
SIG: Web Application Penetration Testing – Was bringen automatisierte Tools?

Motivation

Der Markt und die Open Source Community bieten heute diverse Werkzeuge, die Web Application Penetration Tests weitgehend automatisieren können. Was diese Tools, die auch als Web Application Vulnerability Scanner bezeichnet werden, genau können, ist jedoch häufig unklar und man findet auch kaum Studien, die die Fähigkeiten dieser Tools analysieren und sie miteinander vergleichen. Ebenfalls gehen die Meinungen von „diese ersetzen manuelle und damit teure Tests weitgehend“ bis zu „damit können nur ganz offensichtliche Schwachstellen aufgedeckt werden“ weit auseinander. In dieser SIG soll auf die Möglichkeiten und Limiten der automatisierten Penetration Tests eingegangen werden um verbindliche Antworten auf diese Fragen zu finden.

Ziele

Das Ziel dieser SIG ist es, die Möglichkeiten und Limiten von automatisierten Penetration Testing Tools zu analysieren und eine Empfehlung bezüglich deren sinnvollen Einsatz zu machen. In diesem Zusammenhang sollen folgende Punkte bearbeitet werden:

- Welche mächtigen Tools sind heute verfügbar? Dabei sollen sowohl kommerzielle (wie z.B. Core Impact¹) als auch Open Source (wie z.B. w3af²) Tools betrachtet werden. Ebenfalls ist es wohl sinnvoll, semi-automatisierte Tools (wie z.B. WebScarab³) in die Betrachtung einzubeziehen. Es geht hier nicht primär darum, eine sehr umfangreiche Liste zusammenzutragen, vielmehr sollen vor allem solche Tools betrachtet werden, mit welchen die SIG-Teilnehmer bereits praktische Erfahrung aufweisen und zu denen entsprechend qualifizierte Aussagen gemacht werden können.
- Welche Arten von Schwachstellen können diese Tools zuverlässig erkennen? Als Basis für das Spektrum der Schwachstellen können hier die OWASP Top Ten⁴ Vulnerabilities verwendet werden.
- Wie einfach ist der Einsatz bzw. die Bedienung der Tools? Wieviel Know-How über Web Application Vulnerabilities ist notwendig, um ein Tool effizient einzusetzen und um die Ergebnisse zu verstehen?
- Kommerzielle Tools sind recht teuer. Inwiefern unterscheiden sich kommerzielle und Open Source Produkte? Können Open Source Produkte bezüglich der Qualität, die sie liefern, mithalten?
- Wo sind die Limiten der automatisierten Tools? Welche Schwachstellen können von automatisierten Tools, insbesondere im Vergleich mit einem manuell durchgeführten Test, grundsätzlich schlecht erkannt werden? Wieviele False Positives (irrtümlich gemeldete Schwachstellen) produzieren die Tools?
- Wann machen automatisierte Tests Sinn? Wann sind manuelle Tests angebracht? Inwiefern können sich die beiden Varianten ergänzen bzw. inwiefern kann ein manueller Test die Grundlagen eines automatisierten Tests verwenden und darauf aufbauen?

¹ <http://www.coresecurity.com/content/core-impact-overview>

² <http://w3af.sourceforge.net>

³ http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project

⁴ http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Erwartete Ergebnisse

Die SIG soll den involvierten Personen detaillierte Einblicke bezüglich der praktischen Erfahrungen (Verwendung, Möglichkeiten, Limiten...) mit diversen automatisierten Penetration Testing Tools geben. Dieses Know-How wird direkt hilfreich sein, um die Möglichkeiten von automatisierten Tools besser zu verstehen und um mit diesem Wissen selbst durchgeführte Penetration Tests allenfalls zu verbessern bzw. zu optimieren.

Als öffentlich verfügbares Produkt der SIG wird ein Dokument erwartet, das die Möglichkeiten und Limiten von automatisierten Penetration Testing Tools aufzeigt. Ebenfalls soll das Dokument beschreiben, wo der Einsatz solcher Tools sinnvoll ist und inwiefern sie manuelle Tests ergänzen oder unterstützen können. Das Dokument soll auch für Dritte einen grossen Nutzen haben. Zudem sollen die Ergebnisse an einer geeigneten Fachtagung präsentiert werden.

Teilnehmer

Als Idealgrösse werden 8 – 12 Teilnehmer betrachtet. Wichtig ist die aktive Teilnahme aller Personen, damit die spezifischen Erfahrungen mit verschiedenen Tools und Methoden auch wirklich eingebracht werden können. Die Teilnehmer sollten selbst aktiv Web Application Penetration Tests durchführen bzw. durchgeführt haben. Praktische Erfahrungen mit automatisierten Tools sind nicht zwingend notwendig, es ist aber natürlich umso besser, je mehr Teilnehmer selbst solche Tools einsetzen oder eingesetzt haben, um ihre „hands-on“ Erfahrungen direkt in die SIG einzubringen.

Termine

- Start (Kick-Off): TBD
- Ende: Spätestens 18 Monate nach dem Kick-Off