

```
from google.colab import drive
drive.mount('/content/drive')
import os
os.chdir('/content/drive/My Drive/SSSRP')
print(os.getcwd())

Mounted at /content/drive
/content/drive/My Drive/SSSRP

!ls

data makemodel2.py model myutils.py __pycache__ trymodel2.py w2v

!python makemodel2.py remote_code_execution

2024-11-25 13:36:03.638728: I tensorflow/core/util/port.cc:153] oneDNN custom operations are on. You may see slightly different numerical res
2024-11-25 13:36:03.655506: E external/local_xla/xla/stream_executor/cuda/cuda_fft.cc:485] Unable to register cuFFT factory: Attempting to re
2024-11-25 13:36:03.674811: E external/local_xla/xla/stream_executor/cuda/cuda_dnn.cc:8454] Unable to register cuDNN factory: Attempting to r
2024-11-25 13:36:03.680725: E external/local_xla/xla/stream_executor/cuda/cuda_blas.cc:1452] Unable to register cuBLAS factory: Attempting to
2024-11-25 13:36:03.695042: I tensorflow/core/platform/cpu_feature_guard.cc:210] This TensorFlow binary is optimized to use available CPU ins
To enable the following instructions: AVX2 AVX512F AVX512_VNNI FMA, in other operations, rebuild TensorFlow with the appropriate compiler fla
2024-11-25 13:36:04.921853: W tensorflow/compiler/tf2tensorrt/utils/py_utils.cc:38] TF-TRT Warning: Could not find TensorRT
2024-11-25 13:36:08.837 : INFO : loading Word2Vec object from w2v/word2vec_withString10-100-200.model
2024-11-25 13:36:09.773 : INFO : loading wv recursively from w2v/word2vec_withString10-100-200.model.wv.* with mmap=None
2024-11-25 13:36:09.773 : INFO : loading vectors from w2v/word2vec_withString10-100-200.model.wv.vectors.npy with mmap=None
2024-11-25 13:36:16.473 : INFO : loading synlneg from w2v/word2vec_withString10-100-200.model.synlneg.npy with mmap=None
2024-11-25 13:36:24.938 : INFO : setting ignored attribute cum_table to None
2024-11-25 13:36:25.962 : INFO : Word2Vec lifecycle event {'fname': 'w2v/word2vec_withString10-100-200.model', 'datetime': '2024-11-25T13:36:
finished loading. 13:36
cutoff 67255
cutoff2 81666
Creating training dataset... (remote_code_execution)
Creating validation dataset...
Creating finaltest dataset...
Train length: 67255
Test length: 14411
Finaltesting length: 14412
time: 13:39
X_train shape: (67255, 200, 200), dtype: float32
y_train shape: (67255,), dtype: int64
X_test shape: (14411, 200, 200), dtype: float32
y_test shape: (14411,), dtype: int64
X_finaltest shape: (14412, 200, 200), dtype: float32
y_finaltest shape: (14412,), dtype: int64
numpy array done. 13:40
67255 samples in the training set.
14411 samples in the validation set.
14412 samples in the final test set.
percentage of vulnerable samples: 8.99%
absolute amount of vulnerable samples in test set: 1254
Starting CNNResNet: 13:40
Dropout: 0.2
Neurons: 100
Optimizer: adam
Epochs: 20
Batch Size: 128
max length: 200
2024-11-25 13:40:07.717857: W tensorflow/core/common_runtime/gpu/gpu_bfc_allocator.cc:47] Overriding orig_value setting because the TF_FORCE
2024-11-25 13:40:07.720878: I tensorflow/core/common_runtime/gpu/gpu_device.cc:2021] Created device /job:localhost/replica:0/task:0/device:GF
Model: "functional"
```

Layer (type)	Output Shape	Param #	Connected to
input_layer (InputLayer)	(None, 200, 200)	0	-
conv1d (Conv1D)	(None, 200, 64)	38,464	input_layer[0][0]
batch_normalization (BatchNormalization)	(None, 200, 64)	256	conv1d[0][0]
re_lu (ReLU)	(None, 200, 64)	0	batch_normalization[0...

