OWASP Project Reboot - Proposal

Eoin Keary

Context

- OWASP projects are vitally important to the foundation.
- Primary reason for foundation existence is to help combat internet [in]security
- Projects are key in fighting this battle
- Projects are key in promoting OWASP
- Industry values OWASP contribution to application security via projects

Context

- “Flagship” OWASP projects are getting old
- Technology has moved on significantly since latest releases of many OWASP projects.
  - Security issues have moved on as a result
  - Old issues still exist, many more “new” issues now exist.
  - Frameworks, Dev techniques, Client-side all have new security issues.
- Many OWASP projects do not address issues faced by developers/testers today
- For OWASP to stay relevant projects need to be updated.

Proposal

- Secure (initial)funding ($100K) for refreshing most “popular” projects.

“Popular” = most used, cited, wiki hits & “useful”

- Focus on Updating such projects
- Focus on quality of information
- Focus on addressing modern secure app dev needs

Proposal - process

- Identification
  - Identify projects for this “Phase” of reboot. (Complete)
- Delegation/Buy-in
  - Identify leaders:
    - Current leaders
    - New blood
  - Identify contributors
- Lifecycle – Milestones
  - Roadmaps
  - Draft deliverables
  - QA
- Delivery
  - Marketing /Awareness
  - Project Tours

Proposal - Identification

- Identification:
  - "The top 6" projects
    - Criterion is based on current project maturity, relevance, popularity, age.
    - Older important projects may require more $$ than younger projects – rewrite, relevance, quality
    - Active projects may only require $$ for marketing support, awareness.

Proposal - Activities

- What shall be achieved per project?
- 2 types of re-boot:
  - Development – type 1
    - Contributors get paid. Agreed within team and GPC/Board
  - Awareness – type 2
    - Paid as used for marketing and awareness purposes.
    - No payment for contributors. Funds used to “spread the word” – Media, tour, training, expenses etc.

Proposal - Activities

- Type 1:
  - Redevelopment of project
    - Rewrite
    - Update
- Type 2:
  - Awareness
  - Marketing

Proposal – Delegation/Buy-in

Team Onboarding:

- Ask current leaders if they still want to lead OR identify new leaders.
- Build teams via lists etc
- Roadmaps for projects –
  - Type 1:
    - 2 milestones: 50% & 50%
  - Type 2:
    - Marketing/awareness roadmap required.

Proposal - QA

- Identify QA personnel
  - OWASP Leaders
  - Known experts
  - Generic reviewers
- All funded projects are reviewed:
  - 1st 50% milestone
  - 2nd 100% milestone

Proposed Breakdown (Suggested)

Project	Activities (relevant) effort required	Votes	Funding Required (Est)	Assumed sample activities	Project quality @ 100%
Testing Guide	Augment (Medium)	7	$10,000	Update	Release
Development Guide	Rewrite (High)	8	$15,000	Complete rewrite	Release
Code Review Guide	Augment (Medium)	6	$12,000	Update	Release
ZAP Proxy	Marketing (Low)	5	$5,000	Awareness campaign	Release
O2*	User Guide /Marketing (Medium)	3	$5,000	User Guide/WBT	Release
Cheat Sheets	Marketing (Low)	4	$5,000	Awareness campaign	Release
Top 10	Refresh (Medium)	4	$7,000	Update	Release
ASVS	Refresh	3	$5,000	Update	
ESAPI	?	3	$5,000*	?	
App Sensor	Marketing (Low)	3	$5,000	Awareness campaign	
WebGoat	?	4	$5,000*	Awareness campaign	Release
Hacking Labs	?	1	$5,000*	Awareness campaign	
Live CD	?	1	$5,000*	?	
Sec Code Practices	Marketing (Low)?	1	$5,000	Awareness campaign	
Mobile Sec	?	1	$5,000*	?	
Total (Top 6) $$			$64,000 (Top 6)	$104,000 (fund all listed)	

*O2 should be funded in addition. It is the “Zap” for source code. Needs widespread adoption

Outcomes/Payment

- Milestones reached
  - Agreed with GPC/Board
  - Dates agreed – Kickoff June 2012

  Payment (for development projects/type 1):

  50% on 1st milestone achieved

  50% on delivery (OWASP “Release” quality)
- Payment divided across main contributors for development projects (type 1)
  - Defined/agreed within team upon completion.
- Payment used on ongoing basis for marketing & awareness projects (type 2).