

From **SAMM** Project Towards **SAMM** Suite

SAMM User Day
May 27th, 2021
Daniel Kefer

Daniel Kefer

- SAMM volunteer since 2015
- SecurityRAT project co-lead
- Head of IT Security @
WEB.DE, GMX, mail.com



[@DKefer](https://twitter.com/DKefer)



[in/kefer/](https://www.linkedin.com/in/kefer/)



The Start of the Journey



Software Assurance Maturity Model

A guide to building security into software development

VERSION 1.1

Seen in Various Places

ASSESSMENT

- ♦ Is there a software security assurance program in place?
- ♦ Are development staff aware of future plans for the assurance program?

ASSESSMENT

- ♦ Is there a software security assurance program in place?
- ♦ Are development staff aware of future plans for the assurance program?

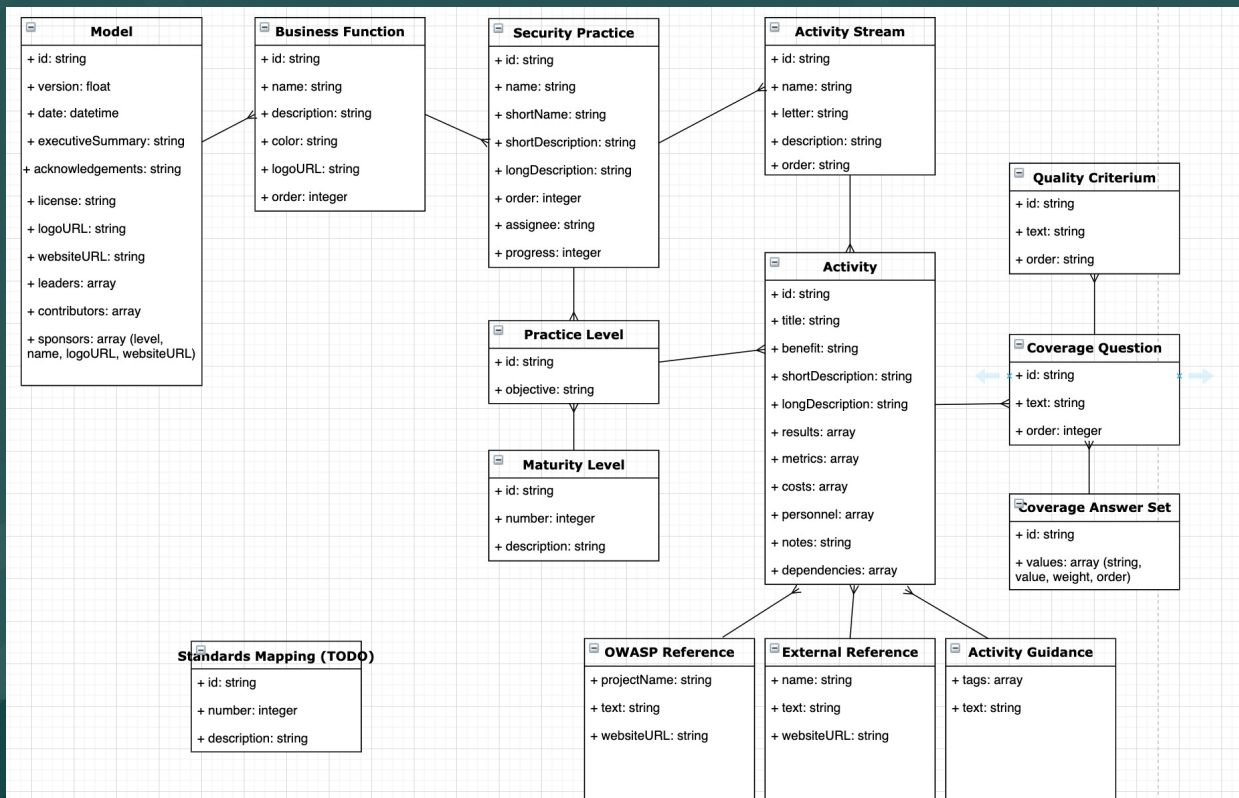
Strategy & Metrics

Yes/No










- ♦ Is there a software security assurance program in place?
- ♦ Are development staff aware of future plans for the assurance program?

Governance		
Strategy & Metrics		Yes/No
SM1	Is there a software security assurance program in place?	Yes
	<i>Guidance:</i> Assurance program is documented and accessible to staff.	
	<i>Guidance:</i> Assurance program has been used in recent development efforts.	
	<i>Guidance:</i> Staff receives training against assurance program and responsibilities.	
	Are development staff aware of future plans for the assurance program?	Yes
	<i>Guidance:</i> Assurance program goals are documented and accessible to staff.	
	<i>Guidance:</i> Assurance program goals have been presented to staff.	
	<i>Guidance:</i> A plan has been put in place to reach those goals in a specific period of time.	

