



OWASP

Open Web Application  
Security Project

# Using JIRA to manage Risks and Security Champions activities

OWASP AppSecEU, Rome, 2016

# Me

- Developer for 25 years
- AppSec for 13 years
- Day jobs:
  - Leader OWASP O2 Platform project
  - Application Security Training for JBI Training
  - Part of AppSec team of:
    - The Hut Group
    - BBC
- AppSec Consultant and Mentor



**OWASP**

Open Web Application  
Security Project

[WWW.OWASP.ORG](http://WWW.OWASP.ORG)

# Books Published

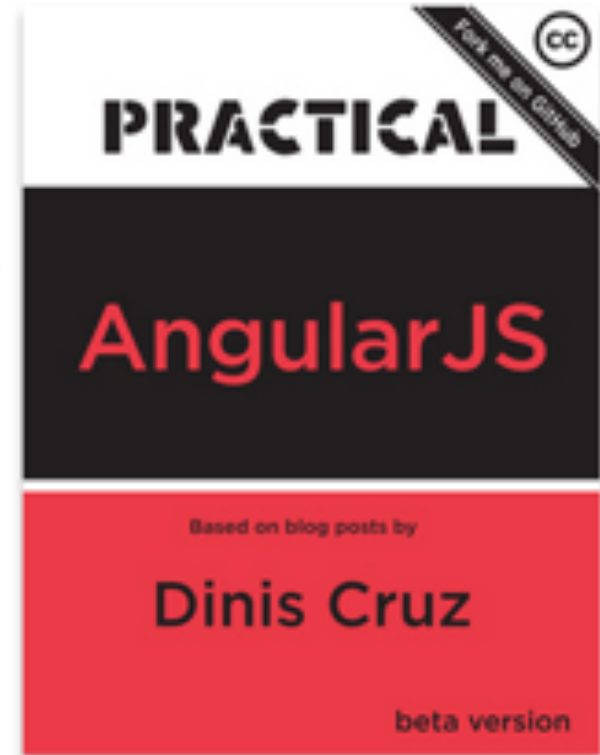
- @Leanpub (buy for 0\$ )
- <http://leanpub.com/u/DinisCruz>



# Books under development



Ideas shown in this presentation  
and a lot more



Major revision with lots of new content  
(based on Maturity Models app)



**OWASP**

Open Web Application  
Security Project

[WWW.OWASP.ORG](http://WWW.OWASP.ORG)



**Dinis Cruz**  
@DinisCruz

TWEETS  
**11.9K**

FOLLOWING  
**264**

FOLLOWERS  
**2,731**

LIKES  
**1,375**

Edit profile

Tweets

Tweets & replies

Media

Pinned Tweet

# Dinis Cruz Blog

A personal blog about: transforming Web Application Security into an 'Application Visibility' engine, the OWASP O2 Platform, Application/Data interoperability and a lot more

Home

Hire me

AppSec Jobs and Projects

OWASP O2 Platform

Real-Time Vulnerability Feedback in VisualStudio

About



**OWASP**  
Open Web Application  
Security Project

WWW.OWASP.ORG

See also:

# NEW ERA OF SOFTWARE WITH MODERN APPLICATION SECURITY

VERSION 1.0 (19/MAR/2016)

CODEMOTION ROME

@DINISCRUZ

<http://blog.diniscruz.com/2016/03/new-era-of-software-with-modern.html>



**OWASP**

Open Web Application  
Security Project

[WWW.OWASP.ORG](http://WWW.OWASP.ORG)

## NEW ERA OF SOFTWARE WITH MODERN APPLICATION SECURITY



My thesis is that

**Application Security** can be used to define and measure Software Quality

## THE POLLUTION ANALOGY



These tools/techniques are designed to

A) Improve code Quality

B) Make AppSec possible

## MODERN APPLICATION SECURITY

- TDD with Code Coverage
- Threat Models
- Docker and Containers
- Test Automation
- SAST/DAST/IAST/WAF
- Clever Fuzzing
- JIRA Risk workflows
- Kanban for Quality fixes
- Web Services visualisation
- ELK

## TECHNICAL DEBT IS A BAD ANALOGY

- The developers are the ones who pays the debt
- Pollution is a much better analogy
- The key is to make the business accept the risk (i.e the debt)
  - Which is done using the JIRA RISK Workflows



**OWASP**

Open Web Application  
Security Project

[WWW.OWASP.ORG](http://WWW.OWASP.ORG)

# APPSEC AND DEVELOPERS



**OWASP**

Open Web Application  
Security Project

[WWW.OWASP.ORG](http://WWW.OWASP.ORG)



# Disclaimers

- **(unit) Test** - For me a test is anything that can be executed with one of these Unit Test Frameworks: [https://en.wikipedia.org/wiki/List\\_of\\_unit\\_testing\\_frameworks](https://en.wikipedia.org/wiki/List_of_unit_testing_frameworks)
- **RISK** - Abuse the concept, found RISK to be best one for the wide range of issues covered by AppSec, while being understood by all players
- **100% Code Coverage** - not the summit, but base-camp (i.e. not the destination). And 100% code is not enough, we really need 500% or more Code Coverage)
- **AppSec ~ = Non Functional requirements** - AppSec is about understanding and controlling app's unintended behaviours



# AppSec vs InfoSec

- This presentations is about AppSec
- AppSec is about:
  - code, apps, CI, secure coding standards, threat models, frameworks, code dependencies, QA, testing, fuzzing, dev environments, DevOps, ....
- InfoSec is about:
  - Networks, Firewalls, Server security, Anti-virus, IDS, Logging, NOC, Policies, end-user security, mobile devices, AD/Ldap management, user provisioning, DevOps, ....
- If your 'InfoSec' team/person cannot code (and would not be hired by the Dev team), then that is NOT AppSec.
- InfoSec is also very important (workflow described here can also be used by them)

# Developers we need you to join AppSec

- You will become a better developer

 Pinned Tweet



**Dinis Cruz** @DinisCruz · Jun 15

Security makes you a better developer, because "You can't do that" becomes "You are not supposed to do that" and eventually "I just did that"

- You will be paid better



**OWASP**

Open Web Application  
Security Project

[WWW.OWASP.ORG](http://WWW.OWASP.ORG)

# MATURITY MODELS APP



**OWASP**

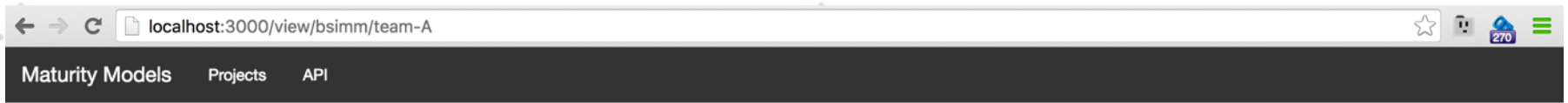
Open Web Application  
Security Project

[WWW.OWASP.ORG](http://WWW.OWASP.ORG)

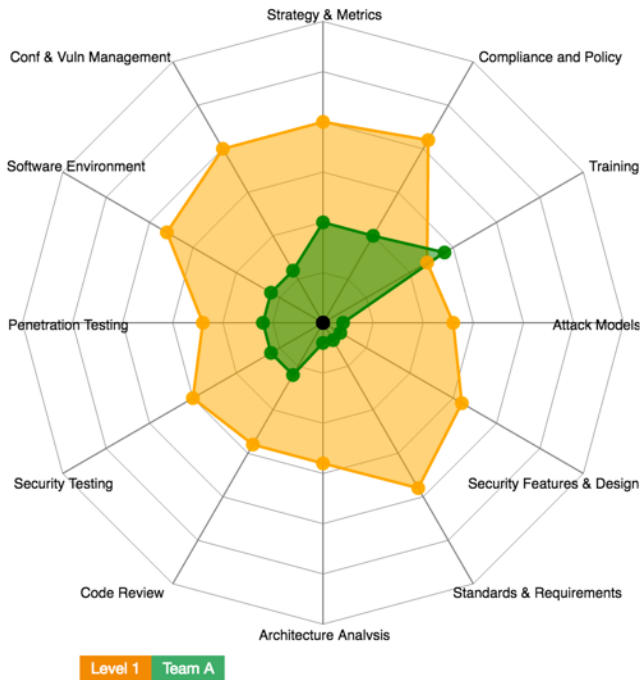
# Maturity Models

- App used on the JIRA tickets examples
- Open Source (<https://github.com/DinisCruz/Maturity-Models>)
- Based on real world mapping of BSIMM on large organisation
- Starting to be compatible with OWASP OpenSAMM (help needed)
- Coded in NodeJS and AngularJS (v1) with 90%+ code coverage and full automated CI

# Visualise Maturity Models



BSIMM TEAM-A view radar edit raw



Governance		Intelligence		SSDL		Deployment	
Activity	Status	Activity	Status	Activity	Status	Activity	Status
SM.1.1	Yes	AM1.2	Maybe	AA.1.1	Maybe	PT.1.1	Maybe
SM.1.4	No	AM1.2.1	Maybe	AA.1.4	Maybe	PT.1.2	Maybe
SM.2.3	Yes	AM1.3	Maybe	CR.1.1	Maybe	PT.2.2	Maybe
CP.1.1	Maybe	AM1.4	Maybe	CR.1.2	Maybe	PT.2.3	Maybe
CP.1.2	Yes	SDF1.1	Maybe	CR.1.5	Maybe	SE.1.1	Maybe
CP.2.1	Yes	SDF1.1	Maybe	CR.2.2	Yes	SE.1.1.1	Maybe
CP.2.2	Maybe	SDF1.2	Maybe	ST.1.1	Maybe	SE.1.1.2	Maybe
CP.2.4	Maybe	SDF1.2.1	Maybe	ST.1.3	Maybe	SE.1.4	Maybe
CP.2.5	Maybe	SR.1.1	Maybe	ST.1.3.1	Maybe	SE.2.2	Maybe
CP.3.2	No	SR.1.2	Maybe	ST.2.1	No	SE.2.4	Maybe
CP.3.2.1	Maybe	SR.1.3	Maybe	ST.2.3	Maybe	SE.3.2	Maybe
CP.3.2.2	Maybe	SR.2.4	No	ST.2.5	Maybe	SE.3.3	Yes
T.1.1	Maybe	SR.2.4.1	No	ST.2.6	Maybe	CMVM.1.1	Maybe
T.1.2	No	SR.2.6	Maybe	ST.3.4	Yes	CMVM.1.2	Yes
T.1.6	Yes	SR.2.5	Maybe	ST.3.5	Maybe	CMVM.2.1	Maybe
T.1.7	No	CMVM.2.2	Maybe				
T.2.5	Yes	CMVM.2.3	Maybe				



# Edit Maturity Model

localhost:3000/view/bsimm/team-random/edit

Maturity Models Projects API

BSIMM TEAM-RANDOM view radar edit raw

Team Name:

Team Random

save

data loaded

## Governance

ID	Yes	No	NA	Maybe
SM.1.1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
SM.1.4	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
SM.2.3	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
CP.1.1	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
CP.1.2	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
CP.2.1	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
CP.2.2	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
CP.2.4	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
CP.2.5	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
CP.3.2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
CP.3.2.1	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
CP.3.2.2	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
T.1.1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
T.1.2	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
T.1.6	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
T.1.7	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
T.2.5	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
T.2.6	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
T.3.2	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
T.3.4	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

## Intelligence

ID	Yes	No	NA	Maybe
AM1.2	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
AM1.2.1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
AM1.3	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
AM1.4	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
SDF1.1	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
SDF1.1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
SDF1.2	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
SDF1.2.1	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
SR.1.1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
SR.1.2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
SR.1.3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
SR.2.4	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
SR.2.4.1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
SR.2.6	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
SR.2.5	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

