OWASP
Open Web Application Security Project

Achieving Secure Continuous Delivery (cont..)

--lightning talk--

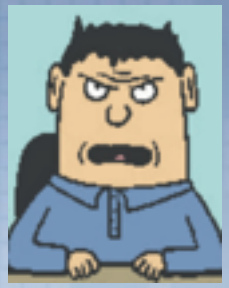
Nikos / Jesus / Lucian

April 2018

Typical discussions…

OWASP
Open Web Application Security Project

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

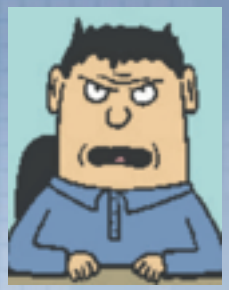
Security sign-off is a bottleneck [choke]

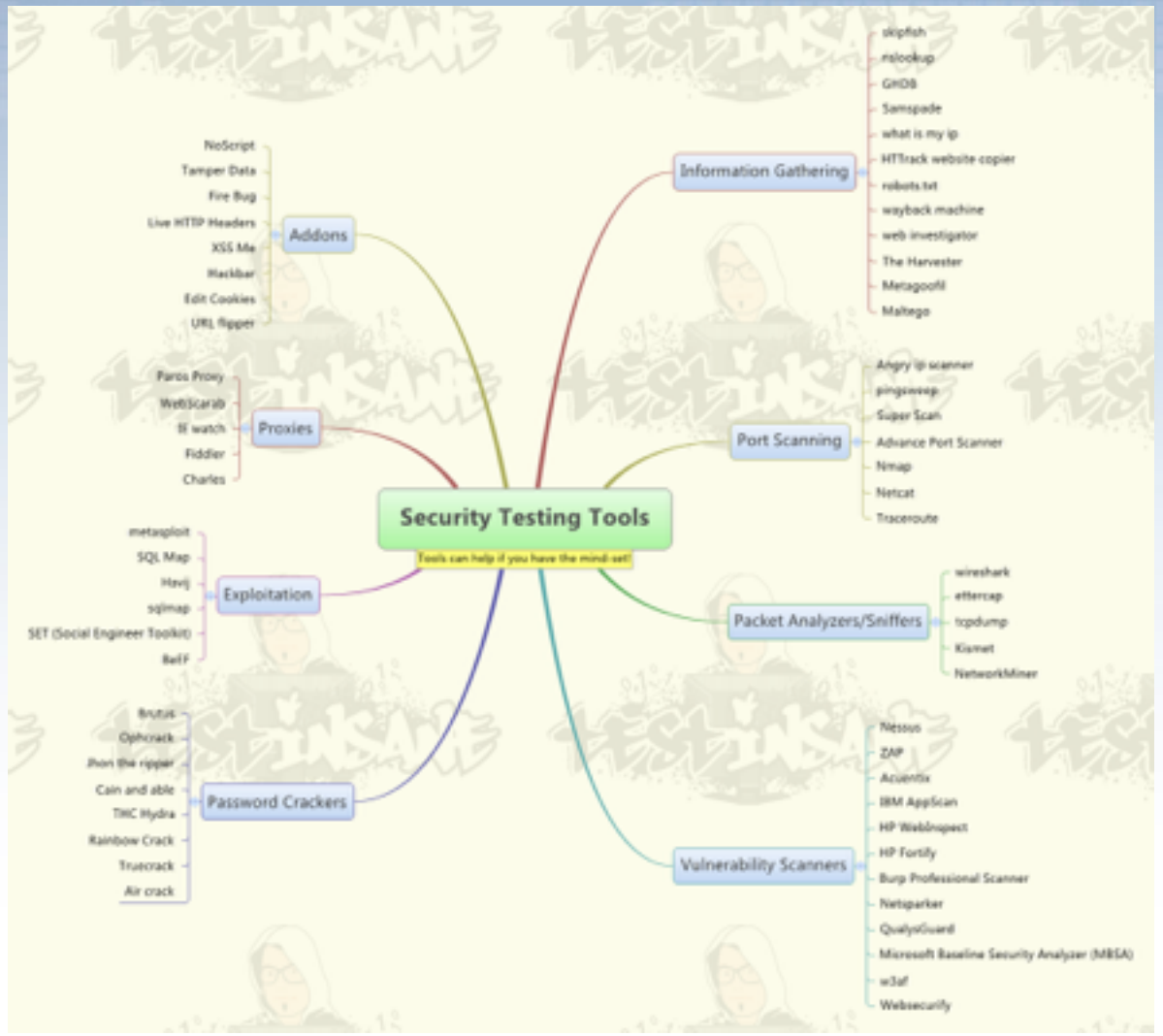
Security testing tools!
Lots of tools!! And reports!!!