Version 2.0



Data Model Implementation

 Function Design.yml	Fix linted files.
 Function Governance.yml	Update Function Governance.yml
 Function Implementation.yml	Textual Optimizations
 Function Operations.yml	Textual Optimizations
 Function Verification.yml	Update Function Verification.yml
 Maturity Level 1.yml	Fix linted files.
 Maturity Level 2.yml	Fix linted files.
 Maturity Level 3.yml	Fix linted files.
 Practice D-Security-Architecture.yml	Textual Optimizations

Data Model Implementation

#The title of this activity

title: Adhere to basic security principles

#Describe the benefit that is achieved by implementing this activity

benefit: Sets of security basic principles available to product teams

#A one sentence description of the activity

shortDescription: Teams are trained on the use of basic security principles during design

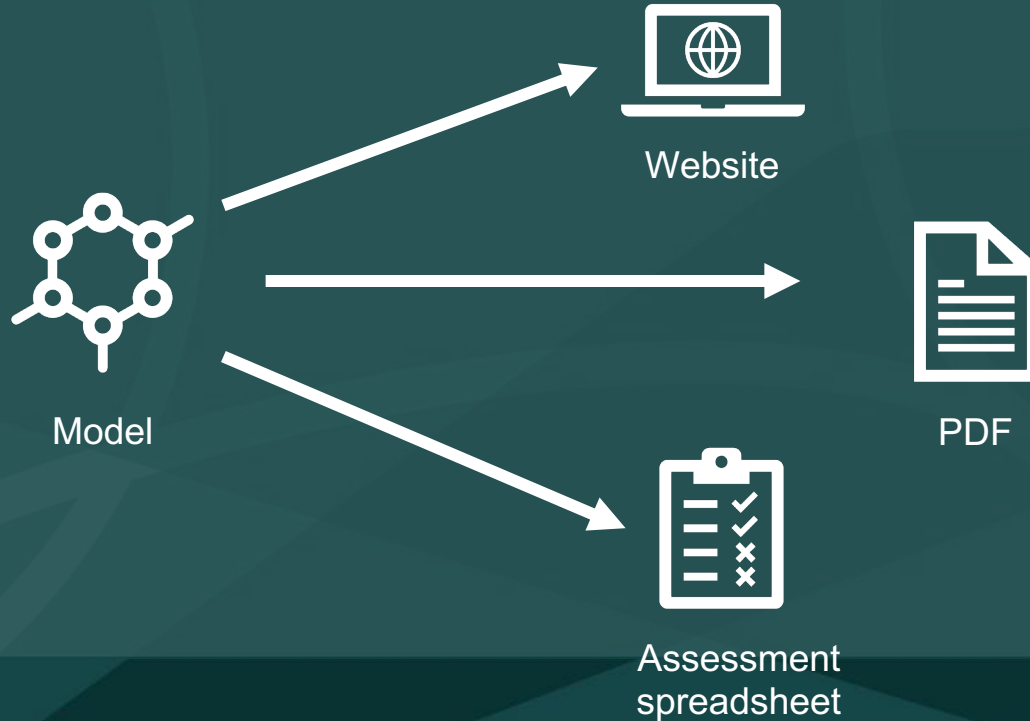
#A multi-paragraph description of the activity

longDescription: |


During design, technical staff on the product team use a short checklist of security principles. T

For perimeter interfaces, the team considers each principle in the context of the overall system a

Data Model & Derived Projects



Up Until Recently

 **OWASP** / samm

Unwatch 67

Star 352

Fork 123

<> Code

Issues 53

Pull requests 16


Actions


Projects 2


Wiki

Security

Insights

 master


 41 branches












 2 tags

Go to file

Add file

Code


 **SebaDele** Merge pull request [#560 from OWASP/sud2021-agenda](#) ... ✓ 23742dc 21 days ago 🕒 1,761 commits

 .github/workflows	fix(ci): update gha to fix build	6 months ago
 Current Releases	Merge pull request #493 from brampat/feature/new_roles	6 months ago
 Supporting Resources	Merge pull request #524 from OWASP/dependabot/npm_and_yarn/Su...	2 months ago
 Website	Removes OpenSamm reference in SUD bio	21 days ago
 v2.0/beta/core/verification	Merge branch 'master' of https://github.com/OWASP/samm	2 years ago
 .gitignore	Ignore .netlify local changes	17 months ago
 .gitmodules	Fix submodule	2 years ago
 .yamllint	Fix linted files.	2 years ago
 CNAME	Create CNAME	3 years ago
 CODE_OF_CONDUCT.md	Create CODE_OF_CONDUCT.md	3 years ago
 README.md	Update README.md	12 months ago


About

Samm stands for Software Assurance Maturity Model.

