InfoSec Ninjas

Longjing

Deep Learning Driven Web Application Firewall

InfoSec Ninjas

Who am I?

Samiux is an Information Security Enthusiast.

- - OSCE, OSCP, OSWP
- - Blogger
- - Linux user

Hobbies :

- - Programming
- - Reading
- - Pentesting

InfoSec Ninjas

What is Longjing?

Longjing is a deep learning driven web application firewall based on Python Scikit-Learn library.

- - Developed by Samiux since 2018
- - Open source under GPLv3 (but not the modeling)

- - For almost all web servers in the market
- - For almost all web applications
- - Detects common web attacks
- - Mainly for detecting SQL injection attacks

InfoSec Ninjas

Main components :

- - Pyhton 3
- - Scikit-Learn Library
- - Anaconda3
- - mitmproxy
- - Ubuntu Server LTS

InfoSec Ninjas

Features :

- - Blocks common SQL Injection attacks
- - Blocks common Directory Traversal attacks
- - Blocks common Cross Site Scripting attacks
- - Blocks common SQLi, XSS and Directory Traversal bypasses
- - Supports SSL/TLS Certificates

InfoSec Ninjas

Why Scikit-Learn?

- - About 2,500 dataset
- - Supervising Neural network
- - Not requires GPU
- - Time for training is fast
- - Python 3

InfoSec Ninjas

Pros :

- - False Positive can be minimized by Python programming
- - Python is available for almost all Linux distributions
- - Free to use

Cons :

- - May requires faster storage media, such as SSD
- - May requires faster CPU
- - May requires more memory (at least 1GB for Longjing)
- - Tested on Ubuntu Server LTS only
- - May not suitable for large scale web applications
- - Source IP addresses cannot be logged
- - Speed of web applications may be slowed down
- - Modeling is close source

InfoSec Ninjas

Demo

- Longjing - https://youtu.be/7ugn1bw4ZTA

Live Target (Online Time is Limited)

- - Longing and Croissants (Intrusion Prevention System)
- - Infosec Projects - http://www.infosec-projects.com/

InfoSec Ninjas

Reference

- Scikit-Learn Library - https://scikit-learn.org/stable/
- Anaconda3 - https://www.anaconda.com/distribution/
- mitmproxy - https://mitmproxy.org/
- Ubuntu - https://ubuntu.com/

- Longjing - https://www.infosec-ninjas.com/longjing
- Infosec Ninjas - https://www.infosec-ninjas.com/

InfoSec Ninjas

Thank You!

Q&A