Data Security, Privacy and Patient Safety in the 21st Century

06-08 APRIL 2016
Med@Tel
LUXEMBOURG
BY ISFTEH

Hans de Raad

Medetel 2016

OpenNovations
by DevHdR

info@hcderaad.nl
www.hcderaad.nl

Introduction

- OpenNovations
  - Company of Hans de Raad
  - Freelance, but not alone
- Specializations
  - Open source and open standards in education, government, healthcare
- Focus on:
  - Information security, privacy, digital sustainability

Security === open source

- Would you run a security testing tool you wouldn't be able to inspect yourself?
- Security testing is not just for finding vulnerabilities, it's about solving them
  - Without proper insight in the issue, that isn't possible

EU Privacy directive

- Liability
  - – Company/organization can be penalized when data-leaks occur
- Jurisdiction
  - – Non-EU cloud services are a problem
    - Safe harbor

From V-model to Agile

- Largescale waterfall types of development are replaced by iterative development processes
  - From **V** to vvvvvvvvv
- These new models introduce opportunities and challenges
  - Release early, release often
  - But how about validation?

Risk based (security) testing approach

- Secure development?
  - Why is this suddenly important and who feels they have something to say about that?
- Testing and development strategies
  - What are TDD and BDD and how do they apply on security?

Risk based (security) testing approach

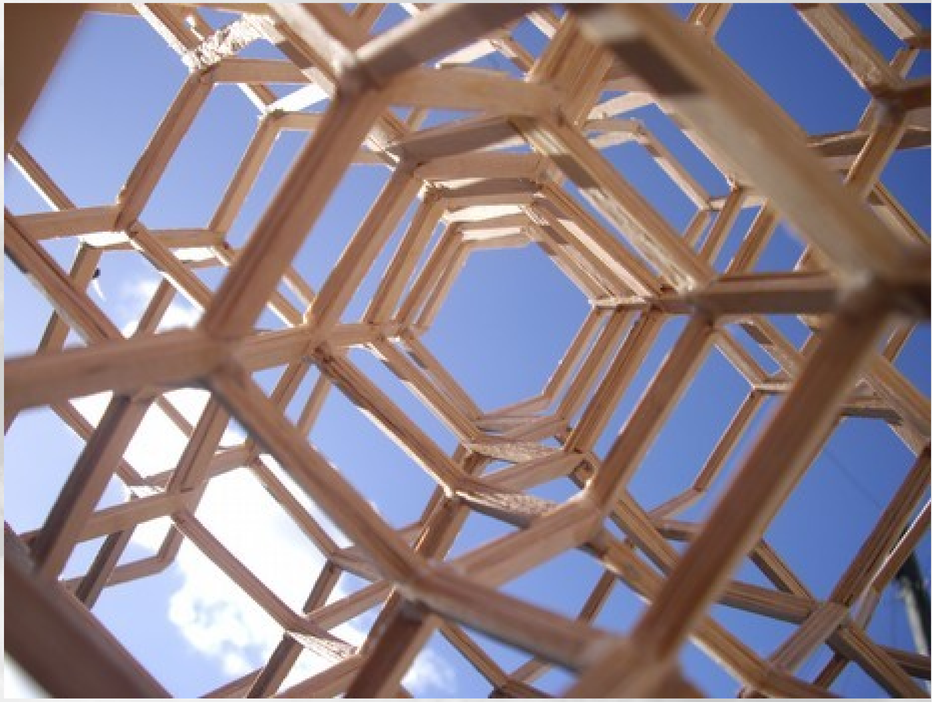
- Testing tools
  - What tools are available, what do they do and how/when to use them?
- Integrating testing tools in development processes / CI
  - How to integrate these tools into the daily working environment?

Secure development (frameworks and standards)

- Quite a lot of separate initiatives, guidelines and standards are available.
  - ISO 27001 / 27002, OWASP, CIP SSD, OSSTMM, ENISA procurement guidelines, etc, etc.
- Applicability depends on business domain and level of security required.
  - What kind of information is processed by an application / process?