[security](#) [maturity-models](#) [owasp-samm](#)












 Readme

Releases 2

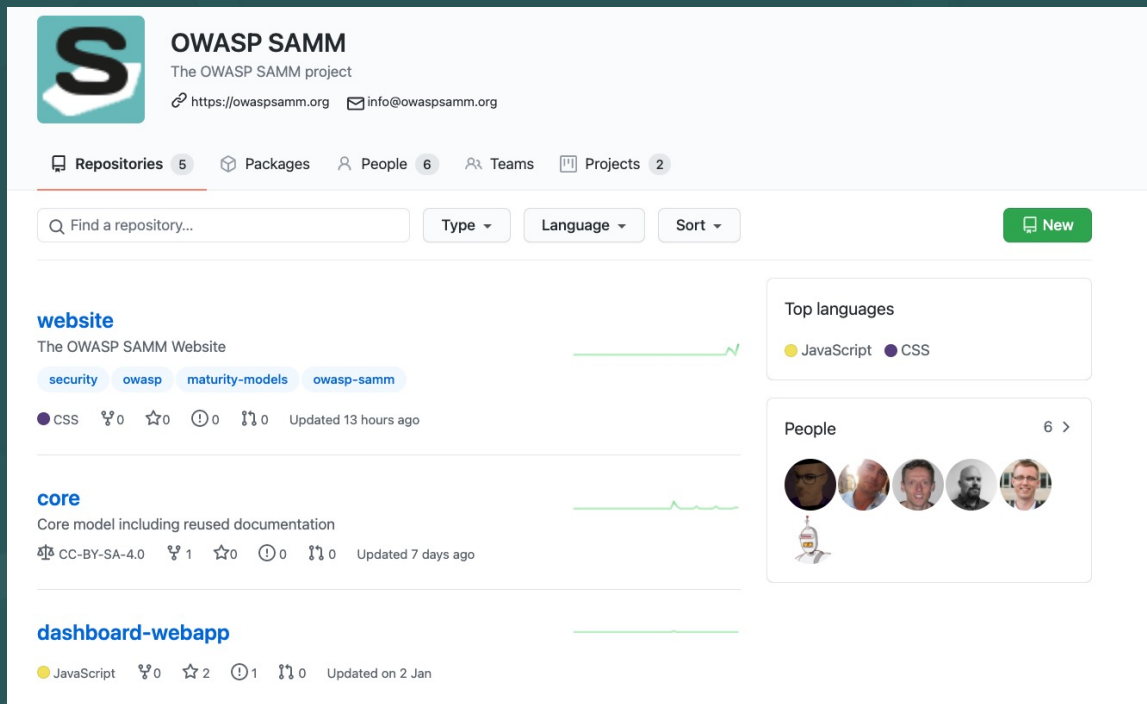
 **OWASP SATT version 2** Latest
on 3 Feb 2020

[+ 1 release](#)

Contributors 34



New GitHub Organization



The screenshot shows the GitHub organization page for OWASP SAMM. At the top, there's a profile section with the organization's logo (a stylized 'S' in a teal square), the name 'OWASP SAMM', and the description 'The OWASP SAMM project'. Below this, there are links to the organization's website and email. The main navigation bar includes 'Repositories' (5), 'Packages', 'People' (6), 'Teams', and 'Projects' (2). A search bar and filters for 'Type', 'Language', and 'Sort' are present, along with a 'New' button. The repository list shows three items: 'website' (The OWASP SAMM Website, updated 13 hours ago), 'core' (Core model including reused documentation, updated 7 days ago), and 'dashboard-webapp' (updated on 2 Jan). Each repository has a green progress bar and icons for forks, stars, issues, and pull requests. On the right, there are sections for 'Top languages' (JavaScript and CSS) and 'People' (6 members).

