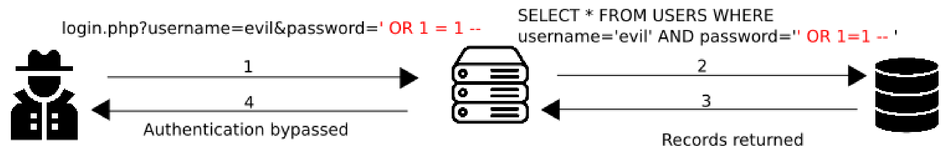
Combinatorial Testing Methods for SQL Injections

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

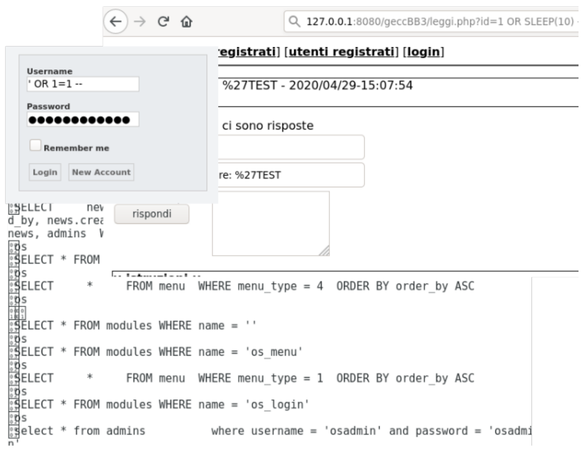
Competence Centers for Excellent Technologies
www.ffg.at/comet

SQL Injection

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

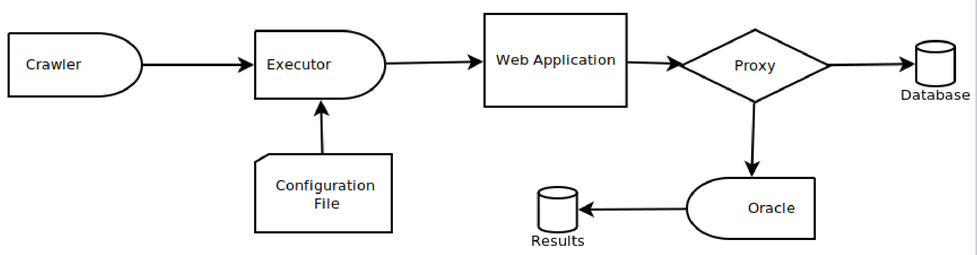


SQL Injection Example



SQLInjector

- 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*.



Combinatorial Security Testing

- Grammar used to define the structure attack vectors with discretized parameters.
- Every parameter represents a parth 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

```
InQ1(5) ::= " | ’ | %22 | %27 | ϵ
WhSp1(9) ::=  | /**/ | %20 | %09 | %A0 | %0A |
 %0B | %0C | %0D
Par(3) ::= ) | %29 | ϵ
Comm1(9) ::= -- | # | /* | %00 | %23 | %2F |
 %2A | %2F%2A | ϵ
InVa(6) ::= 0 | 1 | 2 | a | b | c
CndV1(6) ::= 0 | 1 | 2 | true | !!true | !false
CndV2(6) ::= 0 | 1 | 2 | true | !!true | !false
Cmd(14) ::= OR | Or | oR | or | || | AND | ANd |
AnD | aND | anD | And | aNd | and | &&
AtkVec1(1) ::= InVa InQ1 Par WhSp1 Cmd WhSp1
CndV1 WhSp1 = WhSp1 CndV2 WhSp1 Comm1 WhSp1
```

1, 3, 1, 1, 1, 1, 0, 0	1%27/**/||/**/(Select/**/1+1)/**/#/**/
2, 2, 2, 2, 2, 2, 1, 0	2%22%20&&%20(sElEcT%202|2)%20#%20
0, 3, 0, 3, 0, 0, 2, 0	0%27 and (select 0*0) #

Case Study

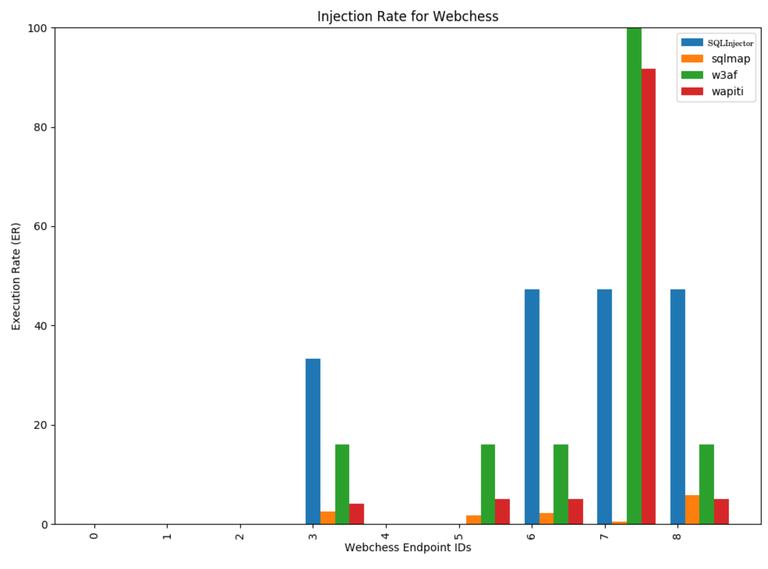
- **WAVSEP**: Well-known verification framework with known vulnerabilities, used to evaluate automated web application vulnerability scanners.
- **Webchess**: A self-hosted PHP-based online chess application.
- **geccBBlite**: Minimalistic bulletin board software.
- **OpenSchool**: Online School Management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

Attack vector comparison

- **sqlmap**: Well known automated SQL injection vulnerability scanner.
- **wapiti**: Web application vulnerability scanner written in *python*.
- **w3af**: Also an automated web application scanner written in *python*.

Evaluation

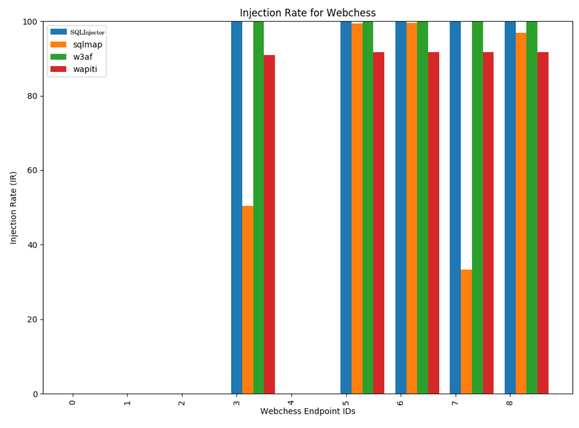
Execution rate for webchess against all vuln. scanners.



Tested parameters for each SUT

SUT	WAVSEP	WTF	webchess	geccBBlite	OpenSchool	zeusCart	uHotelbooking
Tested Params.	48	N/A	9	5	43	24	17
Vulnerable Params.	30	N/A	5	2	4	4	1

Injection Rate for webchess against all vuln. scanners.



Dimitris Simos, Jovan Zivanovic, and Manuel Leithner. Automated combinatorial testing for detecting sql vulnerabilities in web applications. In *14th International Workshop on Automation of Software Test (AST)*, 5 2019.

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.