Automatische Erkennung von Cross-Site Scripting Schwachstellen

Bachelorarbeit / Masterarbeit

Beschreibung

Cross-Site-Scripting ist eine der am häufigsten vorkommenden Schwachstelle in Web-Anwendungen. Unzureichende Prüfung der Nutzer-Eingaben durch die Anwendung, kann zu Situationen führen, die es einem Angreifer erlauben, beliebigen HTML- oder Javascript-Code in die Anwendung einzuschleusen.

Diese Schwachstellen werden meistens durch manuelle Analyse einer Web-Anwendung, z.B. im Rahmen eines *Penetration Tests* gefunden.

Im Rahmen dieser Arbeit sollen die Grundbausteine für ein Open-Source Tool gelegt werden, mit dessen Hilfe automatisch nach Cross-Site Scripting Schwachstellen in Web-Anwendungen gesucht werden kann.

Ihre Aufgaben

- Einarbeitung in den Stand der Technik bei der Erkennung von Cross-Site-Scripting
- Implementierung eines Open-Source Tools, zum Crawling von Web-Anwendungen und der Fähigkeit einige häufig vorhandene Cross-Site-Scripting Schwachstellen zu erkennen
- Auswertung der Implementierung anhand echter Web-Anwendungen, mit bekannten Cross-Site-Scripting Schwachstellen

Voraussetzungen

- Das Thema kann als Bachelor- oder Masterarbeit bearbeitet werden. Der Umfang der Aufgabenstellung richtet sich nach dem Typ der Arbeit.
- Kenntnisse der Programmiersprache Python sind von Vorteil

Kontakt

Prof. Dr. Lothar Braun <lothar.braun@hs-augsburg.de>