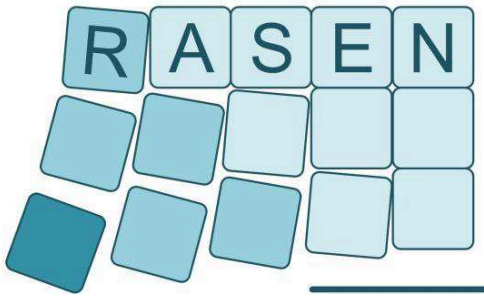
RISK 2015

3rd International Workshop on Risk Assessment and Risk-driven Testing

15.06.15

Berlin - Germany



Compositional Risk Assessment and Security Testing of Networked Systems

Risk-Driven Vulnerability Testing:
Results from eHealth Experiments using Patterns and Model-Based Approach

A. Vernotte, C. Botea, B. Legeard,
A. Molnar, and F. Peureux

femto-st SCIENCES & TECHNOLOGIES DISC

infoworld CONNECTING HEALTHCARE

SEVENTH FRAMEWORK PROGRAMME

Outline

- Context and motivation
- Case Study: MediPedia The Medical Encyclopedia
- Pattern-driven and Model-based Vulnerability Testing
- Experimentation results
- Discussion and conclusion

Context and Motivation

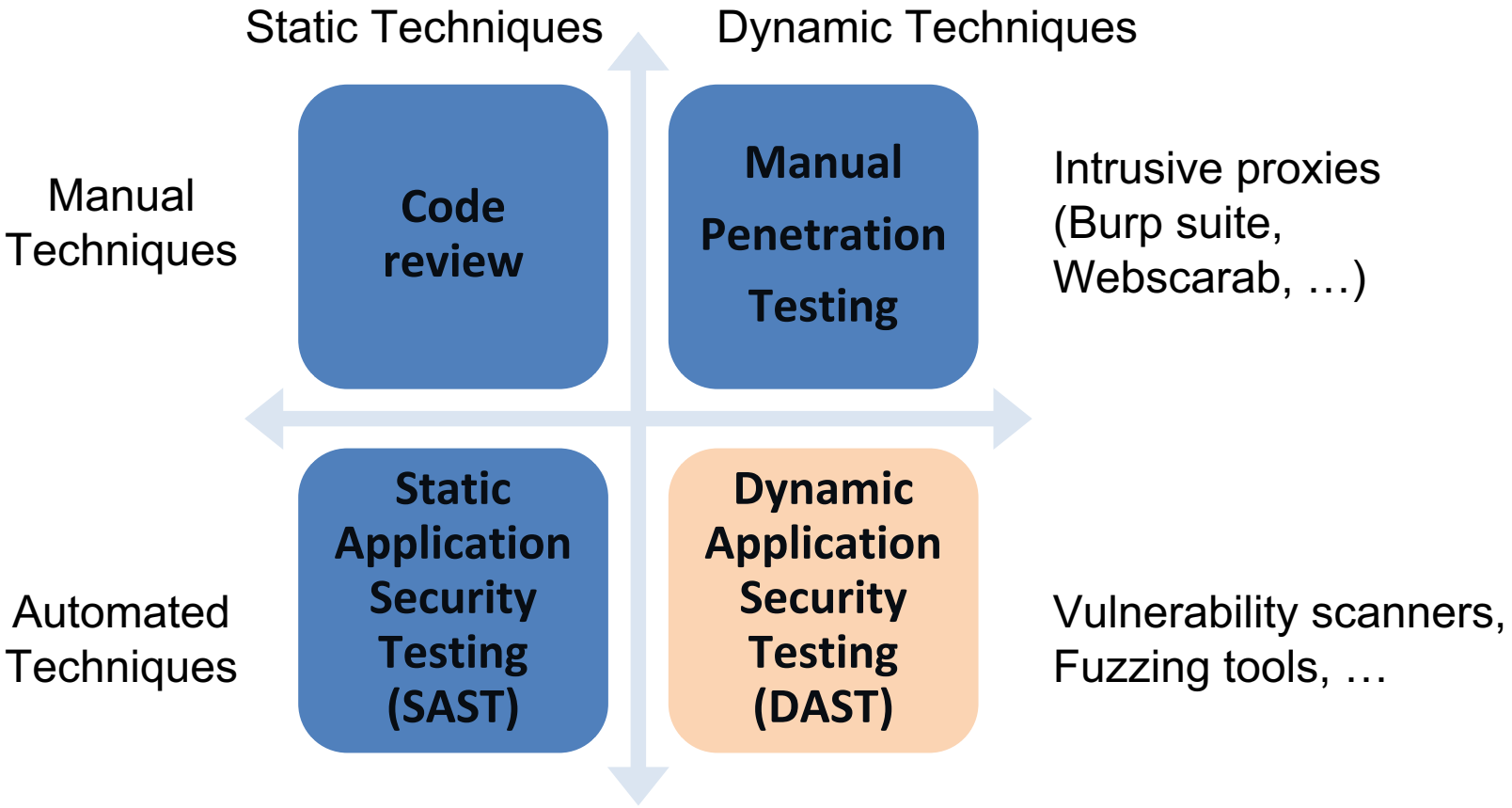
- Continued growth and complexity of the internet:
  - increasing ubiquity of uses (eHealth, eBanking, eCommerce, social...)
  - increasing combination of technologies (server, client)

Maintaining security is a challenging and critical task

- Focus put on Web applications vulnerabilities:
  - Cross-Site Scripting
  - SQL Injections
  - Cross-Site Request Forgery
  - ... (see OWASP Top 10[1] – CWE/SANS TOP 25[2])

1. https://www.owasp.org/index.php/Top_10_2013
2.http://cwe.mitre.org/top25/

Security testing: State of the practice



Existing DAST Approaches

Manual Penetration Testing

- Performed by specialists (Pentesters, Security Testing Engineer)
- Use of multifunction toolboxes (Burp, Metasploit, Fuzzing, …)
- Based on insights and experience
- Being systematic is challenging (compromise between available time / risk)

Automated Testing / Scanners

- Point-and-shoot solutions
- Efficient for a lot of vulnerability types
- Struggle when it comes to complex and logical vulnerability types
- Crawling often misses parts of an application :
  - false positives
  - false negatives

Objectives of the PMVT approach

- To provide a systematic guidance for DAST techniques from risk assessment
- To automate test case derivation and execution using model-based security testing techniques
- To support compositional analysis to manage large scale networked system in complex environments

