Continuous Security Testing

In a DevOps World

OWASP

The Open Web Application Security Project

About Me

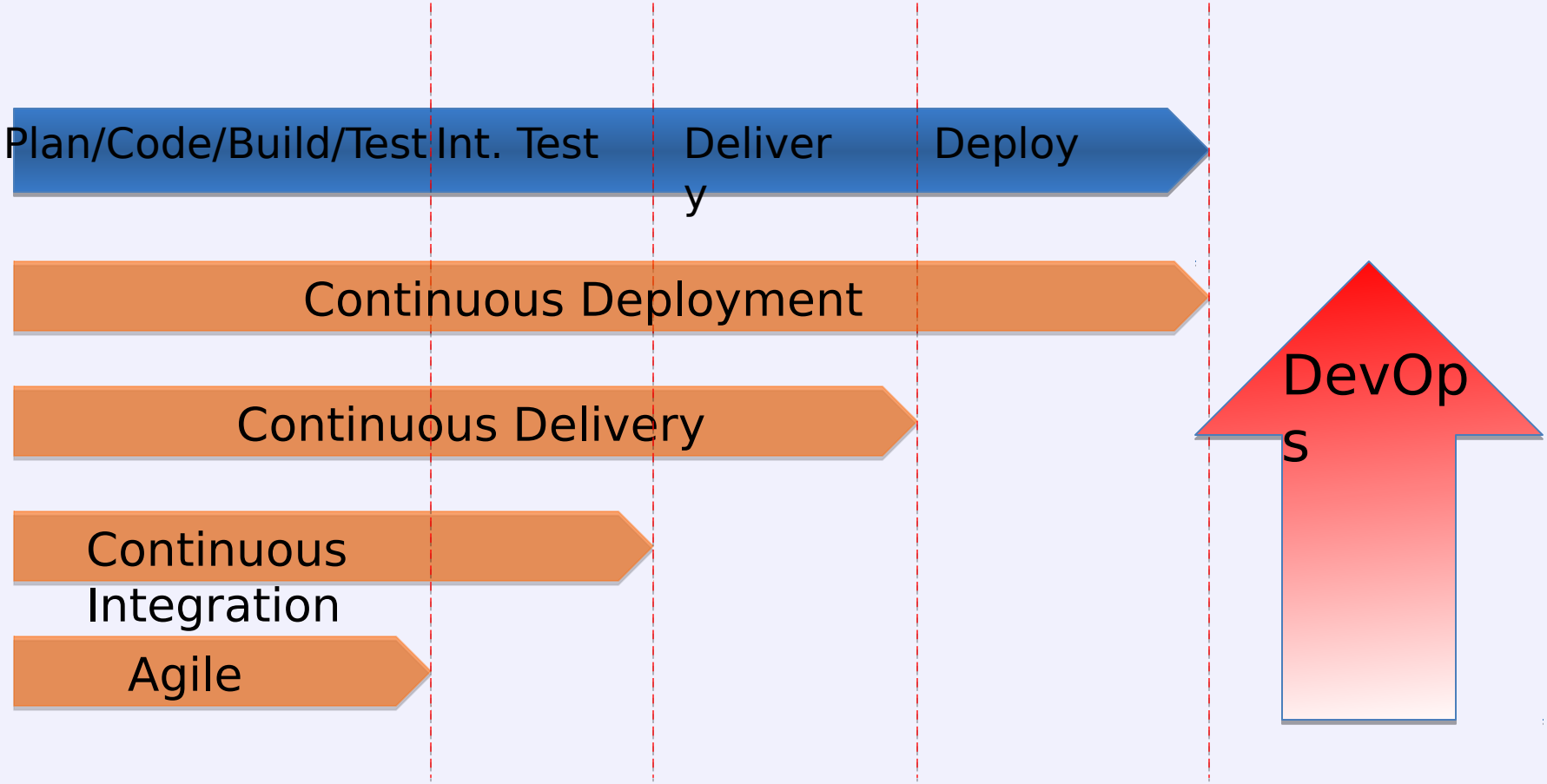
OWASP
The Open Web Application Security Project

- Stephen de Vries
- CTO ContinuumSecurity
- 60% Security consultant 40% Developer
- Author: BDD-Security project

...continuumsecurity...

