



ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH  
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

---

# BÁO CÁO CUỐI KỲ

TẠO BỘ DỮ LIỆU THỬ NGHIỆM CHO BÀI TOÁN  
PHÁT HIỆN TẤN CÔNG XSS BẰNG HỌC SÂU

---

## Nhóm 6:

Nguyễn Trần Bảo Anh      MSSV: 22520066

Nguyễn Thị Trâm Đan      MSSV: 22520185

Dương Anh Vũ      MSSV: 22521688



# Nội dung

---

I. Giới thiệu tổng quan

II. Tạo bộ dữ liệu

III. Huấn luyện mô hình

IV. Đánh giá mô hình



# I. Giới thiệu tổng quan

XSS là một dạng kỹ thuật tấn công vào code injection của máy khách. Nó phép hacker chèn các đoạn mã độc thông qua các đoạn script để thực thi chúng ở phía client và ăn cắp dữ liệu nhận dạng của người dùng, như cookies, session tokens và các thông tin khách.

```
zixem.altervista.org/XSS/1.php?name=zxm<script>alert(document.cookie)</script>
```

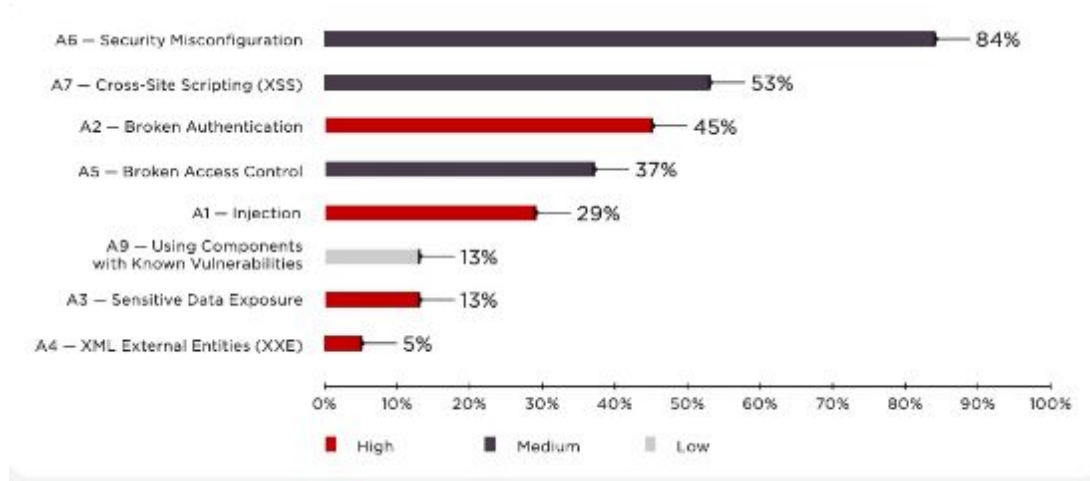
www.zixem.altervista.org says

```
_ga=GA1.1.898391153.1729217722;  
_ga_8SDBJE29YH=GS1.1.1731056996.3.1.1731057403.0.0.0
```

OK



# I. Giới thiệu tổng quan



Tỷ lệ các lỗ hổng bảo mật ứng dụng web (2019)



## II. Tạo bộ dữ liệu

- Sử dụng các bộ dữ liệu có sẵn
- Tạo dữ liệu từ các ứng dụng và trang web thực tế
- Sử dụng các công cụ tự động để tạo dữ liệu
- Tạo dữ liệu thông qua việc sinh ngẫu nhiên



[SQLi challenges](#)

[XSS challenges](#) (new)

[Other challenges](#)

[ZiXeM](#)





# II. Tạo bộ dữ liệu

≡ kaggle

+ Create

Host a Competition

KaggleX Mentorship

Support/Contact

Community Guidelines

Team

Terms

Privacy

📁 Your Work

Search



SYED SAQLAIN HUSSAIN SHAH · UPDATED 5 YEARS AGO

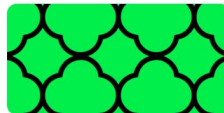
26

New Notebook

Download



## Cross site scripting XSS dataset for Deep learning



Data Card

Code (13)

Discussion (0)

Suggestions (0)

### About Dataset

Usability

4.71

Files

master

Go to file

sqli

traversal

xss

0xsobky.txt

787373.txt

payloads / other / xss / 787373.txt

foospidy moar payloads!

