



OWASP

Open Web Application
Security Project

Achieving Secure Continuous Delivery ([cont..](#))

--lightning talk--

Nikos / Jesus / Lucian

April 2018



Typical discussions...



Pain points



Same problem in 2018!

Difficult access to (uncorrelated) vulnerability data

No clear view on the security risk of a specific build or release

No real agreed security gate (no trigger threshold)

Short memory! Tools get easily forgotten or abandoned...

Product has a Roadmap and Security is (always) not (always) part of it

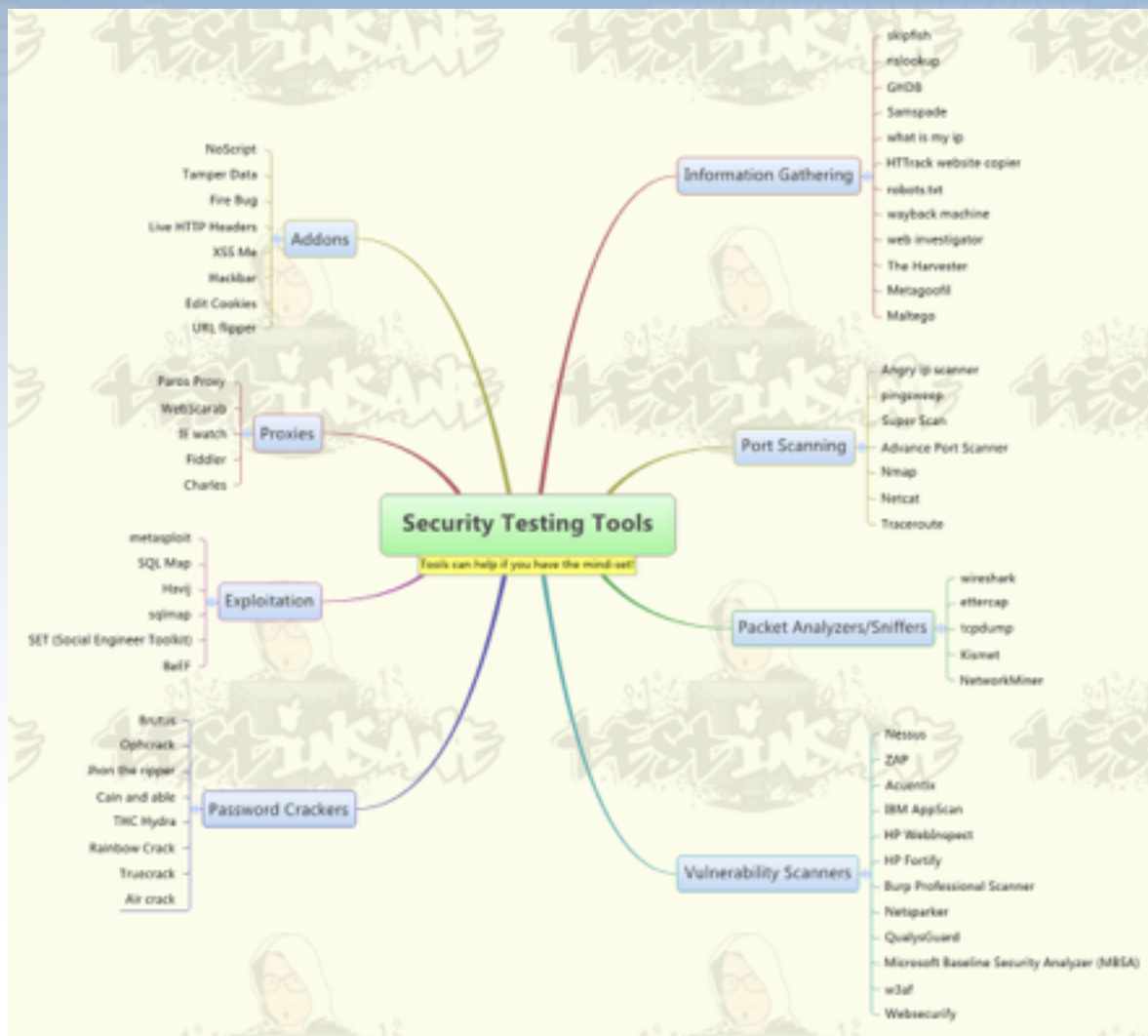
Security requirements appear (dark magic!) when project is almost finished

Security sign-off is a bottleneck [choke]

Security testing tools!
Lots of tools!! And reports!!!

When am I *finally* secure enough? Never!
says Mordac.

Tools!!



SAST list [HERE](#)

DAST list [HERE](#)

Dependency Checking
Tools list [HERE](#)

Container Security tools
[HERE](#)

Google list [HERE](#)

Others [HERE](#)

Link [HERE](#)

The Want



Automation & centralisation of application security testing



Risk based approach to application delivery & deployment



Security Champions process and responsibilities

Existing initiatives

Lots!!!

