Continuous Security Testing in a DevOps World

OWASP

The Open Web Application Security Project

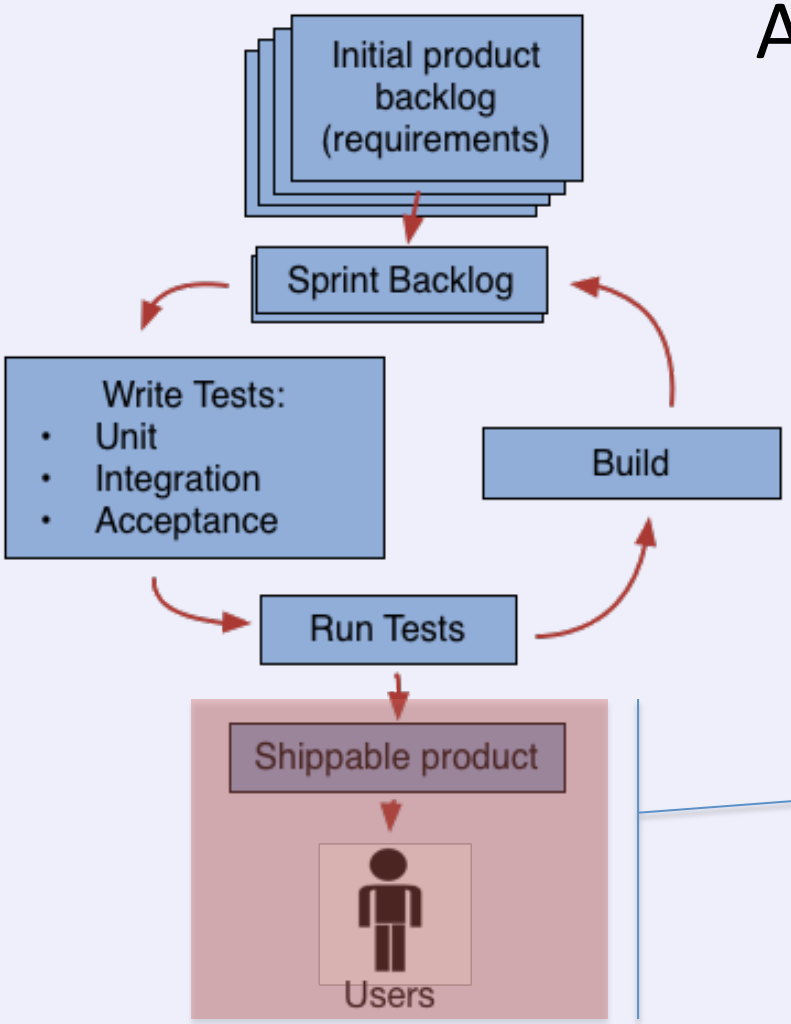
About Me

OWASP
The Open Web Application Security Project

- Stephen de Vries
  - CTO Continuum Security
  - 70% Security Consultant – 30% Developer
  - Author of BDD-Security Project
  - (Ex) Co-founder of OWASP Java Project
  - @stephendv

...ContinuumSecurity...

Agile:



- Small incremental changes
- Fast feedback from tests
- Fast feedback from users
- Easily adapts to change
- Lower risk of project failure