About Me

DevOps is a tool


Plan/Code/Build/Test
Int. Test
Deliver y
Deploy
Continuous Deployment
Continuous Delivery
Continuous Integration
Agile
DevOps

Continuous Delivery Pipeline

DevOps is a tool to operate a continuous delivery pipeline

OWASP
The Open Web Application Security Project

The DevOps challenge to security

- Our project requirements are visible to dev and ops
- Our build, test and deploy process is entirely automated
- Developers can deploy to prod directly
- We deploy to prod multiple times per day
  - Amazon: deploy every 11.6 seconds
  - Etsy: deploys 25+ times/day
  - Gov.uk: deploys 30 times/day

How can we do this securely?

OWASP
The Open Web Application Security Project

Hoff @Beaker · Feb 21

I'm in Security. You new-fangled DevOps dudes and your Jenkins/agile/CD/whatevs got NUTHIN' on my "Continuous Annoyment" model.

OWASP
The Open Web Application Security Project

What can security learn from DevOps?

- **“Bad behaviour arises when you abstract people away from the consequence of their actions”** – Jez Humble
- Collaboration and communication are key: **there is no “them”**
- Continuous monitoring
- Automated Tests to verify

  …tests have expected outcomes

Never send a human to do a machine's job

- Automated tests **are** the security requirements
- Tests are code: stored by SCM
- Automate manual security tests
- Automate scanning process

First attempt:

OWASP
The Open Web Application Security Project

```
@Test
public void change_session_ID_after_login(){
   driver.get("http://localhost:9110/ropeytasks/user/login");
   Cookie preLoginSessionId = getSessionId("JSESSIONID");
   login("bob","password");
   Cookie afterLoginSessionId = getSessionId("JSESSIONID");
   assertThat(afterLoginSessionId.getValue(),
          not(preLoginSessionId.getValue()));
}

public void login(String u,String p){
  driver.findElement(By.id("username")).clear();
  driver.findElement(By.id("username")).sendKeys(u);
  driver.findElement(By.id("password")).clear();
  driver.findElement(By.id("password")).sendKeys(p);
  driver.findElement(By.name("_action_login")).click();
}
```

- Navigation logic is embedded in the test
- Selenium does not expose HTTP
- **Excludes non-developers**

OWASP
The Open Web Application Security Project

BDD-Security Testing Framework

https://github.com/continuumsecurity/bdd-security

OWASP
The Open Web Application Security Project

BDD-Security Testing Framework

```
Scenario: Issue a new session ID after authentication
Meta: @id session_fixation
Given the login page
And the value of the session cookie is noted
When the default user logs in with credentials from: users.table
And the user is logged in
Then the value of the session cookie issued after authentication should
        be different from that of the previously noted session ID
```

OWASP
The Open Web Application Security Project

Demo: BDD Port Scanner

OWASP
The Open Web Application Security Project

- Requirement is described ***before*** implementation
- Requirement is understandable by the whole team
- The requirement is itself an automated test
- Requirement failure == build failure

