

Strumenti software per la verifica di sicurezza nelle applicazioni web - *V0.2*

Luca Carettoni (luca.carettoni@ikkisoft.com)

October 7, 2007

Copyright (c) 2007 Luca Carettoni

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation.

Questo documento ha lo scopo di fornire una panoramica generale sugli strumenti software utilizzabili per la verifica di sicurezza nelle applicazioni web; senza nessuna presunzione di completezza sono qui riportati gran parte dei software automatici e semiautomatici per l'auditing di codice sorgente, per l'analisi di configurazioni su applicazioni/dbms/web server, strumenti per le scansioni black-box, etc.

Gli strumenti software sono divisi in base alla natura del prodotto: *commerciali*, *Open Source* e *progetti di ricerca*. La catalogazione degli strumenti è fatta in base alle modalità di analisi ed alle tipologie di vulnerabilità riscontrabili così come riportato all'interno di *IEEE Security&Privacy Magazine* (July/August 2006) a cui si devono parte dei riferimenti; altre informazioni sono reperibili pubblicamente dalla Rete.

1 Applicativi commerciali

- **Secure Software CodeAssure** (source code analyzer)
www.securesoftware.com/products
- **Ounce Labs Prexis** (source code analyzer)
www.ouncelabs.com/prexis_engine.html
- **Fortify Software Source Code Analysis** (source code analyzer)
www.fortifysoftware.com/products/sca.jsp
- **Coverity Prevent/Extend** (source code analyzer)
www.coverity.com/products/index.html
- **Compuware DP SecurityChecker** (source code analyzer)
www.compuware.com/products/devpartner/securitychecker.htm
- **SPI Dynamics WebInspect** (wa scanner)
www.spidynamics.com
Tool molto potente, controlla circa 1500 vulnerabilità note su web server e applicazioni, e permette anche la ricerca di casi triviali di vulnerabilità di passaggio dei parametri, hidden field, password guessing. Permette controlli customizzabili, ma estremamente semplici. La scansione, come in tutti gli strumenti appartenenti a questa categoria, viene effettuata inviando per ogni possibile parametro in ingresso una serie di payload potenzialmente pericolosi.
- **N-Stealth Security Scanner** (wa scanner)
www.nstalker.com

Prodotto principalmente destinato all'analisi dei web server; dichiara di effettuare ricerche contro oltre 30000 casistiche di problemi su HTTP e HTTPS, oltre a permettere la scrittura di firme di vulnerabilità "personalizzate". Attraverso un motore di aggiornamento compatibile con la notazione CVE (Common Vulnerabilities and Exposures) è possibile mantenersi al passo con le vulnerabilità scoperte. Permette inoltre dei security test veloci che vanno a verificare il web server secondo le vulnerabilità presenti nella nota Top20 SANS/FBI [1].

- **NGSSoftware Typhon** (wa scanner)

www.ngssoftware.com

Evoluzione di Cerberus Internet Scanner (CIS), punta sulla qualità dei controlli più che sul loro numero. Comprende anche dei controlli a livello di applicazioni web, sebbene effettui test anche a livello di networking. Permette la personalizzazione del formato dei report.

- **Watchfire AppScan** (wa scanner)

www.watchfire.com

Ricerca comuni vulnerabilità che affliggono i web server ed a livello applicativo simula situazioni di attacco alla ricerca di falle di sicurezza. Permette l'analisi delle dieci vulnerabilità critiche individuate da OWASP oltre a numerose altre; interessante il supporto legato alle nuove tecnologie del web (XML/SOAP Test, XPath Injection) e la buona capacità di riconoscimento di XSS. Un eccellente report oltre ad una buona velocità nel caso di piccole applicazioni rendono questo prodotto abbastanza interessante.

- **Acunetix Web Vulnerability Scanner** (wa scanner)

www.acunetix.com

La capacità di riconoscimento dichiarata dal produttore spazia dal Cross Site Scripting, SQL Injection, Code execution, File Inclusion all'interessante "Google hacking". Con questo termine si identifica una tecnica tramite la quale eventuali aggressori possono trarre informazioni critiche utilizzando semplicemente un motore di ricerca. Questo prodotto indicizza i contenuti dell'applicazione analizzata tramite un crawler e poi esegue le query classiche utilizzate dagli aggressori. Interessante anche la funzione HTTP Fuzzer con cui è possibile creare delle regole personalizzate che generino degli attacchi dinamici.

- **Application Security Inc. AppDetective** (database scanner)

www.appsecinc.com/products/appdetective/index.shtml

- **DBAppSecurity MatriXay** (database scanner)
www.dbappsecurity.com/index.html
- **BugScan with IDAPro** (binary analysis)
www.logiclibrary.com
- **Compuware BoundsChecker** (runtime analysis)
www.compuware.com/products/devpartner/studio.htm

2 Applicativi Open Source

- **Rough Auditing Tool for Security** (source code analyzer)
www.securesoftware.com/resources/download_rats.html
È uno strumento appositamente studiato per la scansione di sorgenti C, C++, Perl, PHP e Python. È in grado di segnalare numerosi errori di mal programmazione, buffer overflow oltre a problematiche legate a *race condition*.
- **FlawFinder** (source code analyzer)
www.dwheeler.com/flawfinder
- **FindBugs** (source code analyzer)
findbugs.sourceforge.net
- **Nikto** (wa scanner)
www.cirt.net/code/nikto.shtml
Ricerca errori di configurazione, file e script noti, software obsoleto, su HTTP e HTTPS; effettua basilari operazioni di scansione delle porte, ed è aggiornabile automaticamente via Internet. Per le ricerche utilizza un componente, *libwhisker*, direttamente mutuato da un altro progetto [2].
- **BurpProxy** (wa scanner, proxy)
portswigger.net
Permette di intercettare le richieste HTTP/HTTPS che dal browser vengono inviate verso il server; in questo modo è possibile ispezionare e modificare tutti i parametri. Dispone inoltre di un comodo spider integrato e di uno strumento per effettuare attacchi in maniera automatizzata. Con quest'ultimo componente della suite (Burp Intruder) è possibile selezionare dei parametri in maniera dinamica, modificarne il contenuto e inoltrare più volte la richiesta verso il server; una comoda funzione di riconoscimento basata su espressioni regolari determina il risultato della pagina e fornisce un comodo report.

