В общем случае, это любой код, работающий с базой данных и не использующий стандартный функционал Publishing Container или страничного метода GetContentData

Код, в котором отсутствует первичная защита:

- GetData
- GetPageData
- Cnn.GetContentData (страничный метод GetContentData защищен)
- cnn.Execute
- API-функции QP7
- Пользовательский код, устанавливающий собственные соединения с базой данных

Код, в котором отсутствует защита можно искать в

- форматах и шаблонах QP (поиск с помощью like по базе)
- .inc-файлах (для ASP-сайтов) (поиск по файлам через UltraEdit или Total Commander)
- .dll-сборках (для ASP.NET сайтов) (поиск по файлам соответствующего проекта через Visual Studio)

Текущая ситуация

На cluster.quantumart.ru сейчас стоит модифицированная версия 6.7.2.7, в которую включены упомянутые в этом разделе Security фиксы. Основную проблему представляют сервера клиентов, на которых стоит QP версии до 7.1 и на которых первичная защита отстутствует.

Рекомендации

Следует помнить, что первичная защита НЕ ГАРАНТИРУЕТ полную защиту от SQL-инъекции. Это просто была попытка создания быстрой защиты от наиболее часто используемых методов атаки

без переработки сайтов. Для защиты от SQL-инъекции нужно осуществлять валидацию входных параметров. Для Publishing Container справедливы следующие рекомендации

- для написания фильтров для Publishing Container нужно использовать безопасные конструкции “[content_item_id] = ” & NumValue(“id”), “[name] = ‘” & StrValue(“name”) & “’”.
- для динамических значений в полях Start From и Count рекомендуется использовать функцию NumValue
- выражения динамической сортировки и содержимое переменных для динамического изменения контента рекомендуется проверять на допустимые значения по принципу “белого списка”

При написании кода доступа к базе данных не через Publishing Container нужно быть осторожнее вдвойне, так как первичная защита отсутствует.

Уязвимости, найденные в текущей версии QP7

Vote.inc . На американских серверах необходимо проверить, что данный файл не скопирован в папку сайта, а используется централизованно из виртуальной папки Include. Файл vote.inc заменен на qa-qp2.quantumart.com и cluster.quantumart.ru, но необходимо заменить файл у американских клиентов (целевая группа – ASP-сайты, использующие функционал vote.inc для организации голосования (можно искать по базе в текстах форматов строчку “vote.inc”). По результатам исследования именно через функционал vote.inc был осуществлен последний по времени взлом клиентского сайта.

Хранимая процедура qp_fullTextSiteSearch. Фикс применен на qa-qp2.quantumart.com и cluster.quantumart.ru на уровне базы данных. Также фикс добавлен в fix_dbo.sql

Автоматизированное тестирование сайта на наличие SQL-иньекций

Полноценную проверку сайта на уязвимости могут дать только специализированные утилиты тестирования. Из того, что мы пробовали, нам больше всего понравилась коммерческая утилита XSpider. Стандартная лицензия на 1 год с ограничением в 4 тестируемых IP адреса, стоит около 500$. Есть пробная версия, но она основана на старом ядре и не выводит подробности о найденных уязвимостях. http://www.ptsecurity.ru/xs7.asp

Из бесплатных утилит тестирования неплохой вариант – Paros Proxy.
http://download.quantumart.com/injectionTest/paros.exe

Для работы требует Java Runtime Envirionment 6:
http://download.quantumart.com/injectionTest/JRE.exe

Список сканеров безопасности:

http://forum.antichat.ru/showpost.php?p=141796&postcount=2