Secure development (frameworks and standards)

- It is becoming more mainstream to require security certifications/quality assurances in procurement processes.
  - Both in government and enterprise.
  - Cyber liability insurances often require them as well



OSSTMM

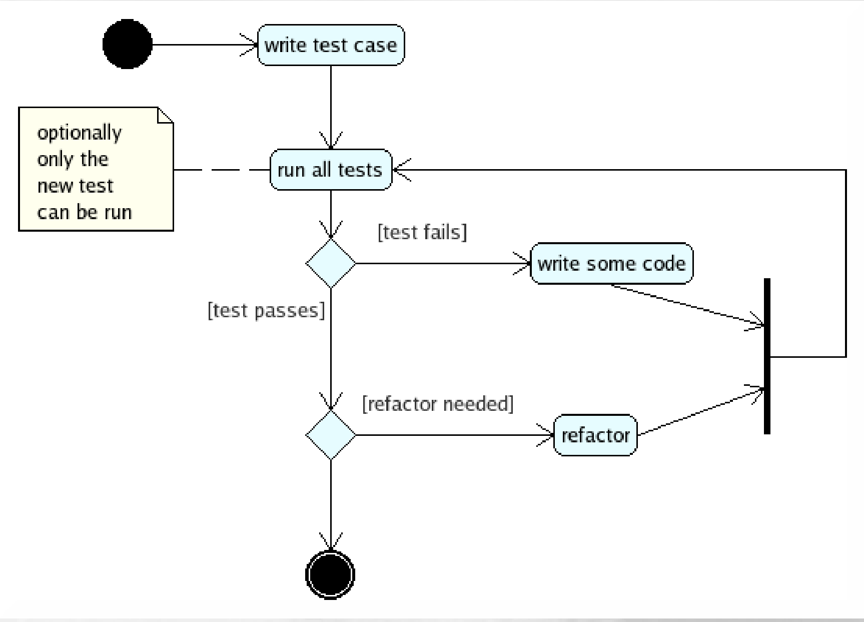
- Open Source Security Testing Methodology Manual
  - A guideline for conducting security analysis for operational security.
  - Aims to provide a scientifically sound and reproducable method for security testing.
  - Aims for “perfect security”, that is both cost effective and sufficient risk coverage with regards to the value of the information in the system/the role of the system.
  - Based on securing the interactions of objects with their surrounding environment (relationships).
    - By itself objects (systems/buildings/etc) can be “black boxes”.

Testing and development strategies

- Test Driven Development: Definition:
  - Test-driven development (TDD) is a software development process that relies on the repetition of a very short development cycle: first the developer writes an (initially failing) automated test case that defines a desired improvement or new function, then produces the minimum amount of code to pass that test, and finally refactors the new code to acceptable standards.

Test Driven Development proces

- Add a test
- Run all tests and see if the new one fails
- Implement (new) feature
- Run tests again
- Refactor code
  if necessary
- Repeat process



