УДК 004.056

**М. В. Карпиеня**

*Белорусский государственный университет*, *Минск*, *Беларусь*,
*karpiyenia.mv@gmail.com*

# ЗАЩИТА ВЕБ-ПРИЛОЖЕНИЙ ОТ SQL-ИНЪЕКЦИЙ

*Цель исследования – изучить, как обнаружить и предотвратить SQL-инъекции в веб-приложении. Объект исследования – SQL-инъекции. Предмет исследования – защита веб-приложений от SQL-инъекций. Результатом исследования является методология предотвращения SQL инъекций в веб-приложениях.*

***Ключевые слова:*** *SQL*, *SQL-инъекция*, *веб-приложение*, *нейронная сеть*, *запрос*, *веб-сервер*, *HTTP протокол*, *переменные сервера*

**M. Karpiyenia**

*Belarusian State University*, *Minsk*, *Belarus*, *karpiyenia.mv@gmail.com*

# PROTECTION WEB APPLICATIONS FROM SQL INJECTIONS

*The aim of the study is to determine how to detect and prevent SQL Injections in web-application. The object of the research is the SQL Injections. The subject of the research is the protecting web-applications from SQL Injections. The result of the study is a methodology for preventing SCL injection in web applications.*

***Keywords:*** *SQL*, *SQL Injection*, *web application*, *neural network*, *query*, *web server*, *HTTP protocol*, *server variables*

Веб-приложения – неотъемлемая часть нашей повседневной жизни. Они становятся все более сложными, поскольку разработчики постоянно добавляют новые функции для улучшения взаимодействия с пользователем. Однако по мере того, как веб-приложения становятся более сложными, количество ошибок программирования и дыр в системах их безопасности увеличивается, подвергая пользователей все большему риску.

Вместе с тем активизируются киберпреступники. Только за январь-июнь 2020 г. в Республике Беларусь было выявлено 4679 киберпреступлений. Поскольку более двух третьих преступлений данного вида были отнесены к хищениям путем использования компьютерной техники, то важность защиты и актуальность механизмов выявления подобных атак трудно переоценить. Зачастую объектами атак становятся веб-приложения.

Уязвимости внедрения, такие как SQL-инъекция и межсайтовый скриптинг, входят в число двух самых важных проблем безопасности веб-приложений в списке первой десятки OWASP (Open Web Application Security Project).

Веб-приложения работают следующим образом:

1) пользователь запрашивает веб-страницу обычно через веб-браузер;

2) запрос, который может включать вводимые пользователем данные, отправляется на целевой веб-сервер по протоколу HTTP;

3) входящие данные становятся входящими данными для прикладной программы, которая выполняется на стороне сервера;

4) программа генерирует новую веб-страницу, которая отправляется обратно пользователю через HTTP;

5) специальные входы, называемые файлами cookie, отслеживают текущее состояние между пользователем и веб-сервером;

6) многие веб-приложения взаимодействуют с базой данных на стороне сервера, чтобы хранить постоянные данные, относящиеся к приложению, такие как информация об учетной записи пользователя, информация о продукте;

7) программа взаимодействует с базой данных, создавая операторы SQL и выполняя их через систему управления базами данных [1, с. 372].

Уязвимость в любой системе определяется как ошибка, лазейка, слабое место или недостаток, существующие в системе, которые могут быть использованы неавторизованным пользователем для получения неограниченного доступа к сохраненным данным. Атака обычно означает незаконный доступ к приложению или системе, полученный с помощью хорошо продуманных механизмов. Атака с использованием SQL-инъекции (SQLIA) – это тип атаки, при которой злоумышленник (созданный пользователь) добавляет вредоносные ключевые слова или операторы в запрос SQL (например, операторы вредоносного кода SQL), а затем вводит их в поле ввода пользователя веб-приложения. Это позволяет злоумышленнику иметь незаконный и неограниченный доступ к данным, хранящимся в серверной базе данных.