Code

Blame

233 lines (233 loc) · 25 KB

Code 55% faster with GitHub Copilot

```
1 <IMG SRC=javascript:alert(String.fromCharCode(88,83,83))>
2 "><script>alert(0)</script>
3 <script src=http://yoursite.com/your_files.js></script>
4 </title><script>alert(/xss/)</script>
5 </textarea><script>alert(/xss/)</script>
6 <IMG LOWSRC="javascript:alert('XSS')">
```



## II. Tạo bộ dữ liệu

```
import pandas as pd

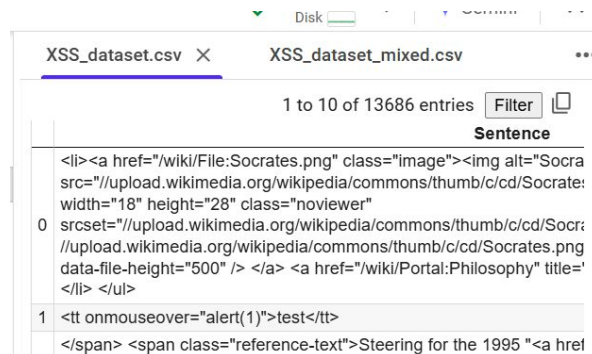
# Đọc dữ liệu từ hai file CSV
df1 = pd.read_csv('XSS_dataset.csv')
df2 = pd.read_csv('new-xss-data.csv')

# Gộp hai DataFrame lại với nhau
combined_df = pd.concat([df1, df2])

# Loại bỏ các dòng trùng lặp
combined_df = combined_df.drop_duplicates()

# Ghi dữ liệu kết quả vào một file CSV mới
combined_df.to_csv('XSS_dataset_mixed.csv', index=False)

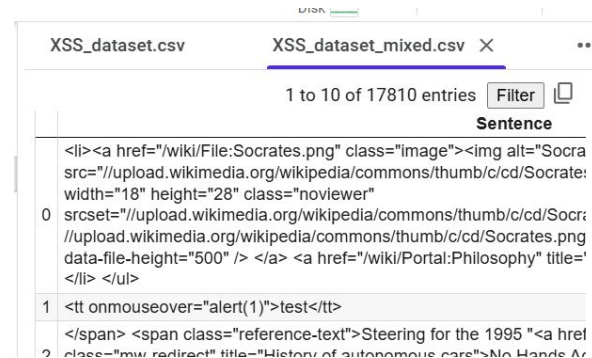
print("Đã gộp file thành công và loại bỏ dòng trùng lặp.")
```



XSS\_dataset.csv X XSS\_dataset\_mixed.csv

1 to 10 of 13686 entries

	Sentence
	<li><a href="/wiki/File:Socrates.png" class="image"> </a> <a href="/wiki/Portal:Philosophy" title=' </li> </ul>
1	<tt onmouseover="alert(1)">test</tt>
	</span> <span class="reference-text">Steering for the 1995 "<a href



