Web Vulnerability Scanner (WVS)

Teammitglieder: Marius Hopp, Maurice Mundi, Paul Lehnart

Problemstellung:

Webseiten und Webanwendungen sind zunehmend Ziel von Cyberangriffen, die durch Sicherheitslücken wie SQL-Injections, Cross-Site-Scripting (XSS) oder unsichere Protokolle ermöglicht werden. Betreiber von Webanwendungen, die sich über potenzielle Schwachstellen nicht im Klaren sind, riskieren Datenverlust, Rufschädigung und sogar rechtliche Konsequenzen.

Lösungsidee:

Der Web Vulnerability Scanner (WVS) ist ein Tool zur automatisierten Erkennung von Sicherheitslücken in Webseiten und Webapplikationen. Der Scanner führt umfassende Tests durch, um bekannte Schwachstellen schnell zu identifizieren, sodass Nutzer proaktiv Maßnahmen ergreifen können, bevor Angreifer sie ausnutzen. Unser Ansatz fokussiert sich auf eine tiefgehende, automatisierte Analyse, die auch ohne Benutzeroberfläche effizient und ressourcenschonend Schwachstellen erkennt.

Brainstorming-Ergebnisse:

Der Scanner wird sowohl einfache als auch komplexere Schwachstellen prüfen, wie unsichere Header-Konfigurationen und SQL-Injections. Die Behandlung fortgeschrittener Schwachstellen wird dabei zunächst relativ zum verfügbaren Zeit- und Arbeitsaufwand erfolgen.

Abschlussstatement:

Ziel des Projekts ist es, Schwachstellen in Webanwendungen zu identifizieren und Nutzern einen präventiven Schutz vor Cyberangriffen zu bieten. Der Scanner konzentriert sich auf die Erkennung gängiger sowie komplexerer Schwachstellen und ist so aufgebaut, dass er bei Bedarf modular erweitert werden kann, um zukünftigen Bedrohungen gerecht zu werden.

Mannheim, den 05.11.2024