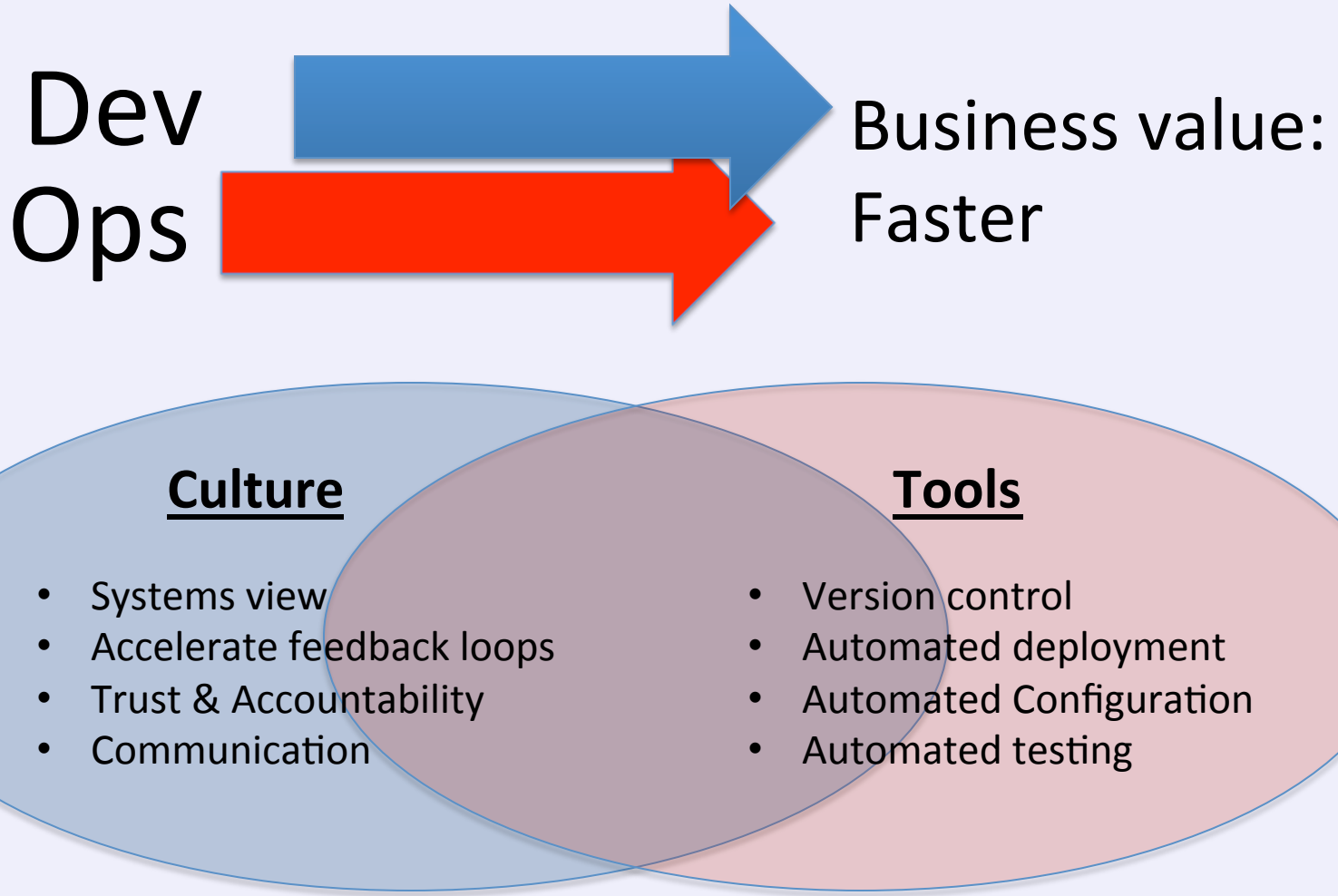
Bottleneck between “Shippable” and “Deployed”