[OWASP AppSec Pipeline](#) [OWASP OWTF](#) [OWASP Defect Dojo](#)

Others talking about this

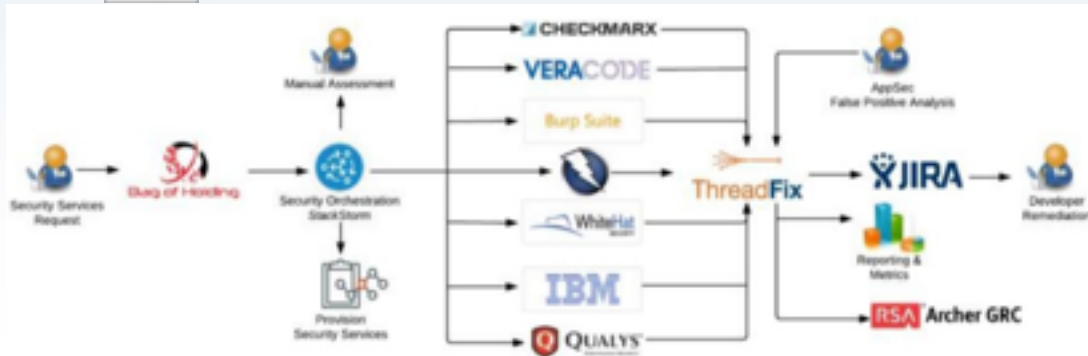
[HERE](#) [HERE](#) [HERE](#) [HERE](#) [HERE](#)
Christian Schneider



OWASP Israel

DENIM GROUP

[HERE](#) [HERE](#) [HERE](#) [HERE](#) [HERE](#) [HERE](#) [HERE](#) [HERE](#) [HERE](#)




SAMPLE

[OWASP AppSec Pipeline](#)




Where we are now


sage




Jenkins



TFS



GitHub



GitLab



sage



Security
Jenkins



FORTIFY



CHECKMARX



OWASP
Dependency-Check



Qualys. WAS



OWASP
Zed Attack Proxy




Nessus




Web Security Project



Ready! API



CLOUDFLARE



iMPERVA



ThreadFix
Powered by Danim Group



JIRA



TFS



waratek



OWASP
Open Web Application
Security Project

Developer Jenkins

direct-debit-manager 

#912 triggered by remote trigger changes by Nikos Savvidis started 5 days ago

Total build time: 10 min 52 sec

Changes:

1698e456796d8be2e1e43f0dedae6463358e19df Nikos Savvidis Turning onboarding creditor verification flow off again.

BUILD

build

5 days ago 5 min 22 sec

Test Result

Total	Failures	Skipped
740	0	3

Warnings High Normal Low

Checkstyle

FindBugs

PMD

DEV

deploy 

5 days ago 1 min 47 sec

test 

4 days ago 3 min 42 sec

QA

deploy


test

DDM Security Testing

DDM Threadfix Security Policy Check

Security Jenkins

1. How does Jenkins run tools

Execute ThreadFix Scan Agent scan 

Application:

Scan Type:

4. How we inform

Slack Notifications

Notify Build Start

Notify Aborted

Notify Failure

Notify Not Built

Notify Success

Notify Unstable

Notify Regression

Notify Back To Normal

2. How does Threadfix receive results

Publish ThreadFix Scan

Teams and Applications

The available teams with their applications on the ThreadFix server

3. Check my policy

Jenkins [APP] 17:14

fortify-direct-debit-manager - #436 Success after 30 min ([Open](#))
Job running all applicable security tests.
If successful then moving to ThreadFix security policy check for this project.

fortify-direct-debit-manager-threadfixsecuritypolicycheck - #370 Success after 0.58 sec ([Open](#))
Check if your build is compliant with the ThreadFix security policy for this project.
If yes, then you're good to go, if no then a Security Champion must check ThreadFix results.

