

1. Projektziel

WebSecBot: KI-gestützte Websicherheitsanalyse für Entwickler:innen

Wir sind ein Team aus Sicherheitsexperten und Entwicklern, die den WebSecBot entwickelt haben - ein innovatives Tool, das die Sicherheit von Webapplikationen durch KI-gestützte Analyse verbessert.

WebSecBot ist ein Browser-Addon für Google Chrome, das es ermöglicht, Websites automatisch auf Sicherheitslücken zu überprüfen und detaillierte Empfehlungen zur Behebung zu erhalten. Es kombiniert moderne KI-Technologie mit dem umfangreichen Wissen der OWASP-Sicherheitsrichtlinien.

Das Tool richtet sich primär an Entwickler:innen und kleine Unternehmen, die nicht die Ressourcen für professionelle Penetrationstests haben, aber dennoch ihre Webapplikationen absichern möchten. Es unterstützt das Shift-Left-Security-Konzept, indem es Sicherheitsprobleme bereits während der Entwicklungsphase erkennt. WebSecBot funktioniert in zwei Hauptschritten: Zunächst analysiert es die aktuelle Website automatisch auf Sicherheitsprobleme basierend auf OWASP-Standards. Anschließend bietet es einen interaktiven Security-Chat, in dem Nutzer:innen spezifische Fragen stellen und maßgeschneiderte Lösungen für identifizierte Probleme erhalten können.

2. Projektergebnisse

Kurzbeschreibung der erreichten Projektergebnisse jeweils mit Open Source Lizenz und Webadresse (netidee Vorgaben beachten!)

1	Projektzwischenbericht	CC BY-SA 4.0	https://www.netidee.at/websecbot
2	Projektendbericht	CC BY-SA 4.0	https://www.netidee.at/websecbot
3	Entwickler_innen-DOKUMENTATION	CC BY-SA 4.0	https://www.netidee.at/websecbot
4	Anwender_innen-DOKUMENTATION	CC BY-SA 4.0	https://www.netidee.at/websecbot
5	Veröffentlichungsfähiger Einseiter / Zusammenfassung	CC BY-SA 4.0	https://www.netidee.at/websecbot
6	Dokumentation Externkommunikation zur Erreichung Sichtbarkeit / Nachhaltigkeit (separates Dokument oder als Teil des Endberichtes)	CC BY-SA 4.0	https://www.netidee.at/websecbot
7	Browser Addon	MIT	https://www.github.com/sschritt/WebSecBot https://www.netidee.at/websecbot
8	OWASP-basierte Wissensdatenbank für RAG	MIT	https://www.github.com/sschritt/WebSecBot https://www.netidee.at/websecbot

3. Geplante weiterführende Aktivitäten nach netidee-Projektende

Nach Projektende sind mehrere Aktivitäten geplant, um die Nachhaltigkeit und Weiterentwicklung von WebSecBot sicherzustellen. Zum einen ist ein umfangreicher Forschungsantrag im Bereich der Automatisierung von Cybersecurity in Vorbereitung, bei dem die im Rahmen des WebSecBot-Projekts erzielten Ergebnisse als wichtige Vorarbeiten dienen. Zum anderen soll der WebSecBot weiterentwickelt und gezielt in der anvisierten Zielgruppe verbreitet und vorgestellt werden.

4. Anregungen für Weiterentwicklungen durch Dritte

WebSecBot bietet zahlreiche Möglichkeiten für Weiterentwicklungen durch Dritte:

- Integration weiterer Sicherheits-Scanning-Tools und -Techniken
- Erweiterung für zusätzliche Browser wie Firefox, Safari oder Edge
- Implementierung von Custom-Checks für unternehmensspezifische Sicherheitsrichtlinien
- Verbesserung der LLM-Komponente durch Training mit spezialisierten Datensätzen
- Entwicklung einer IDE-Integration für beliebte Entwicklungsumgebungen
- Erweiterung um API-Sicherheitstests für Backend-Services
- Unterstützung für CI/CD-Pipelines zur automatisierten Sicherheitsprüfung
- Aufbau einer Community-Plattform zum Austausch von Custom-Prompts und Sicherheitsprüfungen

Die umfangreiche OWASP-basierte Wissensdatenbank, die wir erstellt haben, kann als Grundlage für weitere Sicherheitstools dienen. Entwickler:innen können diese Daten für eigene RAG-Systeme nutzen oder sie für spezifische Sicherheitsdomänen erweitern.

Die modulare Architektur des WebSecBot ermöglicht es Entwickler:innen, an einzelnen Komponenten zu arbeiten, ohne das gesamte System verstehen zu müssen, was die Einstiegshürde für Beiträge senkt.