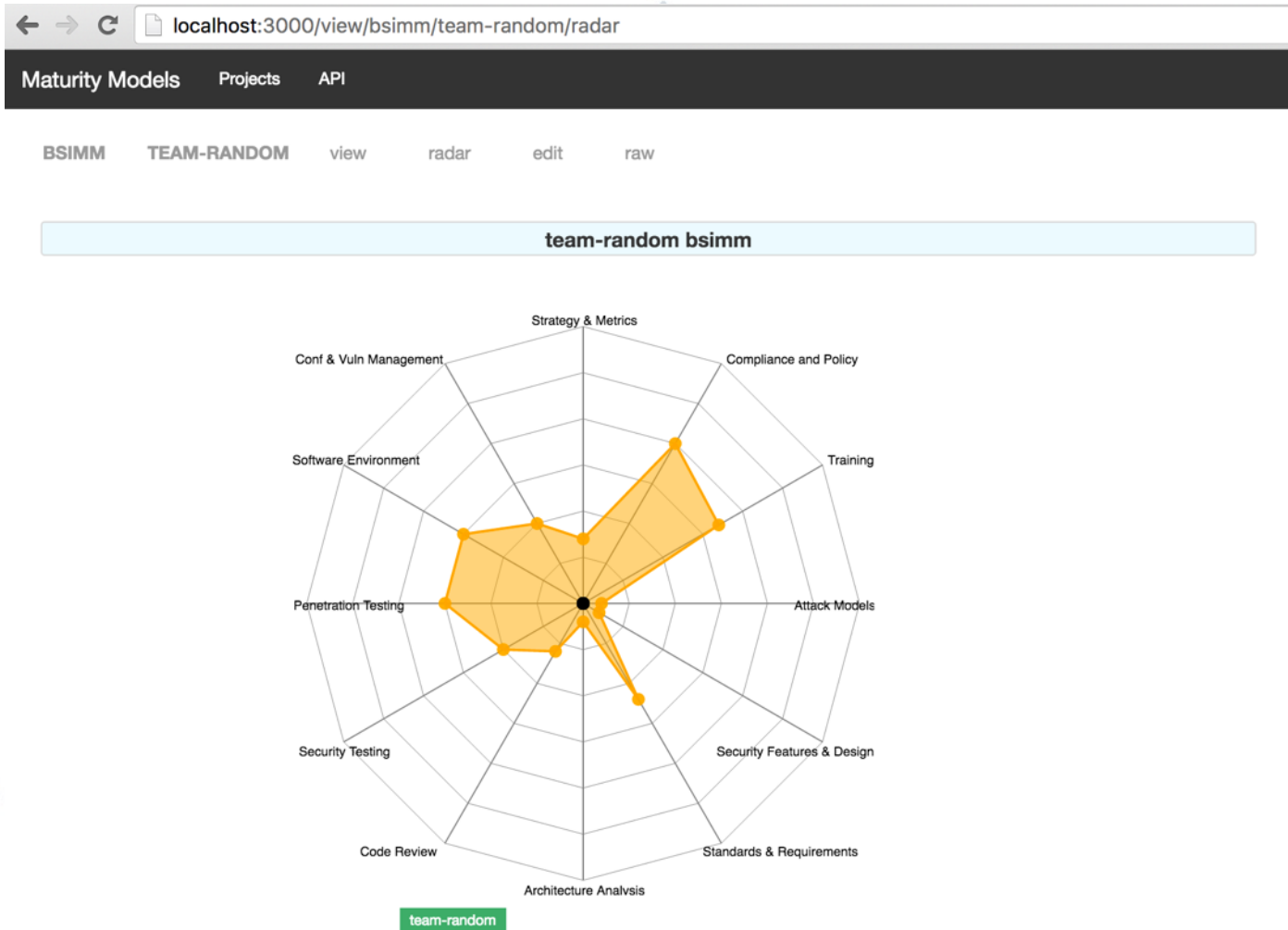
## SSDL

ID	Yes	No	NA	Maybe
AA.1.1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
AA.1.4	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
CR.1.1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
CR.1.2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
CR.1.5	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
CR.2.2	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ST.1.1	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
ST.1.3	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
ST.1.3.1	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
ST.2.1	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
ST.2.3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
ST.2.5	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
ST.2.6	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
ST.3.4	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
ST.3.5	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## Deployment

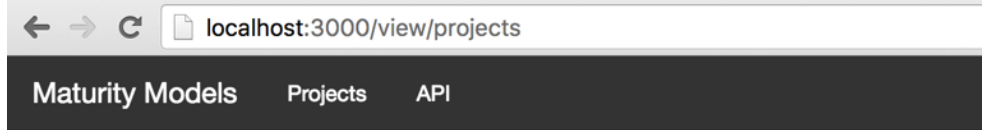
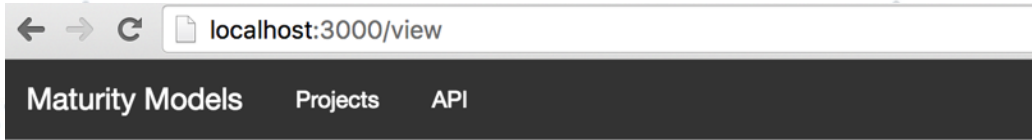
ID	Yes	No	NA	Maybe
PT.1.1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PT.1.2	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PT.2.2	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
PT.2.3	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
SE.1.1	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
SE.1.1.1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
SE.1.1.2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
SE.1.4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
SE.2.2	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
SE.2.4	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
SE.3.2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
SE.3.3	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
CMVM.1.1	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
CMVM.1.2	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
CMVM.2.1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
CMVM.2.2	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
CMVM.2.3	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
CMVM.3.1	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
CMVM.3.2	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

# View Maturity Model Radar chart



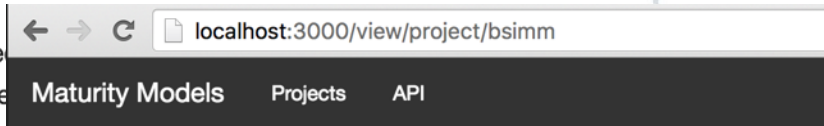


# View projects and schema



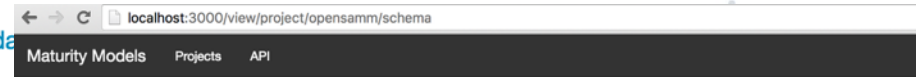
## Projects

- [appsec](#) , see
- [bsimm](#) , see
- [opensamm](#)



## Project bsimm

- [coffee-da](#)
- [empty](#)
- [json-data](#)
- [save-test](#)
- [team-A](#)
- [team-B](#)
- [team-C](#)
- [team-ran](#)



## Schema for Project opensamm - 77 activities

Key	Level	Activity
SM.1.A	1	Is there a software security assurance program in place?
SM.1.B	1	Are development staff aware of future plans for the assurance program?
SM.1.C	1	Do the business stakeholders understand your organization's risk profile?
SM.2.A	2	Are many of your applications and resources categorized by risk?
SM.2.B	2	Are risk ratings used to tailor the required assurance activities?
SM.2.C	2	Does the organization know about what's required based on risk ratings?
SM.3.A	3	Does the organization know about what's required based on risk ratings?
SM.3.B	3	Does your organization regularly compare your security spend with that of other organizations?
PC.1.A	1	Do project stakeholders know their project's compliance status?
PC.1.B	1	Are compliance requirements specifically considered by project teams?
PC.2.A	2	Does the organization utilize a set of policies and standards to control software development?
PC.2.B	2	Are project teams able to request an audit for compliance with policies and standards?
PC.3.A	3	Are projects periodically audited to ensure a baseline of compliance with policies and standards?
PC.3.B	3	Does the organization systematically use audits to collect and control compliance evidence?
EG.1.A	1	Have developers been given high-level security awareness training?
EG.1.B	1	Does each project team understand where to find secure development best-practices and guidance?
EG.2.A	2	Are those involved in the development process given role-specific security training and guidance?
EG.2.B	2	Are stakeholders able to pull in security coaches for use on projects?



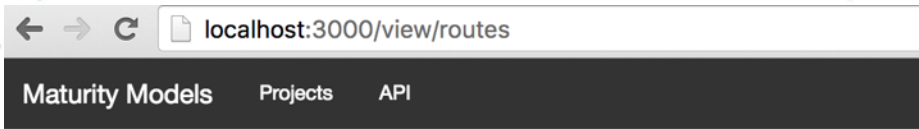
OWASP

Open Web Application  
Security Project

WWW.OWASP.ORG



# Mapped Attack Surface



## API methods

/

/api/v1/data/bsimm/coffee-data/radar

/api/v1/data/bsimm/empty/radar

/api/v1/data/bsimm/json-data/radar

/api/v1/data/bsimm/save-test/radar

/api/v1/data/bsimm/team-A/radar

/api/v1/data/bsimm/team-B/radar

/api/v1/data/bsimm/team-C/radar

/api/v1/data/bsimm/team-random/radar

/api/v1/logs/file/:index

/api/v1/logs/list

/api/v1/logs/path

/api/v1/project/get/:project

/api/v1/project/list

/api/v1/project/schema/:project

/api/v1/routes/list

/api/v1/routes/list-raw

/api/v1/table/bsimm/coffee-data

/api/v1/table/bsimm/empty

/api/v1/table/bsimm/json-data

/api/v1/table/bsimm/save-test

/api/v1/table/bsimm/team-A

/api/v1/table/bsimm/team-B

/api/v1/table/bsimm/team-C

/api/v1/table/bsimm/team-random

/api/v1/team/:project/list

/api/v1/team/bsimm/get/coffee-data

/api/v1/team/bsimm/get/empty

/api/v1/team/bsimm/get/json-data

/api/v1/team/bsimm/get/save-test

/api/v1/team/bsimm/get/team-A

/api/v1/team/bsimm/get/team-B

/api/v1/team/bsimm/get/team-C

/api/v1/team/bsimm/get/team-random

/api/v1/team/bsimm/save/coffee-data

/api/v1/team/bsimm/save/empty

/api/v1/team/bsimm/save/json-data

/api/v1/team/bsimm/save/save-test

/api/v1/team/bsimm/save/team-A

/api/v1/team/bsimm/save/team-B

/api/v1/team/bsimm/save/team-C

/api/v1/team/bsimm/save/team-random

/ping

/view\*



OWASP

Open Web Application  
Security Project

WWW.OWASP.ORG

# Continuous Integration (CI)

1. Dev pushes code to GitHub
2. Github (main code repo)
  - sends web hook to Travis
3. Travis
  - clones repo, runs tests (API and UI)
  - builds Docker Image (if all tests pass)
  - push Docker Image to Docker Hub
  - clones QA repo fork, sync with QA repo, adds extra commit to QA repo fork, pushes to QA repo Fork
4. Docker Hub
  - sends web hook to Docker Cloud
5. Docker Cloud
  - contacts mapped Node (Digital Ocean VM with Docker installer)
  - docker host pulls image from Docker cloud
  - docker container starts
6. Github (QA fork repo)
  - sends web hook to Travis
7. Travis
  - clones repo, runs tests (QA against deployed docker image on Digital ocean)
  - (in the future) will send web hook to deploy to production (if all tests pass)



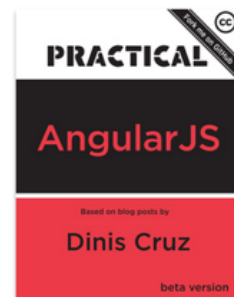
# Technologies used (40x)

This section contains all the different technologies that I used in the development of the Maturity-Models project

In alphabetical order

- [Agile-using-Kandan-WIP](#)
- [Bower](#)
- [CoffeeScript](#)
- [Css](#)
- [D3](#)
- [Digital Ocean](#)
- [Docker](#)
  - [Docker Hub](#)
  - [Docker Cloud](#)
- [Electrium](#)
- [Foundation](#)
- [Git](#)
  - [Git Branches](#)
  - [Git Commits](#)
  - [Git SourceTree](#)
  - [Git Submodules](#)
  - [Git Tags](#)
  - [Git Rebase](#)
- [GitHub](#)
- [Gulp](#)
- [Html](#)
- [Javascript](#)
- [Jira](#)
- [jQuery](#)
- [Node](#)
  - [Node Express](#)
  - [Node Fluentnode](#)
  - [Node JsDom](#)
  - [Node Karma](#)
  - [Node Mocha](#)
  - [Node Morgan](#)
  - [Node Npm](#)
  - [Node PhantomJS](#)
  - [Node modules](#)
  - [Node Supertest](#)
- [Open Source](#)
- [Pug](#)
- [Travis](#)
- [WallabyJs](#)
- [WebStorm](#)

see book for details on each of these technologies



# SECURITY CHAMPIONS



**OWASP**

Open Web Application  
Security Project

[WWW.OWASP.ORG](http://WWW.OWASP.ORG)

# Security Champions (SC)

## What are Security Champions and what do they do?

Security Champions are a key element of an AppSec team, since they create an cross-functional team focused on Application Security

Here is an good definition for you to customise to your culture and workflows:

### What is an Security Champion?

- Security Champions are active members of a team that may help to make decisions about when to engage the Security Team
- Act as the "voice" of security for the given product or team
- Assist in the triage of security bugs for their team or area

### What do they do?

- Actively participate in the AppSec JIRA and WIKI
- Collaborate with other security champions
  - Review impact of 'breaking changes' made in other projects
- Attend weekly meetings
- Are the single point of contact for their assigned team
- Ensure that security is not a blocker on active development or reviews
- Assist in making security decisions for their team
  - Low-Moderate security impact
    - Empowered to make decisions
    - Document decisions made in bugs or wiki
  - High-Critical security impact
    - Work with AppSec team on mitigations strategies
- Help with QA and Testing
  - Write Tests (from Unit Tests to Integration tests)
  - Help with development of CI (Continuous Integration) environments

<http://blog.diniscruz.com/2015/10/what-are-security-champions-and-what-do.html>



**OWASP**

Open Web Application  
Security Project

[WWW.OWASP.ORG](http://www.owasp.org)

# If you don't have an SC, get a Mug



Basically that 'Security Expert' Mug should represent the fact that at the moment when a developer has an Application Security question, he might as well ask the dude on that Mug for help :)

I also like that it re-enforces the idea, that for most developer teams, **just having somebody assigned to application security**, is already a massive step forward!!