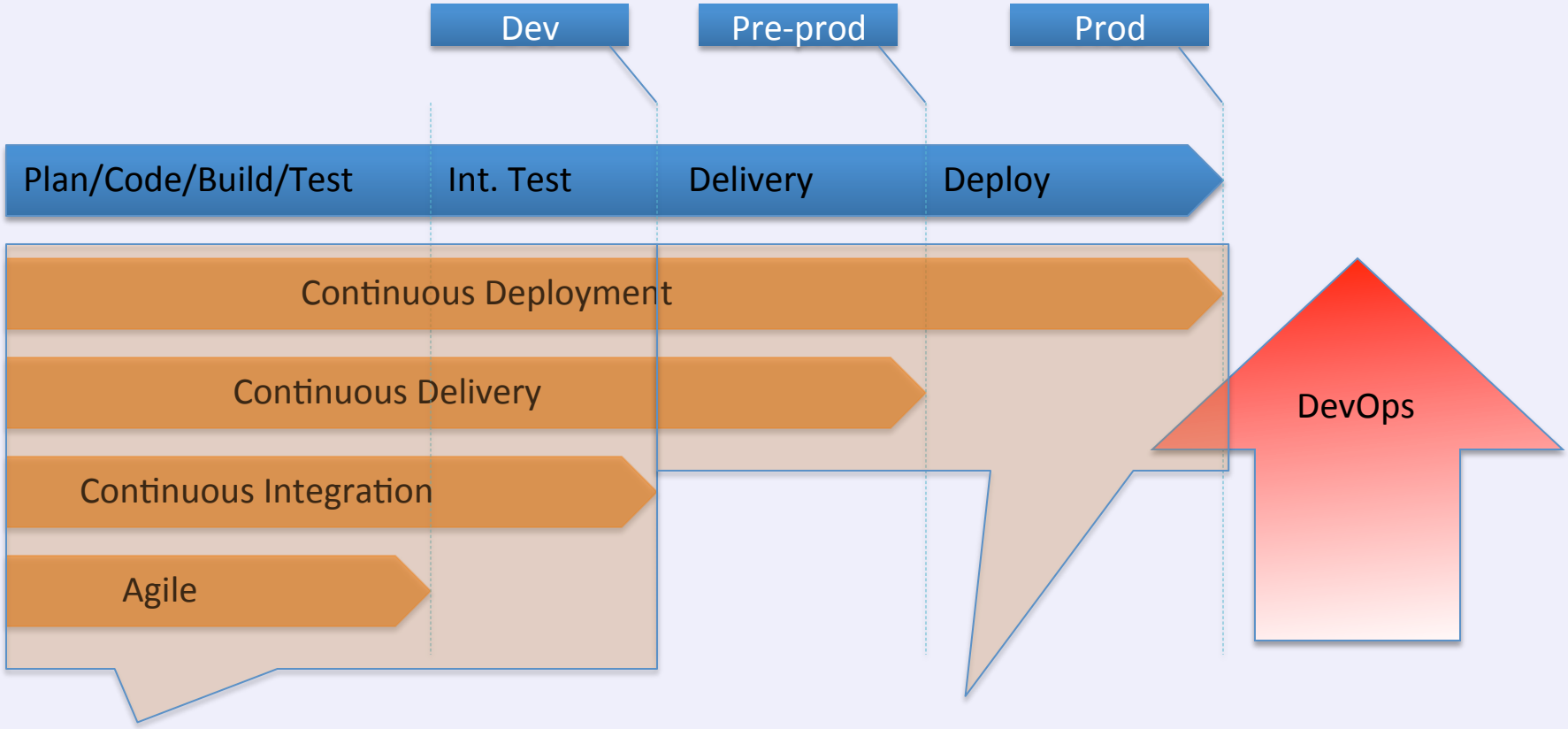
Operations

- Value stability
- Manual processes
- Manual testing

Developers

- Value faster incremental changes
- Automated testing


Dev
Ops
Business value:
Faster
Culture
Systems view
Accelerate feedback loops
Trust & Accountability
Communication
Tools
Version control
Automated deployment
Automated Configuration
Automated testing



- Requirements as stories
- Unit testing
- Automated Functional testing

- Auto. Config + deploy
- Auto. Acceptance testing
- Monitoring
- Easy rollback

OWASP
The Open Web Application Security Project

The DevOps challenge to security:

- As DevOps we understand the process of built, test and deploy
- We've largely automated this process in a delivery pipeline
- We deploy to production multiple times per day