BDD-Security Testing Framework

OWASP
The Open Web Application Security Project

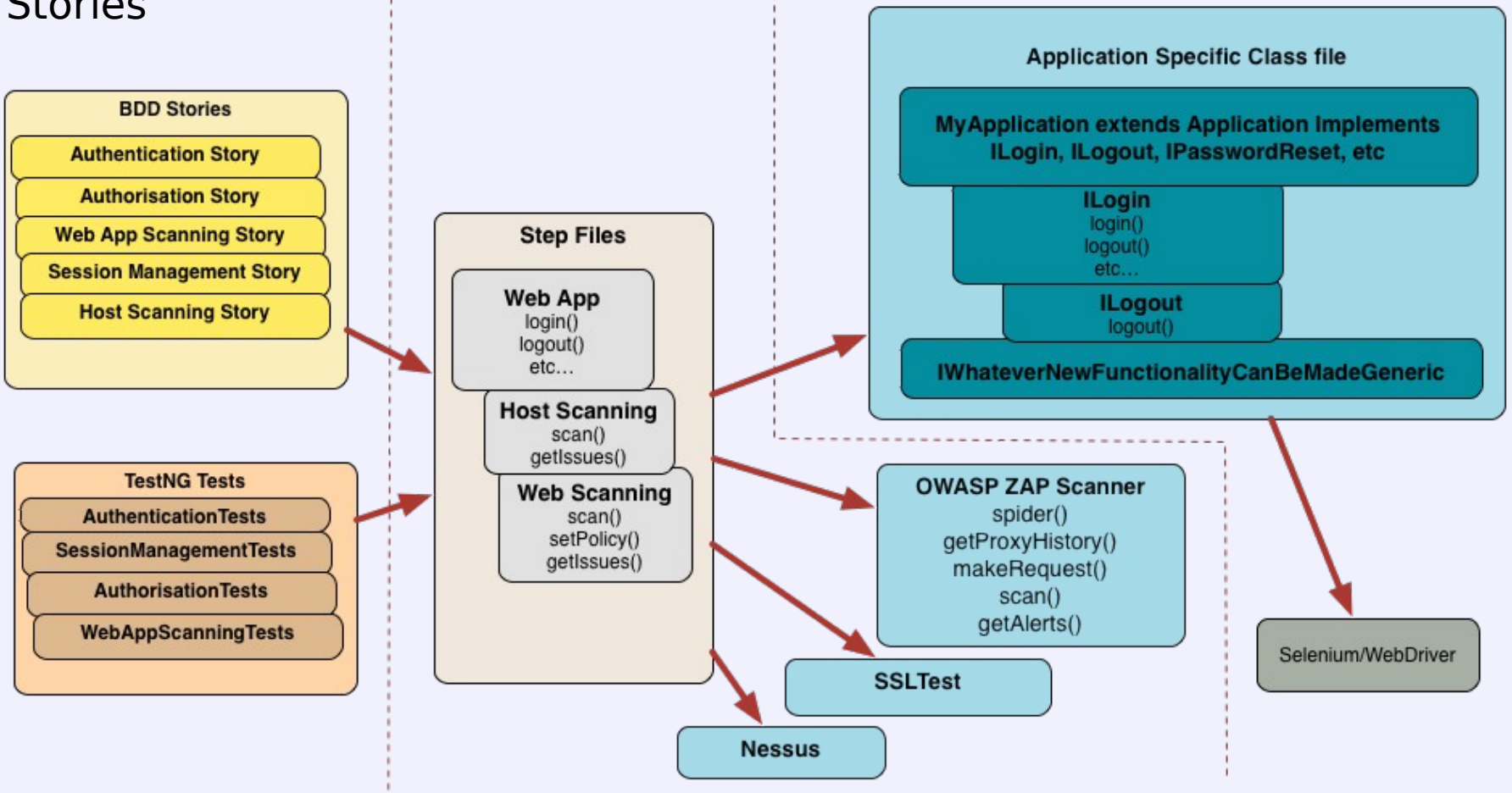
- Must be able to automate manual security testing
  - Selenium + OWASP ZAP API
- Tests must be understandable by all stakeholders
  - Behaviour Driven Development (BDD) with JBehave
- Must fit into dev workflow and continuous integration pipelines
  - Runs in IDE, cmd line
  - Runs in Jenkins
  - Test results in JUnit wrapper +HTML in Jenkins
- The logic of the security tests should be independent from navigation code
- Provide a baseline of ready-to-use security tests

OWASP
The Open Web Application Security Project

BDD Security Stories

Java core

Java + Selenium Steps



OWASP
The Open Web Application Security Project

Demo

- Initial configuration
- BDD tests of functional app security
- BDD wrappers around security processes
- BDD tests of non-functional app security