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

OWASP
Open Web Application Security Project

Tools!!





Link HERE

SAST list HERE

DAST list HERE

Dependency Checking Tools list HERE

Container Security tools HERE

Google list HERE

Others HERE

OWASP
Open Web Application Security Project

The Want

Automation & centralisation of application security testing

Risk based approach to application delivery & deployment

Security Champions process and responsibilities

OWASP
Open Web Application Security Project

Existing initiatives

Lots!!!

OWASP AppSec Pipeline OWTF OWASP Defect Dojo

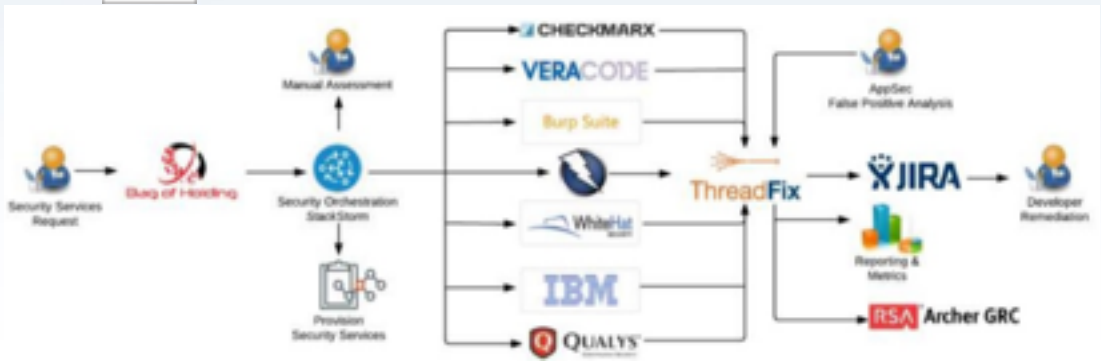
OWASP Israel

Others talking about this HERE HERE HERE HERE HERE HERE HERE HERE HERE HERE HERE HERE HERE HERE HERE