```
!python makemodel2.py xss

2024-11-25 13:46:39.822243: I tensorflow/core/util/port.cc:153] oneDNN custom operations are on. You may see slightly different numerical res
2024-11-25 13:46:39.839140: E external/local_xla/xla/stream_executor/cuda/cuda_fft.cc:485] Unable to register cuFFT factory: Attempting to re
2024-11-25 13:46:39.858757: E external/local_xla/xla/stream_executor/cuda/cuda_dnn.cc:8454] Unable to register cuDNN factory: Attempting to r
2024-11-25 13:46:39.864604: E external/local_xla/xla/stream_executor/cuda/cuda_blas.cc:1452] Unable to register cuBLAS factory: Attempting to
2024-11-25 13:46:39.879067: I tensorflow/core/platform/cpu_feature_guard.cc:210] This TensorFlow binary is optimized to use available CPU ins
To enable the following instructions: AVX2 AVX512F AVX512_VNNI FMA, in other operations, rebuild TensorFlow with the appropriate compiler fla
2024-11-25 13:46:41.093696: W tensorflow/compiler/tf2tensorrt/utils/py_utils.cc:38] TF-TRT Warning: Could not find TensorRT
2024-11-25 13:46:42.972 : INFO : loading Word2Vec object from w2v/word2vec_withString10-100-200.model
2024-11-25 13:46:43.020 : INFO : loading wv recursively from w2v/word2vec_withString10-100-200.model.wv.* with mmap=None
```

```
2024-11-25 13:46:43,021 : INFO : loading vectors from w2v/word2vec_withString10-100-200.model.wv.vectors.npy with mmap=None
2024-11-25 13:46:43,124 : INFO : loading synlneg from w2v/word2vec_withString10-100-200.model.synlneg.npy with mmap=None
2024-11-25 13:46:43,226 : INFO : setting ignored attribute cum_table to None
2024-11-25 13:46:44,223 : INFO : Word2Vec lifecycle event {'fname': 'w2v/word2vec_withString10-100-200.model', 'datetime': '2024-11-25T13:46:43.021'}
finished loading. 13:46
cutoff 38625
cutoff2 46902
Creating training dataset... (xss)
Creating validation dataset...
Creating finaltest dataset...
Train length: 38625
Test length: 8277
Finaltesting length: 8277
time: 13:48
X_train shape: (38625, 200, 200), dtype: float32
y_train shape: (38625,), dtype: int64
X_test shape: (8277, 200, 200), dtype: float32
y_test shape: (8277,), dtype: int64
X_finaltest shape: (8277, 200, 200), dtype: float32
y_finaltest shape: (8277,), dtype: int64
numpy array done. 13:48
38625 samples in the training set.
8277 samples in the validation set.
8277 samples in the final test set.
percentage of vulnerable samples: 8.62%
absolute amount of vulnerable samples in test set: 770
Starting CNNResNet: 13:48
Dropout: 0.2
Neurons: 100
Optimizer: adam
Epochs: 20
Batch Size: 128
max length: 200
2024-11-25 13:48:52.984256: W tensorflow/core/common_runtime/gpu/gpu_bfc_allocator.cc:47] Overriding orig_value setting because the TF_FORCE_
2024-11-25 13:48:52.984474: I tensorflow/core/common_runtime/gpu/gpu_device.cc:2021] Created device /job:localhost/replica:0/task:0/device:GPU:0
Model: "functional"
```

Layer (type)	Output Shape	Param #	Connected to
input_layer (InputLayer)	(None, 200, 200)	0	-
conv1d (Conv1D)	(None, 200, 64)	38,464	input_layer[0][0]
batch_normalization (BatchNormalization)	(None, 200, 64)	256	conv1d[0][0]
re_lu (ReLU)	(None, 200, 64)	0	batch_normalization[0][0]

```
!python makemodel2.py path_disclosure
```

```
2024-11-25 14:15:29.048927: I tensorflow/core/util/port.cc:153] oneDNN custom operations are on. You may see slightly different numerical results
2024-11-25 14:15:29.068094: E external/local_xla/xla/stream_executor/cuda/cuda_fft.cc:485] Unable to register cuFFT factory: Attempting to register
2024-11-25 14:15:29.088715: E external/local_xla/xla/stream_executor/cuda/cuda_dnn.cc:8454] Unable to register cuDNN factory: Attempting to register
