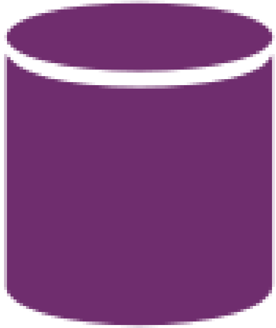
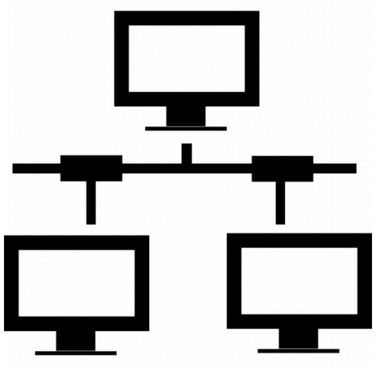
Toolkit

Security related demos



SQL injection



Eavesdropping

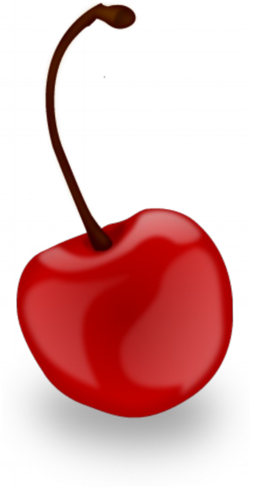
Steganography

Demos

- SQL injection playground
  - Website to experiment with SQL injection
  - Database generated at runtime
- Eavesdropping/packet sniffing
  - One-way messaging
- Image steganography
  - Encode messages into image data

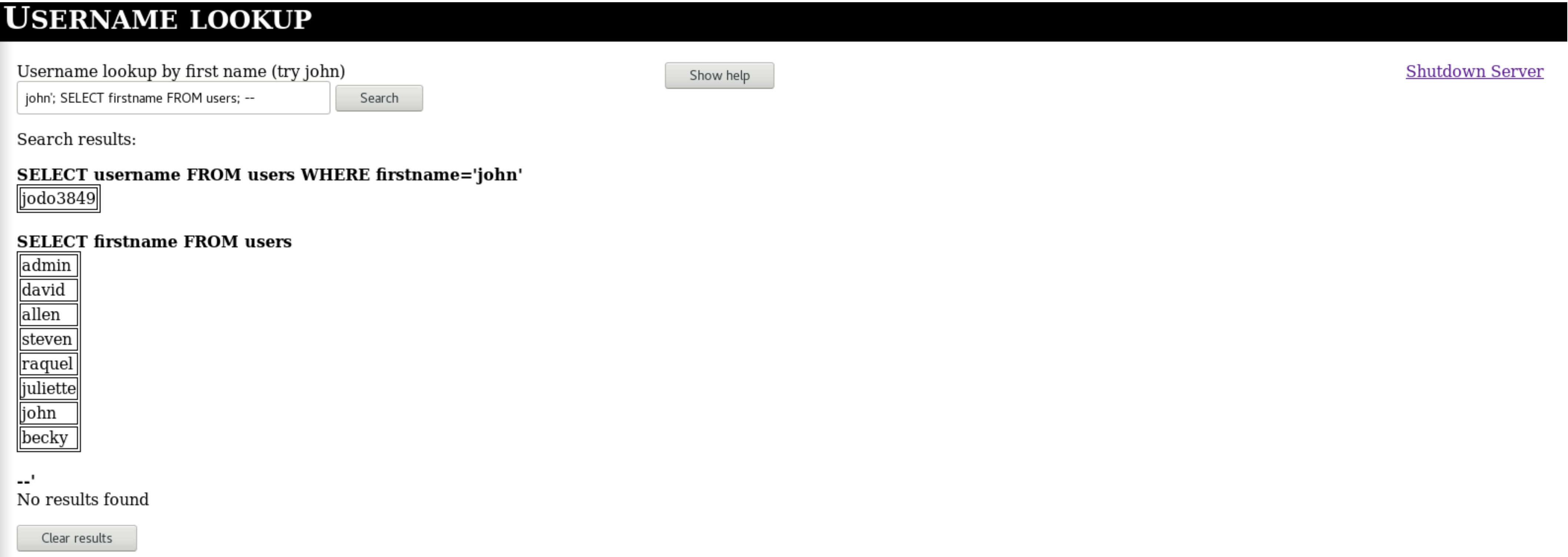
Techs and Reqs

- **GUI**
  - Launcher
  - Steganography frontend
- **Non-GUI**
  - Eavesdropping
    - Wireshark (tshark)
  - Steganography backend
    - Python Image Library (PIL)
- **Web & database**
  - SQL injection
    - CherryPy server
    - SQLite3 database



SQL injection

- Tech used
  - SQLite3
  - CherryPy
- Bobby tables proof
  - Database generated at runtime – drop all the tables you like!