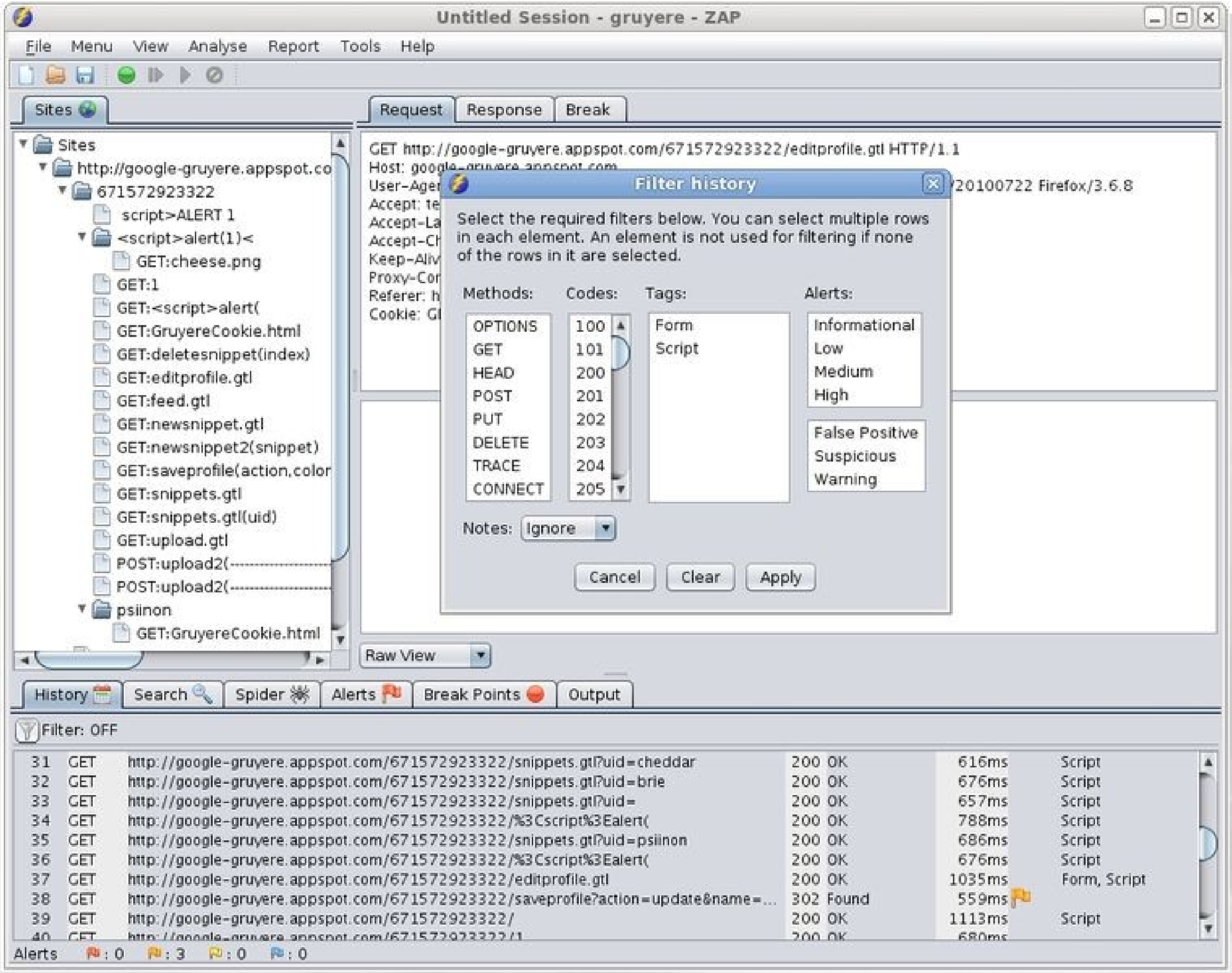
Behavior Driven Development

- Evolution of TDD, focussed on application workflows/functionality rather than programming code/objects.
- Test cases are written in human readable language (Gherkin)
  - As a [User], When I [activate function], Then [Result]
  - Close relation to agile user stories.

Test tooling

- Performance testing
  - PhantomJS (headless browser)
- Code analysis (standards, duplication, technical debt)
  - SonarQube
- Frontend testing
  - Selenium, Behat
- Security testing
  - OWASP Zap, Arachni, Nikto, etc.

Tooling: OWASP ZAP



```
GET http://google-gruyere.appspot.com/671572923322/editprofile.gtl HTTP/1.1
Host: google-gruyere.appspot.com
User-Agen                                                    /20100722 Firefox/3.6.8
Accept: te
Accept-La
Accept-Ch
Keep-Aliv
Proxy-Cor
Referer: h
Cookie: Gl
```

Select the required filters below. You can select multiple rows in each element. An element is not used for filtering if none of the rows in it are selected.

