Seminar: Analyse und Angriffe auf Netzwerke
SQL Injection

Gennaro Piano

8. Juni 2014

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Dieses Seminar behandelt das Thema Analyse und Angriffe auf Netzwerk. Eine weitverbreitete Art um in einem Netzwerk schaden anzurichten, sind sogenannte SQL Injections. Dieses Projekt befasst sich mit SQL Injections. Dieses Kapitel erklärt den Begriff SQL Injection und befasst sich mit der genauen Aufgabenstellung des Projekts.

1.1 Ausgangslage

SQL-Injections sind eine häufige Angriffsart, weil sie einfach durchzuführen sind und sehr effizient sein können. SQL-Injections sind eingeschleuste SQL Abfragen, welche einem nicht autorisiertem Benutzer Zugriff zur Datenbank gewähren. Somit kann ein nicht autorisierter Benutzer Daten aus der Datenbank lesen oder gar ändern und löschen.

1.2 Ziel der Arbeit

Das Ziel dieser Arbeit ist es aufzuzeigen, was mit SQL Injections alles möglich ist und wie man Anwendung gegen SQL Injections schützen kann. Der Seminarbericht soll die Analyse dieser Schwachstelle beinhalten. Nebenbei soll eine Testumgebung entwickelt werden, welche aufzeigt wie Datenbank von Dritten manipuliert werden können und wie man sich vor solchen Angriffen schützen kann.

1.3 Aufgabenstellung

Es werden zwei grafisch identische Websites erstellt, welche an die gleiche Datenbank angebunden sind.

Eine Website ist gegen SQL Injections geschützt, die andere nicht.

Auf beiden Websites wird versucht anhand von SQL Injections Daten aus der Datenbank zu lesen und zu ändern.

1.4 Erwartete Resultate

Als Resultat wird eine Dokumentation erwartet, welche die Resultate dokumentiert und wie man sich gegen SQL Injections schützen kann.

1.5 Sourcecode

Der Sourcecode der Websites wird aus Platzgründen nicht in die Dokumentation eingefügt, jedoch kann er direkt aus dem GitHub Repository heruntergeladen werden. Das Repository befindet sich unter
https://github.com/pianogen/Seminararbeit/SQLInjections.

1.6 Bemerkung

Der praktische Teil dieser Arbeit wird nur zur Analyse der SQL Statements verwendet und wird nie produktiv genutzt, somit wird das gesamte Testverfahren der Applikation nicht berücksichtigt.

2