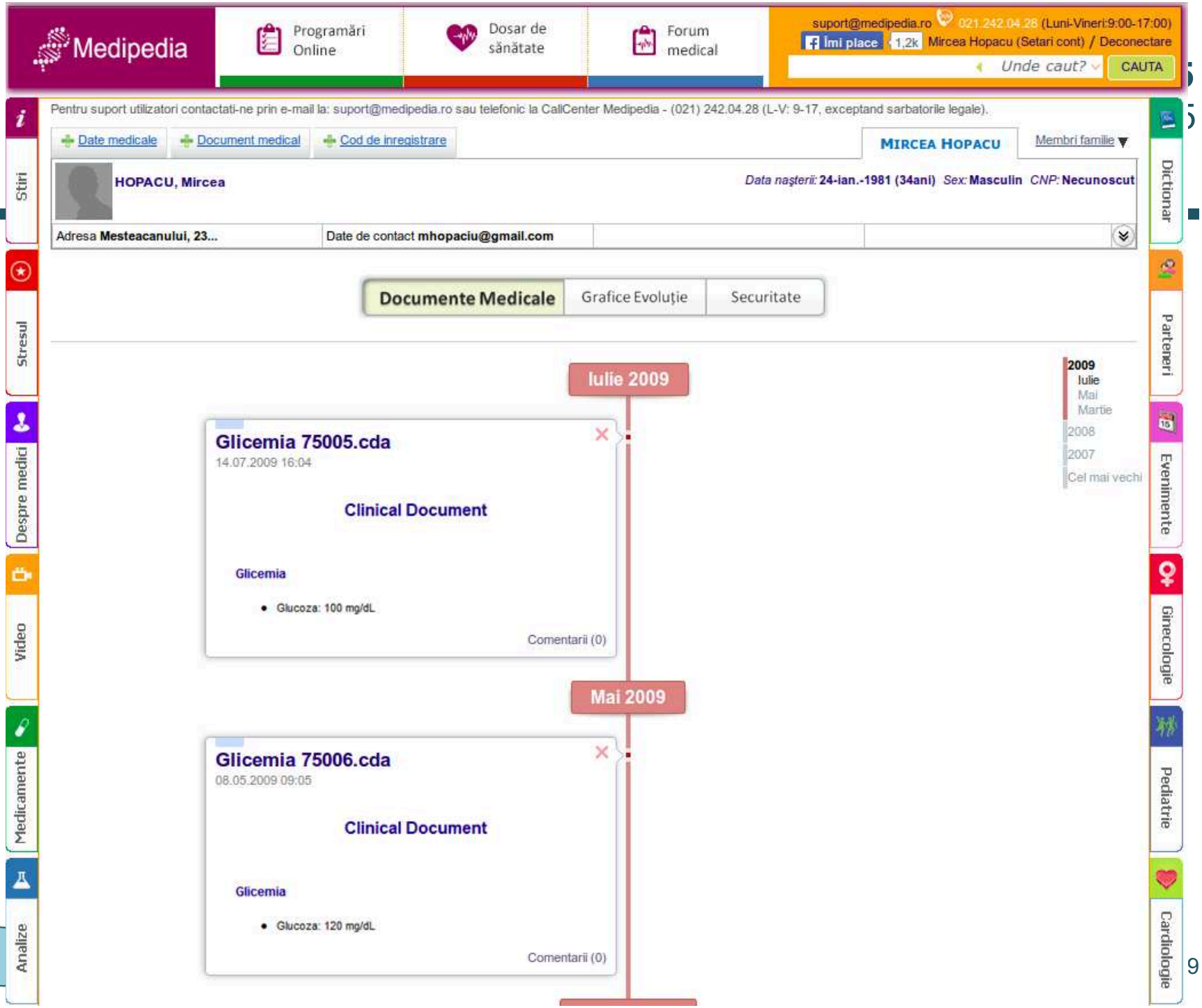
Use Case: MediPedia

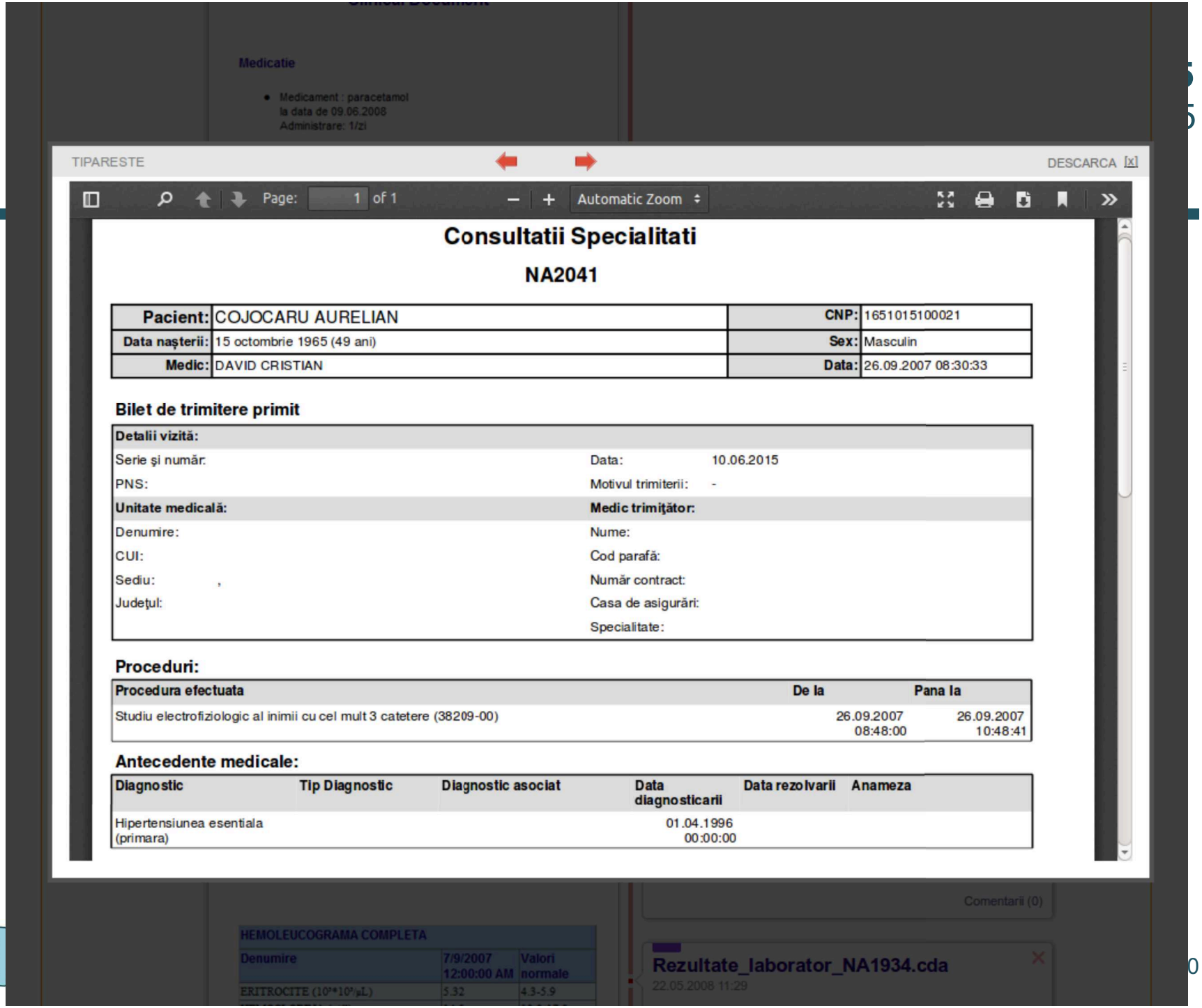
The Medical Encyclopedia

- Complex eHealth Romanian web portal developed by Info Worl (http://www.medipedia.ro)
- 125k+ weekly visits, 36k+ active accounts
- Stores highly sensitive personal data
- Selection of features:
  - Users can manage their electronic health records
  - Integrated with nation-wide Medcenter labs (analyses are automatically uploaded to user's account)
  - Allows scheduling appointments
  - Forum for interacting with peers and medical practitioners

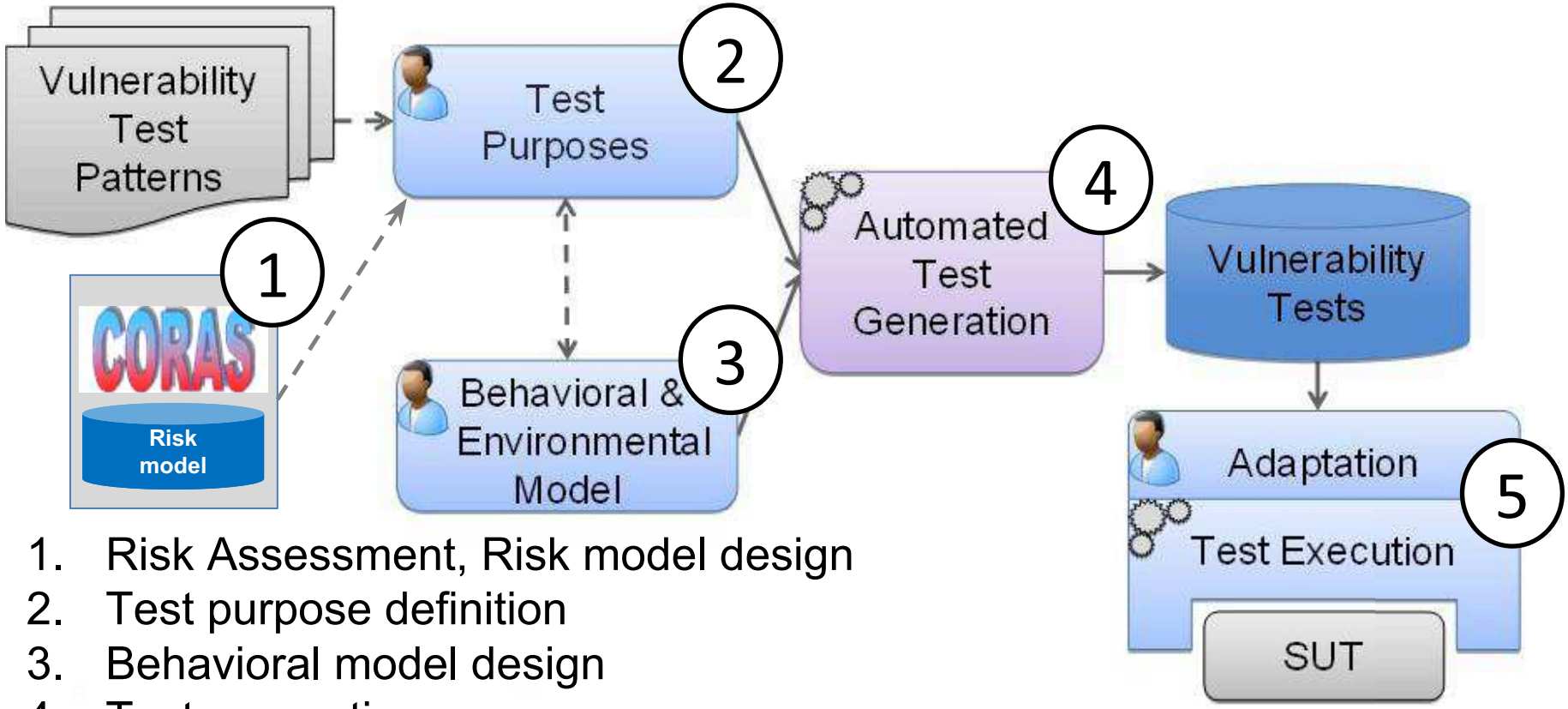
Use Case: MediPedia

The Medical Encyclopedia


Medipedia
Programări Online
Dosar de sănătate
Forum medical
suport@medipedia.ro 021.242.04.28 (Luni-Vineri:9:00-17:00)
Îmi place 1,2k Mircea Hopacu (Setari cont) / Deconectare
Unde caut?
CAUTA
Pentru suport utilizatori contactati-ne prin e-mail la: suport@medipedia.ro sau telefonic la CallCenter Medipedia - (021) 242.04.28 (L-V: 9-17, exceptand sarbatorile legale).
Date medicale
Document medical
Cod de inregistrare
MIRCEA HOPACU
Membri familie
HOPACU, Mircea
Data nașterii: 24-ian.-1981 (34ani) Sex: Masculin CNP: Necunoscut
Adresa Mesteacanului, 23...
Date de contact mhopaciu@gmail.com
Documente Medicale
Grafice Evoluție
Securitate
Iulie 2009
Glicemia 75005.cda
14.07.2009 16:04
Clinical Document
Glicemia
Glucoza: 100 mg/dL
Comentarii (0)
Mai 2009
Glicemia 75006.cda
08.05.2009 09:05
Clinical Document
Glicemia
Glucoza: 120 mg/dL
Comentarii (0)
2009
Iulie
Mai
Martie
2008
2007
Cel mai vechi
Știri
Stresul
Despre medici
Video
Medicamente
Analize
Dictionar
Parteneri
Evenimente
Ginecologie
Pediatrie
Cardiologie

