Project Review

☐ Save my progress and resume later | Resume a previously saved form

Thank you for volunteering to complete a project review. This document will guide you through the process and can be a collection point for your review findings.

Information about the project

What is the name of the project you are reviewing? *

Automated Threats to Web Applications

What type of project is this *

- ○ Code
- ○ Tool
- ◉ Documentation

What is the purpose for the review *

- ○ New Project
- ◉ Incubator to Lab
- ○ Lab to Flagship
- ○ Health Assessment

Current Project Status *

- ◉ Incubator
- ○ Lab
- ○ Flagship

Project Leader Name *

Colin Watson

Project Leader Email *

colin.watson@owasp.org

2nd Leader Name

Tin Zaw

2nd Leader Email

tin.zaw@owasp.org

Purpose/Goal of the Project *

The initial objective was to produce an ontology on automated threats to web

Link to Mailing List Archives *

http://lists.owasp.org/pipermail/automated

Wiki Page History Link *

https://www.owasp.org/index.php?title=OW

Date of next major milestone *

January 2017

Next Major Milestone - Description *

We have some pending potential new threats to consider for inclusion. These will

Your Name *

Colin Watson

Your email address *

colin.watson@owasp.org

Project Quality

Project quality review is determined through the access and review of the project content on GitHub or other repository

Can the project be built correctly? *

- (•) Yes
- ( ) No

Why/Why Not? *

PDF screen file published. Lulu published. But all source files are avail

URL to any areas that need to be addressed

None

How many active (commits) does the project have in the last 6 months? *

900 extra words adde

How many? *

[this question may be incorrect - add "releases"?] One minor release

How many active releases has the project had in the last 6 months? *

One minor (1.1)

Link to Release

https://www.owasp.org/index.php/File:Automated-threat-handbook.

Has the project leader updated the project wiki page or project website to reflect the latest releases? *

- (•) Yes
- ( ) No

Incubator to Lab Checks

The project has a version number with a clear release schedule *

- (•) Yes
- ( ) No

The project has GitHub source control and a public issue tracking system *

- ( ) Yes
- (•) No

How many commits in the last 6 months? *

9,000 extra words added to handbook, plus readability and design imp

How many releases? *

One

Stable build and release *

- (•) Yes
- ( ) No

Instructions on how to use and build the project properly. *

- (•) Yes
- ( ) No

Additional Comments on Incubator to Lab Graduation *

As a document, we are not sure a 6-monthly release cycle is reasonable (for example the Top Ten is every 2-3 years). However, we have undertaken a release in the last 6 months, and will be doing another minor release in the next 3 months.

Additional Comments on Project Quality *

Automated Threats to Web Applications is one of the few OWASP documentation projects that publishes its raw source files (in this case Adobe InDesign) which allows anyone to use the project fully under its free and open licence.

The project is also referenced by a growing number of vendors in this area

Project Health

Project health assessment can be done through review of the project wiki page.

Does the project have a relevant project summary? *

- (•) Yes
- ( ) No

Check the project wiki page description and introduction sections

Why/Why Not? *

The project has had a full summary from when it was started in 2015, and the wiki page is maintained frequently.

Does the project have a relevant project Roadmap? *

- (•) Yes
- ( ) No

Check a tab call Roadmap, see if there any sore of planning or projection on releases or deliverables

Why/Why Not? *

The roadmap is published on the wiki and is updated

Does the project have a good track record of resolving issues and answering questions from project consumers? *

- (•) Yes
- ( ) No

The best place to check this is the repository issues and wiki page of the projects. Does the project have one? Is it easy to find? How many issues are open/closed?

Why/Why Not? *

Mailing list activity is low, and some suggestions

Does the project use an appropriate Community Friendly License? *

- (•) Yes
- ( ) No

The project wiki page should contain a description with the type of license provided

Why/Why Not? *

Creative Commons Attribution-ShareAlike 3.0

Are project deliverables, information, and releases readily available and accessible to the public? *

- (•) Yes
- ( ) No

Does the project have a release version?

