Google Skipfish - Web Application Security Scanner

401 Administrator Mon, Mar 22, 2010 Web Development 0 4223

Google released Skipfish, a free fully automated, active **web application security** reconnaissance tool. It prepares an interactive sitemap for the targeted site by carrying out a recursive crawl and dictionary-based probes. The safety of the Internet is of paramount importance to Google, and helping web developers build secure, reliable web applications is an important part of the equation. Skipfish will be a valuable contribution to the information security community, making security assessments significantly more accessible and easier to execute.

The resulting map is then annotated with the output from a number of active (but hopefully non-disruptive) security checks. The final report generated by the tool is meant to serve as a foundation for professional web application security assessments.

Key Features:

- High speed: Pure C code, highly optimized HTTP handling, minimal CPU footprint - easily achieving 2000 requests per second with responsive targets.
- Ease of use: Heuristics to support a variety of quirky web frameworks and mixed-

technology sites, with automatic learning capabilities, on-the-fly wordlist creation, and form auto completion.
- Cutting-edge security logic: High quality, low false positive, differential security checks, capable of spotting a range of subtle flaws, including blind injection vectors.

A rough list of the **security checks** offered by the skipfish tool is outlined below.

- Server-side SQL injection (including blind vectors, numerical parameters).
- Explicit SQL-like syntax in GET or POST parameters.
- Server-side shell command injection (including blind vectors).
- Server-side XML / XPath injection (including blind vectors).
- Format string vulnerabilities.
- Integer overflow vulnerabilities.
- Stored and reflected XSS vectors in document body (minimal JS XSS support present).
- Stored and reflected XSS vectors via HTTP redirects.
- Stored and reflected XSS vectors via HTTP header splitting.
- Directory traversal (including constrained vectors).
- HTTP credentials in URLs.
- Self-signed SSL certificates.
- Internal warnings like failed resource fetch attempts, exceeded crawl limits, Failed 404 behaviour checks etc.
- and many more...

The tool supports Linux, FreeBSD 7.0+, MacOS X, and Windows (Cygwin) environments. To download the scanner, please visit this page; detailed project documentation is available here.