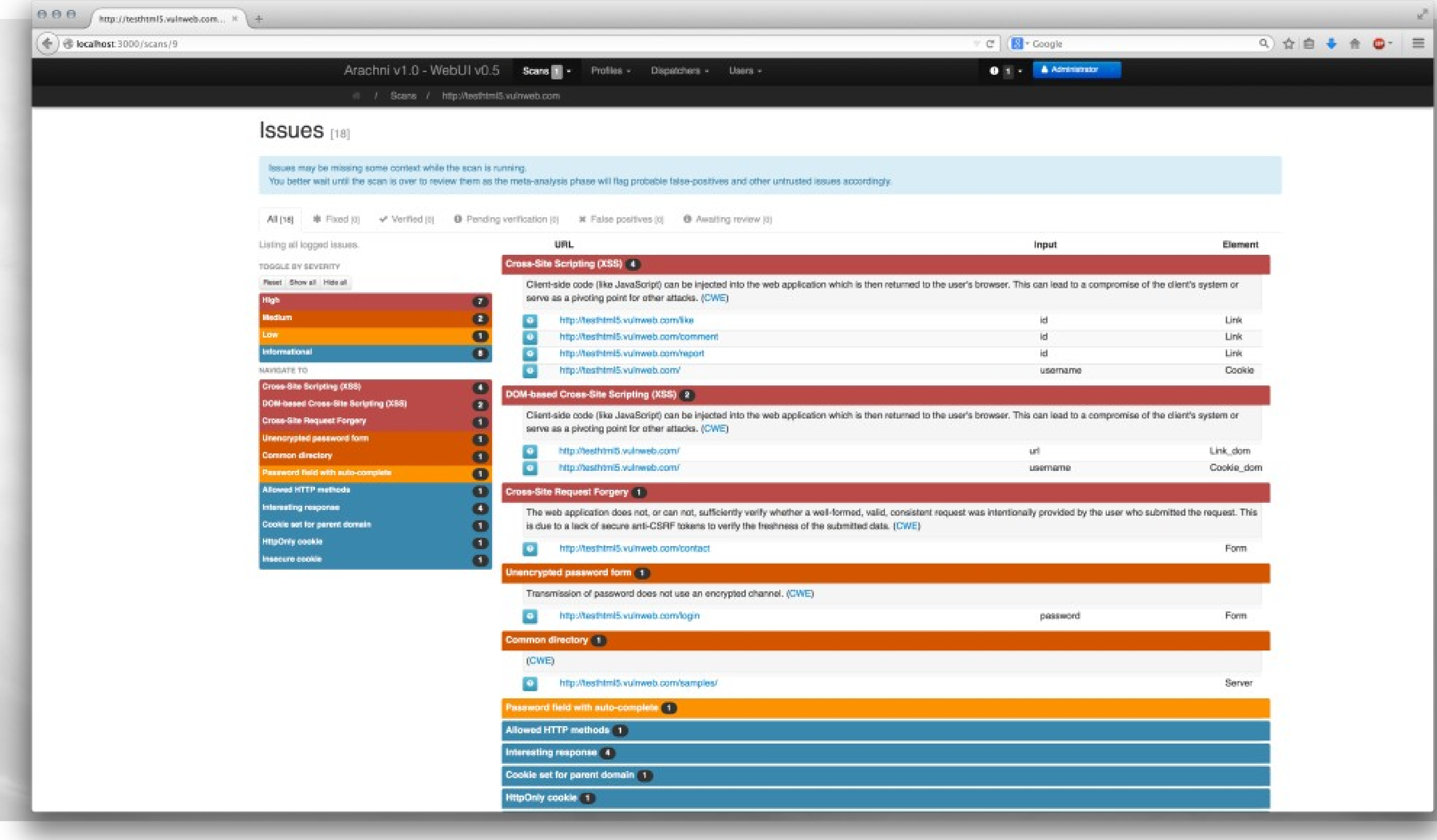
Filter: OFF

```
31  GET  http://google-gruyere.appspot.com/671572923322/snippets.gtl?uid=cheddar        200 OK      616ms  Script
32  GET  http://google-gruyere.appspot.com/671572923322/snippets.gtl?uid=brie           200 OK      676ms  Script
33  GET  http://google-gruyere.appspot.com/671572923322/snippets.gtl?uid=               200 OK      657ms  Script
34  GET  http://google-gruyere.appspot.com/671572923322/%3Cscript%3Ealert(              200 OK      788ms  Script
35  GET  http://google-gruyere.appspot.com/671572923322/snippets.gtl?uid=psiinon        200 OK      686ms  Script
36  GET  http://google-gruyere.appspot.com/671572923322/%3Cscript%3Ealert(              200 OK      676ms  Script
37  GET  http://google-gruyere.appspot.com/671572923322/editprofile.gtl                 200 OK     1035ms  Form, Script
38  GET  http://google-gruyere.appspot.com/671572923322/saveprofile?action=update&name=...  302 Found   559ms
39  GET  http://google-gruyere.appspot.com/671572923322/                               200 OK     1113ms  Script
40  GET  http://google-gruyere.appspot.com/671572923322/1                              200 OK      680ms
```

Alerts : 0 : 3 : 0 : 0

OpenNovations
by DevHdR

Tooling: Arachni



http://testhtml5.vulnweb.com...
localhost:3000/scans/9
Google
Arachni v1.0 - WebUI v0.5
Scans 1
Profiles
Dispatchers
Users
1
Administrator
/ Scans / http://testhtml5.vulnweb.com

Issues [18]

Issues may be missing some context while the scan is running.
You better wait until the scan is over to review them as the meta-analysis phase will flag probable false-positives and other untrusted issues accordingly.