Why/Why Not? *

Everything is published on the OWASP wiki

Do the project leaders and contributors perform their duties in accordance to applicable laws? *

- (•) Yes
- ( ) No

This is very difficult to access but try using Google search and finding information about the leaders of the project

Why/Why Not? *

Both project leaders are long term OWASP

Do the project leaders and contributors treat everyone with respect and dignity? *

- (•) Yes
- ( ) No

This is very difficult to access but try using Google search and finding information about the leaders of the project. The project mailing lists history is a good source for this information

Why/Why Not? *

All contributions are welcome, encouraged and

Is the project vendor neutral *

- (•) Yes
- ( ) No

Check for things like Logos in their wiki page or repository, mentioning of commercial activities, logos of vendors in their presentation

Why/Why Not? *

Some of the 100% sources of information surveyed

Is the project free and open and not-for-profit? *

- [x] Yes
- [ ] No

again , difficult to asses , but try researching through google and find if in any form the leaders are commercial exploiting directly the project by charging users in any form

Why/Why Not? *

Everything has been free. No-one working on the

Additional Comments on Project Health *

The project has contributed to the OWASP Top Ten project by suggesting that "lack of anti-automation" might be a candidate for inclusion in the next release, and has attempted to encourage others to contribute relevant threat data to the Top Ten project.

Documentation Review

Does the project have a publicly accessible bug tracking system established, and source code repository? *

- [ ] Yes
- [x] No

Explain your answer *

Errata and changes are received by email, or identified during proof reading. All the source Adobe files have been published. There is no tracking of issues, other than our own notes

Documentation Review bug tracking Print Screen if needed

Choose File no file selected

Is the document in a format which can be converted into an OWASP book? *

- [x] Yes
- [ ] No

Explain your answer *

Yes, and v1.1 is already published on Lulu at http://www.lulu.com/shop/owasp-foundation/automated-threat-handbook/paperback/product-22932107.html

Documentation Review Book Print Screen if Necessary

Choose File no file selected

Does the project release/deliverable have a table of contents that links all the wiki content together? *

- ○ Yes
- ◉ No

Explain your answer *

The primary deliverable (the Handbook) links to the wiki, but does not reference every tab/file on the wiki individually.

Documentation Review Table of Contents Print Screen if necessary

Choose File no file selected

Is the project release/deliverable available for download on the OWASP project wiki page? *

- ◉ Yes
- ○ No

Explain your answer *

See wiki link provided before. Also shown as "quick download".

Documentation Review Deliverable Print Screen if necessary

Choose File no file selected

Has all release/deliverable content been reviewed by a technical editor to ensure that English grammar is correct, understandable, and the content flows well? *

- ○ Yes
- ◉ No

Explain your answer *

No, but both project leaders have reviewed the document. And we fixed errata supplied back to us by the community.

Documentation Review Editor Print screen if necessary

Choose File no file selected

Additional Comments on this project's documentation output. *

The output has also been notified to Mitre's CAPEC discussion list.

Overall Project Review Summary

Project Abstract Summary *

Web applications are subjected to unwanted automated usage – day in, day out. Often these events relate to misuse of inherent valid functionality, rather than the attempted exploitation of unmitigated vulnerabilities. Also, excessive misuse is commonly mistakenly reported as application denial-of-service (DoS) like HTTP-flooding, when in fact the DoS is a side-effect instead of the primary intent. Frequently these have sector-specific names. Most of these

Overall Status *

- (•) On Track: Project is progressing quite well.
- ( ) At Risk: Potential issues for project's progress.
- ( ) High Risk: At risk, with a high risk of going off track.
- ( ) Off Track: Potential issues that can become a stopper for developer.

Captcha

Please enter the characters you see in this picture:

Characters

This helps prevent automated form submissions. If you are not sure what the characters are, make your best guess. You will have another try in the next screen.

Can't see the image? Click here for an audible version in English.

Submit

Save my progress and resume later | Resume a previously saved form

Need assistance with this form?