Basically we have such a skill shortage in our industry for application security devs that **'if you have a heart-beat you qualify'**



**OWASP**

Open Web Application  
Security Project

[WWW.OWASP.ORG](http://WWW.OWASP.ORG)



# JIRA WORKFLOW



**OWASP**

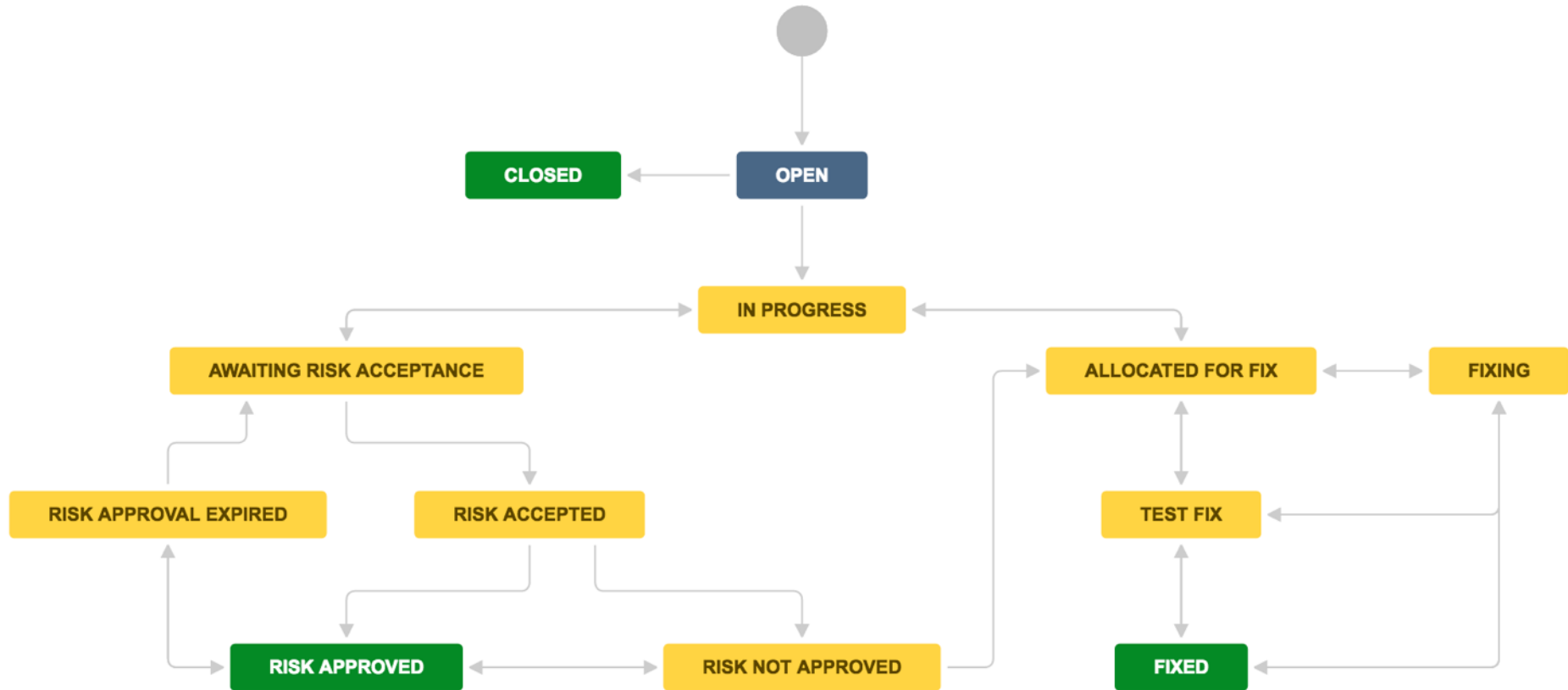
Open Web Application  
Security Project

[WWW.OWASP.ORG](http://WWW.OWASP.ORG)

# Proposed JIRA workflow

1. Open JIRA issues for all AppSec issues
2. Write passing tests for issues reported
3. Manage using AppSec RISK workflow
  1. **Fix Path:** Open, Allocated for Fix, Fix, Test Fix, Close
  2. **Accept Risk Path:** Open, Accept Risk, Approve Risk, (Expire Risk)
4. Automatically report RISK's status

# RISK Workflow (using JIRA in Cloud)

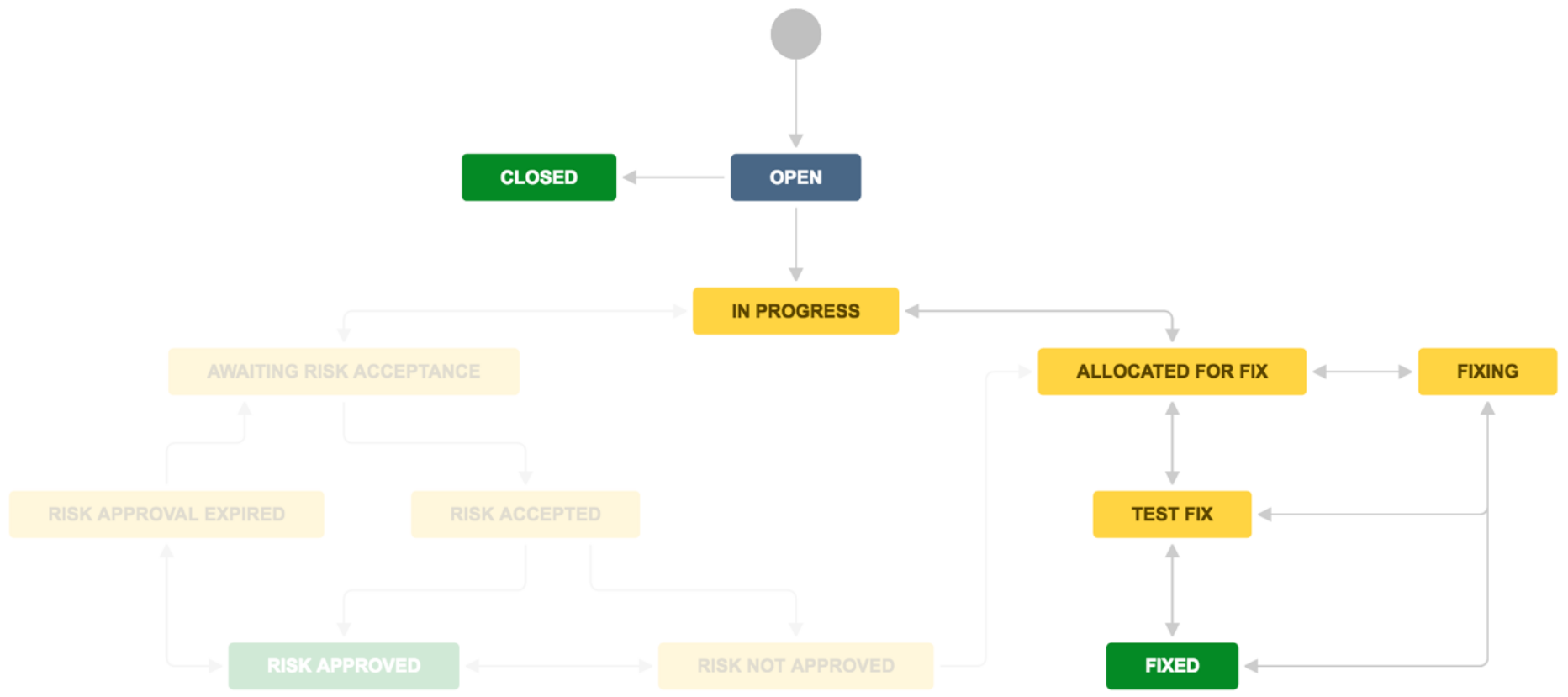


**OWASP**

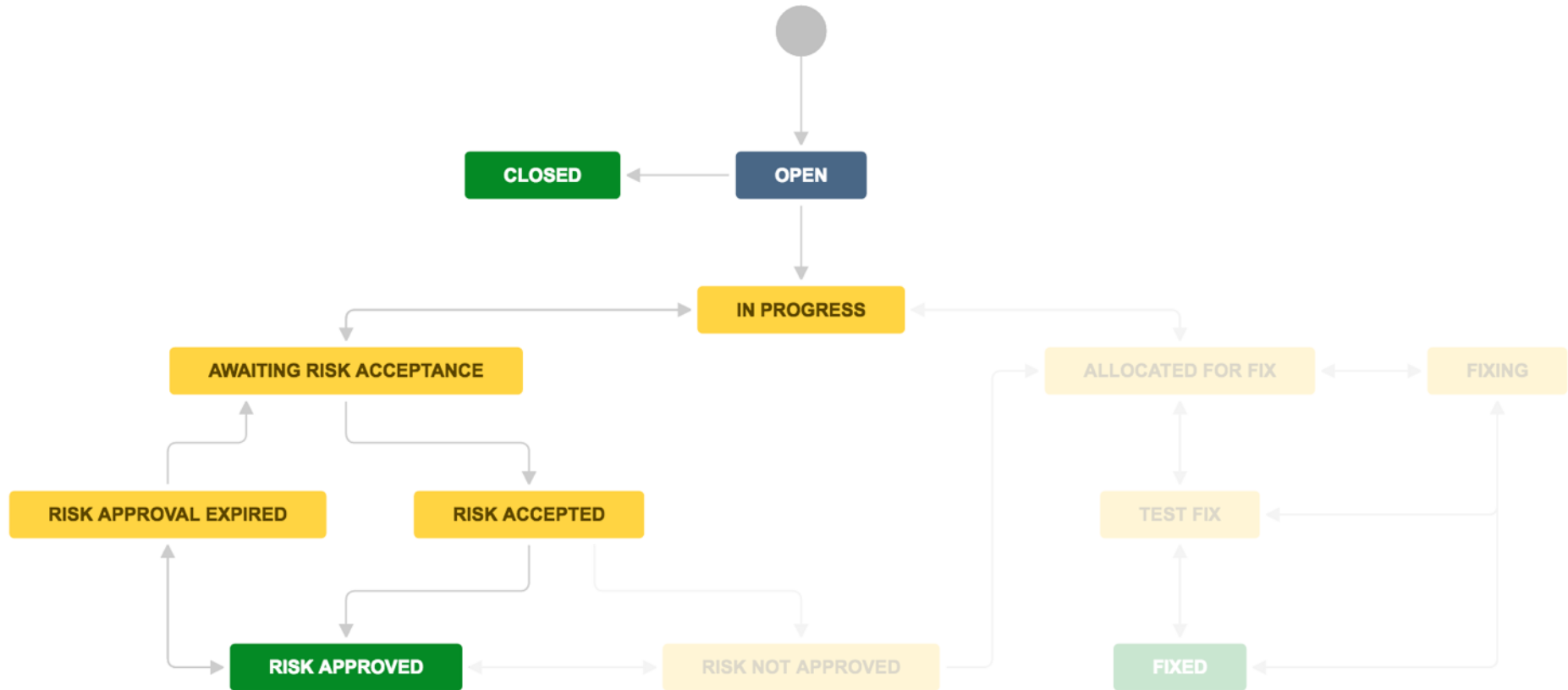
Open Web Application  
Security Project

[WWW.OWASP.ORG](http://WWW.OWASP.ORG)

