



Bachelorarbeit/Masterarbeit

Exploits für Web-Anwendungen

Ziel

Um die Sicherheit eines IT-Netzwerkes zu bewerten, werden häufig sogenannte Penetration Tests in Auftrag gegeben. Ziel dieser Tests ist es Schwachstellen zu finden und ihre Ausnutzbarkeit zu demonstrieren.

Penetration Tester stoßen im Rahmen ihrer Untersuchungen häufig auf Web-Anwendungen mit bekannten Schwachstellen, die häufig schon per Update vom Hersteller behoben wurden. Falls ein solches Update von einem Administrator nicht eingespielt wurde, dann besteht ein Sicherheitsrisiko in dem betroffenen System.

Für Penetration Tester sind solche verwundbaren Systeme besonders dann interessant, wenn für diese ein sogenannter Exploit existiert. Mit Hilfe solcher Exploits können Schwachstellen ausgenutzt werden. Sie erlauben es somit einem Penetration Tester einfach praktisch nachzuweisen, dass ein IT-Sicherheitsrisiko in dem betroffenen System besteht.

Penetration Tester suchen daher in manueller und zeitaufwändiger Arbeit gezielt nach Schwachstellen, für die in gängigen Datenbanken ein Exploit zu finden ist.

Ziel dieser Arbeit ist es, diesen Prozess möglichst zu automatisieren. Dazu soll ein Tool implementiert werden, mit dem möglichst automatisiert eine Web-Anwendung untersucht und potentielle Exploits für die Anwendung gesucht werden können.

Anforderungen und Voraussetzungen

- Grundlegendes Verständnis von Web-Anwendungen
- Programmierkenntnisse in Python

Ansprechpartner

Prof. Dr. Lothar Braun | ✉ lothar.braun@hs-augsburg.de | ☎ +49 821 5586/0000

HSA_innos

Das Institut für innovative Sicherheit (HSA_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 HSA_innos kennen.

Weitere Informationen auch unter www.hsainnos.de