XSS\_dataset.csv XSS\_dataset\_mixed.csv X

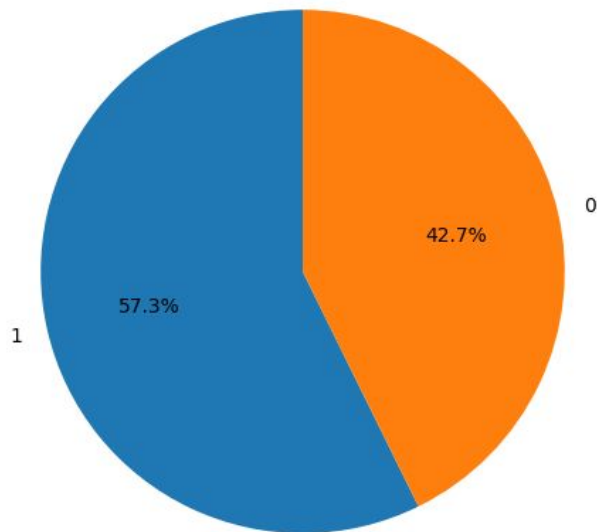
1 to 10 of 17810 entries

	Sentence
	<li><a href="/wiki/File:Socrates.png" class="image"> </a> <a href="/wiki/Portal:Philosophy" title=' </li> </ul>
1	<tt onmouseover="alert(1)">test</tt>
	</span> <span class="reference-text">Steering for the 1995 "<a href
2	class="mw redirect" title="History of autonomous cars">No Hands Ar

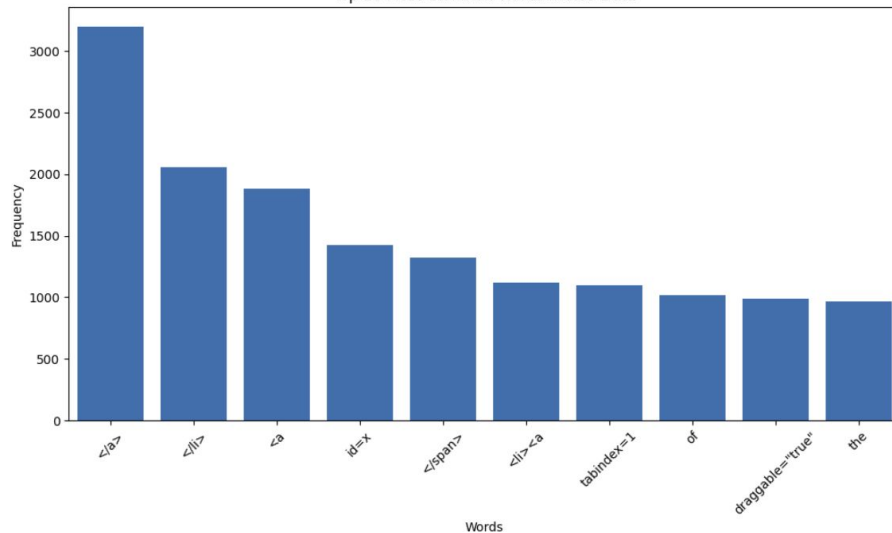


## II. Tạo bộ dữ liệu

Distribution of Labels



Top 10 Most Common Words in XSS Data







# III. Huấn luyện mô hình

Create

Community Guidelines

Team

Terms

Privacy

Your Work

VIEWED

Cross site scripting ...

XSS detection CNN

Cross site scripting ...

Cross site scripting ...

Search

HAI ĐĂNG PHAN · 9MO AGO · 1,028 VIEWS

XSS detection CNN

Copied from Syed Saqlain Hussain Shah (+41,-133)

Notebook Input Output Logs Comments (0)

Retrain\_XSS\_detection\_CNN.ipynb

File Edit View Insert Runtime Tools Help All changes saved

Files

sample\_data

XSS\_dataset\_mixed.csv

weights.weights.h5

Import Libraries

In [51]:

```
import numpy as np
import pandas as pd
import glob
```

+ Code + Text

1 from google.colab import files

2 uploaded = files.upload()

Choose Files XSS\_dataset\_mixed.csv

XSS\_dataset\_mixed.csv(text/csv) - 2036228 bytes, last modified: 12/6/2024 - 100% done

