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
Documentation

What is the purpose for the review
Incubator to Lab

Current Project Status
Incubator

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 applications providing a common language for developers, architects, operators, business owners, security engineers, purchasers and suppliers/ vendors, to facilitate clear communication and help tackle the issues. The project continues to work on supporting material to identify symptoms, mitigations and controls in this problem area.

Link to Mailing List Archives
http://lists.owasp.org/pipermail/automated_threats_to_web_applications/

Wiki Page History Link
https://www.owasp.org/index.php?title=OWASP_Automated_Threats_to_Web_Applications&action=history

Date of next major milestone
01/30/2017

Next Major Milestone - Description
We have some pending potential new threats to consider for inclusion. These will be considered via the mailing list and discussion documents prior to issuing a new release (v1.2) in the new year.

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

Why/Why Not?
PDF screen file published. Lulu published. But all source files are available on the wiki too at https://www.owasp.org/index.php/File:Owasp-automated-threat-handbook-source-files.zip

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 added to handbook, plus readability and design improvments.

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.pdf

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

Incubator to Lab Checks

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

The project has GitHub source control and a public issue tracking system
No

How many commits in the last 6 months?
9,000 extra words added to handbook, plus readability and design improvments.

How many releases?
One

Stable build and release
Yes

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

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 e.g. search "owasp automated threats -site:owasp.org"

Project Health

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

Does the project have a relevant project summary?
Yes

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

Why/Why Not?
The roadmap is published on the wiki and is updated frequently.

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

Why/Why Not?
Mailing list activity is low, and some suggestions come in directly instead. Errata from v1.10 sent by email to CW were updated in v1.1 and the contributor thanked and acknowledged. The project has asked for input on draft changes (e.g. emails to the project list and leaders' list) and attended the summit at AppSec USA.

Does the project use an appropriate Community Friendly License?
Yes

Why/Why Not?
Creative Commons Attribution-ShareAlike 3.0 license

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

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

Why/Why Not?
Both project leaders are long term OWASP contributors and understand its values and goals, and conform to applicable laws and regulations in their work and lives.

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

Why/Why Not?
All contributions are welcome, encouraged and acknowledged.

Is the project vendor neutral
Yes

Why/Why Not?
Some of the 100% sources of information surveyed include vendor papers, but the project is neutral on vendors, technologies and countermeasures. No vendor logos in the outputs or presentations. An approach by a vendor to sponsor the release of v1.1 was declined since it might be perceived the project as not being vendor neutral.

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

Why/Why Not?
Everything is free and open.

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. The project has been presented at AppSec USA 2015 and LASCON 2016. The project participated in the OWASP Project Summit at AppSec 2016. Papers have been submitted to AppSec Cali 2017 and RSA 2017 (both pending response).

Documentation Review

Does the project have a publicly accessible bug tracking system established, and source code reposit
No

Explain your answer
Errata and changes are received by email, or identified during proof reading. All the source Adc files have been published. There is no tracking of issues, other than our own notes. The text additions for v1.1 were produced, edited and reviewed vias Google doc here: https://docs.google.com/document/d/1QcULATjxEZLiAmMcNZC4LXwF1yVTEPL3N5IUfKhcRUQ/ - this is now read-only. Changes for v1.2 are being documented here: https://docs.google.com/document/d/1yW7JBMvkboLt7VDSRQAiN5JqgFq0EF7LgZHqsWDc8vw/

Documentation Review bug tracking Print Screen if needed

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

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 Notably our proj was ALSO the publisher of the last previously created book on Lulu.

Documentation Review Book Print Screen if Necessary

Does the project release/deliverable have a table of contents that links all the wiki content together?
No

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

Documentation Review Table of Contents Print Screen if necessary

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

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

Documentation Review Deliverable Print Screen if necessary

Has all release/deliverable content been reviewed by a technical editor to ensure that English gramma correct, understandable, and the content flows well?
No

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

Documentation Review Editor Print screen if necessary

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 problems seen regularly by web application owners are not listed in any OWASP Top Ten or other top issue list. Furthermore, they are not enumerated or defined

adequately in existing dictionaries. These factors have contributed to inadequate visibility, and an inconsistency in naming such threats, with a consequent lack of clarity in attempts to address the issues. Without sharing a common language between devops, architects, business owners, security engineers, purchasers and suppliers/vendors, everyone has to make extra effort to communicate clearly. Misunderstandings can be costly. The adverse impacts affect the privacy and security of individuals as well as the security of the applications and related system components. The OWASP Automated Threats to Web Applications project attempts to rectify these issues by providing a common language, identification methods and countermeasures for all stages of the software development lifecycle.

Overall Status

On Track: Project is progressing quite well.