All [18] | ✱ Fixed [0] | ✓ Verified [0] | Pending verification [0] | ✖ False positives [0] | Awaiting review [0]

Listing all logged issues.

TOGGLE BY SEVERITY

Reset | Show all | Hide all

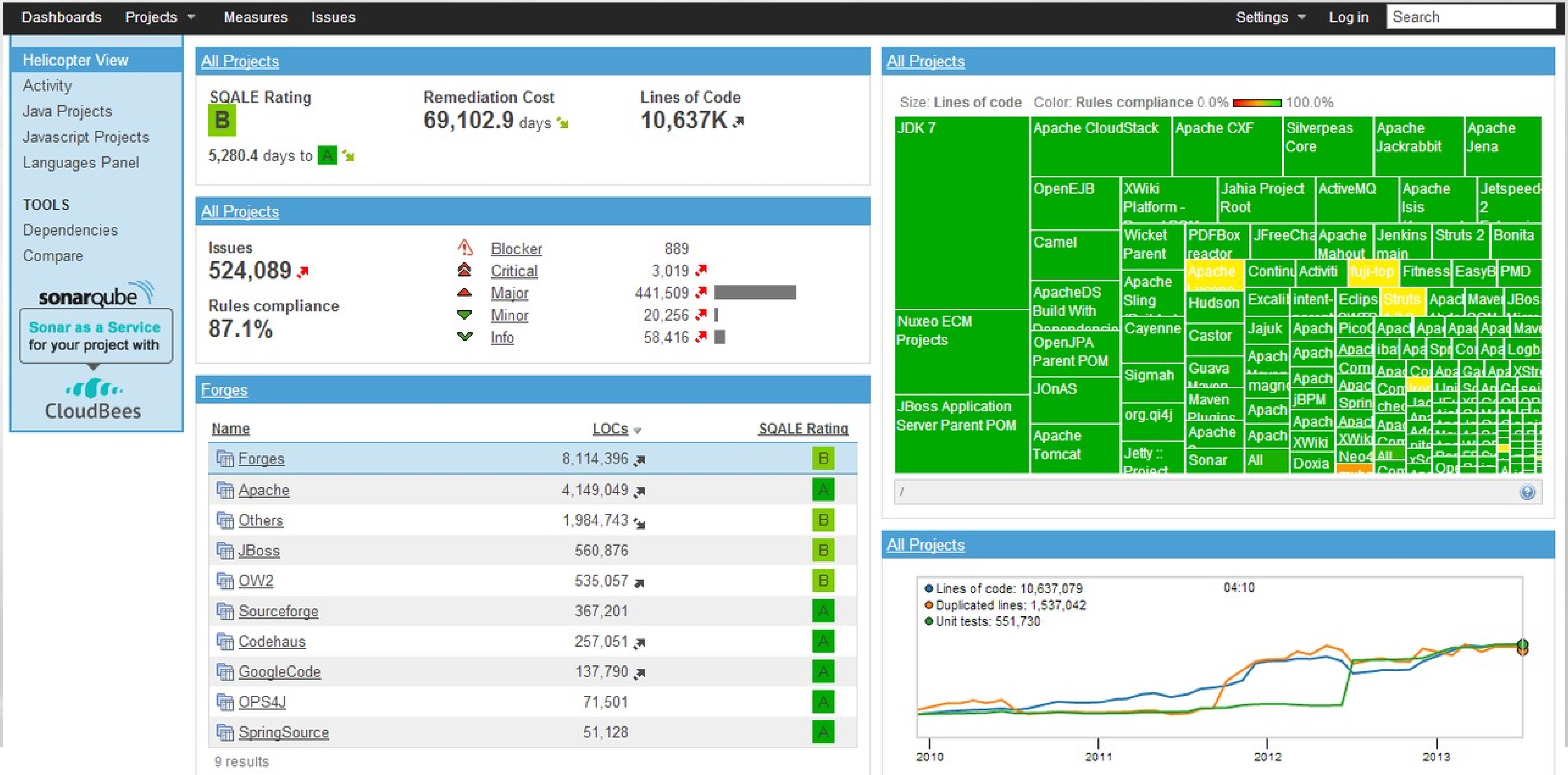
High	7
Medium	2
Low	1
Informational	8

NAVIGATE TO

Cross-Site Scripting (XSS)	4
DOM-based Cross-Site Scripting (XSS)	2
Cross-Site Request Forgery	1
Unencrypted password form	1
Common directory	1
Password field with auto-complete	1
Allowed HTTP methods	1
Interesting response	4
Cookie set for parent domain	1
HttpOnly cookie	1
Insecure cookie	1

URL	Input	Element
Cross-Site Scripting (XSS) 4		
Client-side code (like JavaScript) can be injected into the web application which is then returned to the user's browser. This can lead to a compromise of the client's system or serve as a pivoting point for other attacks. (CWE)		
http://testhtml5.vulnweb.com/like	id	Link
http://testhtml5.vulnweb.com/comment	id	Link
http://testhtml5.vulnweb.com/report	id	Link
http://testhtml5.vulnweb.com/	username	Cookie
DOM-based Cross-Site Scripting (XSS) 2		
Client-side code (like JavaScript) can be injected into the web application which is then returned to the user's browser. This can lead to a compromise of the client's system or serve as a pivoting point for other attacks. (CWE)		
http://testhtml5.vulnweb.com/	url	Link_dom
http://testhtml5.vulnweb.com/	username	Cookie_dom