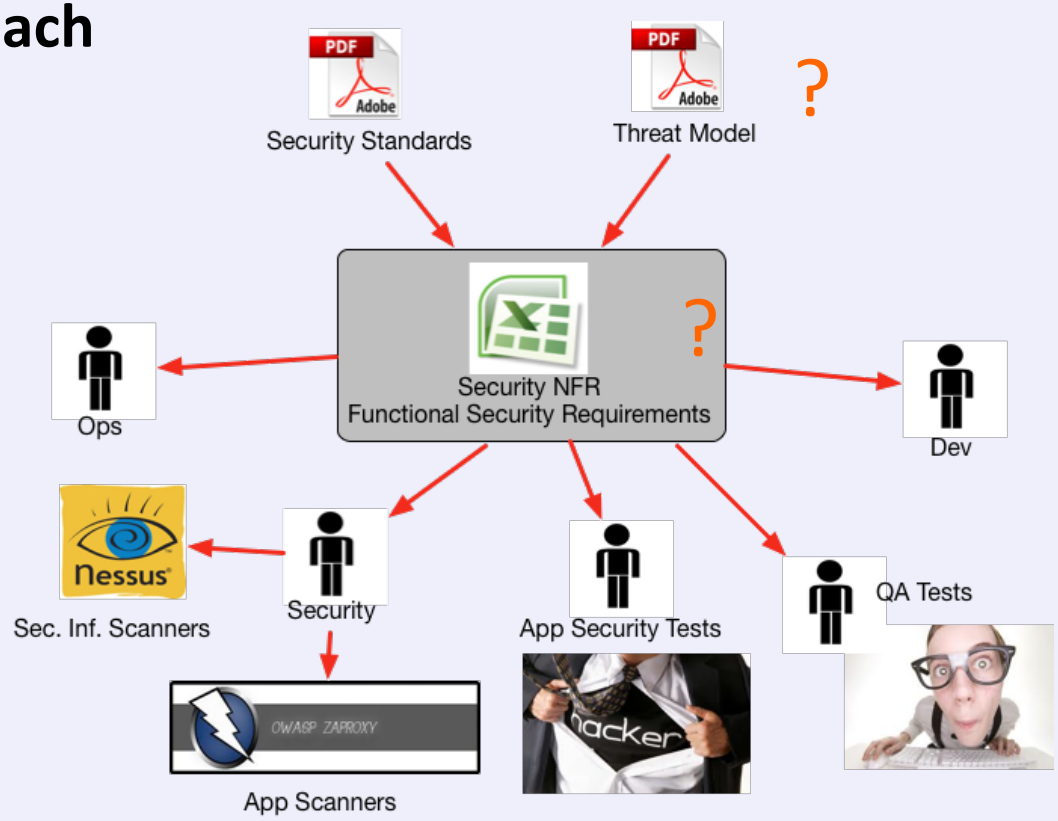
How can we do this securely?

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.

Traditional Security Approach

- Dead documents
- Reliance on manual processes
- Tools don't fit the deployment pipeline



How can we provide security at DevOps speed?

Security is not special

Don’t add security…

…make it disappear

OWASP
The Open Web Application Security Project

What can security learn from Agile/CD/DevOps?

- Security goals must be driven by the business and must be **clearly stated**
- Collaboration and communication means exposing your processes
  - Do it well enough and there is no “them”

“Never send a human to do a machine’s job” – Agent Smith

- Record manual security tests for automation
- Automate scanning process
- Automated tests **<u>are</u>** the security requirements

OWASP
The Open Web Application Security Project

First attempt:

```
@Test
public void change_session_ID_after_login() {
     driver.get("http://localhost:9110/ropeytasks/user/login");
     Cookie preLoginSessionId = getSessionId("JESSSIONID");
     login("bob", "password");
     Cookie afterLoginSessionId = getSessionId("JESSSIONID");
     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();
}
```