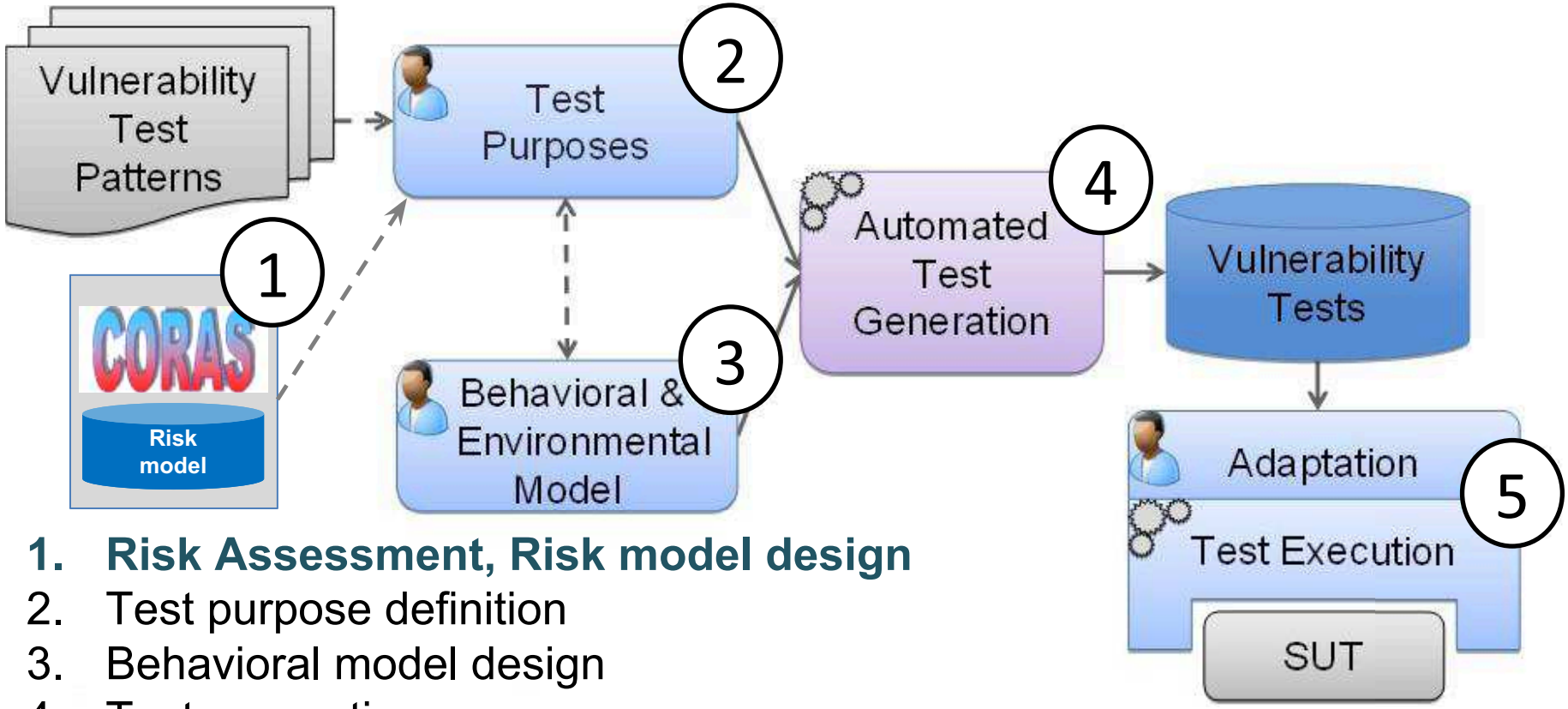

Medicatie
Medicament : paracetamol
la data de 09.06.2008
Administrare: 1/zi
TIPARESTE
DESCARCA [x]
Page: 1 of 1
Automatic Zoom
Consultatii Specialitati
NA2041
Pacient: COJOCARU AURELIAN
CNP: 1651015100021
Data nașterii: 15 octombrie 1965 (49 ani)
Sex: Masculin
Medic: DAVID CRISTIAN
Data: 26.09.2007 08:30:33
Bilet de trimitere primit
Detalii vizită:
Serie și număr:
Data: 10.06.2015
PNS:
Motivul trimiterii: -
Unitate medicală:
Medic trimițător:
Denumire:
Nume:
CUI:
Cod parafă:
Sediu:
Număr contract:
Județul:
Casa de asigurări:
Specialitate:
Proceduri:
Procedura efectuata
De la
Pana la
Studiu electrofiziologic al inimii cu cel mult 3 catetere (38209-00)
26.09.2007 08:48:00
26.09.2007 10:48:41
Antecedente medicale:
Diagnostic
Tip Diagnostic
Diagnostic asociat
Data diagnosticarii
Data rezolvarii
Anameza
Hipertensiunea esentiala (primara)
01.04.1996 00:00:00
Comentarii (0)
HEMOLEUCOGRAMA COMPLETA
Denumire
7/9/2007 12:00:00 AM
Valori normale
ERITROCITE (10^6*10^3/µL)
5.32
4.3-5.9
Rezultate_laborator_NA1934.cda
22.05.2008 11:29

Pattern-driven and Model-based Vulnerability Testing Process



1. Risk Assessment, Risk model design
2. Test purpose definition
3. Behavioral model design
4. Test generation
5. Concretization, test execution and verdict assignment