Saving XSS\_dataset\_mixed.csv to XSS\_dataset\_mixed.csv

Import Libraries

1

2 import numpy as np

3 import pandas as pd

4 import glob

5 import time

6 import pandas as pd

7 # from xml.dom import minidom

8

9

10 import os

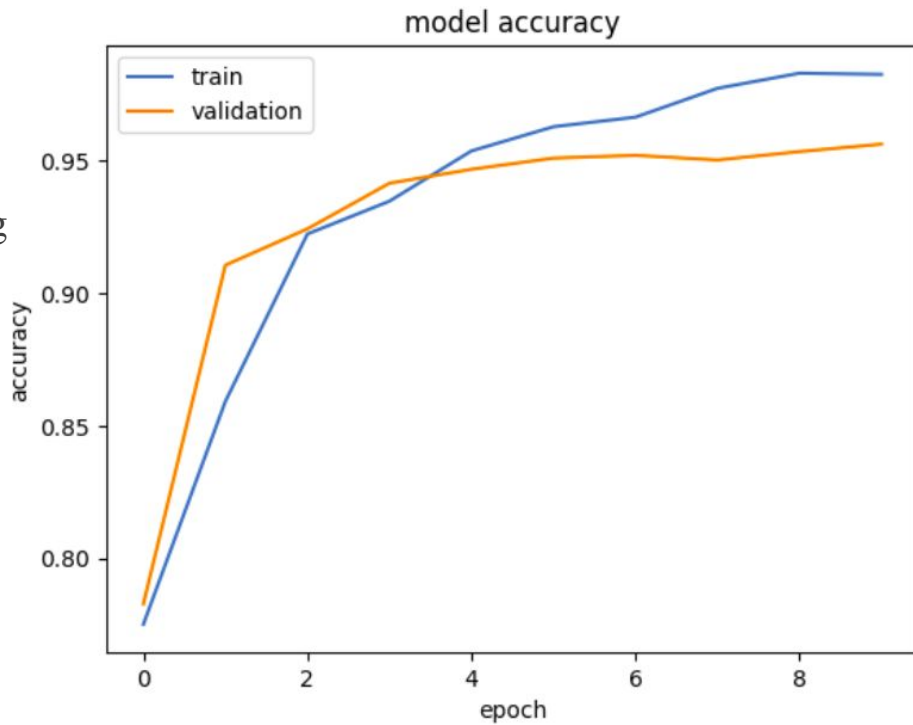
11 import matplotlib.pyplot as plt



## IV. Đánh giá mô hình

### Phân tích biểu đồ hiển thị quá trình huấn luyện:

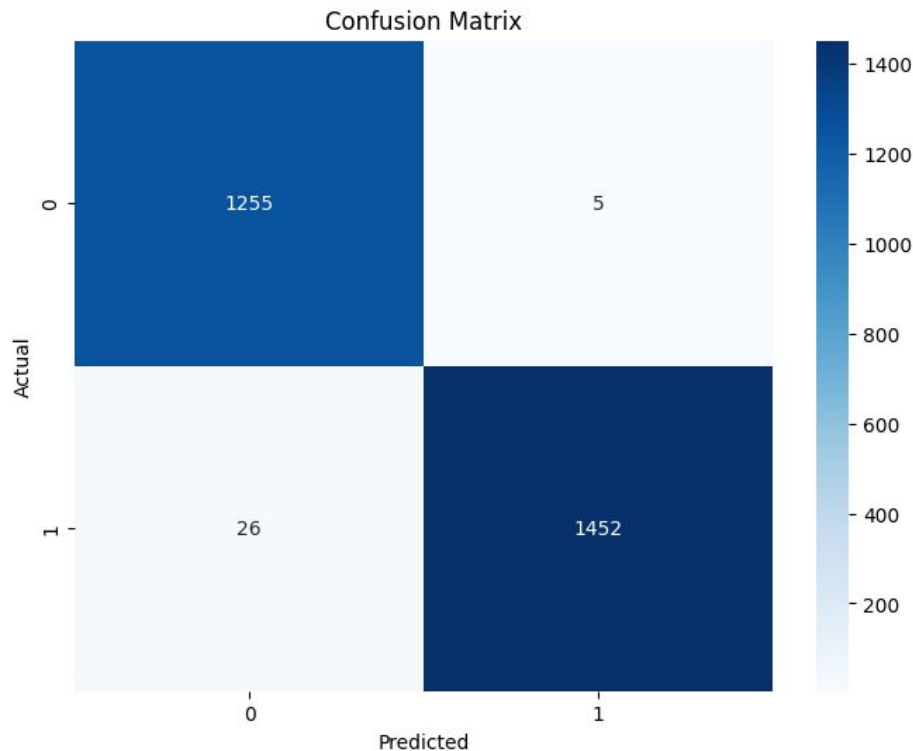
- Đường màu xanh (train): Đường này thể hiện độ chính xác trên tập huấn luyện. Chúng ta có thể thấy rằng độ chính xác trên tập huấn luyện tăng đều qua các epoch, cho thấy mô hình đang học tốt từ dữ liệu huấn luyện.
- Đường màu cam (validation): Đường này thể hiện độ chính xác trên tập xác thực. Độ chính xác của tập xác thực tăng nhanh đến một thời điểm nào đó rồi bắt đầu giảm nhẹ sau một số epoch. Điều này có thể chỉ ra hiện tượng overfitting, khi mô hình học quá mức từ dữ liệu huấn luyện và không thể tổng quát hóa tốt trên dữ liệu chưa thấy.





