Combinatorial Testing Methods for SQL Injections

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

SQL Injection
- Unsanitized user input used inside SQL statements.
- Malicious user can execute arbitrary commands on the database.

SQL Injection Example

```
login.php?username=username&password=password OR 1 = 1
```

Records returned

Combinatorial Security Testing
- Grammar used to define the structure attack vectors with discretized parameters.
- Every parameter represents a path that has a specific purpose inside the attack vector, e.g., quotation marks for escaping.
- Input Parameter Model (IPM) used to define the attack grammar.
- Each row of a Covering Array (CA) represents an attack vector.

Attack Model

**SQLInjection**
- Developed prototype tool for executing CT-generated attack vectors.
- Uses a database proxy for collecting queries.
- Potentially malicious queries are compared against known valids.
- Changes in syntax indicate successful SQL injection.

**SQL Injector**

Case Study
- WAVSEP: Well-known verification framework with known vulnerabilities, used to evaluate automated web application vulnerability scanners.
- Webchess: A self-hosted PHP-based online chess application.
- geccBBlite: Minimalistic bulletin board software.
- OpenSchool: Online School Management Interface.
- zeusCart: Open-source shopping cart for online stores.
- uHotelbooking: Online hotel reservation system.
- modesecurity: Web Application Firewall.

Evaluation

Execution rate for webchess against all vuln. scanners.

**Tested parameters for each SUT**

<table>
<thead>
<tr>
<th>SUT</th>
<th>WAVSEP</th>
<th>WITF</th>
<th>Webchess</th>
<th>geccBBlite</th>
<th>OpenSchool</th>
<th>zeusCart</th>
<th>uHotelbooking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tested Params.</td>
<td>48</td>
<td>N/A</td>
<td>9</td>
<td>5</td>
<td>43</td>
<td>24</td>
<td>17</td>
</tr>
<tr>
<td>Vulnerable Params.</td>
<td>30</td>
<td>N/A</td>
<td>5</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

Injection Rate for webchess against all vuln. scanners.