Nicholas Zimmerer
June 29th 2017

Toolkit

Abstract

The Toolkit is a collection of applications which demonstrate a variety of topics of computer security. The main goal of the Toolkit is to teach users about the topic, along with providing a playground to test and develop their understanding in. The Toolkit focuses on three security concepts: SQL injection, steganography, and encryption.

SQL injection is a vulnerability found when the code to execute database querys is written improperly. The Toolkit includes a demo for users to query a database and see the response. The query function has a SQLi vulerability that the user can exploit to manipulate the database.

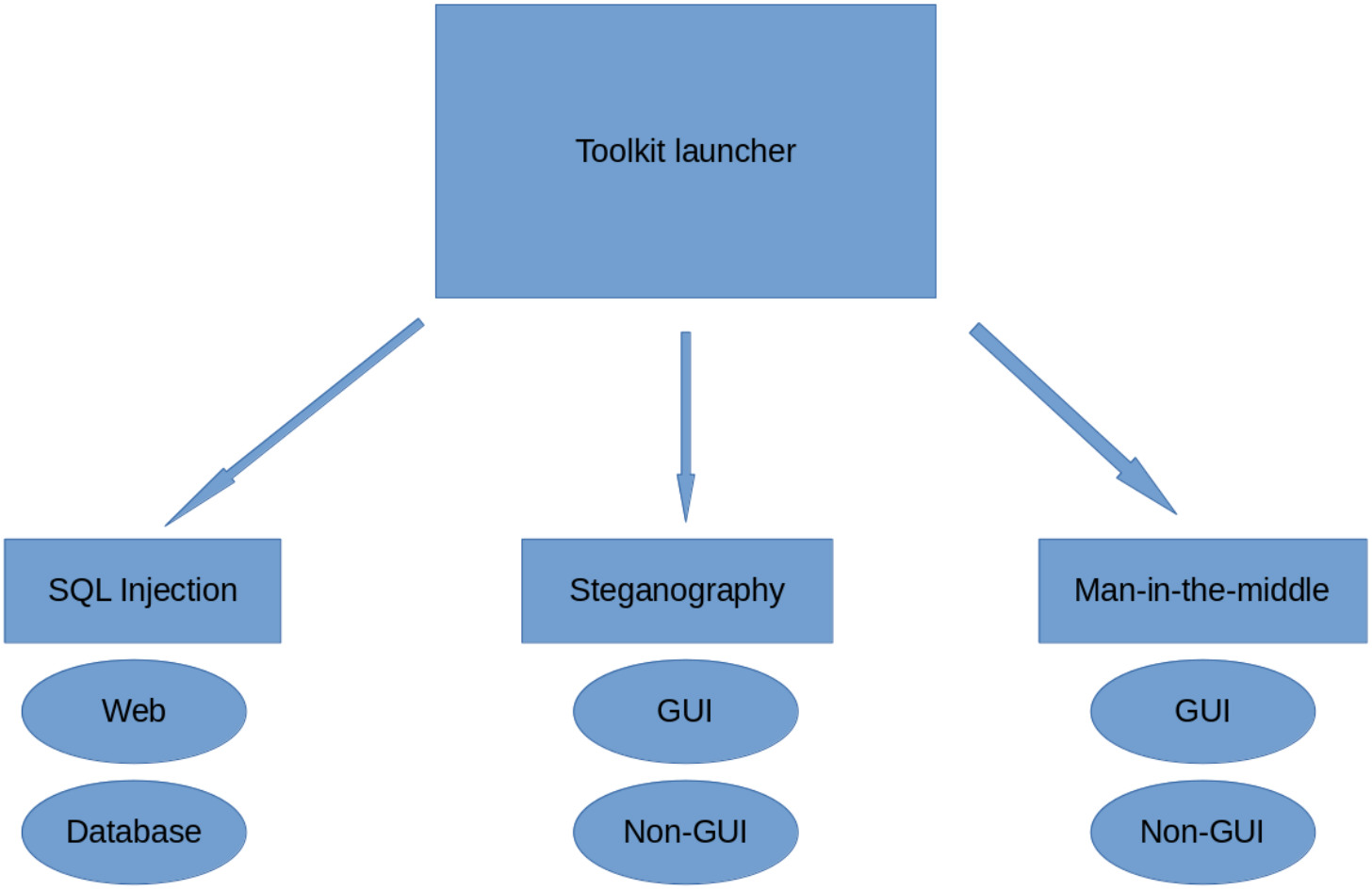
Steganography is the practice of concealing one set of data within the contents of another set of data. While there are many forms of media to conseal data in (video, audio, etc) the algorithm employed within Toolkit encodes a message into an image file. The Toolkit's provided application allows the user to select an image, input a message, and visually inspect the two images side-by-side. Additionally, the process can be reversed to extract and display the encoded message to the user, as a proof on concept. While this is a simple application, there are far-reaching implications: steganography has been used to covertly exfiltrate data or download malware configuration files.

Man-in-the-middle attacks are a notable concern for networked communications. By sending unencrypted data between two computers, an attacker can tap the connection to collect (passive) or manipulate (active) the dataflow. The Toolkit demonstrates passive eavesdropping (via packet sniffing) on an unencrypted communication.

Requirements

- GUI
  - Toolkit main launcher
  - Stegonography frontend
  - Man-in-the-middle IM frontend
- NON-GUI
  - Stegonography algorithm
  - Man-in-the-middle networking backend
- Web
  - SQL injection webpage
- Database
  - SQL injection database access and rebuilding scripts

Toolbox Application Overview



Stretch Goals

Add encryption functionality to man-in-the-middle TCP connection. Implement SSH encryption to demonstrate the lack of eavesdropping capabilities on encrypted connections.