

Masterarbeit

Automatisiertes Pentesting von Web-Anwendungen

Ziel

Penetrationstests von Web-Anwendungen bestehen aus vielen Einzelschritten, bei denen verschiedene Werkzeuge zum Einsatz kommen, etwa Nmap, OWASP ZAP, sqlmap oder Nuclei. Ein bestehendes Framework automatisiert diese Schritte bereits und führt die Werkzeuge selbstständig aus. Welches Werkzeug wann und worauf angewendet wird, ist jedoch in **statischen Konfigurationen** festgelegt. Dadurch kann das Framework kaum auf Zwischenergebnisse reagieren, z. B. auf neu entdeckte Endpunkte, eingesetzte Technologien oder Hinweise auf eine Schwachstelle.

Ziel dieser Masterarbeit ist es, das Framework um eine **dynamische, LLM-gesteuerte Entscheidungsfindung** zu erweitern. Ein LLM bzw. Agent soll die Ergebnisse der Werkzeuge **auswerten**, daraus die nächsten Schritte ableiten und gezielt weitere Werkzeuge mit passenden Parametern ausführen. Der Ansatz wird an verschiedenen **Open-Source-Web-Anwendungen** (z. B. OWASP Juice Shop, DVWA) evaluiert und mit der bisherigen statischen Konfiguration verglichen. Mögliche Schwerpunkte:

- Agenten-Architektur für Planung und Werkzeugauswahl
- LLM-gestützte Auswertung und Priorisierung der Werkzeug-Ergebnisse
- Begrenzung und Kontrolle der Agenten-Aktionen
- Evaluation, z. B. anhand gefundener Schwachstellen, Laufzeit und Fehlalarmen

Anforderungen und Voraussetzungen

- Einarbeitung in Web-Security, Pentesting-Werkzeuge und das bestehende Framework
- Einordnung bestehender LLM-basierter Pentesting-Ansätze
- Konzeption und Implementierung der LLM-gesteuerten Komponente
- Evaluation an verschiedenen Open-Source-Web-Anwendungen
- Programmierkenntnisse (z. B. Python), Linux-Erfahrung, Interesse an IT-Sicherheit

Ansprechpartner

Prof. Dr. Lothar Braun | ✉ lothar.braun@tha.de | ☎ +49 8215586-3378

THA_innos

Das Institut für innovative Sicherheit (THA_innos) bietet eine Vielzahl von Abschluss- und Projektarbeiten im Themenfeld der Cyber Security an. Unser Team unterstützt Studierende dabei mit Know-How und Praxiserfahrung und ist zudem offen für eigene Themenvorschläge. Durch die enge Zusammenarbeit mit der Forschungsgruppe vor Ort im MRM-Gebäude lernen Studierende sowohl das Institutsleben, als auch die aktuelle Forschung von THA_innos kennen.

Weitere Informationen auch unter <https://innos.tha.de>