Google Hacking Project Inquiry Report

Prepared by OWASP Global Projects Committee Co-Chairs Brad Causey and Jason Li

Scope

The scope of this document is to address the accusations of various OWASP leaders that: (1) the Google Hacking Project does not meet the standards of an OWASP Project, and (2) the project leader abused the OWASP name in promoting this project. The inquiry process is limited to the Google Hacking Project as it pertains to these accusations.

This inquiry does *not* address issues surrounding the OWASP Australia chapters nor does it address issues surrounding messages of unverified origin on the Google Hacking mailing list. These issues are separate and independent of the accusations against the Google Hacking Project and are more appropriately addressed by the Global Chapters Committee.

Additionally, this inquiry does *not* address the behavior of any individuals involved in the dispute. The behavior of individual OWASP community members is more appropriately addressed by the OWASP Board.

Background

History

The Google Hacking Project is a Perl-based code project that encapsulates functionality of the now deprecated Google Search SOAP API. The project was presented at RUXCON2K8, OWASP AppSec US 2008, OWASP Australia 2009, and several other conferences. During the 2009 OWASP Projects Self Update Survey, the project was identified by the GPC as no longer undergoing active development ("inactive").

Timeline

- Project Inception [1] *Thu Jul 17 2008*
- OWASP NYC AppSec Conference 2008 [2] *Wed, Sep 24, 2008*
- ToorCon X Presentation [3] *Fri-Sun, Sep 26-28, 2008*
- SecTor 2008 Presentation [4] *Tue-Wed, Oct 7-8 2008*
- RUXCON2K8 Presentation [5] *Sat-Sun Nov 29-30, 2008*

---

[1] Initial Wiki Page Creation by Paulo on behalf of Project
[2] OWASP AppSec US 2008 Conference
[3] ToorCon X Presentation Schedule copied by online blogger (official site unavailable)
[4] SecTor 2008 Sessions
[5] RUXCON 2008 Presentations

- PoC v0.1 2008 Release [6] (*did not happen* [7]) — *Dec 2008*
- Google Plans Retirement of SOAP Search API [8] — *Tue Mar 3, 2009*
- OWASP Project Survey Submission [9] — *Thu Mar 19 2009*
- Google Officially Retires SOAP Search API [10] — *Tue Sep 7 2009*
- Request For Project Source By :
    - Brad Empeigne [11] — *Thu Jun 10 2010*
    - George Anelopolis [12] — *Fri Jun 11 2010*
    - Steven Steggles [13] — *Sun Jun 13 2010*
    - Jeff Williams [14] — *Sat Jun 19 2010*
    - Paulo Coimbra [15] — *Fri Jun 25 2010*
    - Dinis Cruz [16] — *Mon Jul 14 2010*
- Project Source Re-released [17] — *Sun Jun 27 2010*
- Call for Inquiry Dinis Cruz [18] — *Sun Jul 4 2010*

Purpose

At the direction of the OWASP Board, the OWASP Global Projects Committee (GPC) began a discovery process into the accusations made by OWASP leaders. The GPC analyzed emails available on the Google Hacking Project mailing list, the OWASP-Leaders mailing list, the OWASP-Global-Projects-Committee mailing list, and emails between the Google Hacking Project Lead, and the OWASP Projects Manager, Paulo Coimbra. The GPC also examined publicly available information including information from the Google Hacking Project home page, conference pages, and available video presentations. The purpose of this discovery was to: (1) identify and summarize accusations made by specific OWASP leaders against the Google Hacking Project; (2) establish a timeline for the evolution of the Google Hacking Project; (3) determine if any of the accusations made against the project are substantiated.

Points

The GPC identified four main topics relevant to the Google Hacking Project:

1. OWASP leaders, including Jeff [19], Paulo [20], and Dinis [21], question whether the source code for the Google Hacking Project was openly available

---

[6] Project History from Christian
[7] Revision History from Google Code showing no changes between Feb 4, 2009 and Jun 27, 2010
[8] Google SOAP Search API Retirement Annoucement
[9] OWASP Projects Spring 2009 Self Update
[10] Google SOAP Search API Retirement
[11] GHP Mailing List Message from Brad Empeigne (unverified source)
[12] GHP Mailing List Message from George Anelopolis (unverified source)
[13] GHP Mailing List Message from Steven Steggles (unverified source)
[14] GPC Mailing List Message from Jeff
[15] GPC Mailing List Message from Paulo
[16] GPC Mailing List Message from Dinis
[17] Revision History from Google Code showing release of code Jun 27, 2010
[18] Leaders Mailing List Message from Dinis asking for Inquiry
[19] GPC Mailing List Message from Jeff

