Combinatorial Methods for Dynamic Gray-Box SQL Injection Testing

Bernhard Garn, Jovan Zivanovic, Manuel Leithner & Dimitris E. Simos

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet

SBA Research

MATRIS

Problem & Motivation

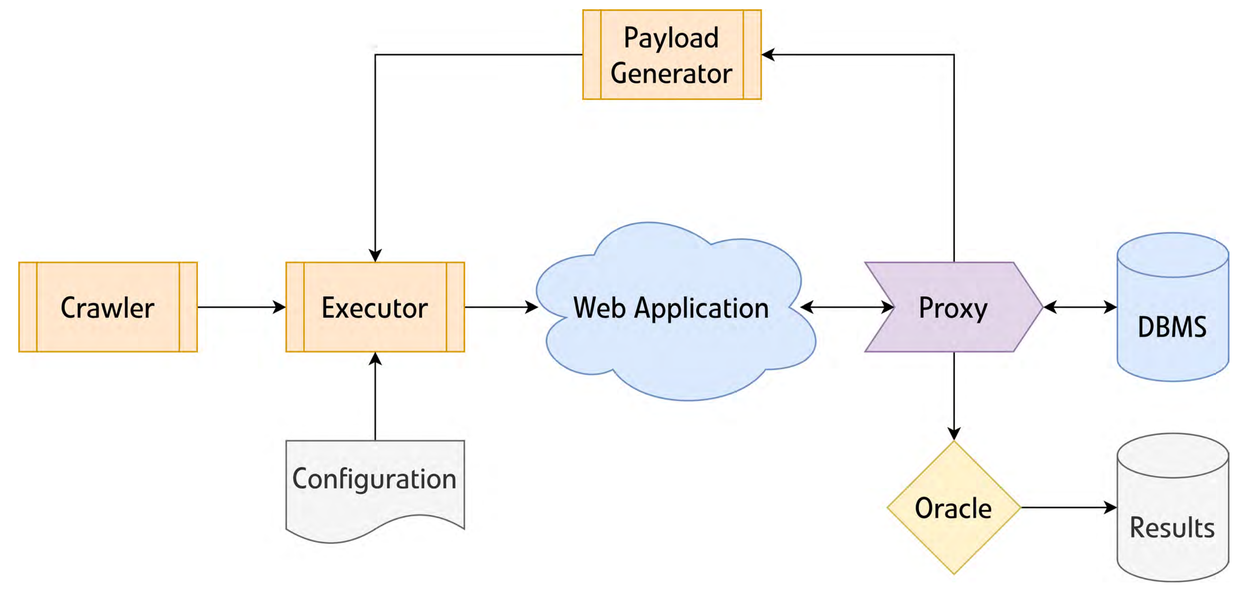
SQL injection remains one of the most popular classes of security flaws in web applications.

While modern frameworks prevent SQLi in most situations, security testing is still required.

Popular tools primarily use hardcoded lists of exploit vectors.

SQLInjector+

- Grammar-based exploit vector generation
- Selected & refined based on context in query
- Evaluated against popular security testing tools



Approach

- **Context-specific grammars**
  - Optimized for specific location in query
  - Adapted at runtime, avoids filtered characters
  - E.g. `WHERE`, `LIMIT`, `ORDER`, ...
- **Combinatorial coverage guarantees**
  - Guaranteed coverage and diversity
  - Small, efficient test sets
  - Strength chosen by user
- **DBMS proxy**
  - Intercepts queries
  - Identifies injection context
  - Supports oracle decision

Listing 1: Excerpt of grammar for injections inside the *WHERE* clause. S_{string} and $S_{payload}$ are sub-grammars for escaping string environments and constructing payloads.

```
<S_cond> ::= <S_string><WhSp><Op><WhSp><S_payload><WhSp><Comm><WhSp>

<WhSp> ::= _ | /**/ | %20 | %0A | \n
<Op> ::= or | || | && | and
<Comm> ::= # | -- | %00 | %23 | %2F%2A | ϵ
```

Proven efficacy

Our prototype implementation `SQLInjector+` finds previously undetected flaws and leads the pack in a comparison with the state of the art (sqlmap, w3af, wapiti...).

Evaluation

- **Tools:**
  sqlmap, w3af, wapiti, FuzzDB, SQLInjector (predecessor)
- **Training targets:**
  WAVSEP, DVWA, Web4Pentester, MCIR-SQLOL
- **Real-world web apps:**
  WebChess, geccBBlite, zeusCart, OpenSchool, ModSecurity (with synthetic web app)

Results

Detection rate (DR): Ratio of successfully exploited endpoints over all endpoints.

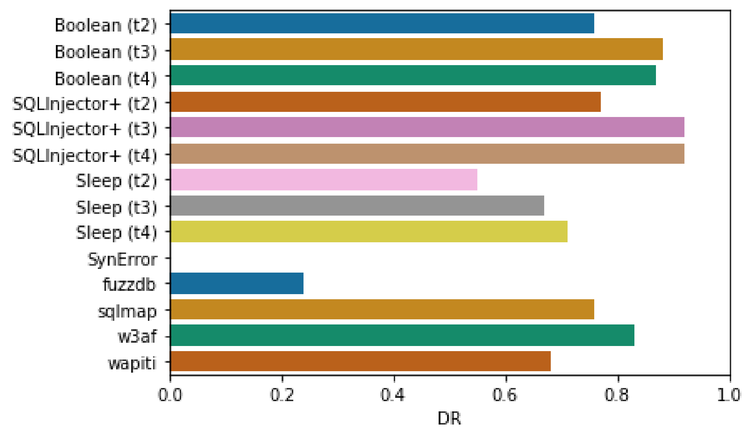


Figure 1: Detection Rate across all SUTs; higher is better.

Conclusion

- Context-specific, gray-box combinatorial security testing
- Geared towards SQL injections, theoretically applicable to other classes
- Adjust test set size based on resource limits and preference
- Finds new vulnerabilities
- Identifies more flaws than state of the art
- Offers various string tainting & escape techniques

Bernhard Garn, Jovan Zivanovic, Manuel Leithner, and Dimitris E Simos. Combinatorial methods for dynamic gray-box sql injection testing. *Software Testing, Verification and Reliability*, 32(6):e1826, 2022.

This research was further funded by the Austrian Research Promotion Agency (FWF): Grant no. 865248 (SECuring Web technologies with combinatorial Interaction Testing - SecWIT).

Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
Bundesministerium Digitalisierung und Wirtschaftsstandort
FFG Forschung wirkt.
wirtschaftsagentur wien Ein Fonds der Stadt Wien
Europäische Kommission
FWF Der Wissenschaftsfonds.
netidee OPEN INNOVATIONS

SBA Research (SBA-K1) is a COMET Centre within the framework of COMET – Competence Centers for Excellent Technologies Programme and funded by BMK, BMDW, and the federal state of Vienna. The COMET Programme is managed by FFG.