Christian Schneider

STDD

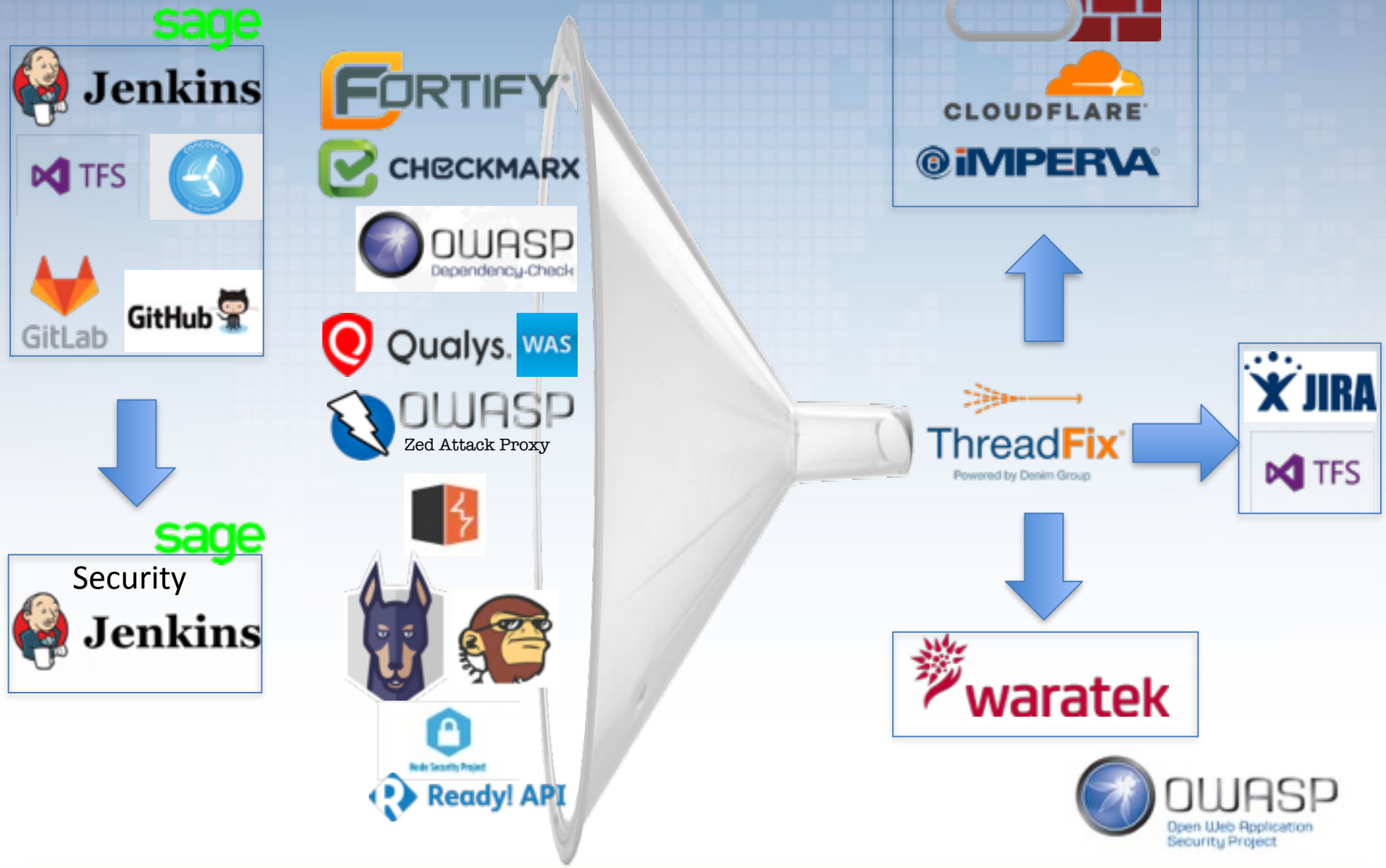
SAMPLE



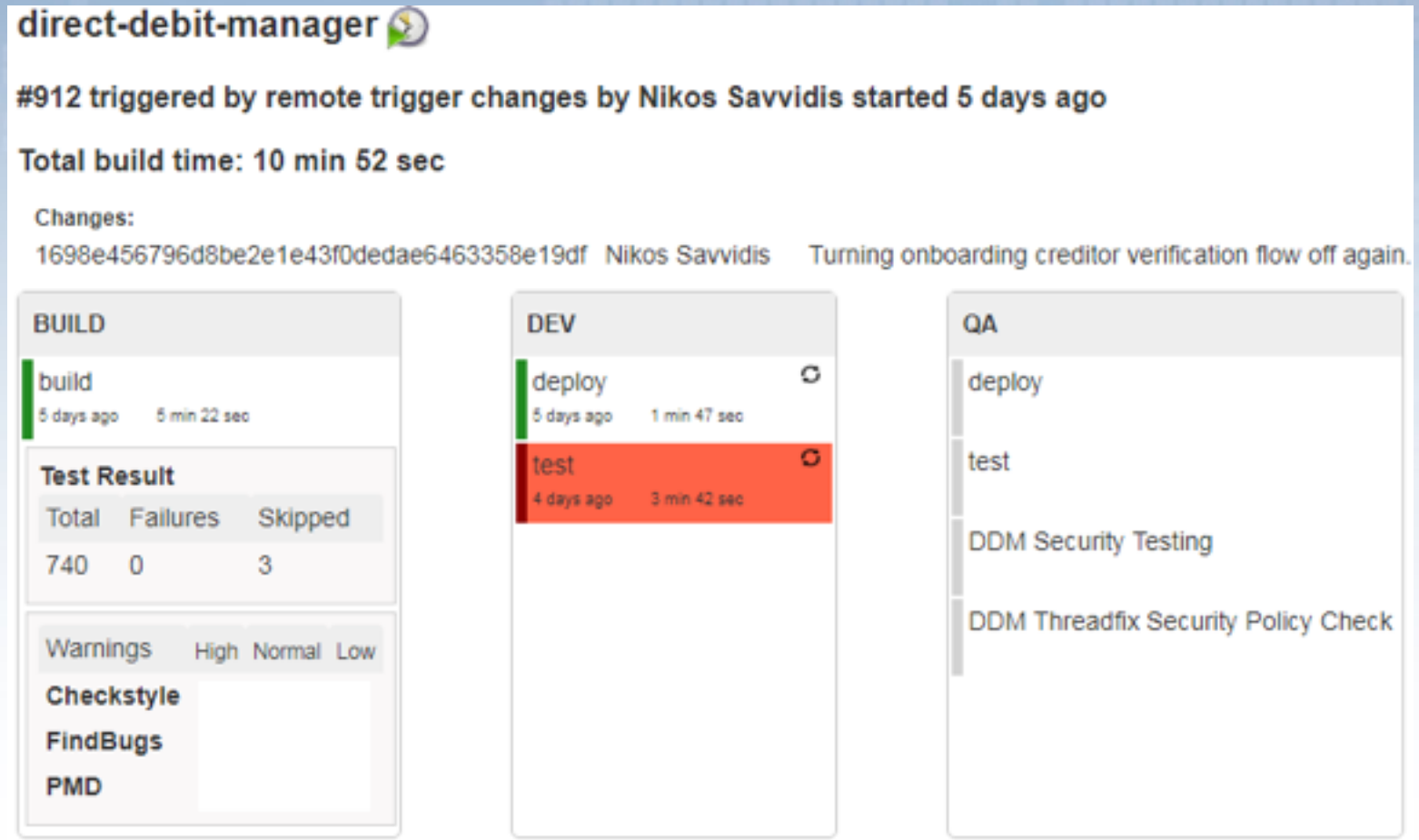
OWASP AppSec Pipeline

OWASP Open Web Application Security Project

Where we are now

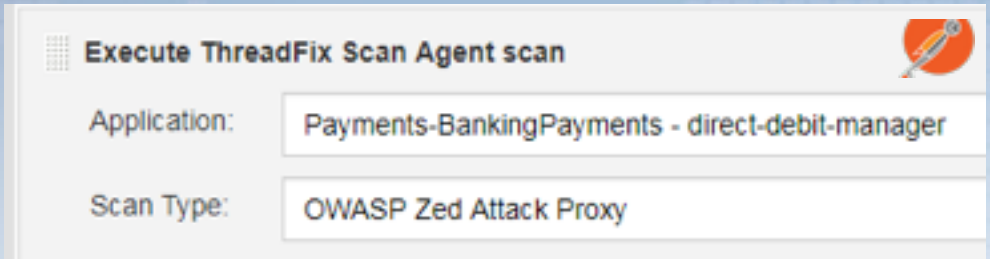


Developer Jenkins

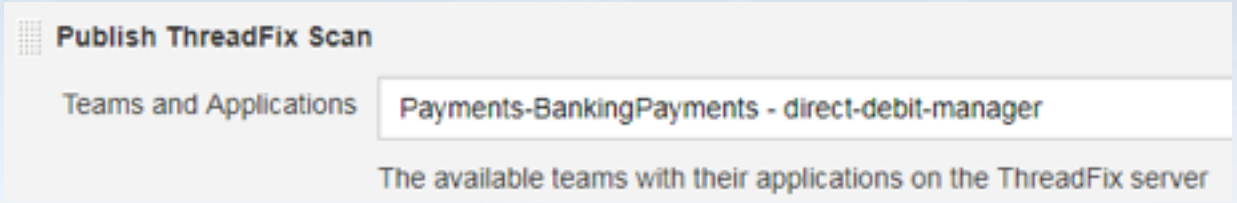


Security Jenkins

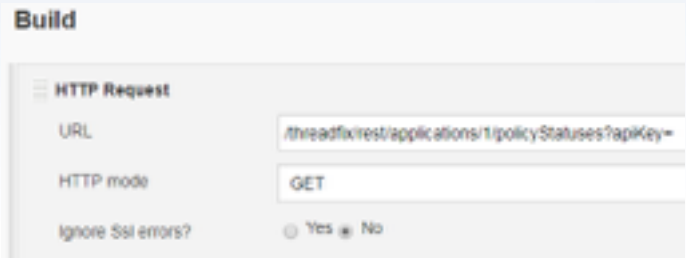
1. How does Jenkins run tools



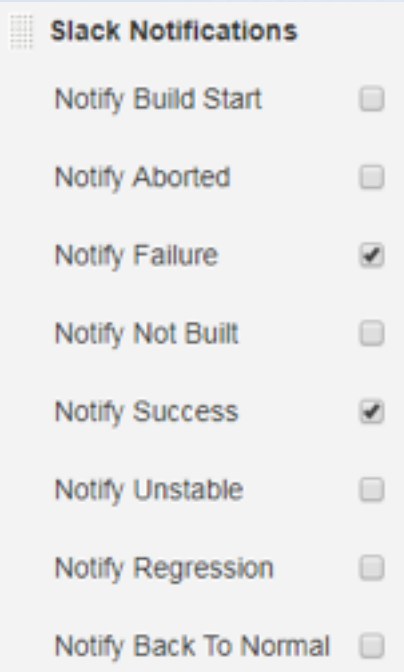
2. How does Threadfix receive results

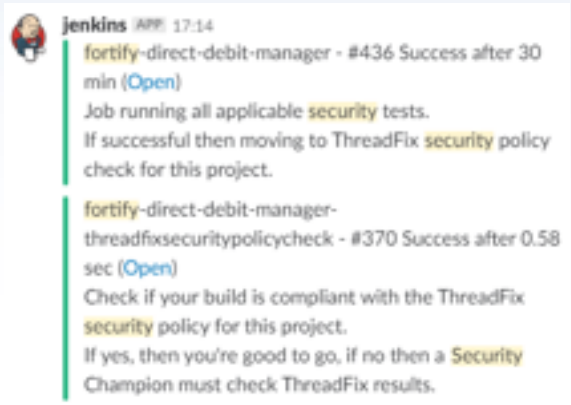