2024-11-25 14:15:29.095091: E external/local_xla/xla/stream_executor/cuda/cuda_blas.cc:1452] Unable to register cuBLAS factory: Attempting to register
2024-11-25 14:15:29.110410: I tensorflow/core/platform/cpu_feature_guard.cc:210] This TensorFlow binary is optimized to use available CPU instructions
To enable the following instructions: AVX2 AVX512F AVX512_VNNI FMA, in other operations, rebuild TensorFlow with the appropriate compiler flags
2024-11-25 14:15:30.301788: W tensorflow/compiler/tf2tensorrt/utils/py_utils.cc:38] TF-TRT Warning: Could not find TensorRT
2024-11-25 14:15:32,245 : INFO : loading Word2Vec object from w2v/word2vec_withString10-100-200.model
2024-11-25 14:15:32,299 : INFO : loading wv recursively from w2v/word2vec_withString10-100-200.model.wv.* with mmap=None
2024-11-25 14:15:32,299 : INFO : loading vectors from w2v/word2vec_withString10-100-200.model.wv.vectors.npy with mmap=None
2024-11-25 14:15:32,772 : INFO : loading synlneg from w2v/word2vec_withString10-100-200.model.synlneg.npy with mmap=None
2024-11-25 14:15:33,242 : INFO : setting ignored attribute cum_table to None
2024-11-25 14:15:34,318 : INFO : Word2Vec lifecycle event {'fname': 'w2v/word2vec_withString10-100-200.model', 'datetime': '2024-11-25T14:15:32.245'}
finished loading. 14:15
cutoff 91842
cutoff2 111523
Creating training dataset... (path_disclosure)
Creating validation dataset...
Creating finaltest dataset...
Train length: 91842
Test length: 19681
Finaltesting length: 19680
time: 14:19
X_train shape: (91842, 200, 200), dtype: float32
y_train shape: (91842,), dtype: int64
X_test shape: (19681, 200, 200), dtype: float32
y_test shape: (19681,), dtype: int64
X_finaltest shape: (19680, 200, 200), dtype: float32
y_finaltest shape: (19680,), dtype: int64
numpy array done. 14:20
91842 samples in the training set.
19681 samples in the validation set.
19680 samples in the final test set.
percentage of vulnerable samples: 11.68%
absolute amount of vulnerable samples in test set: 2235
Starting CNNResNet: 14:20
Dropout: 0.2
Neurons: 100
```

```
Optimizer: adam
Epochs: 20
Batch Size: 128
max length: 200
2024-11-25 14:20:58.511023: W tensorflow/core/common_runtime/gpu/gpu_bfc_allocator.cc:47] Overriding orig_value setting because the TF_FORCE_
2024-11-25 14:20:58.511348: I tensorflow/core/common_runtime/gpu/gpu_device.cc:2021] Created device /job:localhost/replica:0/task:0/device:GPU:0
Model: "functional"
```

Layer (type)	Output Shape	Param #	Connected to
input_layer (InputLayer)	(None, 200, 200)	0	-
conv1d (Conv1D)	(None, 200, 64)	38,464	input_layer[0][0]
batch_normalization (BatchNormalization)	(None, 200, 64)	256	conv1d[0][0]
re_lu (ReLU)	(None, 200, 64)	0	batch_normalization[0][0]

```
!python trymodel2.py xss
```

```
2024-11-25 14:11:44.761632: I tensorflow/core/util/port.cc:153] oneDNN custom operations are on. You may see slightly different numerical result:
2024-11-25 14:11:45.332321: E external/local_xla/xla/stream_executor/cuda/cuda_fft.cc:485] Unable to register cuFFT factory: Attempting to regis
2024-11-25 14:11:45.630423: E external/local_xla/xla/stream_executor/cuda/cuda_dnn.cc:8454] Unable to register cuDNN factory: Attempting to regi
2024-11-25 14:11:45.700081: E external/local_xla/xla/stream_executor/cuda/cuda_blas.cc:1452] Unable to register cuBLAS factory: Attempting to reg
2024-11-25 14:11:45.736955: I tensorflow/core/platform/cpu_feature_guard.cc:210] This TensorFlow binary is optimized to use available CPU instruc
To enable the following instructions: AVX2 AVX512F AVX512_VNNI FMA, in other operations, rebuild TensorFlow with the appropriate compiler flags.