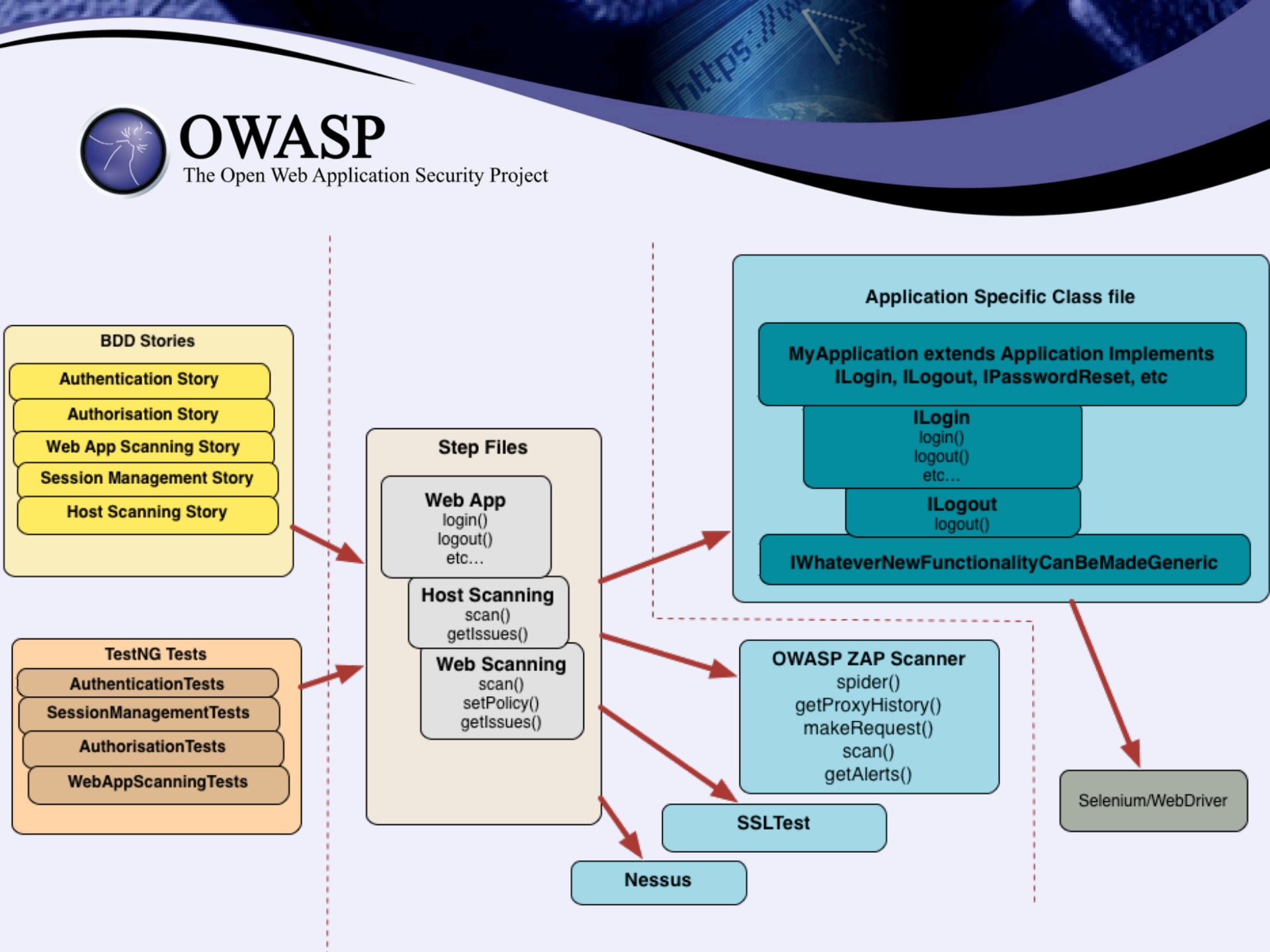
- Navigation logic is embedded in the test
- Selenium does not expose HTTP
- Excludes non-developers

OWASP
The Open Web Application Security Project

Introducing BDD-Security

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

- Tests must be understandable by all stakeholders
  - Behaviour Driven Development (BDD): **JBehave**
- Must be able to automate manual security testing
  - Selenium + OWASP ZAP API + Nessus + …
- Must fit into dev workflow and CI/CD pipelines
  - Runs in IDE, cmd line
  - Runs in Jenkins
  - Test results in JUnit wrapper + HTML
- 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 Stories
Authentication Story
Authorisation Story
Web App Scanning Story
Session Management Story
Host Scanning Story
TestNG Tests
AuthenticationTests
SessionManagementTests
AuthorisationTests
WebAppScanningTests
Step Files
Web App
login()
logout()
etc…
Host Scanning
scan()
getIssues()
Web Scanning
scan()
setPolicy()
getIssues()
Application Specific Class file
MyApplication extends Application Implements
ILogin, ILogout, IPasswordReset, etc
ILogin
login()
logout()
etc…
ILogout
logout()
IWhateverNewFunctionalityCanBeMadeGeneric
OWASP ZAP Scanner
spider()
getProxyHistory()
makeRequest()
scan()
getAlerts()
SSLTest
Nessus
Selenium/WebDriver