Build

HTTP Request

URL

HTTP mode

Ignore Ssl errors? Yes No

Threadfix policies



authserver

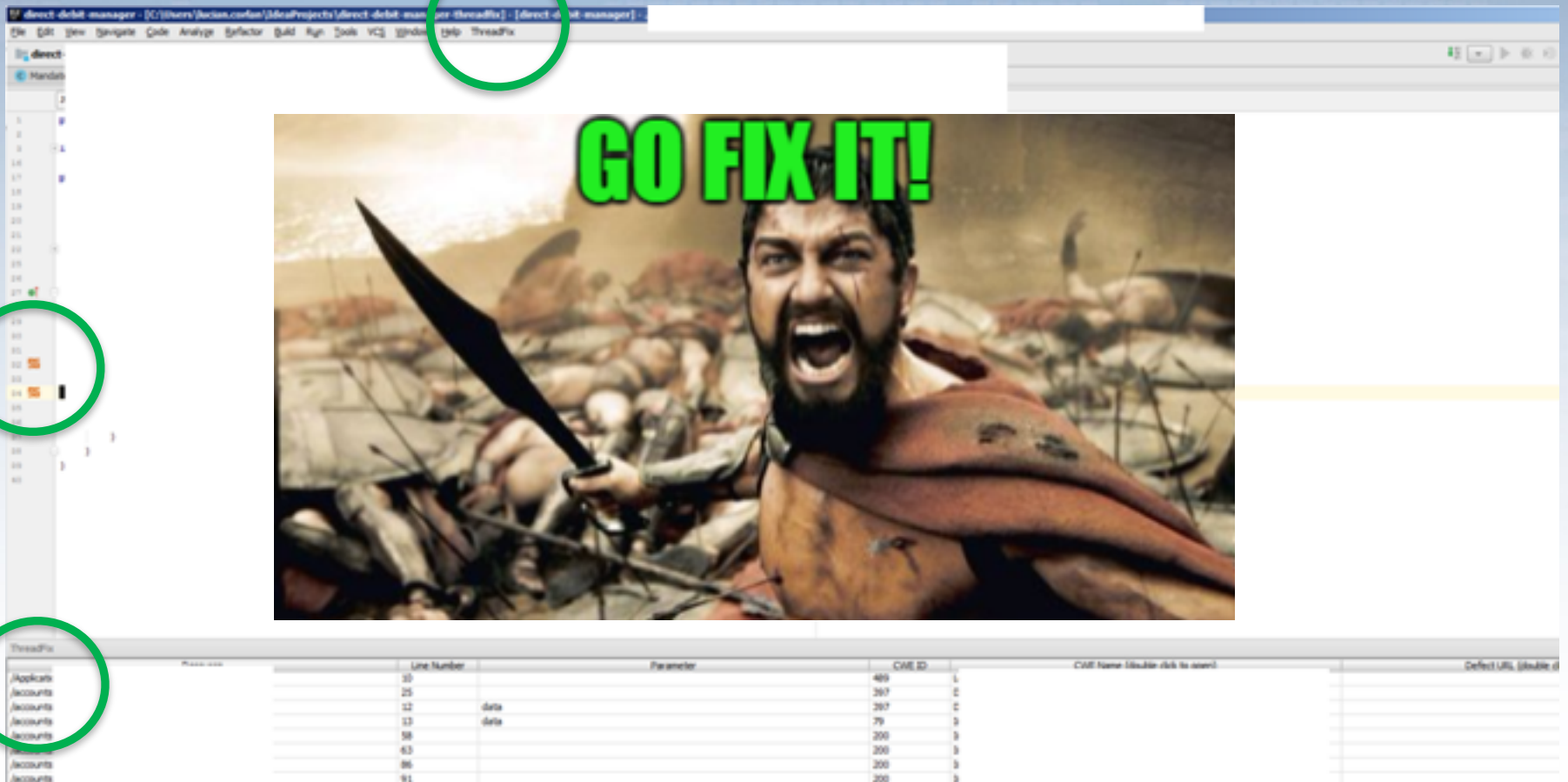
Action ▾

Policy Status **PASSING**

```
← → ↻ 🏠 /threadfix/rest/applications/15/policyStatuses?apiKey
{"message":"","success":true,"responseCode":-1,"object":[{"id":30,"passing":true,"statusLastChanged":1521221063000,"name":"CHLM","filterName":"CHLM","id":1,"service","lastEvaluated":1521221063000,"policy":{"name":"XSS","filterName":"XSS-filter","id":37,"passing":true,"statusLastChanged":1511952021000,"name":"integration-service","id":52,"passing":true,"statusLastChanged":1503393905000,"name":"integration-service","id":84,"passing":true,"statusLastChanged":1503394302000,"name":"integration-service","id":5}},{"id":68,"passing":true,"statusLastChanged":1503394233000,"name":"int Injection","filterName":"Injection","id":6}},{"id":135,"passing":true,"statusLast service","lastEvaluated":1523385615000,"policy":{"name":"CH","filterName":"CH","id":8}}]}
```

Name	Filter Name	Status
CHLM	CHLM	PASS
XSS	XSS-filter	PASS
CHLW	CHLW	PASS
CSRF	CSRF	PASS
SQL Injection	SQL Injection	PASS
Injection	Injection	PASS
CH	CH	PASS

Fixing the stuff



The screenshot shows a web application security tool interface. The top menu bar includes 'File', 'Edit', 'View', 'Navigate', 'Code', 'Analyze', 'Defactor', 'Build', 'Run', 'Tools', 'VCS', 'Find', and 'ThreadFix'. The main area displays a list of issues on the left and a table of findings at the bottom. A meme featuring a warrior shouting 'GO FIX IT!' is overlaid on the central part of the interface. Three green circles highlight specific elements: the 'ThreadFix' menu item, a list of issues, and the 'ThreadFix' table header.

ThreadFix	Message	Line Number	Parameter	CWE ID	CAP Name (Should click to open)	Defect URL (Should click to open)
Accounts		10		409	L	
Accounts		25		207	C	
Accounts		12	data	207	C	
Accounts		13	data	79	D	
Accounts		58		200	D	
Accounts		43		200	D	
Accounts		86		200	D	
Accounts		91		200	D	

Next?



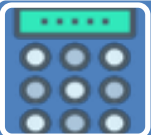
What is best for you and your businesses' appetite?



Get a DevSecOps team to build and maintain toolz&stuff for you £££



OWASP project (Pipelines?) to support all free tool inputs into one central repo



(Somehow) work with commercial tool providers to support that



Inspire and empower your Security Champions

Q/A