## IV. Đánh giá mô hình

- **True Positive (TP):** 1255 mẫu được dự đoán là lớp 0 và đúng là lớp 0.
- **True Negative (TN):** 1452 mẫu được dự đoán là lớp 1 và đúng là lớp 1.
- **False Positive (FP):** 5 mẫu được dự đoán là lớp 0 nhưng thực tế là lớp 1.
- **False Negative (FN):** 26 mẫu được dự đoán là lớp 1 nhưng thực tế là lớp 0.





## IV. Đánh giá mô hình

- **TPR (Recall):** 0.9824 (98.24%) — Tỷ lệ mẫu thực tế là lớp 1 mà được dự đoán đúng.
- **FPR (False Positive Rate):** 0.0040 (0.40%) — Tỷ lệ mẫu thực tế là lớp 0 nhưng được dự đoán là lớp 1 rất thấp, cho thấy mô hình không bị nhiễu loạn loại I.
- **FNR (False Negative Rate):** 0.0176 (1.76%) — Tỷ lệ mẫu thực tế là lớp 1 nhưng được dự đoán là lớp 0 cũng thấp, cho thấy mô hình không bỏ sót nhiều mẫu lớp 1.

	precision	recall	f1-score	support
0	0.9797	0.9960	0.9878	1260
1	0.9966	0.9824	0.9894	1478
accuracy			0.9887	2738
macro avg	0.9881	0.9892	0.9886	2738
weighted avg	0.9888	0.9887	0.9887	2738

[[1255	5]	
[	26 1452]]	
TPR	FPR	FNR
0.9824	0.0040	0.0176



## IV. Đánh giá mô hình

- **Accuracy (độ chính xác): 0.9887 (98.87%)**

— Mô hình có độ chính xác rất cao, cho thấy nó phân loại đúng đến 98.87% số mẫu trên tổng số mẫu kiểm tra.

	precision	recall	f1-score	support
0	0.9797	0.9960	0.9878	1260
1	0.9966	0.9824	0.9894	1478
accuracy			0.9887	2738
macro avg	0.9881	0.9892	0.9886	2738
weighted avg	0.9888	0.9887	0.9887	2738

- **F1-Score (hiệu suất mô hình):** Mô hình gần như dự đoán chính xác gần tất cả các trường hợp trong tập kiểm tra (test set).

[[1255 5]		
[ 26 1452]]		
TPR	FPR	FNR
0.9824	0.0040	0.0176



## IV. Đánh giá mô hình

---

### **Đánh giá tổng quát**

Mô hình hoạt động rất tốt với độ chính xác và các chỉ số khác đều ở mức cao. Tỷ lệ lỗi rất thấp, đặc biệt là tỉ lệ sai loại I (FPR) và tỉ lệ sai loại II (FNR). Mô hình có khả năng phân loại chính xác cả hai lớp mà không bị thiên lệch nghiêng về lớp nào. Đây là một mô hình rất hiệu quả cho bài toán phân loại tấn công XSS.

**THANKS FOR LISTENING**