OWASP Project Reboot - Proposal

V1.1
Approved by the OWASP Board 5\textsuperscript{th} April 2012
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.
  – Leaders can propose projects.

• 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 may get paid but NOT OWASP Leaders. Agreed
      within team and GPC/Board.
    • Hire professionals to perform QA technical writing review,
      graphic design.
  – Awareness – type 2
    • Paid as used for marketing and awareness purposes.
    • Funds used to “spread the word” – Media, tour, training,
      expenses etc.
Proposal - Activities

• Type 1:
  – Redevelopment of project
    • Rewrite
    • Update
    • Achieve release quality

• 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:
  – 1\textsuperscript{st} 50\% milestone
  – 2\textsuperscript{nd} 100\% milestone
# Proposed Breakdown (Suggested)

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

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

Activity types:

**Type 1:** Update, rewrite & complete guides or tools.
   This "type" is aimed at both existing and new tools or guides which require development effort to update, augment, rewrite, develop in order to achieve a high quality release quality product.

**Examples:**

- "Mini" Project based summits: Expenses associated with getting global workshops, with the aim of releasing a new version of a project.
- Paying contributors for their time and effort. *OWASP Leaders can not be paid but other team members are eligible.*
- Paying for user guides etc to be professionally developed (technical writing etc).

**Type 2:** Market, Training, Awareness, increase adoption.
   Existing, healthy robust tools and guides can utilise Type 2 activities to help with creating awareness and increasing adoption of that project.

**Examples:**

- Assisting with expenses associated with marketing a project.
- Costs facilitating OWASP project focused training and awareness events