This document gives an overview of the automatic and manual components provided by ZAP that are recommended for testing each of the OWASP Top 10 2013 risks.

Note that the OWASP Top Ten Risks cover a wide range of underlying vulnerabilities, some of which are not really possible to test for in a completely automated way. If a completely automated tool claims to protect you against the full OWASP Top Ten then you can be sure they are being ‘economical with the truth’!

This is the printable version of this document, and was last updated on November 26th 2014.

The latest version of this document is available at: https://www.owasp.org/index.php/ZAPpingTheTop10

<table>
<thead>
<tr>
<th>General purpose components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual Intercepting Proxy</td>
</tr>
<tr>
<td>Manual Manual request / Resend</td>
</tr>
<tr>
<td>Manual Scripting</td>
</tr>
<tr>
<td>Manual Search</td>
</tr>
</tbody>
</table>

A1 Injection

- Automated Active scan rules (Release, Beta* and Alpha*)
- Automated SQLMap Injection Engine (Beta*)
- Manual Fuzzer, combined with the FuzzDb (Release*) and SVN Digger (Beta*) files
- Manual Diviner (Alpha*)

A2 Broken Auth and Session Management

- Manual Http Sessions tab
- Manual Spider
- Manual Forced Browse (Beta)
- Manual Token Generator (Beta*)
- Manual Diviner (Alpha*)
- Manual Vehicle (Alpha*)

A3 Cross-Site Scripting (XSS)

- Automated Active scan rules (Release)
- Manual Fuzzer, combined with the FuzzDb (Release*) and SVN Digger (Beta*) files
- Manual Plug-n-Hack (Beta)
- Manual Diviner (Alpha*)
<table>
<thead>
<tr>
<th>A4</th>
<th>A4 Insecure Direct Object References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual</td>
<td>Params tab</td>
</tr>
<tr>
<td>Manual</td>
<td>Diviner (Alpha*)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A5</th>
<th>Security Misconfiguration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated</td>
<td>Active scan rules (Release, Beta* and Alpha*)</td>
</tr>
<tr>
<td>Automated</td>
<td>Passive scan rules (Release, Beta* and Alpha*)</td>
</tr>
<tr>
<td>Manual</td>
<td>HttpsInfo (Alpha*)</td>
</tr>
<tr>
<td>Manual</td>
<td>Port Scanner (Beta*)</td>
</tr>
<tr>
<td>Manual</td>
<td>Technology detection (Alpha*)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A6</th>
<th>Sensitive Data Exposure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated</td>
<td>Active scan rules (Release, Beta* and Alpha*)</td>
</tr>
<tr>
<td>Automated</td>
<td>Passive scan rules (Release, Beta* and Alpha*)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A7</th>
<th>Missing Function Level Access Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual</td>
<td>Spider</td>
</tr>
<tr>
<td>Manual</td>
<td>Ajax Spider (Beta*)</td>
</tr>
<tr>
<td>Manual</td>
<td>Session comparison</td>
</tr>
<tr>
<td>Manual</td>
<td>Access Control (Currently only available in Weekly release)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A8</th>
<th>Cross-Site Request Forgery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated</td>
<td>Active scan rules (Beta*)</td>
</tr>
<tr>
<td>Automated</td>
<td>Passive scan rules (Beta*)</td>
</tr>
<tr>
<td>Manual</td>
<td>Generate Anti CSRF Test Form</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A9</th>
<th>Using Components With Known Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated</td>
<td>Passive scan rules (Alpha*) and Retire (Alpha*)</td>
</tr>
<tr>
<td>Manual</td>
<td>Technology detection (Alpha*)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A10</th>
<th>Unvalidated Redirects and Forwards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated</td>
<td>Active scan rules (Release)</td>
</tr>
<tr>
<td>Manual</td>
<td>Diviner (Alpha*)</td>
</tr>
</tbody>
</table>

The stared add-ons are not included by default in the full ZAP release but can be downloaded from the ZAP Marketplace via the 'Manage add-ons' button on the ZAP main toolbar.