2024-11-25 14:11:48.342085: W tensorflow/compiler/tf2tensorrt/utils/py_utils.cc:38] TF-TRT Warning: Could not find TensorRT
Loading model from: model/CNNResNet_model_xss.h5
2024-11-25 14:11:55.652373: W tensorflow/core/common_runtime/gpu/gpu_bfc_allocator.cc:47] Overriding orig_value setting because the TF_FORCE_GPU_
2024-11-25 14:11:55.655757: I tensorflow/core/common_runtime/gpu/gpu_device.cc:2021] Created device /job:localhost/replica:0/task:0/device:GPU:0
Model loaded successfully.
Loading test data from: data/xss_dataset_finaltest_X and data/xss_dataset_finaltest_Y
Test data loaded successfully.
8277 samples in the final test set.
Percentage of vulnerable samples: 9.00%
Absolute number of vulnerable samples: 745
Starting predictions...
WARNING: All log messages before absl::InitializeLog() is called are written to STDERR
I0000 00:00:1732543930.981629 15315 service.cc:146] XLA service 0x79b9ac063160 initialized for platform CUDA (this does not guarantee that XLA
I0000 00:00:1732543930.981680 15315 service.cc:154] StreamExecutor device (0): NVIDIA A100-SXM4-40GB, Compute Capability 8.0
2024-11-25 14:12:11.051543: I tensorflow/compiler/mlir/tensorflow/utils/dump_mlir_util.cc:268] disabling MLIR crash reproducer, set env var `MLIR
2024-11-25 14:12:11.287271: I external/local_xla/xla/stream_executor/cuda/cuda_dnn.cc:531] Loaded cuDNN version 8906
I0000 00:00:1732543932.721800 15315 device_compiler.h:188] Compiled cluster using XLA! This line is logged at most once for the lifetime of tl

Evaluation Metrics:
Accuracy: 0.9756
Precision: 0.9563
Recall: 0.7638
F1 Score: 0.8493
```

```
!python trymodel2.py remote_code_execution
```

```
2024-11-25 14:12:37.488652: I tensorflow/core/util/port.cc:153] oneDNN custom operations are on. You may see slightly different numerical result:
2024-11-25 14:12:37.505427: E external/local_xla/xla/stream_executor/cuda/cuda_fft.cc:485] Unable to register cuFFT factory: Attempting to regis
2024-11-25 14:12:37.525018: E external/local_xla/xla/stream_executor/cuda/cuda_dnn.cc:8454] Unable to register cuDNN factory: Attempting to regi
2024-11-25 14:12:37.531266: E external/local_xla/xla/stream_executor/cuda/cuda_blas.cc:1452] Unable to register cuBLAS factory: Attempting to reg
2024-11-25 14:12:37.545706: I tensorflow/core/platform/cpu_feature_guard.cc:210] This TensorFlow binary is optimized to use available CPU instruc
To enable the following instructions: AVX2 AVX512F AVX512_VNNI FMA, in other operations, rebuild TensorFlow with the appropriate compiler flags.
2024-11-25 14:12:38.895407: W tensorflow/compiler/tf2tensorrt/utils/py_utils.cc:38] TF-TRT Warning: Could not find TensorRT
Loading model from: model/CNNResNet_model_remote_code_execution.h5
2024-11-25 14:12:41.280838: W tensorflow/core/common_runtime/gpu/gpu_bfc_allocator.cc:47] Overriding orig_value setting because the TF_FORCE_GPU_
2024-11-25 14:12:41.281087: I tensorflow/core/common_runtime/gpu/gpu_device.cc:2021] Created device /job:localhost/replica:0/task:0/device:GPU:0
Model loaded successfully.
Loading test data from: data/remote_code_execution_dataset_finaltest_X and data/remote_code_execution_dataset_finaltest_Y
Test data loaded successfully.
14412 samples in the final test set.
Percentage of vulnerable samples: 8.89%
Absolute number of vulnerable samples: 1281
Starting predictions...
