Combinatorial Fault Localization for Web Security Testing

Dimitris E. Simos, Bernhard Garn, Manuel Leithner, Yu Lei, Angelo Gargantini

Combinatorial Testing & Combinatorial Fault Analysis

Motivation
- We cannot test everything.
- Exhaustive search of problem space increases time needed exponentially.
- Automated detection of security vulnerabilities.

Combinatorial Security Testing (CST)
- Parameters and values provide abstract models of attacks
- Generated test sets provide 100% coverage of t-way parameter value combinations.
- Automated test set generation, execution and evaluation via dedicated test oracle.

Technical Challenges
- Generation of minimal t-way test sets is a hard combinatorial optimization problem.
- Modelling of parameters, values and constraints is domain-specific.
- Deploy CST to all application layers of information security.

Cross-Site Scripting (XSS)
- **Vulnerability**: Response from web server contains parts of unsufficently sanitized user input.
- **Threat**: Attacker can execute malicious JavaScript.
- **Goal**: Automatically generate XSS attack vectors for testing purposes.
- **Targets**: HTTP parameters of web applications.
- **Model**: Parameters map to parts of the URL.
- **Example**: `<script>` `onLoad` `</script>`.

Combinatorial Analysis of XSS Vulnerabilities
- XSS attack vectors generated with CST.
- Successful vectors are analyzed for their combinatorial structure.
- Identification of XSS-inducing combinations provides insights.
- Approach evaluated against four sanitization functions from the Web Application Vulnerability Scanner Evaluation Project (WAVSEP).
- Results show effective identification of XSS-inducing combinations.

Fault-driven Combinatorial Process for Model Evolution in XSS
- Knowledge base (KB) contains model for XSS.
- Iterative evolvement of KB for XSS security testing of web applications.
- KB gives rise to attack strings for exploiting XSS vulnerabilities.
- Testing results are annotated and added back to KB.
- Process uses BEN tool internally.
- Increases capabilities of KB for subsequently requested attack models.

Combinatorial Fault Analysis (FLA)

Theory
- A combination is called suspicious if it appears only in a failing test case.
- A combination c is failure-inducing if any test f in which c is contained, fails.
- Identification of minimal failure-inducing combinations.
- Active research area in CT.

BEN Tool
- CT-based fault analysis tool.
- Input: executed t-way test set with pass/fail assignments.
- Output: ranking of combinations in terms of their likelihood to be failure-inducing.
- Adaptive approach: small number of additional tests might required.
- Written in Java and provides both GUI and CLI interfaces.