ZAPping
the OWASP Top 10

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**

	General purpose components
Manual	**Intercepting Proxy**
Manual	**Manual request / Resend**
Manual	**Scripting**
Manual	**Search**
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*)

A4	A4 Insecure Direct Object References
Manual	**Params tab**
Manual	**Diviner** (Alpha*)
A5	Security Misconfiguration
Automated	**Active scan rules** (Release, Beta* and Alpha*)
Automated	**Passive scan rules** (Release, Beta* and Alpha*)
Manual	**HttpsInfo** (Alpha*)
Manual	**Port Scanner** (Beta*)
Manual	**Technology detection** (Alpha*)
A6	Sensitive Data Exposure
Automated	**Active scan rules** (Release, Beta* and Alpha*)
Automated	**Passive scan rules** (Release, Beta* and Alpha*)
A7	Missing Function Level Access Control
Manual	**Spider**
Manual	**Ajax Spider** (Beta*)
Manual	**Session comparison**
Manual	**Access Control** (Currently only available in Weekly release)
A8	Cross-Site Request Forgery
Automated	**Active scan rules** (Beta*)
Automated	**Passive scan rules** (Beta*)
Manual	**Generate Anti CSRF Test Form**
A9	Using Components With Known Vulnerabilities
Automated	**Passive scan rules** (Alpha*) and **Retire** (Alpha*)
Manual	**Technology detection** (Alpha*)
A10	Unvalidated Redirects and Forwards
Automated	**Active scan rules** (Release)
Manual	**Diviner** (Alpha*)

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.