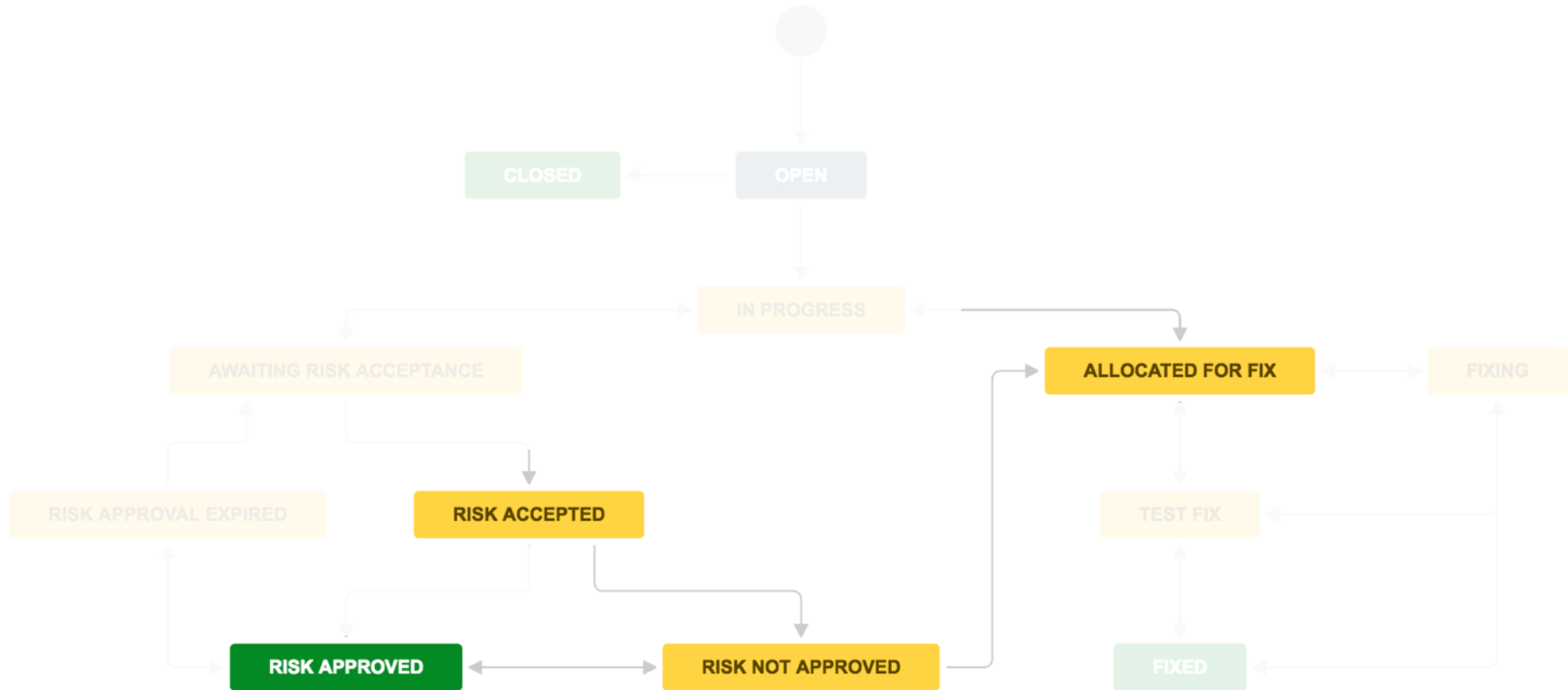
# PATH #1 - Fix issue



# PATH #2 - Accept and Approve RISK



# PATH #2 - Variation when risk not approved



# 'FIX' PATH



**OWASP**  
Open Web Application  
Security Project

[WWW.OWASP.ORG](http://WWW.OWASP.ORG)

# Issue: Data\_Files.set\_File\_Data - Path Traversal

Create issue Configure Fields

Project RISK - AppSec (RISK)

Issue Type Risk

---

Summary Data\_Files.set\_File\_Data - Path Traversal

Reporter Dinis [Administrator]  
Start typing to get a list of possible matches.

Component/s **None**

Description

Style | B | I | U | A |  $\frac{3}{4}A$  | | | | | | + |

Current implementation of Data\_Files.set\_File\_Data (here and below) is vulnerable by design to an Path Traversal attack.

This will allow any caller to write into files outside the expected data folder

```
{code}
set_File_Data: (filename, file_Contents) ->
  if not filename or not file_Contents
    return null
  if type of file_Contents is not string!
```

Create another Create Cancel





# Status: OPEN



RISK - AppSec / RISK-4

## Data\_Files.set\_File\_Data - Path Traversal

Edit Comment Assign More Close to 'In Progress' Admin

Export

### Details

Type: Risk Status: **OPEN**  
Priority: Medium (View Workflow)  
Resolution: Unresolved  
Labels: None

### People

Assignee: Unassigned  
Assign to me  
Reporter: Dinis [Administrator]  
Votes: 0  
Watchers: 1 Stop watching this issue

### Description

Current implementation of Data\_Files.set\_File\_Data (here and below) is vulnerable by design to an Path Traversal attack.

This will allow any caller to write into files outside the expected data folder

```
set_File_Data: (filename, file_Contents) ->  
  if not filename or not file_Contents  
    return null  
  if typeof file_Contents isnt 'string'  
    return null  
  file_Path = @.find filename  
  if file_Path is null or file_Path.file_Not_Exists()  
    file_Path = @.data_Path.path_Combine filename  
  file_Path.file_Write file_Contents  
  return file_Path
```

At the moment this method is not wired to a controller, but that is exactly what will happen next (since the point of this method is to allow the existing BSIMM mappings to be edited

### Dates

Created: Just now

Risk Workflow



OWASP

Open Web Application Security Project

WWW.OWASP.ORG

# Status: IN PROGRESS



RISK - AppSec / RISK-4

## Data\_Files.set\_File\_Data - Path Traversal

Edit

Comment

Assign

More

Allocate for Fix

Request Risk Acceptance

Admin



Export

### Details

Type: Risk  
Priority: Medium  
Labels: None  
Status: **IN PROGRESS**  
(View Workflow)  
Resolution: Unresolved

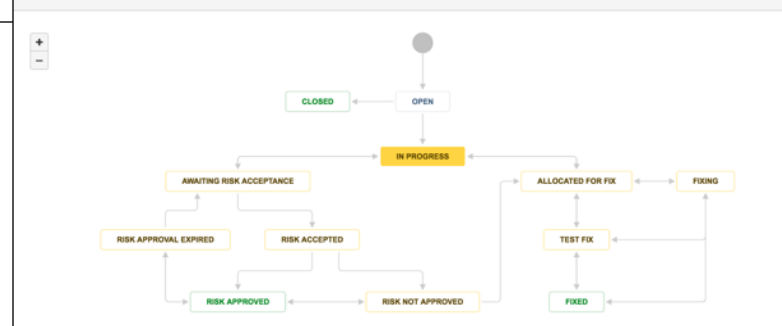
### People

Assignee: Unassigned  
[Assign to me](#)  
Reporter: Dinis [Administrator]  
Votes: 0  
Watchers: 1 [Stop watching this issue](#)

### Description

Current implementation of Data\_Files.set\_File\_Data (here and below) is vulnerable by design to an Path Traversal attack.  
This will allow any caller to write into files outside the expected data folder

Risk Workflow



OWASP

Open Web Application Security Project

WWW.OWASP.ORG

# Status: ALLOCATED FOR FIX



RISK - AppSec / RISK-4

## Data\_Files.set\_File\_Data - Path Traversal

[Edit](#) [Comment](#) [Assign](#) [More ▾](#) [Fixing](#) [Test Fix](#) [to 'In Progress'](#) [Admin ▾](#) [Export ▾](#)

### Details

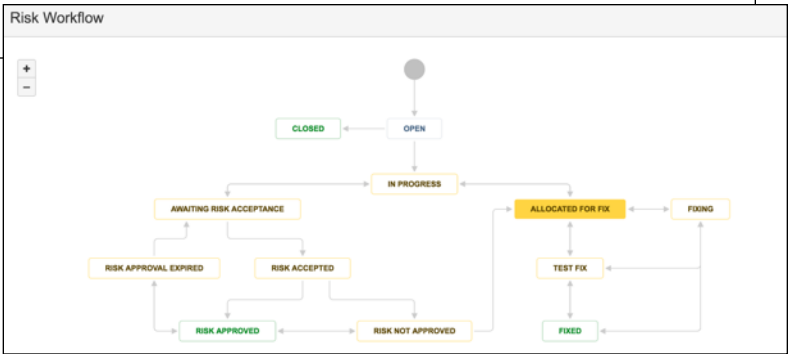
Type:  Risk Status: **ALLOCATED FOR FIX**  
(View Workflow)  
Priority: **↑ Medium** Resolution: Unresolved  
Labels: None

### People

Assignee: Unassigned  
[Assign to me](#)  
Reporter: Dinis  
[Administrator]  
Votes: **0**  
Watchers: **1** [Stop watching this issue](#)  
[Issue](#)

### Description

Current implementation of Data\_Files.set\_File\_Data (here and below) is vulnerable by design to an Path Traversal attack.  
This will allow any caller to write into files outside the expected data folder



# Status: FIXING



RISK - AppSec / RISK-4

## Data\_Files.set\_File\_Data - Path Traversal

[Edit](#) [Comment](#) [Assign](#) [More](#) [Fixed](#) [Test Fix](#) [back to 'Allocated...](#) [Admin](#) [Export](#)

### Details

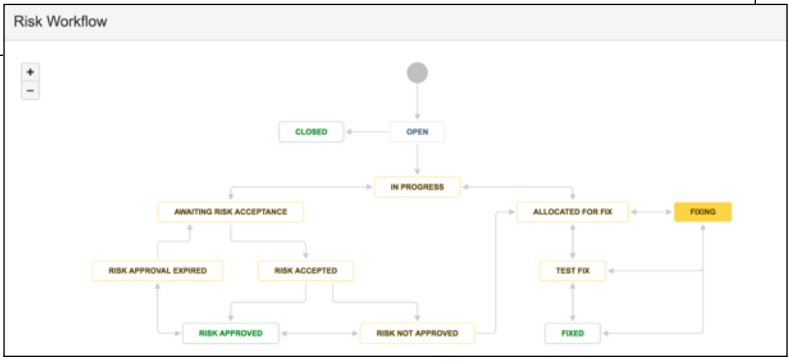
Type:  Risk Status: **FIXING**  
Priority: **Medium** (View Workflow)  
Labels: None Resolution: Unresolved

### People


Assignee: Unassigned (Assign to me)  
Reporter: Dinis [Administrator]  
Votes: 0  
Watchers: 1 Stop watching this issue

### Description

Current implementation of Data\_Files.set\_File\_Data (here and below) is vulnerable by design to an Path Traversal attack.  
This will allow any caller to write into files outside the expected data folder



# Status: TEST FIX

 RISK - AppSec / RISK-4  
**Data\_Files.set\_File\_Data - Path Traversal**

Edit Comment Assign More **Fixed** back to 'Allocated... back to 'Fixing' Admin Export

**Details**

Type:  Risk Status: **TEST FIX**  
Priority:  Medium (View Workflow)  
Labels: None Resolution: Unresolved

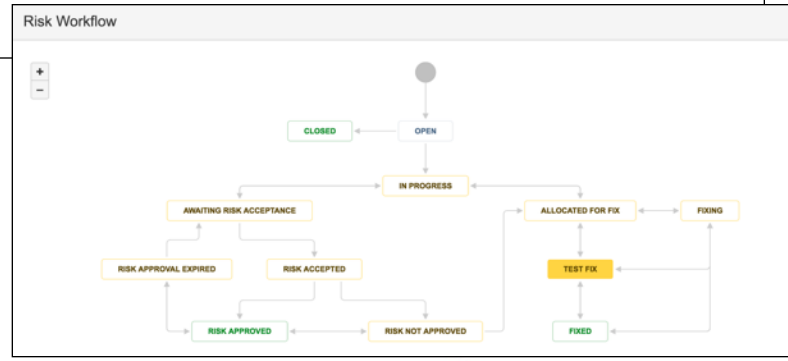
**People**

Assignee: Unassigned (Assign to me)  
Reporter: Dinis [Administrator]  
Votes: 0  
Watchers: 1 Stop watching this issue

**Description**

Current implementation of Data\_Files.set\_File\_Data (here and below) is vulnerable by design to an Path Traversal attack.

This will allow any caller to write into files outside the expected data folder



# Status: FIXED



RISK - AppSec / RISK-4

## Data\_Files.set\_File\_Data - Path Traversal

Edit

Comment

Assign

More

back to 'Fixing'

back to 'Test Fix&...'

Admin



Export

### Details

Type:  Risk Status: **FIXED**  
Priority:  Medium (View Workflow)  
Resolution: Unresolved  
Labels: None

### People

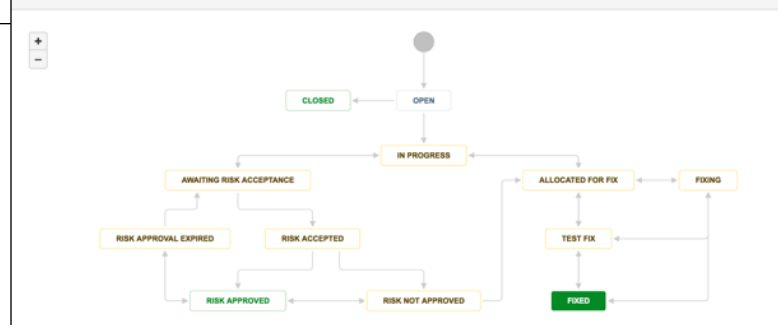
Assignee: Unassigned  
[Assign to me](#)  
Reporter: Dinis  
[Administrator]  
Votes: 0  
Watchers: **1** Stop watching this issue

### Description

Current implementation of Data\_Files.set\_File\_Data (here and below) is vulnerable by design to an Path Traversal attack.