OWASP SAMM
The OWASP SAMM project
<https://owaspsamm.org> info@owaspsamm.org

Repositories 5 Packages People 6 Teams Projects 2

Find a repository... Type Language Sort New

website
The OWASP SAMM Website
security owasp maturity-models owasp-samm
CSS 0 forks 0 stars 0 issues 0 pull requests Updated 13 hours ago

core
Core model including reused documentation
CC-BY-SA-4.0 1 fork 0 stars 0 issues 0 pull requests Updated 7 days ago

dashboard-webapp
JavaScript 0 forks 2 stars 1 issue 0 pull requests Updated on 2 Jan

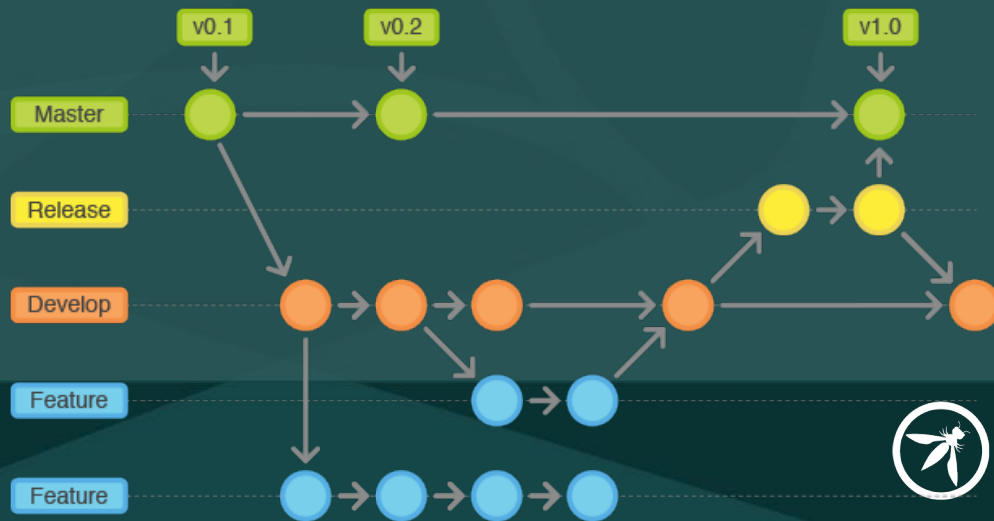
Top languages
JavaScript CSS

People 6 >

<https://github.com/owaspsamm>

Implications on the Core Model

- Switch to semantic versioning: MAJOR.MINOR.PATCH
 - SAMMv2.0 vs SAMM v2.0.0
 - Possibly different releases of language versions
 - Switch to git-flow
-
- ```
graph TD; A[v0.1] --> B[v0.2]; B --> C[v0.1]; C --> D[v0.2]; D --> E[v0.1]; A --- D; C --- E; B --- D
```




# CI/CD Pipeline: GitHub Actions


```
name: Release




on:
 pull_request:
 branches:
 - main
 types:
 - closed

jobs:
 release:
 name: Publish new release
 runs-on: ubuntu-latest
 if: github.event.pull_request.merged == true # only merged pull requests must trigger this job
 steps:
 - name: Extract version from branch name (for release branches)
 if: startsWith(github.event.pull_request.head.ref, 'release/')
 run: |
 BRANCH_NAME="${{ github.event.pull_request.head.ref }}"
 VERSION=${BRANCH_NAME#release/}
 echo "RELEASE_VERSION=$VERSION" >> $GITHUB_ENV
```



# Assessment Spreadsheet Example







 **Publish this Action to Marketplace**  
Make your Action discoverable on GitHub Marketplace and in GitHub search.

[Draft a release](#) 


 **main**  **1 branch**  **1 tag**

[Go to file](#) [Add file](#) [Code](#)

 **dkefer** Update toolkit\_updater.py c01f6e1 3 days ago  **6 commits**


|                                                                                                            |                           |             |
|------------------------------------------------------------------------------------------------------------|---------------------------|-------------|
|  <b>resources</b>          | various updates           | 3 days ago  |
|  <b>.gitignore</b>         | first commit              | 11 days ago |
|  <b>Dockerfile</b>         | various changes           | 3 days ago  |
|  <b>action.yml</b>         | various changes           | 3 days ago  |
|  <b>requirements.txt</b>   | first commit              | 11 days ago |
|  <b>toolkit_updater.py</b> | Update toolkit_updater.py | 3 days ago  |


## v2.0.36


 **github-actions** released this 3 days ago


Merge pull request #51 from samm-test/release/v2.0.36


Release/v2.0.36

 **Assets 4**

 [samm.tar.gz](#)

 [SAMM\\_spreadsheet.xlsx](#)

 [Source code \(zip\)](#)

 [Source code \(tar.gz\)](#)

# Work In Progress & Next Steps

- Assessment spreadsheet and PDF generator (website already done)
- Migration of issues & archiving the old repository
- Translations (integration with Crowdin)



# Thank you!

<https://owaspsamm.org/contact/>