Виявлення аномалій в SQL запитах

Владислав Степанов[1], Віталій Мартовицький[2]

1. Кафедра безпеки інформаційних технологій,
Харківський національний університет радіоелектроніки,
УКРАЇНА, г. Харків, пр. Науки, 14,
E-mail: vladyslav.stepanov@nure.ua

2. Кафедра електронних обчислювальних машин,
Харківський національний університет радіоелектроніки,
УКРАЇНА, г. Харків, пр. Науки, 14,
E-mail: vitalii.martovytskyi@nure.ua

***Коротка анотація** – The paper deals with the possibility of using machine learning for tasks of classification of attacks not web system. A method for detecting anomalies in the form of SQL injection with the use of an autoencoder with Seq2Seq architecture has been developed, and the testing of the operation of the given transactions is performed.*

Ключові слова – SQL-ін'єкція, WEB-ресурси, SQL, машинне навчання, автоенкодер.

I. Вступ

Сучасне підприємство має розвинену мережеву інфраструктуру, в якій працюють корпоративні інформаційні системи, що забезпечують підтримку всіх бізнес-процесів організації. Головним джерелом бізнес-інформації в таких мережевих інфраструктурах є сховища та бази даних, в яких зберігається внутрішня оперативна та фінансова інформація, персональні дані співробітників, інформація про замовників та клієнтів, інтелектуальна власність, дослідження ринку та аналіз діяльності конкурентів, платіжна інформація.

За деякими даними, в промислово розвинених країнах середній збиток від одного злочину в сфері комп`ютерної інформації становить приблизно 450 тис. дол., а щорічні сумарні втрати в США і Західній Європі, за даними, що наводять В. Гайкович та А. Прешин, досягають 100 млрд. і 35 млрд. дол. В останні десятиріччя зберігалася стійка тенденція до зростання збитків, пов'язаних із злочинністю в сфері комп'ютерної інформації. В пресі та літературі наведено багато подібних прикладів [1].

Сьогодні більшість фірм виробників систем управління сховищами та базами даних намагаються удосконалити засоби захисту, але їхні зусилля, як правило, скеровані тільки на усунення відомих вразливостей власних продуктів.

Основними напрямками розвитку технологій систем управління базами даних (СКБД) є реляційні та нереляційні СКБД.

Враховуючи все вищезазначене, актуальною задачею є комплексне дослідження і систематизація питань захисту сховищ та баз даних з урахуванням загальних тенденцій розвитку підходів до забезпечення інформаційної безпеки та усунення загроз з використанням технології інтелектуального аналізу даних.

Це обумовлено, наприклад, легкістю виявлення і експлуатування уразливостей баз даних і, як наслідок, їх використання зловмисниками, що івдображено в статтях [2-4]. Тому, побудова моделей і методів для виявлення SQL-ін'єкцій у веб-ресурсах є актуальним завданням.

II. ОСНОВНИЙ МАТЕРІАЛ

Проблема виявлення веб-атак розглядається з точки зору виявлення аномалій. На етапі навчання моделі видаються тільки нормальні HTTP-запити. На етапі тестування модель визначає, чи отриманий запит аномальним чи ні.

Для виявлення аномалій в HTTP-запиті використовується архітектура Seq2Seq. Модель Seq2Seq [5] складається з двох багатошарових LSTM - кодера і декодера. Кодер відображає вхідну послідовність в вектор фіксованої довжини. Декодер декодує цільової вектор, використовуючи вихід кодера. При навчанні автоенкодер є модель, в якій цільові значення встановлюються такими ж, як вхідні значення.

Ідея полягає в тому, щоб навчити мережу декодувати речі, які вона бачила, або, іншими словами, наближати тотожне відображення. Якщо навченому автоенкодеру дають аномальний зразок, він, ймовірно, відтворює його з високим ступенем помилки, просто тому, що ніколи його не бачив. Структура автоенкодеру представлена на рисунку 1.

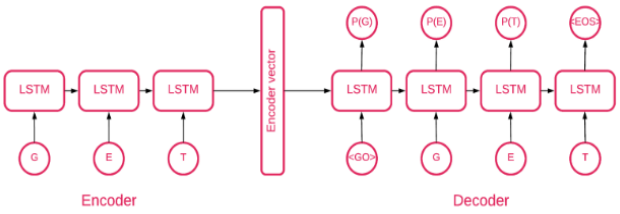

Рисунок 1 – Архітектура Seq2Seq

У відповідності до рисунку дані вводу кодера представлені буквами G, E, T, а дані вводу декодера – GO, P(G), P(E), P(T), <EOS>.