This will allow any caller to write into files outside the expected data folder

Risk Workflow



OWASP

Open Web Application Security Project

WWW.OWASP.ORG

# PATH 'RISK ACCEPT/APPROVE'



**OWASP**  
Open Web Application  
Security Project

[WWW.OWASP.ORG](http://WWW.OWASP.ORG)

# RISK: Support for coffee allows RCE

Create issue Configure Fields

Project

Issue Type

Summary

Reporter   
Start typing to get a list of possible matches.

Component/s **None**

Description 

Related to #24, this is the feature that is currently used to create random data sets (for example on <http://localhost:3000/view/team-random> )

This means that if an attacker is able to edit an data-set (for example on the GitHub repo), he will have RCE on the server (when the team data is loaded)

Note that at the moment only json files are supported for remote editing (see #25)

Fix Version/s **None**

Priority

Create another





# Status: OPEN



RISK - AppSec / RISK-3

## Support for coffee file to create dynamic data sets allow RCE

[Edit](#) [Comment](#) [Assign](#) [More](#) [Close](#) [to 'In Progress'](#) [Admin](#) [Export](#)

### Details

Type:  Risk Status: **OPEN**  
([View Workflow](#))  
Priority: ↑ Medium Resolution: Unresolved  
Labels: None

### People

Assignee: Unassigned  
[Assign to me](#)  
Reporter: Dinis  
[Administrator]  
Votes: 0  
Watchers: **1** [Stop watching this issue](#)

### Description

Related to [#24](#), this is the feature that is currently used to create random data sets (for example on <http://localhost:3000/view/team-random> )

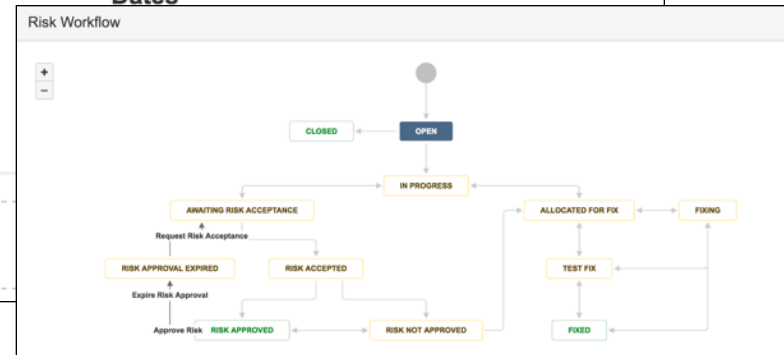
This means that if an attacker is able to edit an data-set (for example on the GitHub repo), he will have RCE on the server (when the team data is loaded)

Note that at the moment only json files are supported for remote editing (see [#25](#))

### Attachments

Drop files to attach, or [browse](#).

### Dates



OWASP

Open Web Application  
Security Project

WWW.OWASP.ORG

# Status: IN PROGRESS



RISK - AppSec / RISK-3

## Support for coffee file to create dynamic data sets allow RCE

[Edit](#) [Comment](#) [Assign](#) [More](#) [Allocate for Fix](#) [Request Risk Acceptance](#) [Admin](#) [Export](#)

### Details

Type:  Risk Status: **IN PROGRESS**  
Priority: **Medium** (View Workflow)  
Labels: None Resolution: Unresolved

### People

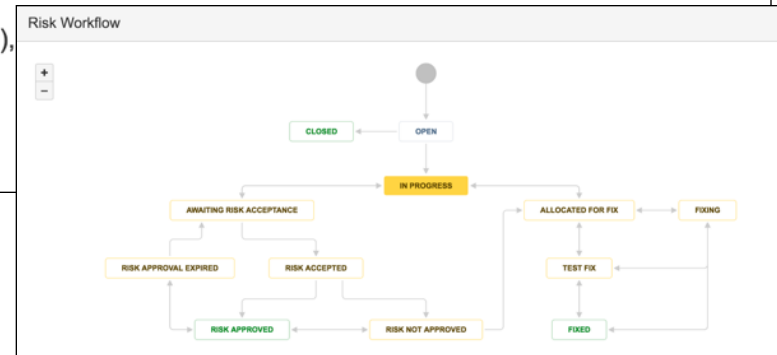
Assignee: Unassigned  
[Assign to me](#)  
Reporter: Dinis [Administrator]  
Votes: 0  
Watchers: 1 [Stop watching this issue](#)

### Description

Related to #24, this is the feature that is currently used to create random data sets (for example on <http://localhost:3000/view/team-random> )

This means that if an attacker is able to edit an data-set (for example on the GitHub repo), will have RCE on the server (when the team data is loaded)

Note that at the moment only json files are supported for remote editing (see #25)



OWASP

Open Web Application Security Project

WWW.OWASP.ORG

# Status: AWAITING RISK ACCEPTANCE



RISK - AppSec / RISK-3

## Support for coffee file to create dynamic data sets allow RCE

[Edit](#) [Comment](#) [Assign](#) [More ▾](#) [Accept Risk](#) [to 'In Progress'](#) [Admin ▾](#) [Export ▾](#)

### Details

Type:  Risk Status: **AWAITING RISK ACC...**  
Priority: ↑ Medium (View Workflow)  
Labels: None Resolution: Unresolved

### People

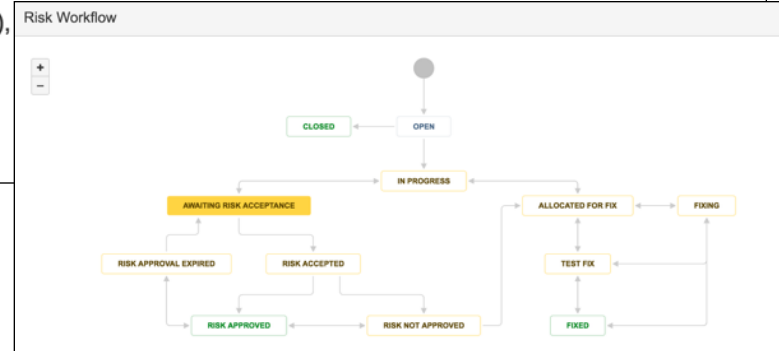
Assignee: Unassigned  
[Assign to me](#)  
Reporter: Dinis  
[Administrator]  
Votes: 0  
Watchers: 1 [Stop watching this issue](#)

### Description

Related to [#24](#), this is the feature that is currently used to create random data sets (for example on <http://localhost:3000/view/team-random> )

This means that if an attacker is able to edit an data-set (for example on the GitHub repo), will have RCE on the server (when the team data is loaded)

Note that at the moment only json files are supported for remote editing (see [#25](#))



OWASP

Open Web Application Security Project

WWW.OWASP.ORG

# Status: RISK ACCEPTED



RISK - AppSec / RISK-3

## Support for coffee file to create dynamic data sets allow RCE

[Edit](#) [Comment](#) [Assign](#) [More](#) [Approve Risk](#) [Don't Approve Risk](#) [Admin](#) [Export](#)

### Details

Type:  Risk Status: **RISK ACCEPTED**  
([View Workflow](#))  
Priority: **Medium** Resolution: Unresolved  
Labels: None

### People

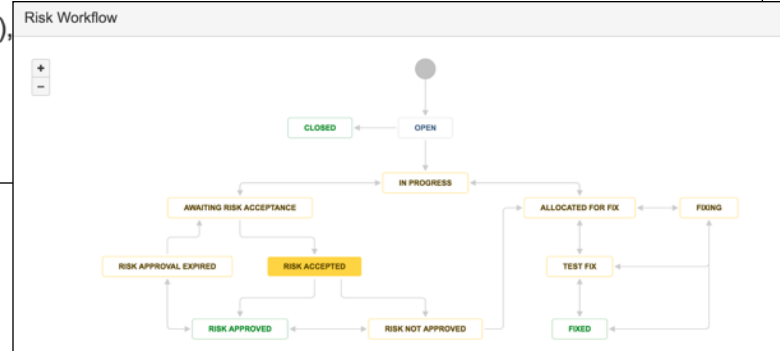
Assignee: Unassigned  
[Assign to me](#)  
Reporter: Dinis [Administrator]  
Votes: 0  
Watchers: **1** [Stop watching this issue](#)

### Description

Related to [#24](#), this is the feature that is currently used to create random data sets (for example on <http://localhost:3000/view/team-random> )

This means that if an attacker is able to edit an data-set (for example on the GitHub repo), will have RCE on the server (when the team data is loaded)

Note that at the moment only json files are supported for remote editing (see [#25](#))



OWASP

Open Web Application Security Project

WWW.OWASP.ORG

# Status: RISK APPROVED



RISK - AppSec / RISK-3

## Support for coffee file to create dynamic data sets allow RCE

[Edit](#) [Comment](#) [Assign](#) [More](#) [Expire Risk Approval](#) [Don't Approve Risk](#) [Admin](#) [Export](#)

### Details

Type:  Risk Status: **RISK APPROVED**  
([View Workflow](#))  
Priority: ↑ Medium Resolution: Unresolved  
Labels: None

### People

Assignee: Unassigned  
[Assign to me](#)  
Reporter: Dinis  
[Administrator]  
Votes: 0  
Watchers: **1** [Stop watching this issue](#)  
[Issue](#)

### Description

Related to [#24](#), this is the feature that is currently used to create random data sets (for example on <http://localhost:3000/view/team-random> )

This means that if an attacker is able to edit an data-set (for example on the GitHub repo), will have RCE on the server (when the team data is loaded)

Note that at the moment only json files are supported for remote editing (see [#25](#))



OWASP

Open Web Application Security Project

WWW.OWASP.ORG

# Status: RISK APPROVED EXPIRED



RISK - AppSec / RISK-3

## Support for coffee file to create dynamic data sets allow RCE

Edit

Comment

Assign

More ▾

Request Risk Acceptance

Approve Risk

Admin ▾



Export ▾

### Details

Type:  Risk Status: **RISK APPROVAL EX...**  
Priority: ↑ Medium (View Workflow)  
Resolution: Unresolved  
Labels: None

### People

Assignee: Unassigned  
[Assign to me](#)  
Reporter: Dinis  
[Administrator]  
Votes: 0  
Watchers: 1 [Stop watching this issue](#)

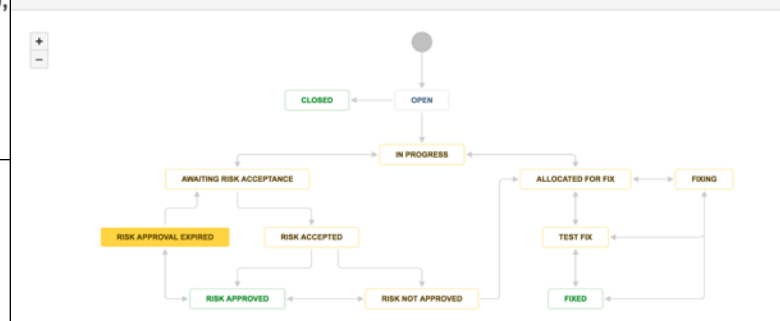
### Description

Related to [#24](#), this is the feature that is currently used to create random data sets (for example on <http://localhost:3000/view/team-random> )

This means that if an attacker is able to edit an data-set (for example on the GitHub repo), will have RCE on the server (when the team data is loaded)

Note that at the moment only json files are supported for remote editing (see [#25](#))

Risk Workflow



OWASP


Open Web Application Security Project

WWW.OWASP.ORG


# All status changes are tracked

**Activity**

All Comments Work log **History** Activity ↑


 [Dinis \[Administrator\]](#) created issue - 5 minutes ago

---

 [Dinis \[Administrator\]](#) made changes - 4 minutes ago


Field	Original Value	New Value
Status	Open [ 1 ]	In Progress [ 3 ]

---

 [Dinis \[Administrator\]](#) made changes - 3 minutes ago


Status	In Progress [ 3 ]	Awaiting Risk Acceptance [ 1 ]
--------	-------------------	--------------------------------

---

 [Dinis \[Administrator\]](#) made changes - 2 minutes ago


Status	Awaiting Risk Acceptance [ 10007 ]	Risk Accepted [ 10008 ]
--------	------------------------------------	-------------------------

---

 [Dinis \[Administrator\]](#) made changes - 1 minute ago


Status	Risk Accepted [ 10008 ]	Risk Approved [ 10009 ]
--------	-------------------------	-------------------------

---

 [Dinis \[Administrator\]](#) made changes - 1 minute ago

Status	Risk Approved [ 10009 ]	Risk Approval Expired [ 1001 ]
--------	-------------------------	--------------------------------

---

 [Dinis \[Administrator\]](#) made changes - Just now

Status	Risk Approval Expired [ 10011 ]	Risk Approved [ 10009 ]
--------	---------------------------------	-------------------------



# CASE STUDY: WHEN I CREATED A VULNERABILITY



**OWASP**

Open Web Application  
Security Project

[WWW.OWASP.ORG](http://WWW.OWASP.ORG)



# Feature request: Allow data editing on UI

- Here is the code I wrote (at the Data Layer)

```
56     set_File_Data: (filename, file_Contents) ->
57         if not filename or not file_Contents
58             return null
59         if typeof file_Contents isnt 'string'
60             return null
61         file_Path = @.find filename
62         if file_Path is null or file_Path.file_Not_Exists()
63             file_Path = @.data_Path.path_Combine filename
64         file_Path.file_Write file_Contents
65         return file_Path
```

- This method is designed to be called by the controller (i.e. rest api endpoint):

# Data\_Files.set\_File\_Data - Path Traversal #19

 **Closed** DinisCruz opened this issue 27 days ago · 2 comments



DinisCruz commented 27 days ago · edited

Owner



Current implementation of Data\_Files.set\_File\_Data ([here](#) and below) is vulnerable by design to an [Path Traversal](#) attack.