OWASP
The Open Web Application Security Project

Getting Started with BDD-Security

OWASP
The Open Web Application Security Project

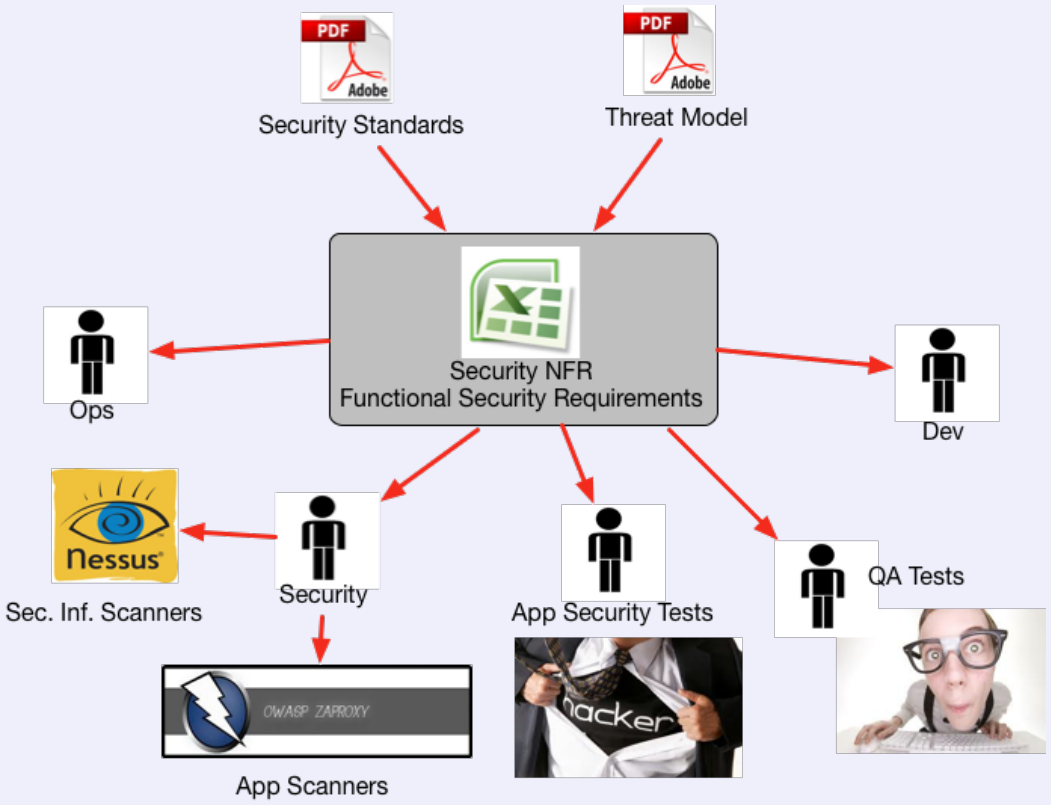
Integration with Jenkins

OWASP
The Open Web Application Security Project

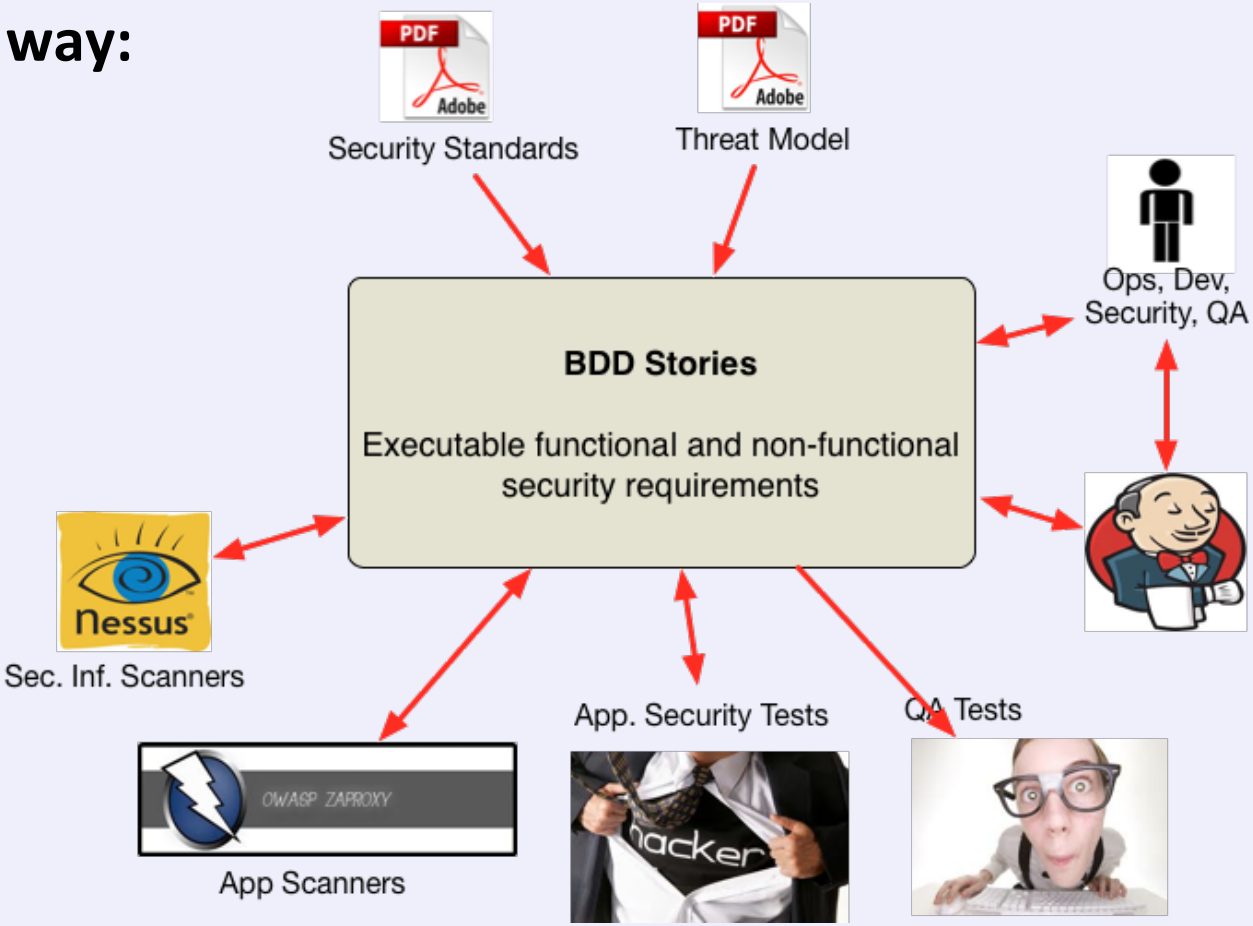
Real world challenges

- Not Anti-CSRF aware
- No difference between test error and test failure
- Test Maintenance
  - Do sanity checks along the way
  - Try to find generic solution
    - E.g.: ISomeBehaviour
- CAPTCHA
  - ICaptcha + deathbycaptcha.com

Old way:


PDF
Adobe
Security Standards
PDF
Adobe
Threat Model
Security NFR
Functional Security Requirements
Ops
Dev
Nessus
Sec. Inf. Scanners
Security
App Security Tests
QA Tests
OWASP ZAPROXY
App Scanners
hacker

New way:


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

Questions?

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

OWASP
The Open Web Application Security Project

Thank you

@stephendv

stephendv@continuumsecurity.net