3. Check my policy



4. How we inform





OWASP
Open Web Application Security Project

Threadfix policies

ThreadFix
Powered by Denim Group

authserver Action

Policy Status **PASSING**

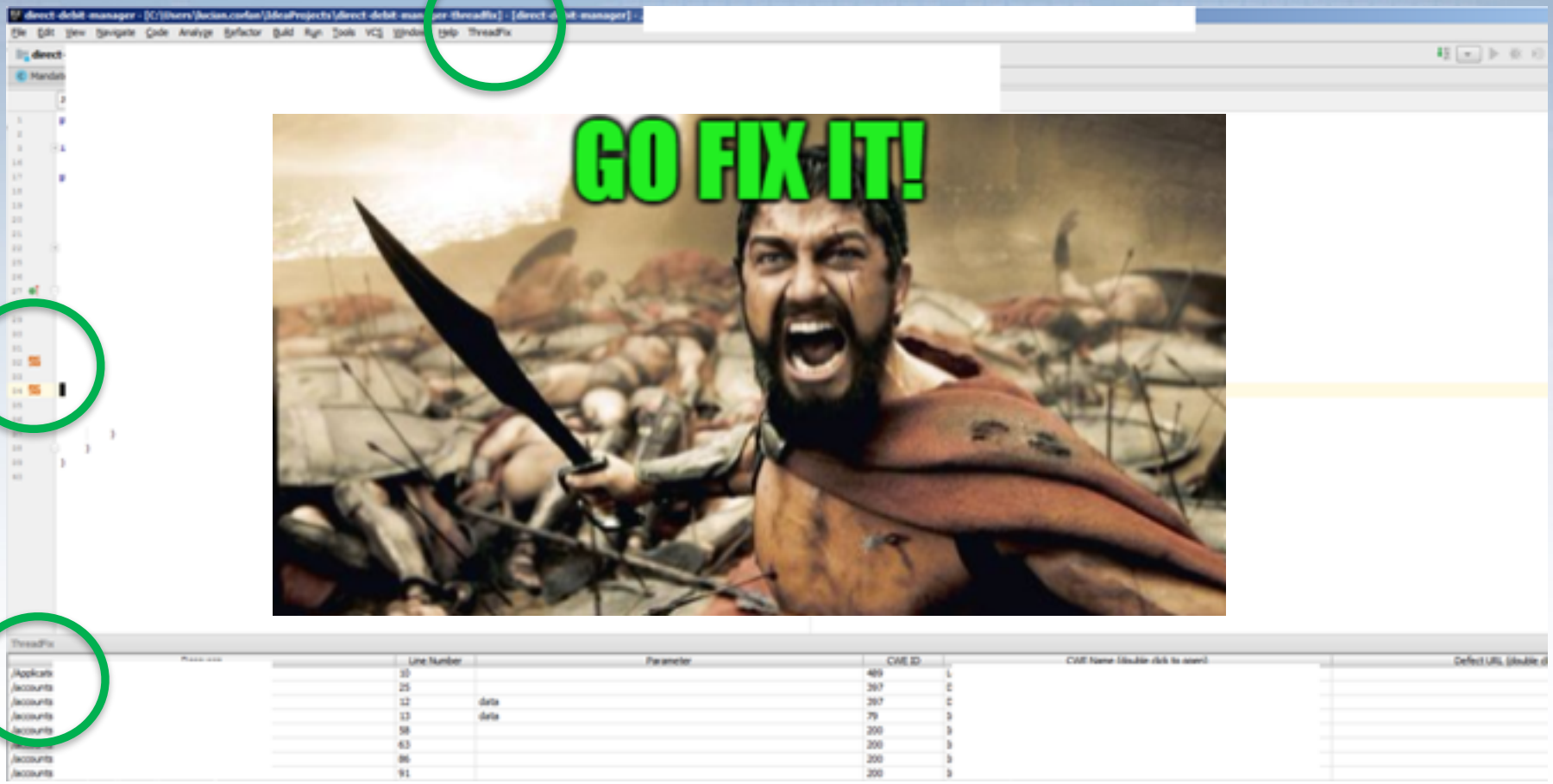
/threadfix/rest/applications/15/policyStatuses?apiKey


```
{"message":"","success":true,"responseCode":-1,"object":[{"id":30,"passing":true,"statusL
service","lastEvaluated":1521221063000,"policy":{"name":"CHLM","filterName":"CHLM","id":1
service","lastEvaluated":1521221063000,"policy":{"name":"XSS","filterName":"XSS-filter","
{"id":37,"passing":true,"statusLastChanged":1511952021000,"name":"integration-service","l
{"id":52,"passing":true,"statusLastChanged":1503393905000,"name":"integration-service","l
{"id":84,"passing":true,"statusLastChanged":1503394302000,"name":"integration-service","l
Injection","id":5}},{"id":68,"passing":true,"statusLastChanged":1503394233000,"name":"int
{"name":"Injection","filterName":"Injection","id":6}},{"id":135,"passing":true,"statusLas
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

OWASP
Open Web Application Security Project

Fixing the stuff



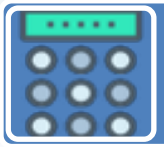
OWASP
Open Web Application Security Project

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

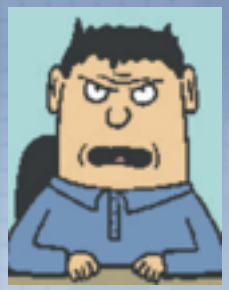


(Somehow) work with commercial tool providers to support that

Inspire and empower your Security Champions

OWASP
Open Web Application Security Project

Q/A



OWASP
Open Web Application Security Project