Cross-Site Request Forgery 1		
The web application does not, or can not, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request. This is due to a lack of secure anti-CSRF tokens to verify the freshness of the submitted data. (CWE)		
http://testhtml5.vulnweb.com/contact		Form
Unencrypted password form 1		
Transmission of password does not use an encrypted channel. (CWE)		
http://testhtml5.vulnweb.com/login	password	Form
Common directory 1		
(CWE)		
http://testhtml5.vulnweb.com/samples/		Server
Password field with auto-complete 1		
Allowed HTTP methods 1		
Interesting response 4		
Cookie set for parent domain 1		
HttpOnly cookie 1		

Tooling: SonarQube



Dashboards | Projects ▾ | Measures | Issues | Settings ▾ | Log in | Search

Helicopter View
Activity
Java Projects
Javascript Projects
Languages Panel

TOOLS
Dependencies
Compare

sonarqube
Sonar as a Service
for your project with
CloudBees

All Projects

SQALE Rating: B
5,280.4 days to A

Remediation Cost: 69,102.9 days

Lines of Code: 10,637K

All Projects

Issues: 524,089

Rules compliance: 87.1%

Blocker	889
Critical	3,019
Major	441,509
Minor	20,256
Info	58,416

Forges

Name	LOCs	SQALE Rating
Forges	8,114,396	B
Apache	4,149,049	A
Others	1,984,743	B
JBoss	560,876	B
OW2	535,057	B
Sourceforge	367,201	A
Codehaus	257,051	A
GoogleCode	137,790	A
OPS4J	71,501	A
SpringSource	51,128	A

