УДК 004.56

А. В. Притула
Л. М. Куперштейн

ВИЯВЛЕННЯ XSS-АТАК ЗА ДОПОМОГОЮ ЗГОРТКОВОЇ НЕЙРОННОЇ МЕРЕЖІ

Вінницький національний технічний університет

Анотація
Проаналізовано загрози від XSS-атак, розроблено модель на основі згорткової нейронної мережі для виявлення XSS-атак.
Ключові слова: xss, owasp, атака, нейронна мережа.
Abstract
Threats from XSS-attacks are analyzed, a model based on a convolutional neural network for detecting XSS-attacks is developed.
Keywords: xss, owasp, attack, neural network.

Вступ

Нейронні мережі дозволяють виконувати пошук складних закономірностей в масивах даних набагато швидше, ніж людина, що робить даний підхід привабливим для використання обробки даних.

Нейронні мережі можуть бути використанні для задач розпізнавання атак у вхідному тексті HTTP запитів, зокрема атак типу Cross Site Scripting (XSS).

За статисткою OWASP Top 10 2021 [1] XSS-атаки піднялись з сьомого на третє місце серед загроз для веб-додатків, тому розробка засобу виявлення такого типу атак є актуальною задачею.

Метою роботи є розробка та навчання нейронної мережі для виявлення XSS-атак.

Результати дослідження

На сьогоднішній день існують дуже багато різних засобів, які допомагають захистити або попередити атаки на інформаційні ресурси. Зазвичай такі рішення коштують дорого і не всі компанії можуть дозволити собі їх встановлення. Тим більше, що для обслуговування потрібен спеціально навчений персонал.

XSS-атаки постійно виявляються та існують навіть вільно доступні автоматизовані інструменти для їх використання. Успішна атака може призвести до серйозних порушень безпеки для веб-серверу та користувача, який отримує до нього доступ. Більш сучасні експлойти можуть вводити довільний код у поля введення користувача та маніпулювати сторінкою, контролювати обліковий запис користувача і навіть викликати відмову в обслуговуванні [2].

XSS зазвичай поділяють на три окремі категорії: відображені, збережені та на основі DOM [1]. Перший включає в себе браузер жертви, який виконує неперевірені та неекрановані введення. Другий трапляється, коли шкідливий код зберігається атакованою програмою, який потім виконується під час використання користувачами сайту. Третій відбувається, коли програма динамічно включає дані, контрольовані зловмисником. Враховуючи поширеність і потенційні ризики, пов’язані з атаками XSS, розробка методів і стратегій для їх зупинення – варта часу і зусиль.

Для виявлення атак такого типу було вирішено розробити і навчити згорткову нейронну мережу (CNN).

CNN – це клас глибинних штучних нейронних мереж прямого поширення, який зазвичай застосовується до аналізу зображень [3]. CNN використовують різновид багатошарових персептронів, розроблений так, щоб вимагати використання мінімальної обробки. Згорткові мережі використовують порівняно мало попередньої обробки, в порівнянні з іншими алгоритмами класифікації. Це означає, що мережа навчається за допомогою фільтрів, що в традиційних алгоритмах приходиться розробляти вручну. Ця незалежність у конструюванні ознак від апріорних знань та людських зусиль є великою перевагою.

Для навчання мережі було використано набір даних з сайту kaggle.com на 13686 записів, при чому він є достатньо збалансованим, оскільки відношення стрічок з атаками і без приблизно 0.54 до 0.46 [4].

Для навчання моделі вхідні дані у вигляді речень перетворювались в ASCII-коди і з них формувалась матриця розміром 100 на 100, на рис. 1 представлено візуальне зображення однієї з матриць.