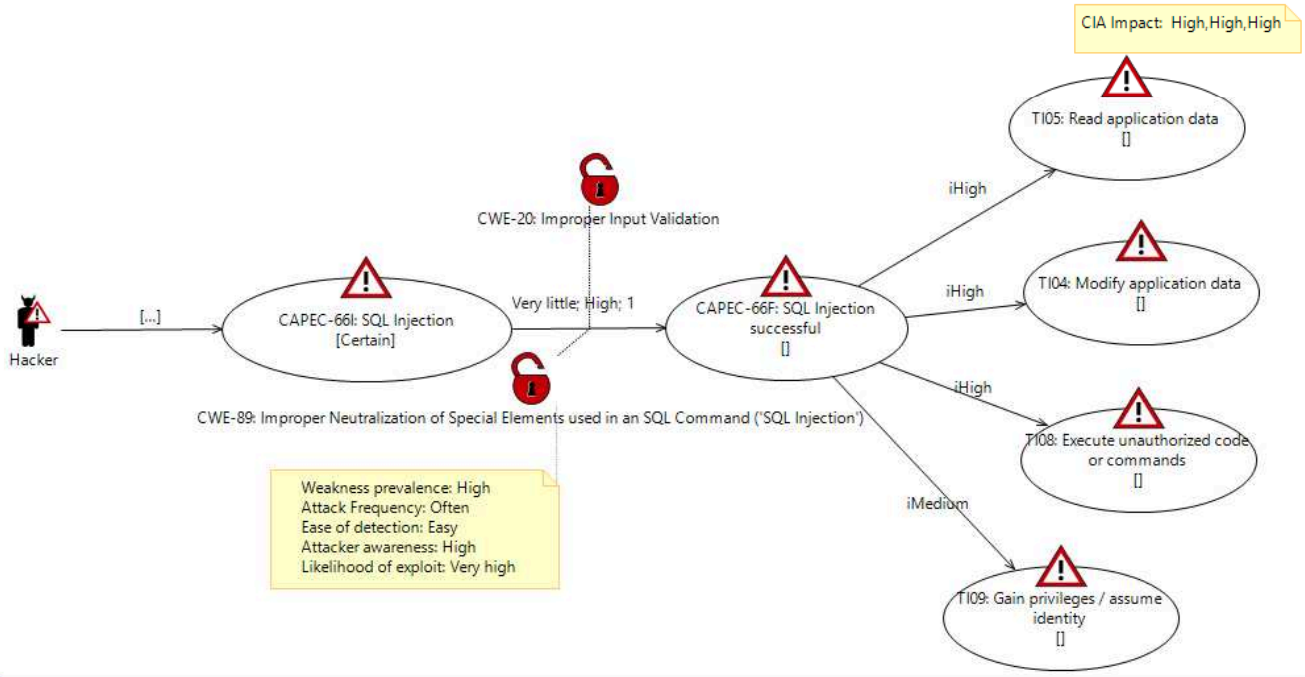
1. Risk Assessment Inputs



1. **Risk Assessment, Risk model design**
2. Test purpose definition
3. Behavioral model design
4. Test generation
5. Concretization, test execution and verdict assignment

Risk Identification and Prioritization

- Using the CORAS approach to provide test objectives identification and prioritization based on the risk analysis:
  - Selection of the test purposes from identified threat scenarios
  - Prioritization of the test purposes regarding risk assessment



Risk Analysis of MediPedia

- Based on a risk analysis of Medipedia using CORAS, we were able to orientate Vulnerability Testing towards five types of flaws:
  - SQL Injection
  - Cross-Site Scripting
  - Cross-Site Request Forgery
  - Auth Bypass & Privilege Escalation
  - Insecure Direct Object Reference
- The present experimental report and presentation focus on the first three mentioned vulnerability types: XSS, SQLi, CSRF.

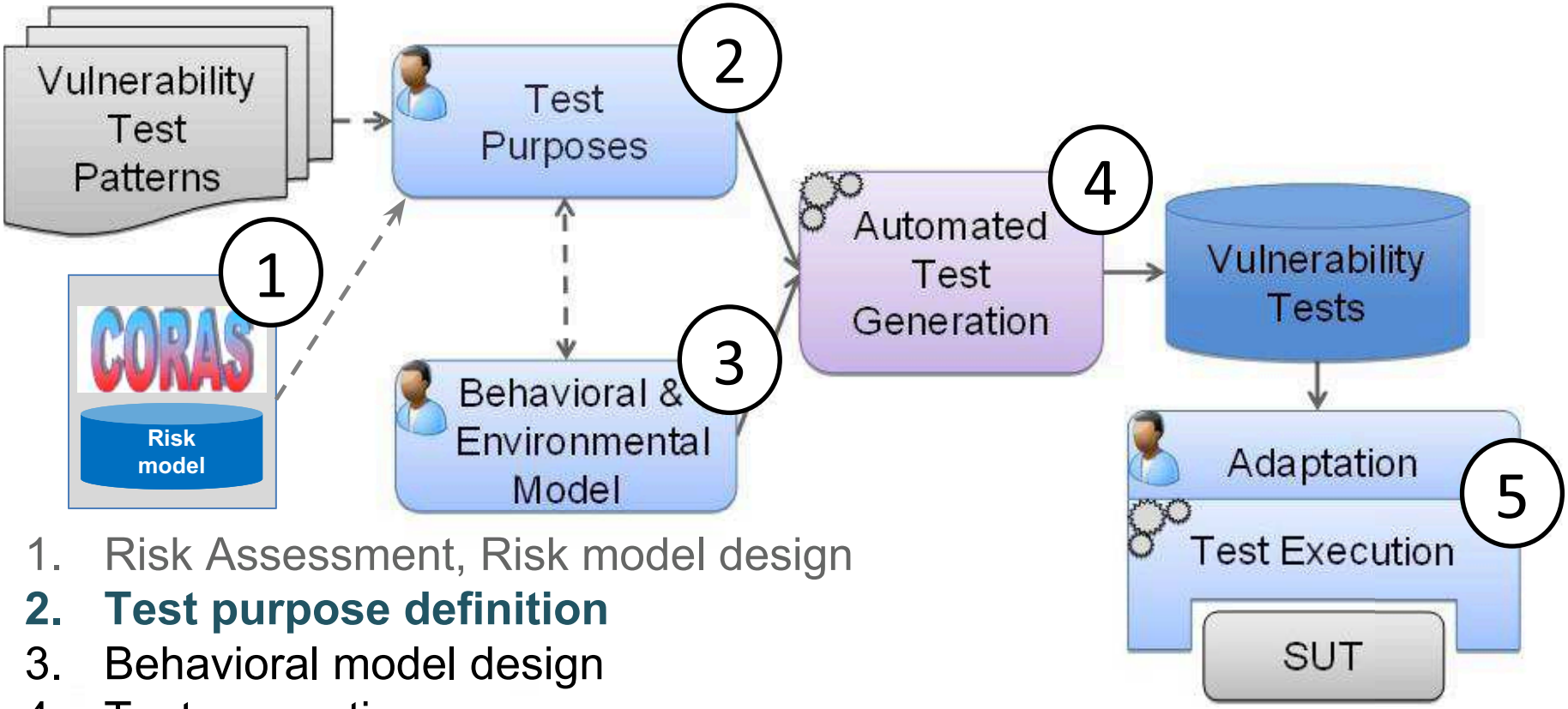
Security Test Patterns

- Security test patterns are typically related to vulnerability catalogues
  - MITRE CWE & CAPEC
  - OWASP Top 10
- Solution
  - one or more **test design technique** and corresponding **strategies,** test **effort** and **effectiveness**
- Test Data
  - instructions for crafting test data
  - references to test data libraries or generators
- Tools
  - references tools that can be used to generate and execute such test cases

Pattern Name	*A meaningful name for the pattern, e.g. the name of the weakness.*	
CWE-ID(s)	*The IDs of a weakness from the Common Weakness Enumeration.*	
Weakness Description	*A high-level description of the weakness.*	
Solution	*How the weakness could be revealed manually.*	
	Test Design Technique	*Test design technique that is able to find the weakness.*
	Test Strategies	*Test strategies specific for a certain test design technique that shall be applied in order to generate test cases for the weakness in question.*
	Effort	*The effort to generate and execute such test cases on a scale with the values 'low', 'medium', and 'high'-*
	Effectiveness	*How effective is the test design technique in finding such a weakness (how many test cases are necessary to find one weakness, how many weaknesses might be missed).*
Description of Test Coverage Items	*Informal description of items to be covered by test cases created on basis of a pattern.*	
Metrics	*Appropriate test and coverage metrics. These will be developed in Task T4.3. This field is omitted within this deliverable.*	
Discussion	*A short discussion on the pitfalls of applying the pattern and the potential impact it has on test design in general and on other patterns applicable to that same context in particular.*	
Test Data	*Actual or references to test data and test data g*	
Tools	*References to tools appropriate for test cas*	
Generalization of	*References to other security test patterns that ar*	
References	*References to OWASP Top 10 weaknesses CWE de*	*CAPEC attack patterns*

Generic

2. Test Purpose Definition



1. Risk Assessment, Risk model design
2. **Test purpose definition**
3. Behavioral model design
4. Test generation
5. Concretization, test execution and verdict assignment

Test Purpose Language

Vulnerability Test Patterns (vTP) are the entry-point of PMVT.