Представлене рішення складається з декількох частин: ініціалізація моделі, навчання, прогнозування та перевірка.

Модель створюється як екземпляр класу Seq2Seq, який має такі аргументи конструктора:

– batch_size - число вибірок в пакеті

– embed_size - розмір простору вбудовування (повинен бути меншим за розмір словника)

– hidden_size - кількість прихованих станів у lstm

– num_layers - кількість блоків lstm

– контрольні точки - шлях до каталогу контрольно-пропускних пунктів

– std_factor - кількість stds, яка використовується для визначення порогу моделі випадання - ймовірність збереження кожного елемента

– vocab - об'єкт лексики

Далі ініціалізуються шари автоенкодера. Спочатку кодер потім декодер

Так як проблема, яку вирішуємо, полягає у виявленні аномалій, цільові значення і вхідні дані збігаються. Далі на основі навчальної вибірки відбувалося навчання нашого автоенкодеру. Навчальна вибірка містить дані з 21991 нормальними і 1097 аномальними HTTP-запитами з банківських додатків, яку було отримано з ресурсу Kagel.

Після кожної епохи найкраща модель зберігається в якості контрольної точки, яку потім можна завантажити. З метою тестування було створено веб-додаток, який було захищено розробленою моделлю, щоб перевірити, чи будуть реальні атаки успішними. На етапі тестування на нашій відкладеної вибірці ми отримали дуже хороші результати: precision і recall близькі до 0,99. та ROC-крива наближається до 1, що показано на рис. 2

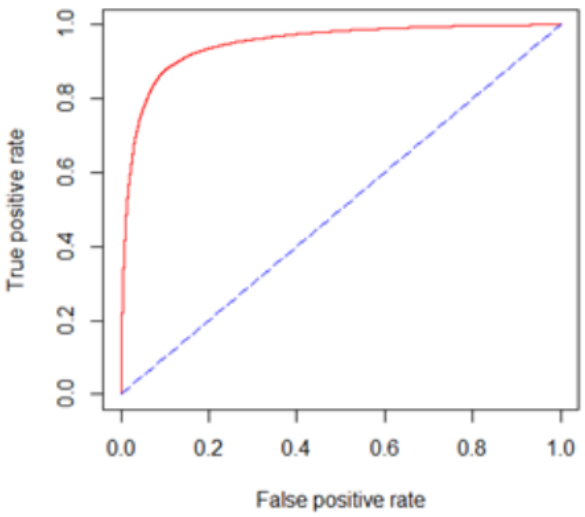

Рисунок 2 – Графік ROC-кривої

Висновки

У роботі розглядається можливість застосування машинного навчання для задач класифікації атак не веб системи.

Розроблено метод виявлення аномалій у вигляді SQL-ін'єкції з використанням автоенкодеру з архітектурою Seq2Seq та протестовоно його роботу на даних транзакцій банківської програми.

Запропонована система оцінки з набором даних, що мають різні запити. Отриманий результат показує, що запропонована система здатна виявити шкідливий запит і, отже, класифікувати користувачів. Надалі цей тип системи також може використовуватися для класифікації атак ботнетів та різних систем безпеки шляхом порівняння відмінностей між запитами, поданими звичайним користувачем та роботами, а також для різних типів атак, таких як міжсайтовий сценарій атаки, атаки з низькою швидкістю у DDOS.

Література

[8] Gupta S., Gupta B. B. Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art //International Journal of System Assurance Engineering and Management. – 2017. – Т. 8. – №. 1. – С. 512-530.

[9] MOH, Melody, et al. Detecting web attacks using multi-stage log analysis. In: *2016 IEEE 6th International Conference on Advanced Computing (IACC)*. IEEE, 2016. p. 733-738.

[10] Aliero, Muhammad Saidu, et al. "Classification of Sql Injection Detection And Prevention Measure." *IOSR Journal of Engineering* 6.02 (2016). – С. 75-93

[11] Shah, Nisharg. "Securing Database Users from the Threat of SQL Injection Attacks." (2017).

[12] Sriram A. et al. Cold fusion: Training seq2seq models together with language models //arXiv preprint arXiv:1708.06426. – 2017.