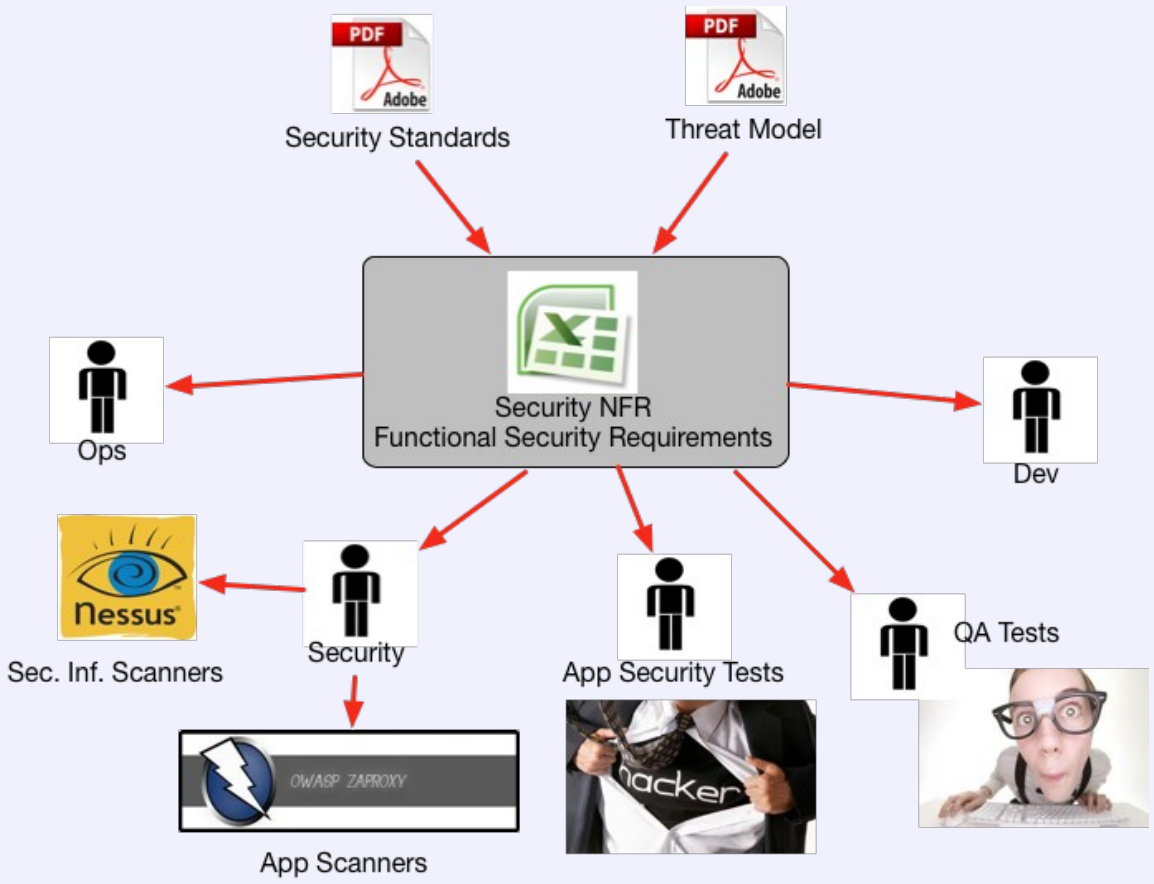
Integration with Jenkins

OWASP
The Open Web Application Security Project

Limitations

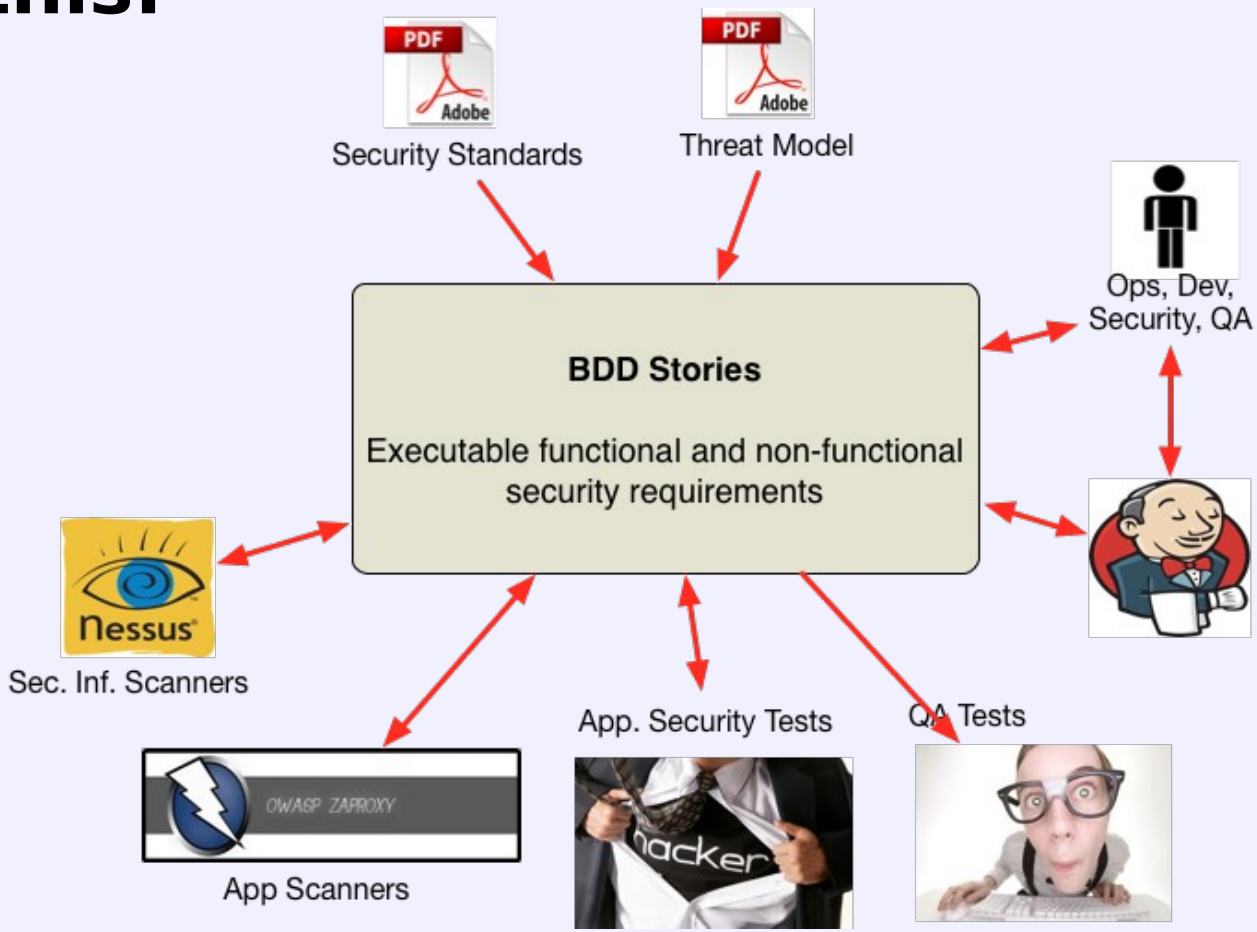
- Email: Not implemented yet!
  - Needed for self-reg
  - Account Lockout
- Access control not CSRF aware
- Test Maintenance
  - Use error checking wherever possible
  - Try to find generic solution
    - E.g.: ISomeBehaviour

From this:



- Dead documents
- Reliance on manual processes
- Tools don’t fit the deployment pipeline
- Tool results don’t translate to business requirements

To this:


PDF
Adobe
Security Standards
PDF
Adobe
Threat Model
Ops, Dev,
Security, QA
BDD Stories
Executable functional and non-functional
security requirements
Nessus
Sec. Inf. Scanners
App. Security Tests
QA Tests
OWASP ZAPROXY
App Scanners
hacker

OWASP
The Open Web Application Security Project

Resources:

- https://github.com/continuumsecurity
  - OWASP ZAP Pure Java client API
  - Resty-Burp RESTful API into Burp Suite
  - Nessus Java Client
  - SSLTest Java SSL analyser
- Related projects:
  - Gauntlt BDD wrapper for sec tools: https://github.com/gauntlt/gauntlt (Ruby)
  - Mittn Burp Integration: https://github.com/F-Secure/mittn (Python)

OWASP
The Open Web Application Security Project

Questions?

@stephendv