The goal is to translate vTP into a machine-readable language.

➡ **Smartesting Test Purpose Language**[1]:

- Textual language based on regular expressions
- Reasons in term of states to be reached and operations to be called
- Drive the (security) test generation process

1. **J. Botella** et. al., *MBT of Cryptographic Components: Lessons Learned from Experience*, ICST 2013.

Test Purposes for MediPedia

The Medical Encyclopedia

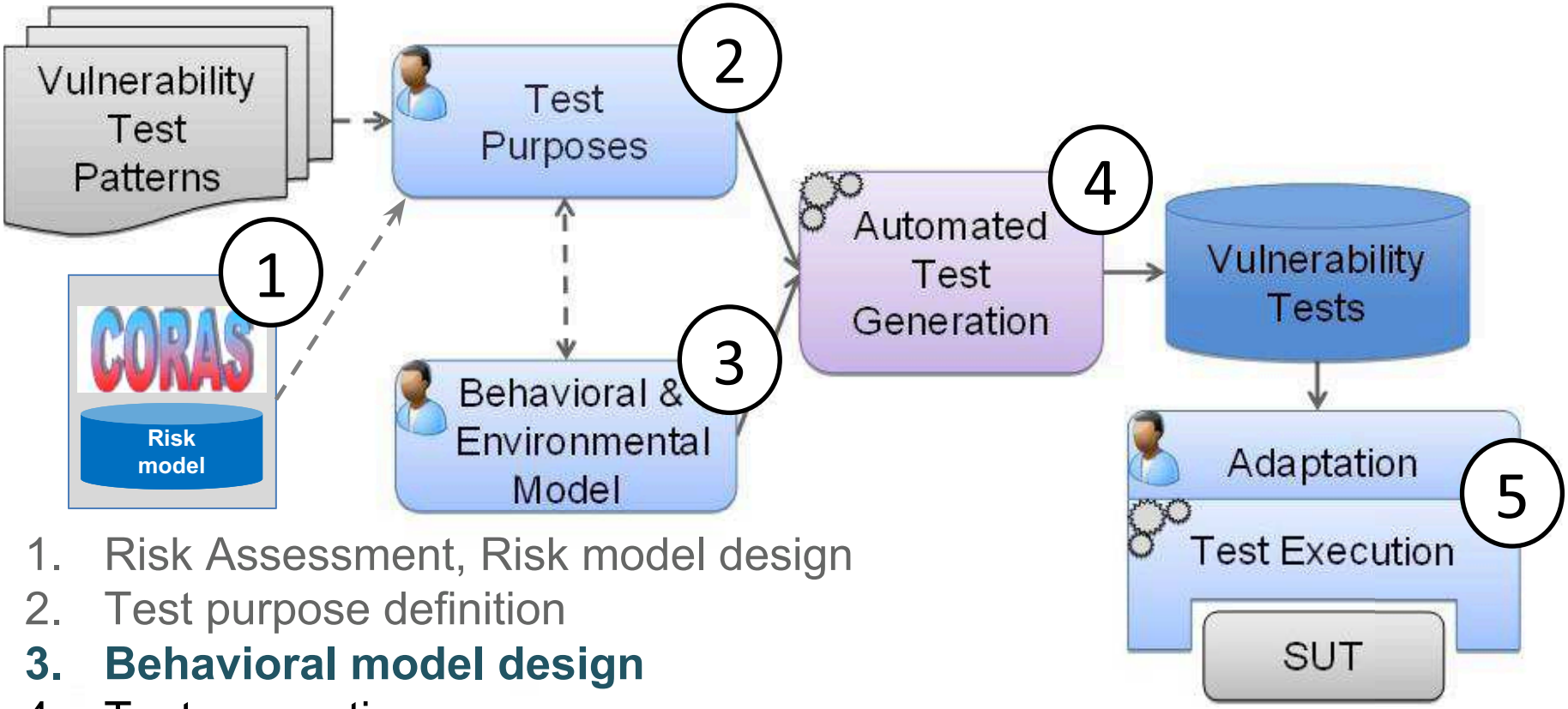
Three test purposes were used to generate test cases for Medipedia:

- Cross-Site Scripting in all its forms
- Standard SQL injection (first and second order)
- Cross-Site Request Forgeries

Test purpose for XSS

```
for_each instance $page from
"Page.allInstances()->select(p:Page|not(p.all_outputs->isEmpty()))" on_instance sut,
for_each instance $param from "self.all_outputs" on_instance $page,
use any_operation any_number_of_times to_reach
 "WackPick.allInstances()->any(true).webAppStructure.ongoingAction.all_inputs->exists(d:Data|d=self)"
on_instance $param
 then use threat.injectXSS($param)
 then use any_operation any_number_of_times to_reach
 "WackPick.allInstances()->any(true).webAppStructure.ongoingAction.oclIsUndefined()
and WackPick.allInstances()->any(true).webAppStructure.current_page=self" on_instance $page
then use threat.checkXSS()
```

