UDC 004.056.57

Advancing XSS Detection in Web Environments via MLP Modeling

Hajjouz A. (ИТМО University)
Scientific director – associate professor, Avksenteva E.Y. (ИТМО University)

Introduction. Web applications are frequently targeted by cross-site scripting (XSS) attacks, a form of security breach where malicious scripts are injected to manipulate user interactions [1]. Identifying and mitigating these attacks are paramount in safeguarding information security. This study advances XSS detection through a Multi-Layer Perceptron (MLP) model, which has been trained and tested using a pre-segregated comprehensive dataset specifically designed to discern benign from malicious JavaScript. The research stands out for its high accuracy levels and a methodical approach to feature selection, crucial for enhancing model performance.

Main part. The original dataset was divided into two sets: a training set, consisting of 13,972 benign and 5,150 malicious scripts, and a test set, comprising 14,096 benign and 10,000 malicious scripts [2]. To address the class imbalance within the training data, the Synthetic Minority Over-sampling Technique for Nominal and Continuous (SMOTENC) was applied, ensuring an equal representation of both benign and malicious scripts.

Feature selection was a critical step in the research methodology, where 46 out of 66 available features were meticulously chosen based on their relevance to XSS characteristics, optimizing the model's ability to make informed classifications. Preprocessing efforts included normalizing the dataset by replacing infinite and negative values with respective column means, ensuring data integrity for the model training.

The MLP model architecture was strategically constructed with an input layer sized to the number of selected features, followed by hidden layers activated by rectified linear units, and culminating in a sigmoid output for binary classification. An early stopping callback was utilized during training to monitor validation loss and mitigate overfitting.

Conclusions. The MLP model demonstrated exemplary performance, with accuracy metrics exceeding 99.82%, and precision, recall, and F1-scores that affirm the model's robust predictive capabilities. The study underscores the efficacy of balancing training data, prudent feature selection, and the significance of a separate evaluation set to gauge the model's performance during training. The approach ensures that the model not only learns effectively but also generalizes well to new, unseen data. Future work will focus on validating the model against a broader dataset, reinforcing the current findings and the model's practicality in real-world applications.

List of sources used:

1. Dora, J. R., & Nemoga, K. (2021). Ontology for Cross-Site-Scripting (XSS) attack in cybersecurity. Journal of Cybersecurity and Privacy, 1(2), 319-339.
2. Mereani, F. A., & Howe, J. M. (2018, January). Detecting cross-site scripting attacks using machine learning. In International conference on advanced machine learning technologies and applications (pp. 200-210). Cham: Springer International Publishing.