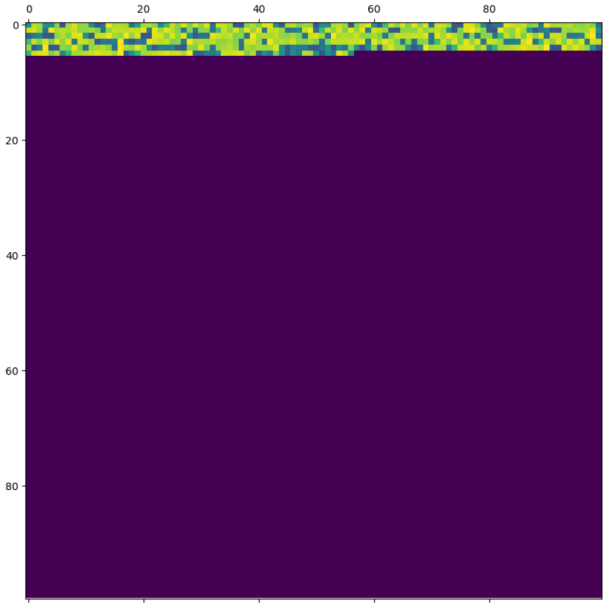

Рисунок 1 – Візуальне представлення обробленої стрічки з набору даних.

Після попередньої обробки даних було натреновано модель, а також проведено її валідацію. Результат наведено на рис. 2.

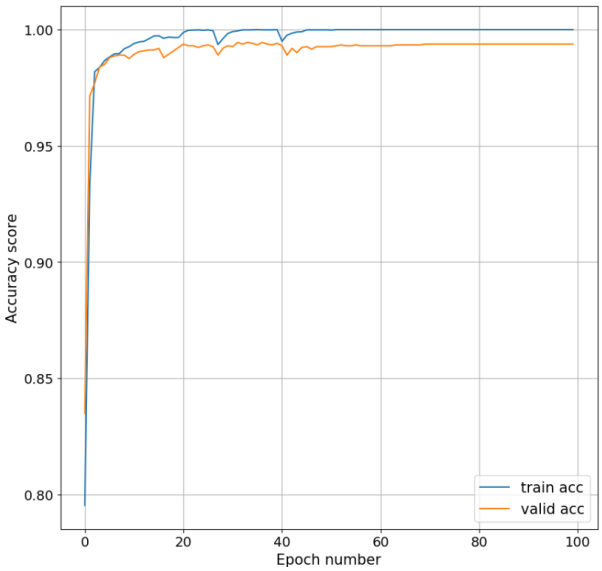

Рисунок 2 – Точність роботи навченої моделі.

Також після навчання моделі було розраховано загальну точність, яка дорівнює 0.98, позитивну точність 0.98, покриття 0.97.

Висновки

В ході проведених досліджень проаналізовано особливості класифікації XSS-атак на основі згорткових нейронних мереж. На основі отриманих результатів дослідження, а саме високої точності виявлення, можна стверджувати, що згорткові нейронні мережі доцільно використовувати як інструмент для підтримки прийняття рішень при класифікації XSS-атак.

СПИСОК ВИКОРИСТАННОЇ ЛІТЕРАТУРИ

1. OWASP Top 10. URL: https://owasp.org/www-project-top-ten/ (дата звернення: 29.05.2022).
2. Hydara, I., Sultan, A. B. M., Zulzalil, H., & Admodisastro, N. (2015). Current state of research on cross-site scripting (XSS)–A systematic literature review. Information and Software Technology, 58, 170-186.
3. Невмержицький Р. В. Згорткові нейронні мережі. Комп'ютерні технології: інновації, проблеми, рішення : Наук. конф., м. Жиитомир, 19–20 жовт. 2018 р. Житомир, 2018. С. 45–46.
4. Cross site scripting XSS dataset for Deep learning. Kaggle. URL: https://www.kaggle.com/datasets/syedsaqlainhussain/cross-site-scripting-xss-dataset-for-deep-learning (дата звернення: 29.05.2022).

Притула Андрій Вікторович – студент групи 1БС-21м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: andrik.pritula@gmail.com.

Куперштейн Леонід Михайлович – к.т.н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця email: kupershtein.lm@gmail.com

Prytula Andrii V. **–** Student of Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, e-mail: andrik.pritula@gmail.com.

Kupershtein Leonid M. — PhD, Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Vinnytsia, email: kupershtein.lm@gmail.com