This will allow any caller to write into files outside the expected [data folder](#)

```
set_File_Data: (filename, file_Contents) ->
  if not filename or not file_Contents
    return null
  if typeof file_Contents isnt 'string'
    return null
  file_Path = @.find filename
  if file_Path is null or file_Path.file_Not_Exists()
    file_Path = @.data_Path.path_Combine filename
  file_Path.file_Write file_Contents
  return file_Path
```



**OWASP**

Open Web Application  
Security Project

WWW.OWASP.ORG

# Regression test that passes on issue

```
describe '_securtiy | A1 - Injection', ->

  # https://github.com/DinisCruz/BSIMM-Graphs/issues/21
  it 'Issue 19 - Data_Files.set_File_Data - Path Traversal', ->
    using new Data_Files(), ->
      folder_Name = 'outside-data-root'
      file_Name = 'some-file.txt'
      file_Content = 'some content'
      target_Folder = @.data_Path.path_Combine('../' + folder_Name) # Create target
                                                                .folder_Create()
                                                                .assert_Folder_Exists() # Confirm it exists

      target_Folder.path_Combine(file_Name) # Create target
      .file_Write(file_Content)
      .assert_File_Exists() # Confirm it exists

      payload = "../#{folder_Name}/#{file_Name}"
      new_Content = 'new - content'

      @.data_Path.path_Combine(payload)
      .file_Contents().assert_Is file_Content # Confirm original content

      @.set_File_Data payload, new_Content

      @.data_Path.path_Combine(payload)
      .file_Contents().assert_Is_Not file_Content # Confirm original content
      .assert_Is new_Content # Confirm that content is new

      target_Folder.folder_Delete_Recursive().assert_Is_True() # Delete temp folder
```



# Data\_Files.set\_File\_Data - DoS via filename #20



DinisCruz opened this issue 27 days ago · 1 comment



DinisCruz commented 27 days ago · edited

Owner



As seen in #19 the `set_File_Data: (filename, file_Contents)` method does not check the size (and contents) of the filename and file\_Contents variables.

The problem is that they are strings, which means that they can be huge:

- <http://appsandsecurity.blogspot.co.uk/2013/05/should-string-be-abstract-class.html>
- [http://1raindrop.typepad.com/1\\_raindrop/2013/04/security-140-conversation-with-john-wilander.html](http://1raindrop.typepad.com/1_raindrop/2013/04/security-140-conversation-with-john-wilander.html)
- [https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global\\_Objects/String](https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global_Objects/String)
- <http://stackoverflow.com/questions/2219526/how-many-bytes-in-a-javascript-string>
- <http://stackoverflow.com/questions/24153996/is-there-a-limit-on-the-size-of-a-string-in-json-with-node-js>

And since those values are used to on the name and contents of files written on disk, in addition to possible probs in the Node Heap, this function can be used to fill up the disk

Here is the test for this issue which proves that we can create large files and also detects some weird behaviours on the file name size (which is different in wallaby, mocha and travis)



OWASP

Open Web Application  
Security Project

WWW.OWASP.ORG

```

it.only 'Issue 20 - Data_Files.set_File_Data - DoS via filename and file_Contents', ->
  using new Data_Files(), ->
    create_File = (file_Size, content_Size, should_Work)=>
      file_Name      = file_Size  .random_String()
      file_Contents  = content_Size.random_String()
      file_Path      = @.data_Path .path_Combine(file_Name)

      file_Path.assert_File_Not_Exists()           # confirm file doesn't exist

      @.set_File_Data file_Name, file_Contents    # PAYLOAD: create file

      if should_Work                             # if it should work
        file_Path.assert_File_Exists()           # confirm file exists
        file_Path.file_Delete().assert_Is_True() # delete temp file
        file_Path.assert_File_Not_Exists()
      else                                         # if not
        file_Path.assert_File_Not_Exists()       # confirm creation failed

# testing multiple file sizes
create_File 10 ,10 , true
create_File 100,10 , true
create_File 156,10 , true
#create_File 157,10 , false           # interesting in wallaby, at
#create_File 208,10 , false         #           in mocha, it's
create_File 512,10 , false         #           in travis the

# testing multiple file contents
create_File 10 ,10 , true           # 10 bytes
create_File 10 ,100 , true         # 100 bytes
create_File 10 ,10000 , true       # 10 Kb
create_File 10 ,1000000 , true     # 1 Mb
create_File 10 ,10000000 , true    # 10 Mb - will work and take
create_File 10 ,100000000 , true   # 100 Mb - will work and take

```



# Data\_Files.set\_File\_Data - allows creation of files with any extension #23

 Closed

DinisCruz opened this issue 27 days ago · 1 comment



DinisCruz commented 27 days ago · edited

Owner



Related to [#19](#) and [#20](#) , at the moment there is no limitations on the type of files that can be saved.

According with the current design, the only file paths that should be supported are `.json` files

Here is the test that proves the issue

```
it 'Issue 23 - Data_Files.set_File_Data - allows creation of files with any extension', -
  using new Data_Files(), ->
  create_File = (extension)=>
    file_Name      = 10.random_String() + extension
    file_Contents  = 10.random_String()
    file_Path      = @.data_Path .path_Combine(file_Name)

    @.set_File_Data file_Name, file_Contents      # PAYLOAD: create file

    file_Path.assert_File_Exists()               # confirm file exists
                .file_Delete().assert_Is_True() # delete temp file

  create_File '.json'                            # these are the ones that st

  create_File '.json5'
  create_File '.coffee'
  create_File '.js'
  create_File '.exe'
  create_File '.html'
  create_File '.css'
  create_File '...'
```



OWASP

Open Web Application  
Security Project

WWW.OWASP.ORG

# Data\_Files.set\_File\_Data - allows editing of coffee-script files (RCE) #24

[Edit](#)[New Issue](#)**Closed**

DinisCruz opened this issue 27 days ago · 3 comments



DinisCruz commented 27 days ago · edited

Owner



Related to [#23](#) it will be possible to do RCE on the server by editing one of the existing data coffee-scripts files (for example the one used to create random data)

Here is the code from `Data-Files` that creates the security issue, note how the file is updated and the code is executed

```
it 'Issue 24 - Data_Files.set_File_Data - allows editing of coffee-script files (RCE)', -
  using new Data_Files(), ->
  # PREPARE
  new_File_Contents = 'module.exports = ()-> 40+2'
  file_Name         = 'coffee-data'
  file_Path         = @.find_File file_Name
  file_Contents     = file_Path.file_Contents()
  @.get_File_Data(file_Name).user.assert_Is 'in coffee'      # confirm original data

  # TEST
  @.set_File_Data file_Name, new_File_Contents               # PAYLOAD make change
  file_Path.file_Contents().assert_Is new_File_Contents     # confirm it was changed
  delete require.cache[file_Path]                           # clean the node cache
  @.get_File_Data(file_Name).assert_Is '42'                 # it should be 42 now (v

  # CLEAN
  @.set_File_Data file_Name, file_Contents                  # restore file contents
  file_Path.file_Contents().assert_Is file_Contents         # confirm it was reset
  delete require.cache[file_Path]                           # clear the cache again
  @.get_File_Data(file_Name).user.assert_Is 'in coffee'     # confirm original data
```

Labels



risk - fixed

risk - high

security

Milestone



No milestone

Assignees



No one—assign yourself

1 participant



Notifications

[Unsubscribe](#)

You're receiving notifications because you modified the open/close state.

[Lock conversation](#)**OWASP**Open Web Application  
Security Project[WWW.OWASP.ORG](http://WWW.OWASP.ORG)

# Fix for Path transversal



DinisCruz commented 27 days ago • edited

Owner



This has now been fixed.

Here is the updated version of this method that doesn't have the path traversal issue

```
set_File_Data: (filename, file_Contents) ->

    if not filename or not file_Contents                # check if both values are set
        return null

    if typeof file_Contents isnt 'string'              # check if file_Contents is a string
        return null

    file_Path = @.find_File filename                   # resolve file path based on file r

    if file_Path is null or file_Path.file_Not_Exists() # check if was able to resolve it
        return null

    file_Path.file_Write file_Contents
```



OWASP

Open Web Application  
Security Project

WWW.OWASP.ORG



# Regression test

For reference here is the regression test that confirms that it is not possible to write to files outside the data folder:

```
describe '_regression | A1 - Injection', ->

# https://github.com/DinisCruz/BSIMM-Graphs/issues/21
it 'Issue 19 - Data_Files.set_File_Data - Path Traversal', ->
  using new Data_Files(), ->
    folder_Name = 'outside-data-root'
    file_Name   = 'some-file.txt'
    file_Content = 'some content'
    target_Folder = @.data_Path.path_Combine('./' + folder_Name)      # Create target
    .folder_Create()
    .assert_Folder_Exists()      # Confirm it exists

    target_Folder.path_Combine(file_Name)      # Create target
    .file_Write(file_Content)
    .assert_File_Exists()      # Confirm it exists

    payload      = "../#{folder_Name}/#{file_Name}"
    new_Content = 'new - content'

    @.data_Path.path_Combine(payload)
    .file_Contents().assert_Is file_Content      # Confirm original content

    assert_Is_Null @.set_File_Data payload, new_Content      # PAYLOAD: Creat

    @.data_Path.path_Combine(payload)
    .file_Contents().assert_Is file_Content      # Confirm original content

    target_Folder.folder_Delete_Recursive().assert_Is_True()      # Delete temp fo
```



OWASP

Open Web Application  
Security Project

WWW.OWASP.ORG

**LET'S SEE HOW IT LOOKED IN  
THE CODE**



**OWASP**  
Open Web Application  
Security Project

[WWW.OWASP.ORG](http://WWW.OWASP.ORG)

# ...before the vuln is created

```
51 #set_File_Data: fileName
52
53 list: ()=>
54   @.files().file_Names()
55
56 files: =>
57   values = []
58   for file in @.data_Path.files_Recursive()
59     if file.file_Extension() in ['.json', '.json5', '.coffee']
60       values.push file.remove(@.data_Path)
61   values
--
```



# ...when the vuln is created

```
56 set_File_Data: (filename, file_Contents) ->
57     if not filename or not file_Contents
58         return null
59     if typeof file_Contents isnt 'string'
60         return null
61     file_Path = @.find filename
62     if file_Path is null or file_Path.file_Not_Exists()
63         file_Path = @.data_Path.path_Combine filename
64     file_Path.file_Write file_Contents
65     return file_Path
```



# ... adding comments

```
56 set_File_Data: (filename, file_Contents) ->
57     if not filename or not file_Contents
58         return null
59     if typeof file_Contents isnt 'string'
60         return null
61     file_Path = @.find filename
62     if file_Path is null or file_Path.file_Not_Exists()
63         file_Path = @.data_Path.path_Combine filename
64     file_Path.file_Write file_Contents
65     return file_Path

# todo: add security issue: that this method will allow the writing
#       of any file (not just the files in the data
#       folder, which are the ones that should be edited)

# todo: add security issue: filename is not validated

# todo: add security issue: directory transvesal
# todo: add security issue: no authorization, will write outside d
```



# ...after issues are created

```
54 # Issue 19 - Data_Files.set_File_Data - Path Traversal
55 # Issue 20 - Data_Files.set_File_Data - DoS via filename and file_Contents
56 # Issue 23 - Data_Files.set_File_Data - allows creation of files with any extension
57 set_File_Data: (filename, file_Contents) ->
58     if not filename or not file_Contents
59         return null
60     if typeof file_Contents isnt 'string'
61         return null
62     file_Path = @.find filename
63     if file_Path is null or file_Path.file_Not_Exists()
64         file_Path = @.data_Path.path_Combine filename
65     file_Path.file_Write file_Contents
66     return file_Path
```



# ...improving comments

```
54 # Issue 19 - Data_Files.set_File_Data - Path Traversal
55 # Issue 20 - Data_Files.set_File_Data - DoS via filename and file_Contents
56 # Issue 23 - Data_Files.set_File_Data - allows creation of files with any extension
57 set_File_Data: (filename, file_Contents) ->
58
59     if not filename or not file_Contents           # check if both values are set
60         return null
61
62     if typeof file_Contents isnt 'string'         # check if file_Contents is a string
63         return null
64
65     file_Path = @.find_File filename             # resolve file path based on file name
66
67     if file_Path is null or file_Path.file_Not_Exists() # check if was able to resolve it
68         return null
69
70     file_Path.file_Write file_Contents
```



