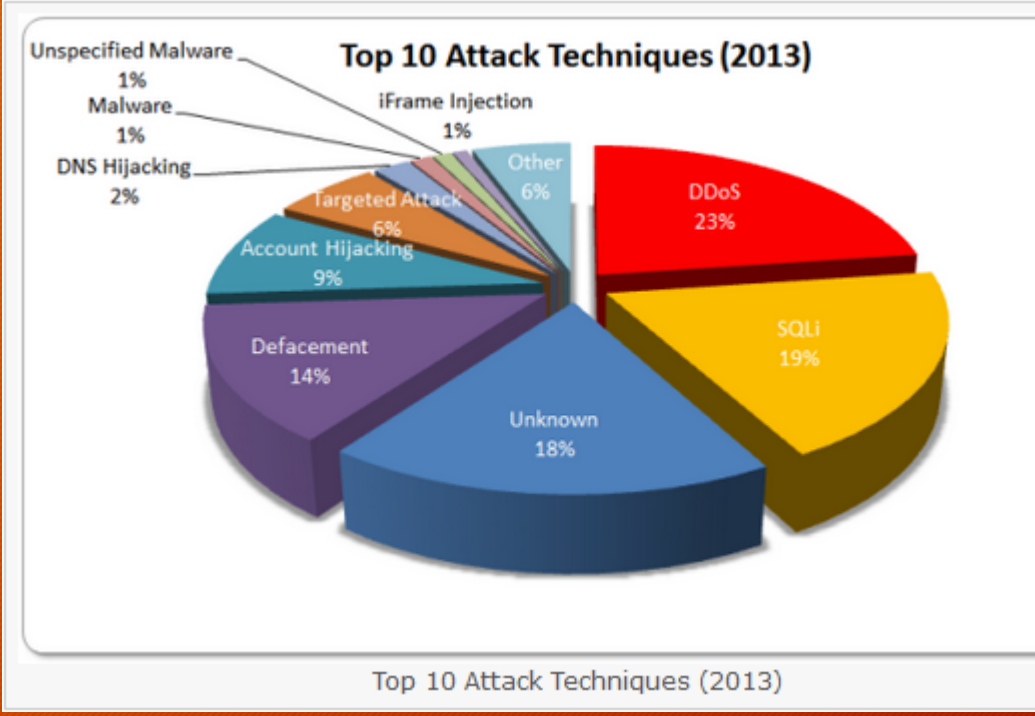
Advancing Defenses against SQL Injection Attacks through a Vulnerability Forensic Parsing service

ohan Malcolm, Sean Thorpe, Julian Jarrett, Tyrone Grandison, Leon Stenneth

Motivation

- Injection is still a weapon being by hackers and script kiddies.
- uary 2014 zero day SQL injection oomla was made publicly lable.
- 013 SQL injection was used to promise the information of users of lifornian-based ISP.



Top 10 Attack Techniques (2013)

Figure taken from hackmegeddon http://hackmageddon.com/category/security/cyber-attacks-statistics/

elated Work

- Parse Trees and SQL Injection
- SQLrand
- AMNESIA
- Web Application Firewall

roposal: Vulnerability Parser (VP)

VP is a parsing tool designed to
ct and classify SQL injection
cks in real time.

VP also introduces post-attack
nsic analysis which is not well
rved in other research tools.

proof of concept a stand alone
er application is being developed
this paper merely shows the
ework within which one can be
esented.