9 results

All Projects

Size: Lines of code Color: Rules compliance 0.0% 100.0%

All Projects

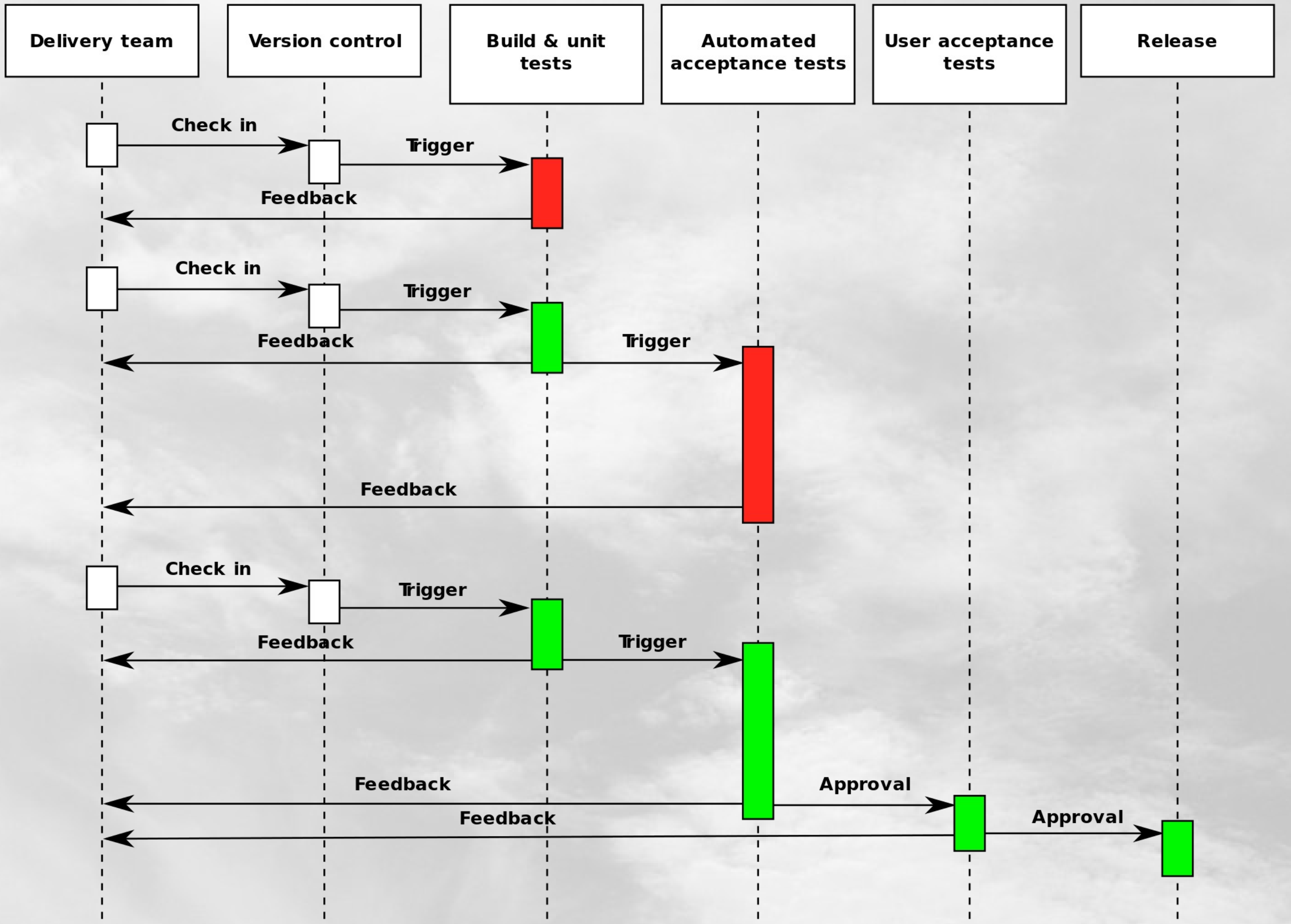
Benefits

- By employing these strategies in your development cycle you can prevent regressions
- Test a very broad spectrum of input options without manually having to resort to slave-labour
- In general, everything that you can repeatedly and reliably test is a good thing.
- But, be aware of pitfalls:
  - False sense of security when coverage is incomplete
  - Always have a second opinion on the test cases
    - Don't “mark your own paper” (or in Dutch the “WC-eend” syndrome)

Continuous integration

- Release early, release often means integrate often
- Source code management, branching strategies
  - Feature development branches, integrate as soon as possible.
- On integration (merging), perform tests
  - Optimal regression prevention. Security issues often originate from regression issues.

Continuous integration and testing



Embed into validation processes

- GAMP (and ISO 17025, etc) require strict (re)validation of software systems
  - IQ, OQ, PQ
  - User acceptance testing, etc
- By embedding automated testing into the development cycle, more focus can go to actual user process testing
  - Regression testing can be performed through automated testing
  - Automated testing can be performed on each change

Questions?

?

Contact

- Hans de Raad
  - OpenNovations
  - www.opennovations.nl
  - E-mail: info@hcderaad.nl