USERNAME LOOKUP

Username lookup by first name (try john)

john'; SELECT firstname FROM users; --

Search results:

SELECT username FROM users WHERE firstname='john'

jodo3849

SELECT firstname FROM users

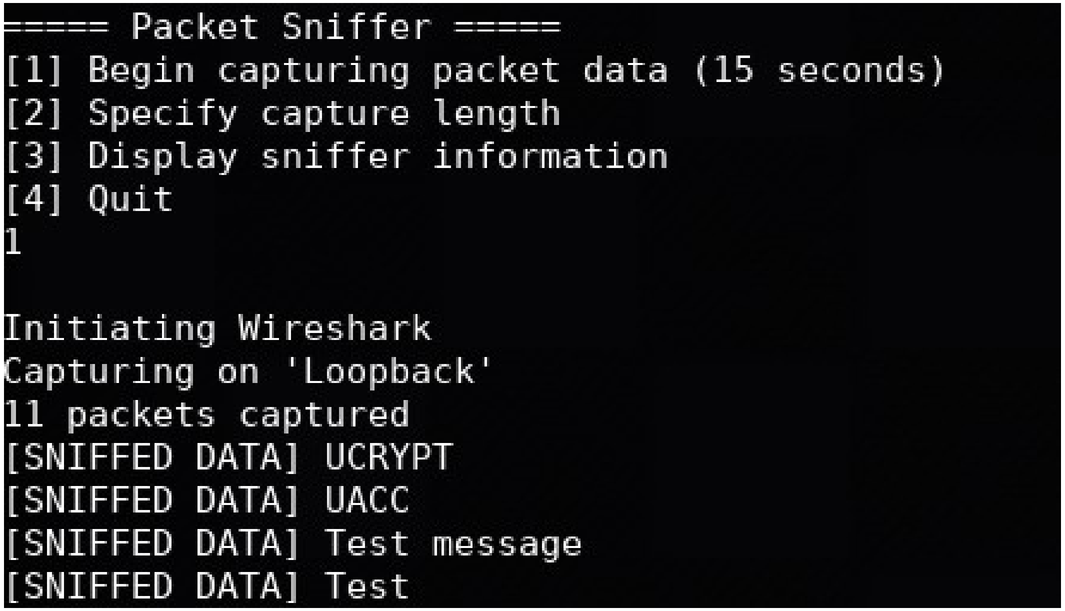
admin
david
allen
steven
raquel
juliette
john
becky

--'

No results found

Eavesdropping

- Sender-reciever relationship for simplicity
  - Supports basic encryption
- Sniffer displays packet data

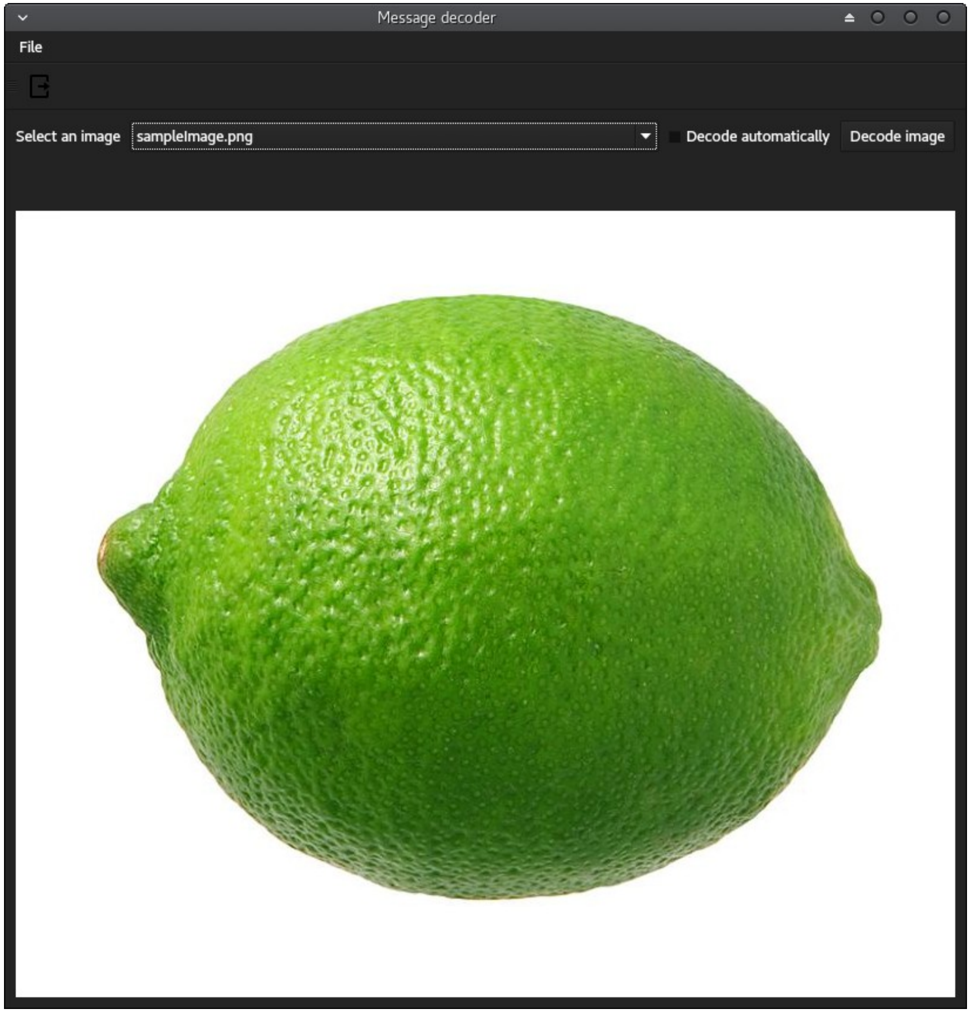


```
===== Packet Sniffer =====
[1] Begin capturing packet data (15 seconds)
[2] Specify capture length
[3] Display sniffer information
[4] Quit
1

Initiating Wireshark
Capturing on 'Loopback'
11 packets captured
[SNIFFED DATA] UCRYPT
[SNIFFED DATA] UACC
[SNIFFED DATA] Test message
[SNIFFED DATA] Test
```