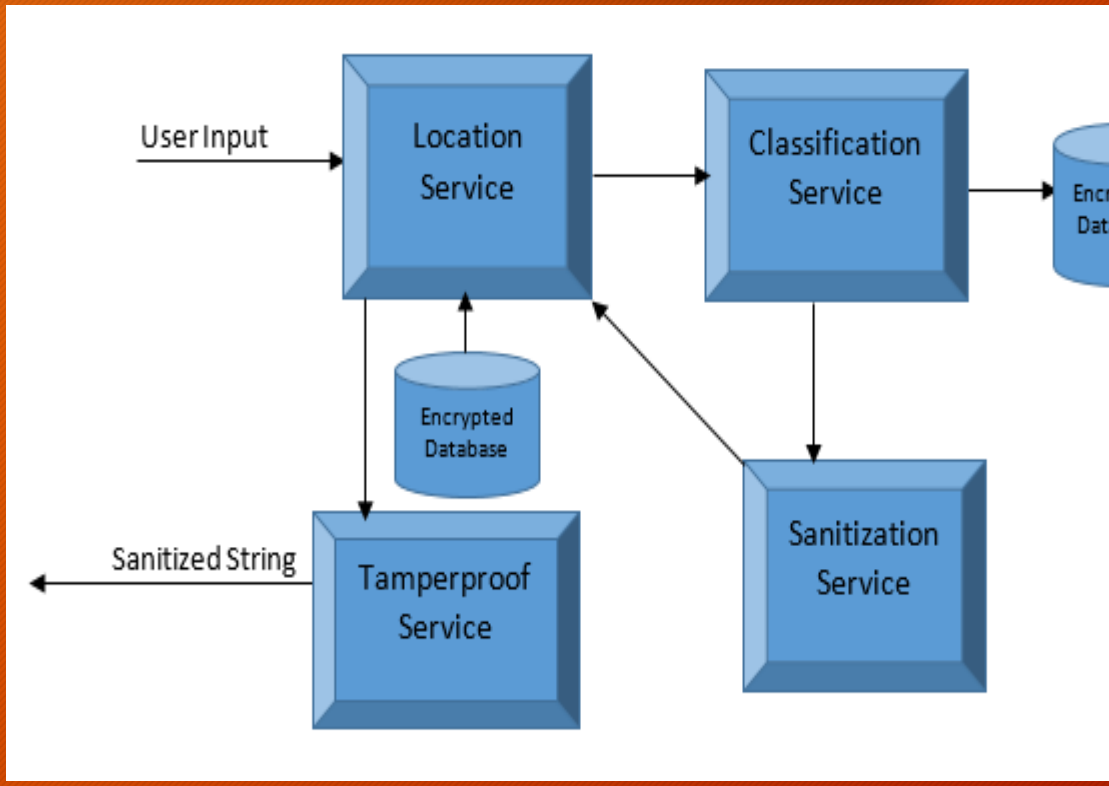


Figure showing the VP architecture

ocation Service

he location service is the starting point for the VP and this is where all ossible SQL injection attacks will be detected.

t is connected to an encrypted database/file which stores information of he known SQL injection attacks.

f an SQL injection attack is discovered it will be passed to the lassification Service else it will be passed to the tamperproof Service.

lassification Service

- The classification service is the area of the VP where a attack is classified into a known attack (for example Tautologies, Logically ncorrect Queries, Union Query, Piggy Backed Query and so on) or isted as an unknown attack if the classification model cannot fit it based on a certainty threshold.
- This notion of unknown attacks is something which we have identified for future work.
- The result of this is also stored in an encrypted database.

anitization Service

- The sanitization service accepts the attack string and outputs a clean string based on the type of attack given.
- t uses a query rewriting algorithm which parses the string for the attack sections and alters them into a non malicious segment. This non malicious segment however should still be a plausible SQL Query that executes safely on the server.
- The query rewriting algorithm is still under development.

amperproof Service

The tamperproof service defines a mechanism in which the output of the location service is checked backed to a known safe state to validate output.

t uses a fusion of cached tables and state checking to ensure that sensitive or stated information is not returned to the user.

Still under development.

uture Work

- Access to a suite of post forensic analysis tools.
- Ability to learn and detect new form of attacks.
- Protect from more than just SQL Injection attacks.

hank You !!!!

For any queries or comments or suggestions please contact.

Rohan Malcolm at Rohan.Malcolm@utech.edu.jm

Dr. Sean Thorpe at sthorpe@utech.edu.jm