# ...updating issues after 1st fix

```
60 # Issue 24 - Data_Files.set_File_Data - allows editing of coffee-script files (RCE)
61 # Issue 25 - Refactor set_File_Data to Set_File_Data_JSON
62 # Issue 26 - Data_Files.set_File_Data - DoS via file_Contents
63 set_File_Data: (filename, file_Contents) ->
64
65     if not filename or not file_Contents           # check if both values are set
66         return null
67
68     if typeof file_Contents isnt 'string'         # check if file_Contents is a string
69         return null
70
71     file_Path = @.find_File filename              # resolve file path based on file name
72
73     if file_Path is null or file_Path.file_Not_Exists() # check if was able to resolve it
74         return null
75
76     file_Path.file_Write file_Contents
```





# ... after final fix

```
60 # Issue 26 - Data_Files.set_File_Data - DoS via file_Contents
61 set_File_Data_Json: (filename, json_Data) ->
62
63     if not filename or not json_Data # check if both values are set
64         return null
65
66     if typeof json_Data isnt 'string' # check if file_Contents is a string
67         return null
68
69     try # confirm that json_Data parses OK into JSON
70         JSON.parse json_Data
71     catch
72         return null
73
74     file_Path = @.find_File filename # resolve file path based on file name
75
76     if file_Path is null or file_Path.file_Not_Exists() # check if was able to resolve it
77         return null
78
79     if file_Path.file_Extension() isnt '.json' # check that the file is .json
80         return null
81
82
83     file_Path.file_Write json_Data # after all checks save file
84
85     return file_Path.file_Contents() is json_Data # confirm file was saved ok
```



# KEY CONCEPTS FOR JIRA RISK WORKFLOW



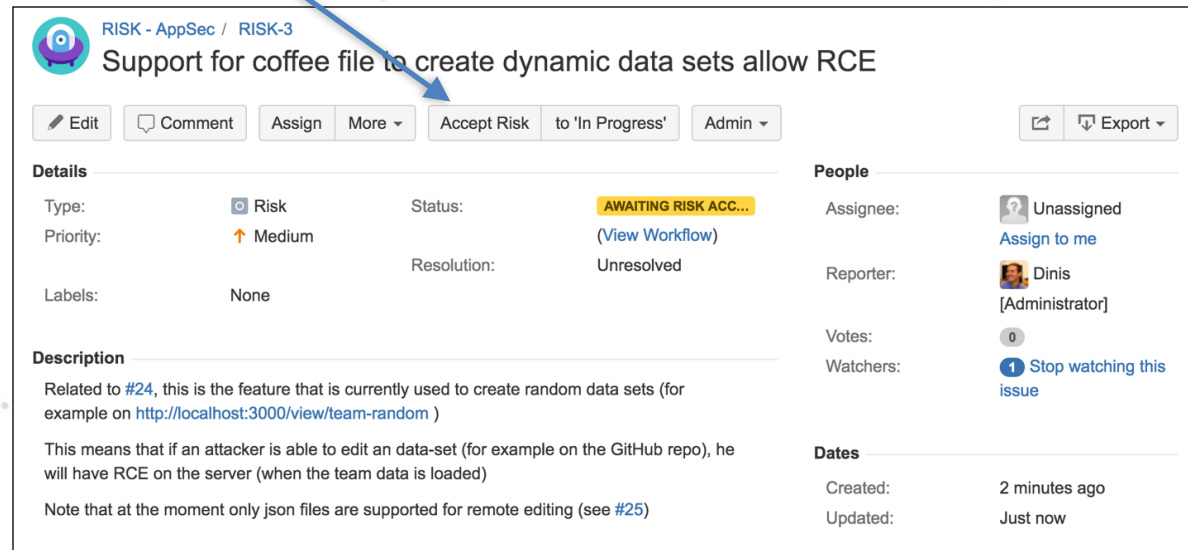
**OWASP**

Open Web Application  
Security Project

[WWW.OWASP.ORG](http://WWW.OWASP.ORG)

# Key for AppSec JIRA workflow is this button

Accept Risk



RISK - AppSec / RISK-3

## Support for coffee file to create dynamic data sets allow RCE

Edit Comment Assign More Accept Risk to 'In Progress' Admin Export

**Details**

Type:	Risk	Status:	AWAITING RISK ACC... (View Workflow)
Priority:	Medium	Resolution:	Unresolved
Labels:	None		

**Description**

Related to #24, this is the feature that is currently used to create random data sets (for example on <http://localhost:3000/view/team-random> )

This means that if an attacker is able to edit a data-set (for example on the GitHub repo), he will have RCE on the server (when the team data is loaded)

Note that at the moment only json files are supported for remote editing (see #25)

**People**

Assignee: Unassigned  
[Assign to me](#)

Reporter: Dinis [Administrator]

Votes: 0

Watchers: 1 [Stop watching this issue](#)

**Dates**

Created: 2 minutes ago

Updated: Just now



OWASP

Open Web Application  
Security Project

WWW.OWASP.ORG

# Separate JIRA project

- This is a separate JIRA repo from the one used by devs
  - I like to call that project 'RISK'
  - This avoids project 'issue creation' politics and 'safe harbour for:
    - known issues
    - 'shadow of a vulnerability' issues
    - 'this could be an problem...' issues
    - 'app is still in development' issues
  - When deciding to fix an issue:
    - that is the moment to create an issue in the target project JIRA (or whatever bug tracking system they used)
  - When issue is fixed (and closed on target project JIRA):
    - AppSec confirms fix and closes RISK



# Always moving until fix or acceptance

- Key is to understand that issues need to be moving on one of two paths:
  - Fix
  - Risk Accepted (and approved)
- Risks (i.e. issues) are never in 'Backlog'
- If an issue is stuck in '**allocated for fix**', then it will be moved into the '**Awaiting Risk Acceptance**' stage

# You need volume

- If you don't have 350+ issues on your JIRA RISK Project, you are not playing (and don't have enough visibility into what is really going on)
- Allow team A to see what team B had (and scale due due to issue description reuse)
- Problem is not teams with 50 issues, prob is team with 5 issues
- This is perfect for Gamification and to provide visibility into who to reward (and promote)



# Threat model

- All issues identified in Threat Models are added to the JIRA RISK project
- Create Threat models by
  - layer
  - feature
  - bug
- ... that is a topic for another talk



# Mapping to InfoSec risks

**Details**

Type:  Risk Status: [Open \(View Workflow\)](#)

Priority:  Major Resolution: Unresolved

Component/s:

Labels:

Risk: Critical

Security Domain: Application development security

- None
- Information security policies
- Organisation of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations and communications security
- Application development security
- Change management
- Information security incident management
- Risk management
- Business continuity and technology disaster recovery
- Information assurance and compliance

Labels for reporting and filters



**OWASP**

Open Web Application  
Security Project

WWW.OWASP.ORG



# Mapping JIRA Tickets to Tests

Risk / RISK-341

**Missing SSL HSTS Header**

Edit Comment Assign More to 'Test Fix' To 'In Progress' Workflow

**Details**

Type: Risk Status: Allocated for Fix  
Priority: Major (View Workflow)  
Component/s: Resolution: Unresolved  
Labels: appsec:HSTS  
Business Impact: Significant  
Likelihood: Possible  
Calculated Risk: High  
Risk: Medium

**Description**

In order to really enforce ssl we also need the JIRA server to set the HSTS header (see [https://www.owasp.org/index.php/HTTP\\_Strict\\_Transport\\_Security](https://www.owasp.org/index.php/HTTP_Strict_Transport_Security))

Test Results 2s 76ms

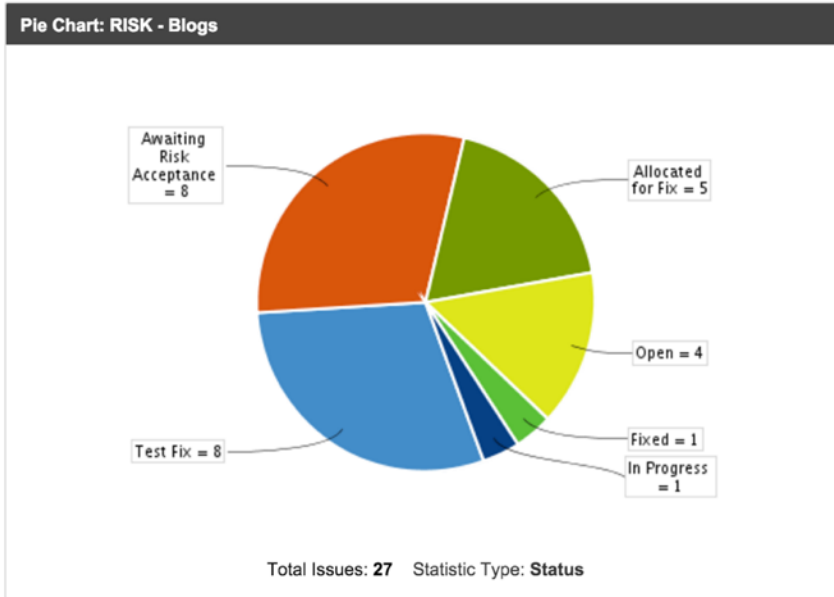
- OK | api | 269ms
- OK | qa | Page\_Home 84ms
- OK | security | regression | live | headers 968ms
- OK | security | regression | live | ssl 443ms
- OK | security | vulns | live | ssl 312ms
- OK | Issue 341 - Missing SSL HSTS header 312ms

```
1 request = require 'request'
2
3 describe 'security | vulns | live | ssl', ->
4   it 'Issue 341 - Missing SSL HSTS header', (done)->
5     url =
6     request.get url, (error, res, data)->
7       res.headers.keys().size().assert_Is 13
8       res.headers.keys().assert_Is [ 'date', 'x-frame-options', 'set-cookie', 'expires', 'cache-control', 'pragma',
9                                     'access-control-allow-origin', 'access-control-allow-methods',
10                                    'access-control-allow-headers',
11                                    'keep-alive', 'connection', 'transfer-encoding', 'content-type' ]
12     assert_Is_Undefined res.headers['strict-transport-security']
13   done()
```

# JIRA AppSec Dashboards

AppSec -

Tools ▾



**Filter Results: Risk -  Awaiting Risk Acceptance**

Key	Summary	Risk	Status
RISK-			Awaiting Risk Acceptance
RISK-			Awaiting Risk Acceptance
RISK-			Awaiting Risk Acceptance
RISK-			Awaiting Risk Acceptance
RISK-			Awaiting Risk Acceptance
RISK-			Awaiting Risk Acceptance
RISK-			Awaiting Risk Acceptance
RISK-			Awaiting Risk Acceptance

1-8 of 8

**Filter Results: Risk -  Allocated for Fix**

Key	Summary	Risk	Status
RISK-		High	Allocated for Fix
RISK-		Low	Allocated for Fix
RISK-		Medium	Allocated for Fix
RISK-		Medium	Allocated for Fix
RISK-		Medium	Allocated for Fix


**Filter Results: Risk -  Risk Accepted**

No matching issues found.

**Filter Results: Risk -  Test Fix**

Key	Summary	Risk	Status
RISK-288		Medium	Test Fix
RISK-284		Medium	Test Fix

# Weekly emails with Risk status

[Redacted] Today at 08:19 

To: [Redacted] Cc: Dinis Cruz  
[Redacted] Risk Accepted

Hi,

We are reviewing the areas of the risk that has been accepted.

The following [screenshot](#) shows your team's related ticket.