WARNING: All log messages before absl::InitializeLog() is called are written to STDERR
I0000 00:00:1732543983.732261 15656 service.cc:146] XLA service 0x788878011a40 initialized for platform CUDA (this does not guarantee that XLA
I0000 00:00:1732543983.732298 15656 service.cc:154] StreamExecutor device (0): NVIDIA A100-SXM4-40GB, Compute Capability 8.0
2024-11-25 14:13:03.749825: I tensorflow/compiler/mlir/tensorflow/utils/dump_mlir_util.cc:268] disabling MLIR crash reproducer, set env var `MLIR
2024-11-25 14:13:03.867610: I external/local_xla/xla/stream_executor/cuda/cuda_dnn.cc:531] Loaded cuDNN version 8906
I0000 00:00:1732543984.663532 15656 device_compiler.h:188] Compiled cluster using XLA! This line is logged at most once for the lifetime of tl

Evaluation Metrics:
Accuracy: 0.9791
Precision: 0.9291
Recall: 0.8283
F1 Score: 0.8758
```

```
!python trymodel2.py path_disclosure
```

```
↩ 2024-11-25 14:25:23.998578: I tensorflow/core/util/port.cc:153] oneDNN custom operations are on. You may see slightly different numerical results
2024-11-25 14:25:24.579099: E external/local_xla/xla/stream_executor/cuda/cuda_fft.cc:485] Unable to register cuFFT factory: Attempting to register
2024-11-25 14:25:24.867670: E external/local_xla/xla/stream_executor/cuda/cuda_dnn.cc:8454] Unable to register cuDNN factory: Attempting to register
2024-11-25 14:25:24.939429: E external/local_xla/xla/stream_executor/cuda/cuda_blas.cc:1452] Unable to register cuBLAS factory: Attempting to register
2024-11-25 14:25:24.975932: I tensorflow/core/platform/cpu_feature_guard.cc:210] This TensorFlow binary is optimized to use available CPU instructions
To enable the following instructions: AVX2 AVX512F AVX512_VNNI FMA, in other operations, rebuild TensorFlow with the appropriate compiler flags.
2024-11-25 14:25:27.492963: W tensorflow/compiler/tf2tensorrt/utils/py_utils.cc:38] TF-TRT Warning: Could not find TensorRT
Loading model from: model/CNNResNet_model_path_disclosure.h5
2024-11-25 14:25:34.553831: W tensorflow/core/common_runtime/gpu/gpu_bfc_allocator.cc:47] Overriding orig_value setting because the TF_FORCE_GPU_USAGE
2024-11-25 14:25:34.557332: I tensorflow/core/common_runtime/gpu/gpu_device.cc:2021] Created device /job:localhost/replica:0/task:0/device:GPU:0
Model loaded successfully.
Loading test data from: data/path_disclosure_dataset_finaltest_X and data/path_disclosure_dataset_finaltest_Y
Test data loaded successfully.
19680 samples in the final test set.
Percentage of vulnerable samples: 11.73%
Absolute number of vulnerable samples: 2308
Starting predictions...
WARNING: All log messages before absl::InitializeLog() is called are written to STDERR
I0000 00:00:1732544770.205036 19923 service.cc:146] XLA service 0x7cd6380511d0 initialized for platform CUDA (this does not guarantee that XLA
I0000 00:00:1732544770.205073 19923 service.cc:154] StreamExecutor device (0): NVIDIA A100-SXM4-40GB, Compute Capability 8.0
2024-11-25 14:26:10.272777: I tensorflow/compiler/mlir/tensorflow/utils/dump_mlir_util.cc:268] disabling MLIR crash reproducer, set env var `MLIR
2024-11-25 14:26:10.506586: I external/local_xla/xla/stream_executor/cuda/cuda_dnn.cc:531] Loaded cuDNN version 8906
I0000 00:00:1732544771.946794 19923 device_compiler.h:188] Compiled cluster using XLA! This line is logged at most once for the lifetime of the
Evaluation Metrics:
Accuracy: 0.9686
Precision: 0.9159
Recall: 0.8068
F1 Score: 0.8579
```

开始借助 AI 编写或生成代码。

开始借助 AI 编写或生成代码。