Steganography

- Hides plaintext ascii message in a PNG image
- Decodes and displays messages

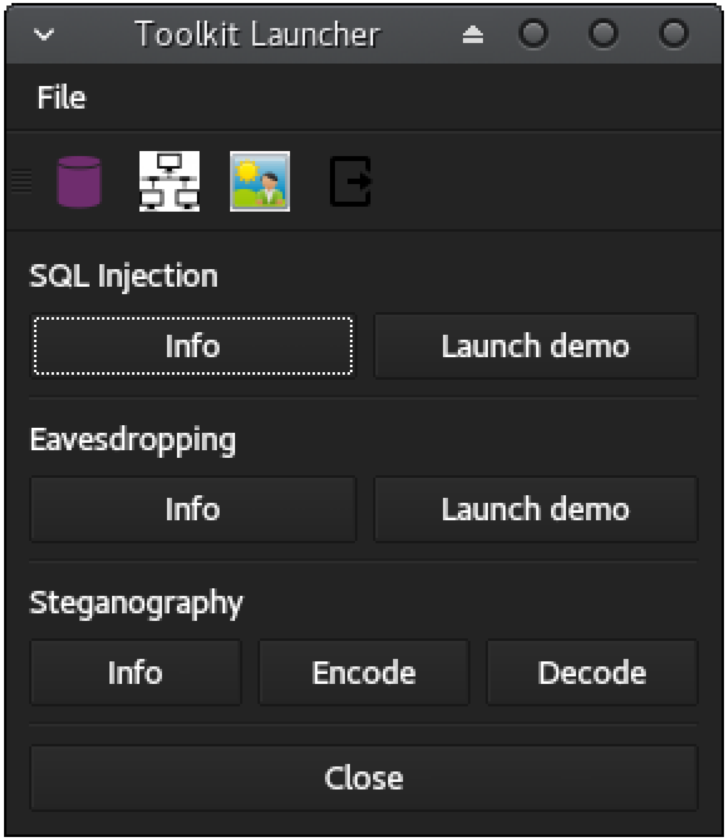


Select an image sampleImage.png

Unfinished business

- Places for improvement:
  - Create database in memory instead of disk
    - Unsure how to pass a db located in memory to javascript
  - Implement RSA key generation and SSH handshake
    - Using an API is a trivial solution
  - Make chat flow both ways
    - 2-way isn’t necessary to illustrate passive eavesdropping
  - Display sniffed sender/receiver data
    - Requires more handling of raw packet data
  - Support additional image types for Steganography
    - Standard JPEG is lossy, makes encoding trickier
- Bugs
  - Steganography window does not resize dynamically
  - Enter key doesn’t connect with button on SQL webpage
  - Auto-launch for eavesdropping only loads terminal, not all three necessary
  - Server gets sad when Client is killed

Live demo


Toolkit Launcher
File
SQL Injection
Info
Launch demo
Eavesdropping
Info
Launch demo
Steganography
Info
Encode
Decode
Close