Combinatorial Fault Localization for Web Security Testing

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

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

SBA Research

MATRIS

Combinatorial Testing & Combinatorial Fault Analysis

Motivation

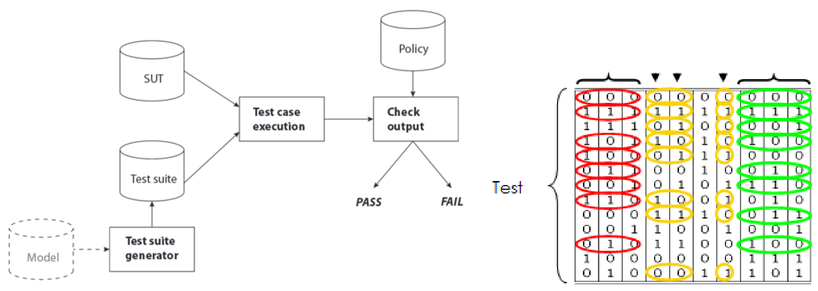
- We cannot test everything.
- Exhaustive search of problem space increases time needed exponentially.
- Automated detection of security vulnerabilities.

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.

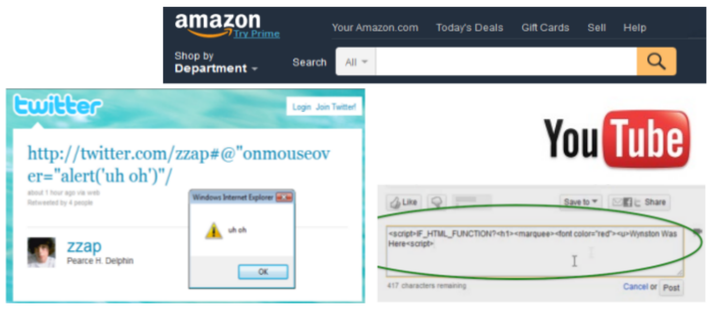
Technical Challenges

- 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 unsufficiently 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**: `<scr<script> ``> onLoad(;\>.`



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.

JSO	WS1	INT	WS2	EVH	WS3	PAY	WS4	PAS	WS5	JSE
"><script>	␣	';	␣	onError=	␣	alert(1)	␣	'>	␣	\>
"><script>	␣	'>	␣	onError=	␣	alert(1)	␣	'>	␣	\>
"><script>	␣	'>	␣	onError=	␣	alert(1)	␣	')	␣	\>
"><script>	␣	€	␣	onError=	␣	alert(1)	␣	'>	␣	\>
"><script>	␣	€	␣	onError=	␣	alert(1)	␣	')	␣	\>
"><script>	␣	'>>	␣	onError=	␣	alert(1)	␣	')	␣	\>
"><script>	␣	';	␣	onError=	␣	src="invalid"	␣	'>	␣	\>
"><script>	␣	'>	␣	onError=	␣	src="invalid"	␣	'>	␣	\>
"><script>	␣	'>	␣	onError=	␣	src="invalid"	␣	')	␣	\>
"><script>	␣	€	␣	onError=	␣	src="invalid"	␣	'>	␣	\>

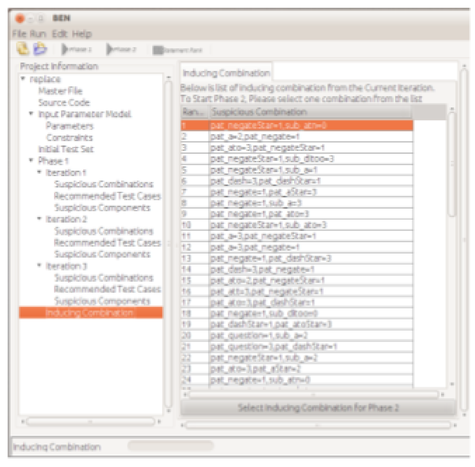
Combinatorial Fault Analysis (FLA)

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.

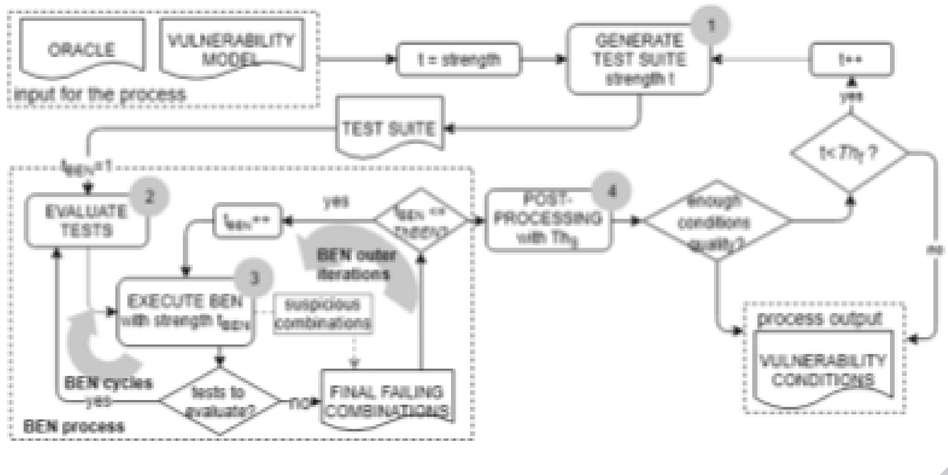
BEN Tool

- 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.



Fault-driven Combinatorial Process for Model Evolution in XSS

- Knowledge base (KB) contais 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 annoted and added back to KB.
- Process uses BEN tool internally.
- Increases capabilites of KB for subsequently requested attack models.



Bernhard Garn, Marco Radavelli, Angelo Gargantini, Manuel Leithner, and Dimitris E. Simos. A fault-driven combinatorial process for model evolution in xss vulnerability detection. In Franz Wotawa, Gerhard Friedrich, Ingo Pill, Roxane Koitz-Hristov, and Moonis Ali, editors, *Advances and Trends in Artificial Intelligence. From Theory to Practice*, pages 207–215, 2019.
Dimitris E. Simos, Kristoffer Kleine, Laleh Shikh Gholamhossein Ghandehari, Bernhard Garn, and Yu Lei. A combinatorial approach to analyzing cross-site scripting (xss) vulnerabilities in web application security testing. In Franz Wotawa, Mihai Nica, and Natalia Kushik, editors, *Testing Software and Systems*, pages 70–85, 2016.

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.