2. Behavioral Model Design

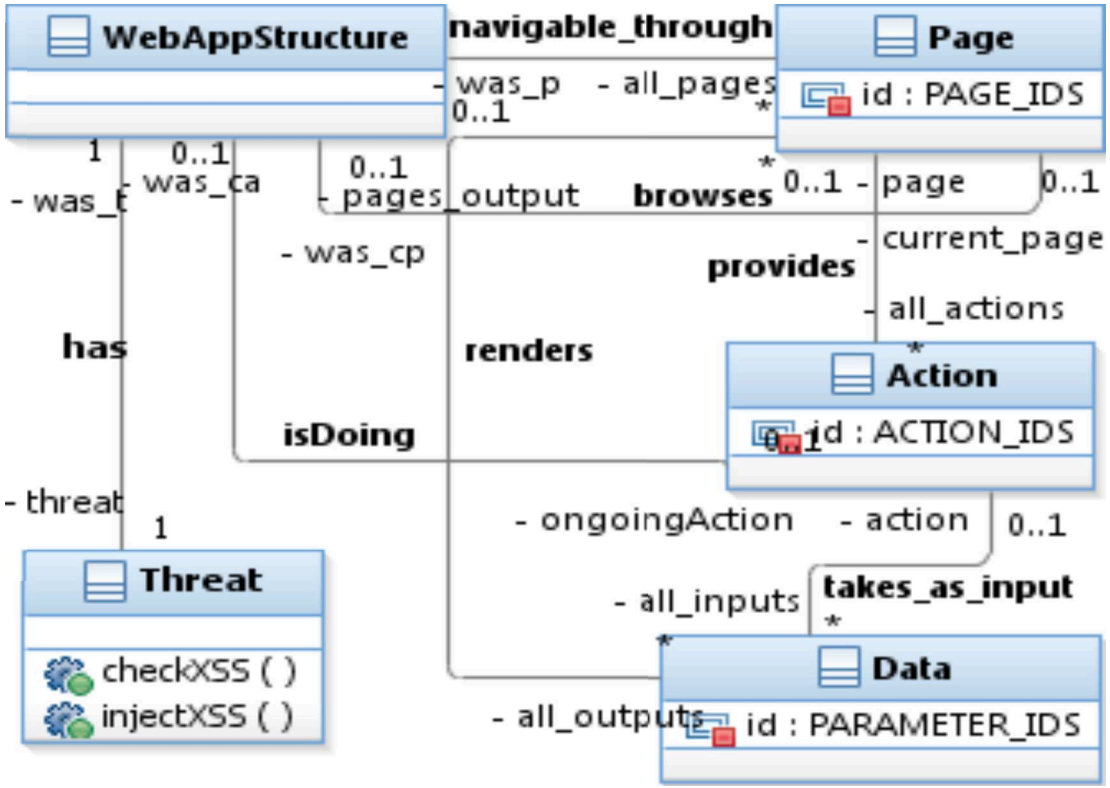


1. Risk Assessment, Risk model design
2. Test purpose definition
3. **Behavioral model design**
4. Test generation
5. Concretization, test execution and verdict assignment

Behavioral Model Design

Behavioral modeling notation is based on UML metamodel:

- **Class diagrams** specify the static structure (points of control and observation)
- **Object diagrams** specify concrete business entities
- **State diagrams** graphically describe its behavioural characteristics



Modeling of MediPedia using DSML

The Medipedia model contains:

- 25 pages
- 20 actions
- 28 navigation links
- 47 data

All three UML diagrams are generated from a dedicated DSML called DASTML.

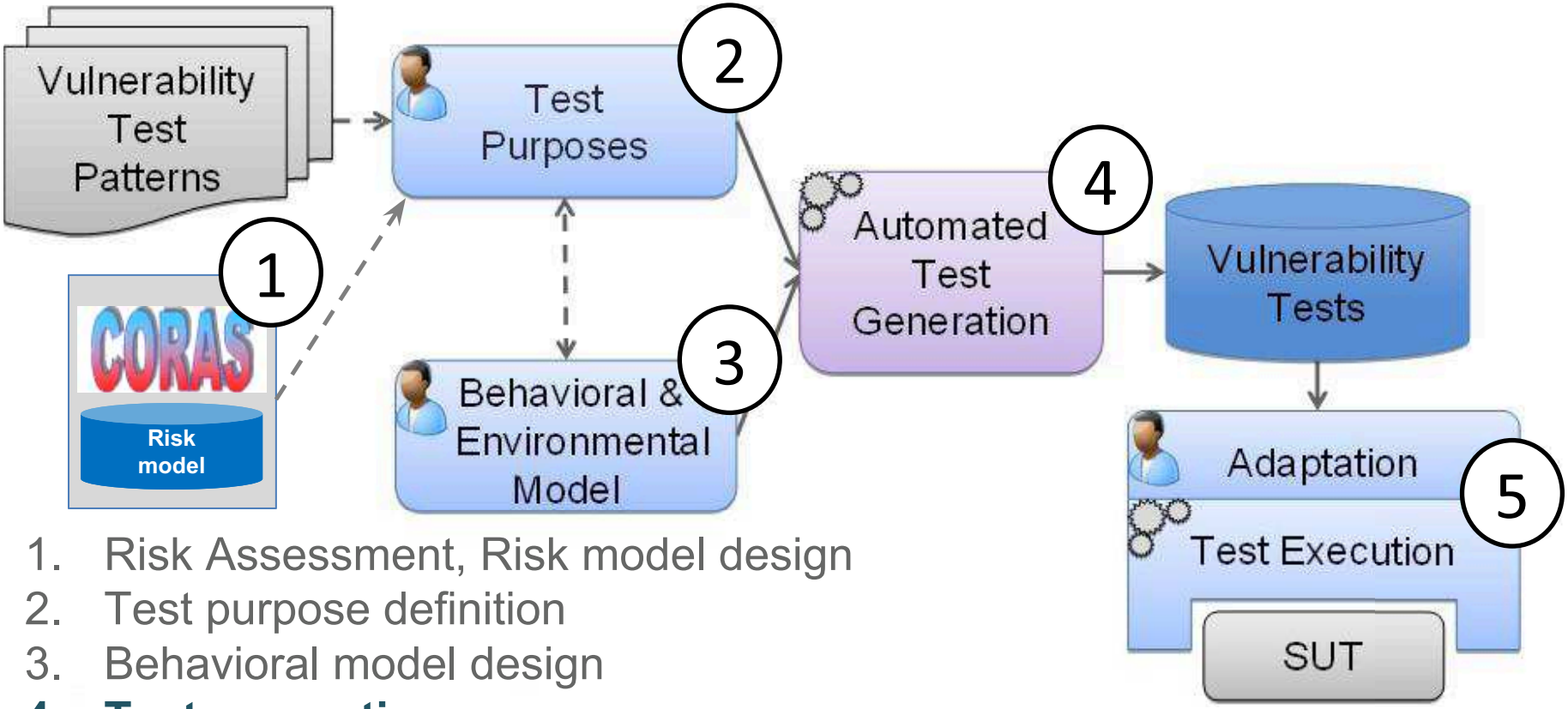
Using DASTML, modeling the targeted Medipedia web pages took approximately **3 hours**.

```
[...]

"PAT_VIEW_TOPIC" {
  ACTIONS {
    "PAT_POST_ANSWER" (
      "PAT_PA_CONTENT" = "PAT_PA_CONTENT_1"
      => {"ANON_VIEW_TOPIC","PAT_VIEW_TOPIC"}
    ),
    "PAT_EDIT_POST" (
      "PAT_PE_CONTENT" = "PAT_PE_CONTENT_1"
      => {"ANON_VIEW_TOPIC","PAT_VIEW_TOPIC"}
    )
  }
  NAVIGATIONS {
    "GOTO_PAT_FORUMS"
      -> "PAT_FORUMS"
  }
}

[...]
```

4. Security Test Generation



1. Risk Assessment, Risk model design
2. Test purpose definition
3. Behavioral model design
4. **Test generation**
5. Concretization, test execution and verdict assignment

