УДК 004.852

ПОДХОД К ВЫЯВЛЕНИЮ SQL-ИНЪЕКЦИЙ С ПРИМЕНЕНИЕМ ГЛУБОКОГО ОБУЧЕНИЯ

Кожич М.Д. [1], **Мишуков О.А.** [1]
Научный руководитель – кандидат технических наук, Мишуков О.А.[1]
1 – Военно-космическая академия имени А.Ф. Можайского
e-mail: vka@mil.ru

Введение. Современные технологии глубокого обучения открывают новые возможности для решения проблемы SQL-инъекций, позволяя создавать более точные и адаптивные системы обнаружения атак. Актуальность исследования обусловлена ростом числа онлайн-сервисов и, как следствие, увеличением угроз кибербезопасности, таких как SQL-инъекции. Использование графовых нейронных сетей (GNN) является перспективным подходом, демонстрирующим выдающиеся результаты в обработке графовых данных.

Основная часть. Предлагаемое решение направлено на повышение точности обнаружения SQL-инъекций за счет применения графовых нейронных сетей GNN.

Объектом исследования являются атаки SQL-инъекции, компрометирующие данные веб-приложений. Предметом исследования выступают методы обнаружения SQL-инъекций с использованием глубокого обучения.

Научная новизна заключается в расширении применения GNN для повышения уровня информационной безопасности, в частности, в области обнаружения SQL-инъекций.

Традиционные подходы, такие как регулярные выражения и поиск шаблонов, оказываются неэффективными для обнаружения SQL-инъекций из-за многообразия способов представления атак. В связи с этим, предлагается новый метод, основанный на анализе SQL-запросов как последовательностей токенов.

Предлагаемый подход включает следующие этапы:

1. Токенизация: SQL-запрос разбивается на последовательность токенов с сохранением порядка и структуры.
2. Построение графа: Создается граф, где каждый токен является узлом, а связи между токенами отражают их взаимодействие.
3. Вычисление признаков: Для каждого токена (узла графа) вычисляются характеристики, позволяющие идентифицировать потенциально вредоносные запросы.
4. Классификация с помощью GNN: Графовая нейронная сеть используется для классификации графа и определения, является ли запрос инъекцией.

Процесс нормализации преобразует запрос в упорядоченную последовательность токенов $(t_1, t_2, \ldots, t_N)$. Для этого генерируется граф $G = (V, E,$ w), в котором:

- каждая вершина V - уникальный токен:
- количество вершин графа $n = N$:
- ребро E представляет собой связь между двумя токенами, будем говорить, что ребро между токенами t_i и t_j существует (его вес отличен от нуля), если токены t_i и t_j появляются в определенном окне S:
- функция w определяет вес ребра. Вес ребра между токенами t_i и t_j обозначается

как w_{ij}.

Вышеуказанные преобразования позволяют перейти от работы со строковыми данными к количественным. После подготовки данных была реализована модель графовой сверточной сети. Для ее реализации было принято решение об использовании нового вида слоя SortPooling. Основная функция данного слоя заключается в сортировке в определенным порядке признаковых дескрипторов, каждый из которых представляет вершину, перед отправкой их в традиционные одномерные сверточные и полносвязные слои.

Полученные результаты исследования показали, что модель, принимающая на вход информацию о положении токенов в запросе, достигла усредненной точности классификации 0,97, а безопасный трафик распознается в 99.9% случаев.

Выводы: Использование графовых сверточных сетей для обработки токенизированных SQL-запросов, представленных в виде графа, является эффективным и применимым подходом для обнаружения SQL-инъекций. Предлагаемый подход может быть применим в реальных системах защиты web-приложений от SQL-инъекций.

Литература:

1. Безопасность лаборатории Касперского (Лаборатория Касперского) : [сайт]. – URL: https://www.kaspersky.com/blog/sql-injection-prevention-methods/15253/.
2. OWASP (Открытый проект безопасности веб-приложений) | Статья: "Preventing SQL Injection" : [сайт]. – URL: https://owasp.org/www-community/attacks/SQL_Injection.
3. MITRE ATT & CK Framework | Статья: «T1055: Проверка ввода» : [сайт]. – URL: https://attack.mitre.org/techniques/T1055/.
4. Институт SANS |Статья: "Шпаргалка по предотвращению SQL-инъекций" : [сайт]. – URL: https://www.sans.org/security-resources/sec530/8.2/sqli-cheat-sheet.pdf.
5. Документы Microsoft | Статья: «Предотвращение внедрения SQL-кода в ASP.NET Core» : [сайт]. – URL: https://docs.microsoft.com/en-us/aspnet/core/web-api/handle-rejections?view=aspnetcore-6.0#sql-injection-prevention.