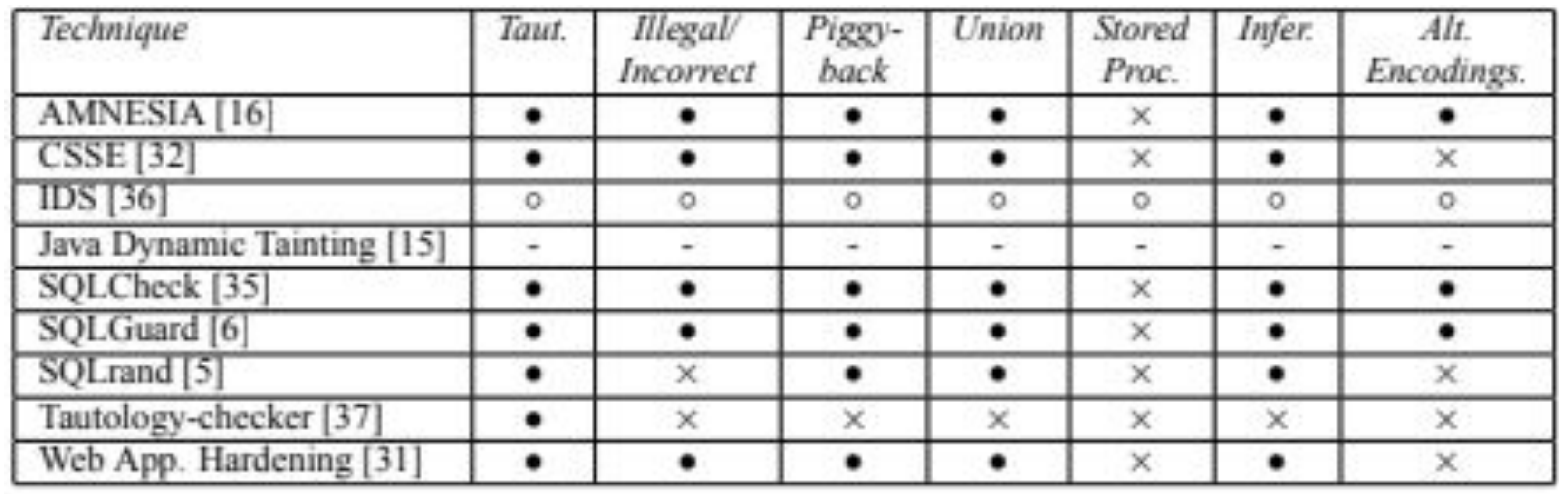
Reviewing Open Source Web Application Vulnerability Scanners and Testing Platforms for Comprehensiveness in Detecting SQL Injection and Cross Site Scripting Vulnerabilities

Michael O’Connell

Motivation

- Comprehensively test *Zed Attack Proxy* (ZAP), and *Vega* for SQL injections (SQLi) and Cross-Site Scripting attacks (XSS).
- Comprehensive testing is necessary to determine the defensive code/practices needed to stop an attacker early during an exploitation attempt. Figure 1 [4] illustrates this point by showing various software effective for detection against each of the SQLi types.



Technique	*Taut.*	*Illegal/ Incorrect*	*Piggy-back*	*Union*	*Stored Proc.*	*Infer.*	*Alt. Encodings.*
AMNESIA [16]	●	●	●	●	×	●	●
CSSE [32]	●	●	●	●	×	●	×
IDS [36]	○	○	○	○	○	○	○
Java Dynamic Tainting [15]	-	-	-	-	-	-	-
SQLCheck [35]	●	●	●	●	×	●	●
SQLGuard [6]	●	●	●	●	×	●	●
SQLrand [5]	●	×	●	●	×	●	×
Tautology-checker [37]	●	×	×	×	×	×	×
Web App. Hardening [31]	●	●	●	●	×	●	×

Table 1: Comparison of detection-focused techniques with respect to attack types.

Web Vulnerability Scanners

- OWASP’s Zed attack proxy (ZAP) is an open source web vulnerability scanner that acts as a proxy that sits in between your computer and the web applications you visit and allows you to intercept traffic and modify responses sent between you and the application.
- Vega is a free and open source web security scanner and web security testing platform. Vega can help find and validate SQL Injection, Cross-Site Scripting (XSS), inadvertently disclosed sensitive information, and other vulnerabilities. It is written in Java, GUI based, and runs on Linux, OS X, and Windows [2].

SQL Injection

In *A Classification of SQL-Injection Attacks and Countermeasures*, W.G. Halfond et al. give a complete description of SQLi types and injection mechanisms [4**]**

Injection mechanisms

- Injection through user input
- Injection through cookies
- Injection through server variables
- Second order injection

Types

- Tautologies
- Illegal/Incorrect Queries
- Union Query
- Piggy-Backed Queries
- Stored Procedures
- Inference
- Alternate Encodings

Cross-Site Scripting Attacks

The Mozilla Developer Network defines three XSS attacks [3]:

- Stored XSS
- Reflected XSS
- DOM-based XSS

The OWASP foundation goes on to explain that because XSS type categorization overlaps, the research community proposed using two separate terms to organize all XSS attacks [1]:

- Client XSS
- Server XSS.

Testing

- Attack code (which I found or researched) was used to confirm true positive rates of detection of vulnerabilities and effective testing subjects. For testing subjects, I used Open Source applications hosted on my machine. Once I found an appropriate vulnerability to test that was determined using manual penetration testing (with attack code on a given testing subject), I determined whether the WVs could detect it and recorded their true positive rates of detection.

References

- [1] OWASP Foundation. DOM Based XSS Software Attack. Retrieved January 12, 2021, from https://owasp.org/www-community/attacks/DOM_Based_XSS.
- [2] Subgraph. “Vega Vulnerability Scanner.” *Subgraph*, subgraph.com/vega/.
- [3] “Types of Attacks.” *Web Security | MDN*, developer.mozilla.org/en-US/docs/Web/Security/Types_of_attacks#cross-site_scripting_xss.
- [4] W. G. Halfond, J. Viegas, and A. Orso. A Classification of SQL-Injection Attacks and Countermeasures. In Proc. of the Intl. Symposium on Secure Software Engineering, Mar. 2006.