SQL-инъекции вводятся в один или несколько условных операторов, поэтому они всегда оцениваются как истинные. При использовании этой техники у нас могут быть следующие типы и сценарии атак:

1. Внедрение строкового SQL-кода. Этот тип внедрения также называется атакой И / ИЛИ. Злоумышленник вводит токены или строки SQL в оператор условного запроса, который всегда оценивается как истинный. Проблема с этим типом атаки заключается в том, что вместо того, чтобы возвращать только одну строку в таблице, в случае успеха она приводит к возврату всех строк в таблице базы данных, на которые направлен запрос.

2. Числовая SQL-инъекция. Этот тип впрыска почти аналогичен рассмотренному выше. Основное отличие в том, что здесь числовые значения используются вместо строк. Следовательно, злоумышленник будет вводить числовые значения в условное выражение запроса, которое всегда будет возвращать истинное утверждение.

3. Атака через комментарии. Этот тип атаки использует преимущества встроенных комментариев, разрешенных SQL – вредоносного кода и комментирует все, что идет после «–» в предложении WHERE. Дело в том, что все, что находится после символов комментария, будет проигнорировано [2, с. 24].

Искусственные нейронные сети – это интеллектуальные модели, которые используют в своих структурах логический нейрон, пытаясь имитировать обработку информации человеческого мозга через систему нескольких взаимосвязанных искусственных нейронов, объединенных с помощью синаптических связей. В упрощенном виде искусственную нейронную сеть можно рассматривать как граф, в котором узлы являются нейронами, а связи функционируют синапсами. Искусственные нейронные сети различаются по своей архитектуре и способу корректировки весов, связанных с подключениями, в процессе обучения. Обучение – это способ, которым нейронная сеть захватывает информацию, предоставленную входными данными и через отношения, а синаптические веса принимают решения по центральной теме базы данных. Архитектура нейронной сети ограничивает тип проблемы, в которой может использоваться сеть, и определяется количеством слоев (один или несколько уровней), количеством узлов в каждом слое, типом соединения между узлами и по их способу действия.

Нечеткие нейронные сети используют структуру искусственной нейронной сети, где классические искусственные нейроны заменены нечеткими нейронами. Эти нейроны реализованы с использованием треугольных правил, которые обобщают операции объединения и пересечения классических множеств, что позволяет использовать их в теории нечетких множеств. Таким образом, нейронная сеть теперь рассматривается как лингвистическая система, сохраняющая способность к обучению.

Использование нечетких систем необходимо в тех случаях, когда классический логический подход становится невозможным для решения проблемы из-за характера ее сложности. Самые известные методы подвержены внезапным изменениям для решения проблем из-за упрощения реальной модели, но нечеткие системы имеют ресурсы (функции соответствия, правила и операторы агрегации), которые позволяют более точное приближение к реальной модели, избегая что решение, генерируемое нечеткой системой, значительно отличается от реальной модели.

Кибератаки имеют растущий мировой масштаб и характеризуются как одна из значительных проблем века. В текущий момент активно разрабатывают вычислительную систему, основанную на интеллектуальных гибридных моделях, которая с помощью нечетких правил позволяет создавать экспертные системы в атаках на кибернетические данные, уделяя особое внимание атаке SQL-инъекций.

Существует возможность построения системы, основанной на нечетких правилах, с точностью классификации кибернетических вторжений в пределах стандартного отклонения (по сравнению с современной моделью при решении данного типа задач). Подобная модель помогает странам подготовиться к защите своих сетей передачи данных и информационных систем, а также создать возможности для экспертных систем для автоматизации выявления атак в киберпространстве.

**Список использованных источников**

1. *Буза*, *М. К.* Архитектура компьютеров : учебник / М. К. Буза. – Минск : Выш. шк., 2015. – 414 с.

2. Криптографическая защита информации / В. Ф. Голиков [и др.] ; Белорус. нац. техн. ун-т. – Минск : БНТУ, 2012. – Ч. 2. – 90 с.