2. OWASP leaders, including Dinis [22], Arshan Dabirsiaghi[23] and Eoin Keary[24], question whether the Google Hacking Project Lead abused the OWASP name in order to further advance the Project Leader's standing
3. Misunderstanding of OWASP leaders as to what is meant by an “abandoned” or “inactive” project
4. OWASP leaders, including Arshan Dabirsiaghi[25] and Eoin Keary[26], question whether the Google Hacking Project meets the quality expected of an OWASP project

Resolutions

Source Code Availability

As an organization based on open principles, all OWASP projects are required to make source available. The GPC confirms that the source code was not available for a substantial period of time following the project’s removal from its Google Code home. We understand that the Google Hacking Project leverages Google functional requiring an API key, but this dependency should not have inhibited the ability of a leader to distribute the source of an OWASP project. If a condition exists that could preclude the distribution the source of a project, a project leader must take that into account when proposing and designing projects. A lack of source of readily available source code is in direct contradiction to the open principles of OWASP and as such, projects that cannot distribute their source cannot be considered OWASP projects. The OWASP Global Projects Committee recommends that the OWASP Board reprimand the Google Hacking Project Leader for not making the source of the project available after presenting the project as an OWASP project at various conferences.

OWASP Brand Abuse

After review of presentations, including video publicly available from a selection of conferences, the GPC does not see a pattern of behavior rising to the level of abuse. The presentations do not overly attempt to leverage the OWASP brand to promote the project. As a result, the OWASP Global Projects Committee recommends that the OWASP Board declares that Christian Heinrich did NOT abuse the OWASP name while presenting and promoting his project.

Moreover, accusations by various OWASP leaders to the contrary have engendered charged, provocative comments from all parties. As a community, we must all remember to be respectful of each other and give each other the benefit of the doubt. We should recognize and value the continuing contributions made by all OWASP community members in a civil manner. To that end, the Global Projects Committee recommends that the OWASP Board direct the appropriate Global Committee to draft a Code of Conduct for OWASP leaders.

---

[20] GPC Mailing List Message from Paulo
[21] GPC Mailing List Message from Dinis
[22] GPC Mailing List Message from Dinis
[23] Leaders Mailing List Message from Arshan
[24] Leaders Mailing List Message from Eoin
[25] Leaders Mailing List Message from Arshan
[26] Leaders Mailing List Message from Eoin

Inactive Project Status

Following the OWASP EU Summit 2008 and the formation of the GPC, we undertook the initiative to catalog all existing OWASP Projects. The purpose of this effort was to identify projects that were:

- no longer actively developed ("inactive")
- relinquished by the project leader ("donated")
- lead by unresponsive leaders ("abandoned")
- of otherwise unknown status ("unknown")

The GPC undertook a major effort and initiative to gather, format and analyze metadata about all such projects. This "group" of projects collective represents the target of a large body of work and as such, we began informally using the terms inactive, abandoned, unknown, and donated interchangeably to refer to this entire grouping of projects. This has led to a great deal of confusion in discussions with various project leaders over the status of any given project. The GPC has begun using the term "archived" to refer to any project that falls into the four categories mentioned above. Any project leader may adopt a donated or abandoned project and the original project leader may bring an inactive project out of archive.

To clarify, the OWASP Global Projects Committee reiterates that the Google Hacking Project is no longer under active development and is properly labeled as INACTIVE. This classification does not imply that the project is abandoned, nor does it imply anything about the project regarding the value, usage, or any other metric.

Project Governance

The GPC recognizes that the Google Hacking Project may not meet the high standards that some members of our community may have for an OWASP project. However, upon examining the stated goals of the project, the Google Hacking Project has met the requirements laid out by the Project Leader. Evaluating a project's functional value and quality is an extremely subjective matter - one which the GPC has recognized in establishing the Assessment Criteria v2. This criteria requires project leaders to submit a detailed project road map that is used both to establish a vision for a project, and to evaluate its progress. Because of the volunteer nature of OWASP, we have long held that a project leader is in the best position to establish appropriate goals for a project and to work with the GPC to identify the proper means of evaluating those goals.

However, we acknowledge that as OWASP continues to grow, the brand value in the OWASP name increases. To protect this value, we need to ensure that the OWASP name is only associated with quality projects. As a result, the OWASP Global Projects Committee recommends that the OWASP Board adopt the following new project governance policy as soon as possible. We recommend making the distinction between OWASP projects and projects "hosted by OWASP". Any and all projects will continue to be welcomed for hosting at the OWASP site. However, projects will no longer automatically be entitled to be use the OWASP name in the project title. Instead, only projects that have been evaluated at Level 2 using the Assessment Criteria v2 will be entitled to use the OWASP name in its title. Until a project reaches this maturity level, it should only be referred to by their proper name (e.g. "Top Ten Project" or "WebGoat Project"). Furthermore, pursuant to the Assessment Criteria v2, a project that does not maintain Level 2 maturity will have the privilege of using the OWASP name revoked. The goal of this project governance change is to encourage project development while ensuring that the OWASP name continues to stand for quality projects.