- **OWASP Pantera** (wa scanner, proxy)
www.owasp.org/index.php/OWASP_Pantera_Web_Assessment_Studio

- **OWASP WebScarab** (wa scanner, proxy)
www.owasp.org/index.php/OWASP_WebScarab_Project
 WebScarab è un framework per l'analisi di WA scritto interamente in Java e per questo portabile su qualsiasi piattaforma. Permette di intercettare ed analizzare il flusso di informazioni tra client e server; permette di effettuare test manuali ma anche di automatizzare alcune richieste.

- **MetaCoretex** (database scanner)
www.securityforest.com/wiki/index.php/Category:Enumeration

- **BugScam** (binary analysis)
www.sourceforge.net/projects/bugscam

- **FoundStone .NETMon** (runtime analysis)
www.foundstone.com/resources/proddesc/dotnetmon.htm

- **NProf** (runtime analysis)
www.mertner.com/confluence/display/NProf/Home

- **FoundStone SSLDigger** (configuration analysis)
www.foundstone.com/resources/proddesc/ssldigger.htm

- **Paros** (proxy)
www.parosproxy.org/index.shtml

- **Suru Web Proxy** (proxy)
www.sensepost.com/research/suru

3 Progetti di ricerca

- **WebSSARI** (source code analyzer) [3]
 Questo interessante tool, a differenza di molte delle soluzioni prima citate, basa il suo funzionamento sull'analisi statica. Anzichè ispezionare il controllo del flusso delle istruzioni, analizza il *flusso delle informazioni*. Significa che vengono attribuite classi di sicurezza ai dati (nel caso più semplice solo due, *sicuro* e *insicuro*), e quando operazioni particolari vengono effettuate con dati non ancora ritenuti sicuri viene sollevata una segnalazione di vulnerabilità.

- **Pixy** (source code analyzer) [4]

Interessante strumento per la scansione di applicativi PHP al fine di determinare, in maniera statica, la presenza di vulnerabilità di Cross Site Scripting. I risultati teorici [5], implementati poi nel tool, si rifanno alla dataflow analysis. Pixy risulta specifico per una particolare tipologia di vulnerabilità; sebbene il metodo sia generalizzabile, gli studi ed il tool rilasciato si riferiscono unicamente alle problematiche di Cross Site Scripting, limitando lo spettro di applicabilità dello strumento.

- **Lapse** (source code analyzer) [6]

LAPSE è l'acronimo di *Lightweight Analysis for Program Security in Eclipse*. È stato sviluppato con l'obiettivo di creare uno strumento versatile per l'auditing di applicazioni Java J2EE integrato direttamente in un'importante ambiente di sviluppo come Eclipse[7]; in particolare LAPSE si focalizza sulla ricerca dei punti di ingresso delle variabili (source), dei metodi potenzialmente pericolosi (sink), cercando di determinare se esistono dei percorsi validi (path source-sink) tra source e sink.

- **Jsec** (source code analyzer)

www.ikkisoft.com

JSEC è l'acronimo di *Java.String Eclipse Checker*. Questo strumento utilizza un nuovo procedimento di analisi delle stringhe e delle operazioni su stringhe al fine di validare la corretta implementazione di checkpoint per problematiche di input validation. Anche questo strumento è integrato direttamente nell'ambiente di sviluppo Eclipse[7]; analizzare applicazioni Java J2EE risulta semplice grazie ad una interfaccia utente minimale e un processo di analisi completamente automatico.

- **OWASP Orizon** (source code analyzer)

www.owasp.org/index.php/Category:OWASP_Orizon_Project

References

- [1] SANS. The top 20 most critical internet security vulnerabilities. www.sans.org/top20.
- [2] wiretrip.net. Whisker. www.wiretrip.net/rfp.
- [3] Yao-Wen Huang, Fang Yu, Christian Hang, Chung-Hung Tsai, Der-Tsai Lee, and Sy-Yen Kuo. Securing web application code by static analysis and runtime protection. In *WWW '04: Proceedings of the 13th international conference on World Wide Web*, pages 40–52. ACM Press, 2004.
- [4] N. Jovanovic, C. Kruegel, and E. Kirda. Pixy: A static analysis tool for detecting web application vulnerabilities, 2006.
- [5] Nenad Jovanovic, Christopher Kruegel, and Engin Kirda. Precise alias analysis for static detection of web application vulnerabilities. In *PLAS '06: Proceedings of the 2006 workshop on Programming languages and analysis for security*, pages 27–36, New York, NY, USA, 2006. ACM Press.
- [6] V. Benjamin Livshits and Monica S. Lam. Finding security errors in Java programs with static analysis. In *Proceedings of the 14th Usenix Security Symposium*, pages 271–286, August 2005.
- [7] The Eclipse Foundation. Eclipse IDE. www.eclipse.org.