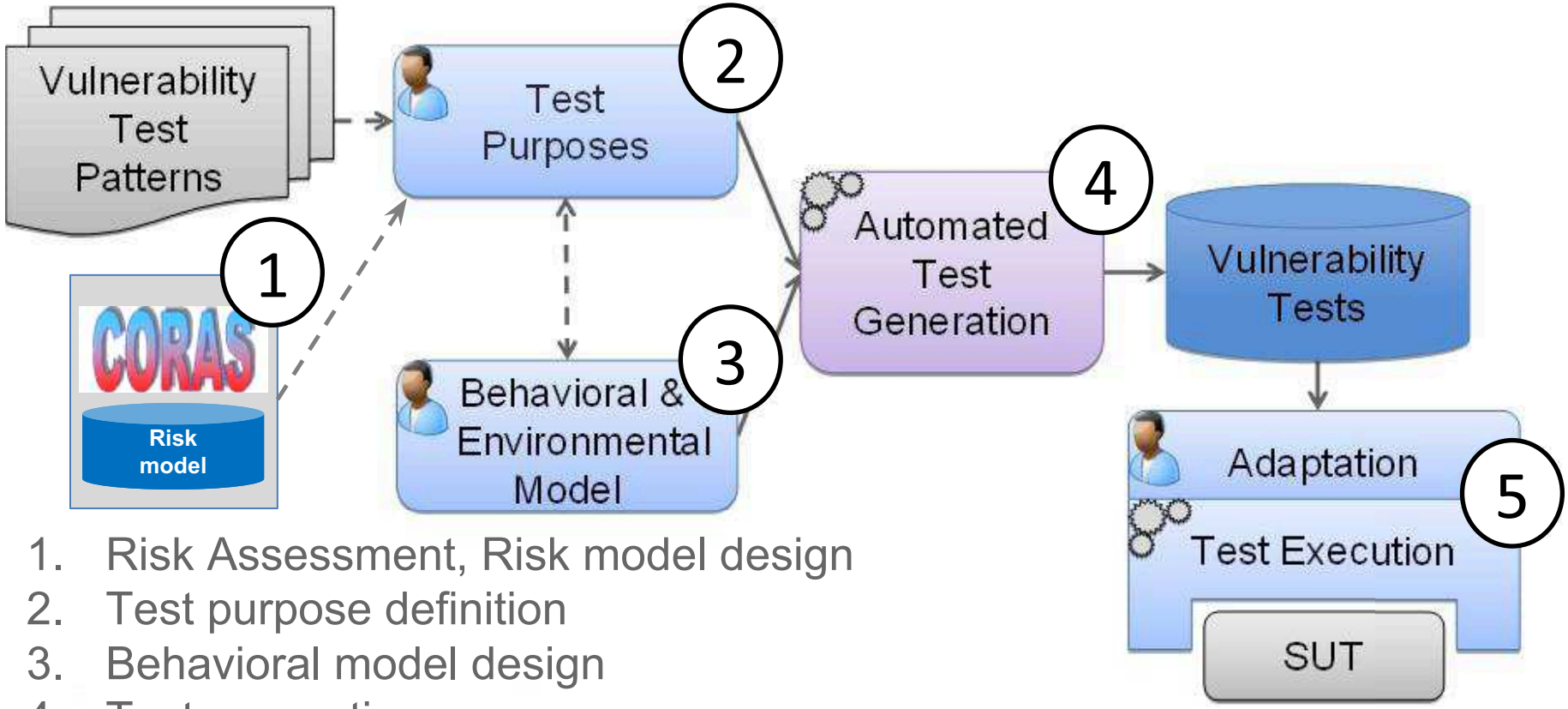
Test generation strategies

Test cases are automatically generated using Smartesting CertifyIt by composing behavioral models and test purposes:

- For one Test Purpose, several (or many) test cases by:
  - Applying usual Test Purpose coverage criteria
  - Applying behavioral fuzzing strategy (Fuzzino) given from Test Patterns
- Risk-based test selection criteria: the highest the priority is, the more combination of iterator values are generated
- Traceability management from security requirements to generated tests is build-in

Result: a suite of abstract vulnerability test cases

5. Test Concretization for Execution



1. Risk Assessment, Risk model design
2. Test purpose definition
3. Behavioral model design
4. Test generation
5. **Concretization, test execution and verdict assignment**

Generation of executable test scripts

JUnit test scripts are automatically generated by CertifyIt using an adaptation layer concretizing abstract data into concrete values:

- For one abstract test case, several (or many) executable test cases by:
  - Using a set of selected test data given from Test Patterns
  - Applying data fuzzing strategy given from Test Patterns
- Traceability management from security requirements to executable tests is build-in

Result: a set of executable vulnerability test scripts

Test results for MediPedia

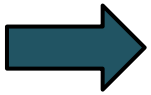
The Medical Encyclopedia

Test generation took **25 minutes**
Test concretization took **6 hours** (including Selenium primitives customization + data mapping)
Test execution took about **50 minutes**

	SQLi	XSS	CSRF
Abstract Test Cases	47	27	11
Attack Vectors	10	105	1
Executable Test Cases	470	2845	11
Detected Vulnerabilities	0	**2**	0
Falses Positives	0	0	**2**
False Negatives	0	**24**	0

Lessons Learnt & Discussion

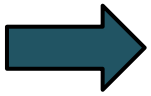
- This Risk-Based Vulnerability Testing technique appears to be **accurate** and **precise**.



Two previously unknown XSS vulnerabilities were found in the forum section of Medipedia.

- It also has its limitations, inherited from MBT:
  - Needed effort to provide Models
  - Needed effort to provide Concrete Data

- Test verdict assignment is not precise enough for CSRF



Two tests came back positive but we were not able to reproduce the attack.

Conclusion and future work

- PMVT approach combines RASEN partners risk assessment and testing techniques:
  - Risk identification and prioritization using CORAS method
  - Import of risk assessment results from CORAS tool into CertifyIt tool
  - Test purpose generation method (CertifyIt)
  - Behavioral and data fuzzing strategies (Fuzzino)
- Extension of security test patterns for risk-based vulnerability test case generation
- Generic formalization of the security test patterns into dedicated test purposes to drive the risk-based test generation
- Promising experimental results on real-life application (undiscovered XSS have been found)

Future investigations:

- Definition of more accurate testing strategies regarding risk prioritization
- Extension of security test patterns and related test purposes
- Enhancement of the MBT modeling activity (e.g., by recording and using execution traces)
- Improvement of the tool integration (especially Test Purpose / fuzzing)
- Improvement of the verdict assignment in order to avoid false positives (cf. CSRF detection)

Thank you for your attention!

RISK 2015
15.06.2015
Berlin

Questions and Comments?