Filter Results: [Redacted] - Risk Accepted

Key	Summary	Assignee	Risk Accepted by
RISK-1			
RISK-2			
RISK-2			
RISK-2			
RISK-2			
RISK-1			
RISK-1			
RISK-1			
RISK-1			
RISK-1			

1-10 of 27 1 2 3 ▶



# Other powerful JIRA features

- Components (one per team or project)
- Labels (to add metadata to issues, for OWASP Top 10)
- Links
  - connect with internal/external issues and
  - external resources
- Auto emails
- Copy and paste of images into description
- Markdown
- Security restrictions (use with care)
- Security lock certain actions
- Extra workflow actions for example when moving state)
- Create APPSEC JIRA project for AppSec related tasks (like 'Create Threat Model for app XYZ')

# GITHUB RISK WORKFLOW

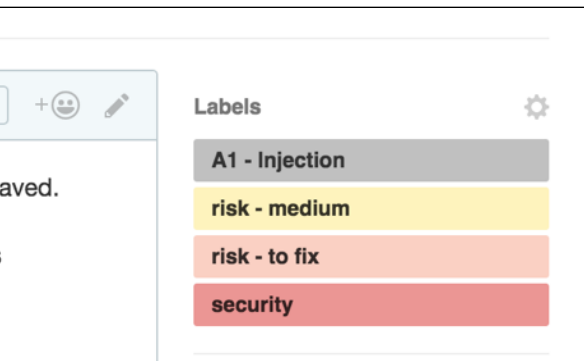












**OWASP**

Open Web Application  
Security Project

[WWW.OWASP.ORG](http://WWW.OWASP.ORG)

# Using GitHub (instead of JIRA)



-  **Server web root (i.e. path) is exposed by API** A6 - Sensitive Data Exposure risk - accepted risk - low security  
test needed  
#31 opened 26 days ago by DinisCruz
-  **All server logs are exposed via API** A6 - Sensitive Data Exposure risk - accepted risk - low security test needed  
#30 opened 26 days ago by DinisCruz
-  **Data\_Files.set\_File\_Data - DoS via file\_Contents** A1 - Injection risk - accepted risk - low security 1
-  **Data\_Files.set\_File\_Data - allows editing of coffee-script files (RCE)** risk - fixed risk - high security 3  
#24 opened 27 days ago by DinisCruz
-  **Data\_Files.set\_File\_Data - allows creation of files with any extension** A1 - Injection risk - medium risk - to fix 1  
security  
#23 opened 27 days ago by DinisCruz
-  **Write regression test to prove that Data-Files.find method is not vulnerable to A1-Injection** A1 - Injection 1  
risk - accepted security test needed  
#22 opened 27 days ago by DinisCruz
-  **Data\_Files.set\_File\_Data - DoS via filename** risk - fixed risk - medium security test needed 1  
#20 opened 27 days ago by DinisCruz
-  **Data\_Files.set\_File\_Data - Path Traversal** A1 - Injection risk - fixed risk - medium security 2  
#19 opened 27 days ago by DinisCruz
-  **Api-Controller - filename is a string and it is not validated** risk - accepted security test needed 1  
#18 opened 28 days ago by DinisCruz
-  **There is no data classification of assets used** A6 - Sensitive Data Exposure risk - accepted risk - low security 1  
#17 opened 28 days ago by DinisCruz



 **Data\_Files.set\_File\_Data - allows editing of coffee-script files (RCE)** risk - fixed risk - high security

#24 opened 27 days ago by DinisCruz

 **Data\_Files.set\_File\_Data - DoS via filename** risk - fixed risk - medium security test needed

#20 opened 27 days ago by DinisCruz

 **Data\_Files.set\_File\_Data - Path Traversal** A1 - Injection risk - fixed risk - medium security

#19 opened 27 days ago by DinisCruz





# Example with DoS issue

Project list gets data from File System and allows DoS (with large amounts of requests) #72

Edit New Issue

**Closed** DinisCruz opened this issue 17 days ago · 3 comments



DinisCruz commented 17 days ago · edited

Owner +😊

Labels



this code will transverse the file system

Here is the test that confirms the DoS prob

```
# returns a list of current projects (which are defined by a folder contain
list: ()=>
  projects = {}
  for folder in @.data_Path.folders_Recursive()
    config_File = folder.path.Combine @.config_File
    if config_File.file_Exists()
      data = config_File.load_json()
      if data and data.key
        projects[data.key] =
          path: folder
          data: data
  projects
```

```
describe '_regression | A11 - DoS', ->
```

```
# https://github.com/DinisCruz/BSIMM-Graphs/issues/72
it 'Issue 72 - Project list gets data from File System and could cause DoS', ()->
  using new Data_Project(), ->
    start = Date.now();
    test_List = (index, next)=>
      @.list().assert_Is_Object()
      next()
```

```
#items = [0..0 ] # 1 takes 15ms
```



DinisCruz added **test needed** **risk - to accept** **security** **A11 - DoS** **risk - accepted** and removed **risk - to accept** labels 17 days ago



DinisCruz commented 17 days ago

Owner



accepting risk



DinisCruz closed this 17 days ago



OWASP

Open Web Application  
Security Project

WWW.OWASP.ORG

**TDD**



**OWASP**  
Open Web Application  
Security Project

[WWW.OWASP.ORG](http://WWW.OWASP.ORG)

# TDD

- For TDD to be productive you need
  - Real time unit test execution (when hands lift)
  - Real time code coverage
- TDD focus needs to be on
  - making developers more productive
  - preventing developers from switching context
- If 99% code coverage doesn't happen 'by default' TDD workflow is not working

# TDD in WebStorm with WallabyJS

```
table.page.pug x
1 h1 table will go here
2 pre {{table}}
```

```
Table-Controller.coffee x
1 angular.module('MM_Graph')
2 .controller 'TableController', ($scope, $routeParams, MM_Graph_API)->
3   project = $routeParams.project
4   team = $routeParams.team
5   if project and team
6     $scope.project = project
7     $scope.team = team
8     MM_Graph_API.view_Table project, team, (data)->
9       $scope.table = data
```

```
table.page.test.coffee x
1 describe 'views | table.page', ->
2
3   project = 'bsi000'
4   team = 'team-A'
5   options =
6     project : project
7     team : team
8     url_Data : path: "/api/v1/table/#{project}/#{team}" , value: { metadata: 42}
9     url_Location : "/view/#{project}/#{team}/table"
10    url_Template_Key: 'pages/table.page.html'
11
12   view = null
13
14   beforeEach ()->
15     module('MM_Graph')
16     inject ($injector)->
17       view = $injector.get('Render_View')(options).run()
18
19   it 'pages/view.page.html', ->
20     view.$('h1').html().assert_Is 'table will go here'
21     view.$('pre').html().assert_Is '{"metadata":42}'
22     view.route.$route.controller.assert_Is 'TableController'
```

```
Table-Controller.test.coffee x
1 describe 'controllers | Projects', ->
2   $scope = null
3   routeParams = null
4   project = 'bsi000'
5   team = 'team-A'
6
7   beforeEach ->
8     module('MM_Graph')
9
10  beforeEach ->
11    inject ($controller, $rootScope)->
12      $scope = $rootScope.$new()
13      routeParams = project : project , team: team
14      $controller('TableController', { $scope: $scope, $routeParams : routeParams })
15
16  it '$controller', ->
17    using $scope, ->
18      @.project .assert_Is project
19      @.team .assert_Is team
```



OWASP

Open Web Application  
Security Project

WWW.OWASP.ORG

# What happens when you increase attack surface

```
Api-Logs.coffee x Server.test.coffee x
1 Api_Base = require './Api-Base'
2
3 class Api_Logs extends Api_Base
4   constructor: (options)->
5     @options = options || {}
6     @logs_Folder = __dirname.path_Combine('../logs')
7     super()
8
9   add_Routes: ()=>
10    @add_Route 'get', '/logs/path' , @.path
11    @add_Route 'get', '/logs/list' , @.list
12    @add_Route 'get', '/logs/file/:index', @.file
13    #@add_Route 'get', '/logs/path_2' , @.path
14    @
15
16   list: (req, res)=>
17     res.send @.logs_Folder.files().file_Names()
18
19   file: (req, res)=>
20     index = parseInt(req.params?.index)
21     if is_Number(index)
22       file_Name = @.logs_Folder.files().file_Names()[index]
23       if file_Name
24         file_Path = @.logs_Folder.path_Combine file_Name
25         if file_Path.file_Exists()
26           return res.send file_Path.file_Contents()
27
28     res.send 'not found'
29
30   path: (req, res)=>
31     res.send @.logs_Folder
32
84 @.server_Url().assert_Is 'http://localhost:12345'
85
86 it 'routes', ()->
87   using server, ->
88     @.setup_Server()
89     @.add_Controllers()
90     @.add_Redirects()
91     @.add_Angular_Route()
92     version = '/api/v1'
93     expected_Routes = [ '/', '/ping', '/view*'
94                         "#{version}/data/:project/:team/radar"
95                         "#{version}/logs/path"
96                         "#{version}/logs/list"
97                         "#{version}/logs/file/:index"
98                         "#{version}/team/:project/list"
99                         "#{version}/team/:project/get/:team"
100                        "#{version}/team/:project/save/:team"
101                        "#{version}/project/list"
102                        "#{version}/project/get/:project"
103                        "#{version}/project/schema/:project"
104                        "#{version}/routes/list"
105                        "#{version}/routes/list-raw"
106                        "#{version}/table/:project/:team" ]
107     current_Routes = @.routes()
108
109     for route in expected_Routes
110       current_Routes.assert_Contains route
111
112     for route in current_Routes
113       #console.log route
114       expected_Routes.assert_Contains route
115
```



OWASP

Open Web Application  
Security Project

WWW.OWASP.ORG

# You want a test to fail

```
Api-Logs.coffee x Server.test.coffee x
1 Api_Base = require './Api-Base'
2
3 class Api_Logs extends Api_Base
4   constructor: (options)->
5     @.options = options || {}
6     @.logs_Folder = __dirname.path_Combine('.././logs')
7     super()
8
9   add_Routes: ()=>
10    @.add_Route 'get', '/logs/path' , @.path
11    @.add_Route 'get', '/logs/list' , @.list
12    @.add_Route 'get', '/logs/file/:index', @.file
13    @.add_Route 'get', '/logs/path_2' , @.path
14    @
15
16   list: (req, res)->
17     res.send @.logs_Folder.files().file_Names()
18
19   file: (req, res)->
20     index = parseInt(req.params?.index)
21     if is_Number(index)
22       file_Name = @.logs_Folder.files().file_Names()[index]
23       if file_Name
24         file_Path = @.logs_Folder.path_Combine file_Name
25         if file_Path.file_Exists()
26           return res.send file_Path.file_Contents()
27
28     res.send 'not found'
29
30   path: (req, res)->
31     res.send @.logs_Folder
32
84 @.server_Url().assert_Is 'http://localhost:12345'
85
86 it 'routes', ()->
87   using server, -> [assert_Contains]
88     @.setup_Server()
89     @.add_Controllers()
90     @.add_Redirects()
91     @.add_Angular_Route()
92     version = '/api/v1'
93     expected_Routes = [ '/', '/ping', '/view*'
94                       "#{version}/data/:project/:team/radar"
95                       "#{version}/logs/path"
96                       "#{version}/logs/list"
97                       "#{version}/logs/file/:index"
98                       "#{version}/team/:project/list"
99                       "#{version}/team/:project/get/:team"
100                      "#{version}/team/:project/save/:team"
101                      "#{version}/project/list"
102                      "#{version}/project/get/:project"
103                      "#{version}/project/schema/:project"
104                      "#{version}/routes/list"
105                      "#{version}/routes/list-raw"
106                      "#{version}/table/:project/:team"]
107     current_Routes = @.routes()
108
109     for route in expected_Routes
110       current_Routes.assert_Contains route
111
112     for route in current_Routes
113       console.log route /api/v1/logs/path_2
114       expected_Routes.assert_Contains route [assert_Contains]
115
```



OWASP

Open Web Application  
Security Project

WWW.OWASP.ORG

# TDD in WebStorm with WallabyJS

```
Server.test.coffee x A1-Injection.coffee x
1 Data_Files = require '../src/backend/Data-Files'
2
3 # These tests represent Injections Security Issues
4 # See https://www.owasp.org/index.php/Top_10_2013-A1-Injection for more references
5 describe '_security | A1 - Injection', ->
6
7 # https://github.com/DinisCruz/BSIMM-Graphs/issues/20
8 it 'Issue 26 - Data_Files.set_File_Data - DoS via file_Contents', ->
9
10 using new Data_Files(), ->
11   project = 'bsimm'
12   file_Name = "save-test"
13   file_Path = @.find_File(project,file_Name)
14   create_File = (size)=>
15     new_File_Contents = { data: size.random_String() }.json_Str()
16     file_Path.assert_File_Exists() # confirm file exist (since the current version only allows files to be modified)
17
18     @.set_File_Data_Json project,file_Name, new_File_Contents # set file with json data
19     .assert_Is_True()
20
21     file_Path.file_Contents().assert_Is new_File_Contents # confirm file was changed
22     .assert_Size_Is (size + 11) # to the expected size (+11 from json data field and padding)
23
24   restore_File = ()=>
25     original_Content = { "will-be": "changed by tests" }
26     @.set_File_Data_Json project,file_Name, original_Content.json_Pretty()
27     .assert_Is_True()
28
29   # testing multiple file contents
30   create_File 10 ,10 # 10 bytes
31   create_File 10 ,100 # 100 bytes
32   create_File 10 ,10000 # 10 Kb
33   create_File 10 ,1000000 # 1 Mb
34   #create_File 10 ,100000000 , true # 10 Mb - will work and take about 250 ms
35   #create_File 10 ,1000000000 , true # 100 Mb - will work and take about 2 secs
36   restore_File()
37
```

- ... but is a topic for another talk :)



OWASP

Open Web Application  
Security Project

WWW.OWASP.ORG



OWASP

Open Web Application  
Security Project

Thanks, any questions

@diniscruz

dinis.cruz@owasp.org