UNIVERSITÄT ZU LÜBECK
INSTITUT FÜR IT-SICHERHEIT

Praktikum 5

SQL-Injections

Zu bearbeiten bis zum 30. Mai 2023

Cybersecurity im Sommersemester 2023

Jan Wichelmann, Anja Köhl

Einführung

In diesem Praktikum geht es um Datenbanksicherheit. Datenbanken sind häufig indirekt über Webseiten erreichbar, sodass wir vor allem dieses Einfallstor betrachten werden. Dazu wurden drei Testwebseiten aufgesetzt, die Sie über den Praktikumsserver erreichen können. An zwei davon werden Sie manuell SQL-Befehle einschleusen, um diese Angriffstechnik zu üben und deren Schwierigkeiten einschätzen zu lernen. Die dritte Testseite werden Sie mit Hilfe des Tools *SQLMap* angreifen. Dies soll Ihnen die vorhandene Toolunterstützung für solche Angriffe näher bringen.

Mit SQL-Injections kann man noch sehr viel mehr machen als Daten und Logins abzugreifen, bis hin zu Root-Zugriff auf den Server. So weit werden wir in diesem Praktikum aber nicht gehen.

Aufgabe 1 Vorbereitung

In diesem Praktikum versuchen wir auf verschiedene Arten, im Namen anderer Benutzer zu handeln oder uns Zugriff auf geschützte Bereiche einer Webseite zu verschaffen. Zwei dieser Webseiten benötigen einen Nutzernamen und ein Passwort, die in einer Datenbank hinterlegt sind (die Datenbanksoftware selbst hat natürlich auch Nutzer und Passwörter, die uns hier aber nicht interessieren). Die Passwörter liegen natürlich nicht im Klartext in der Datenbank, sondern als `SHA-1`-Hashes.

Für einen reibungslosen Ablauf sollten Sie drei Dinge vorbereiten:

- Bereiten Sie zu dem im Moodle zur Verfügung gestellten Wörterbuch eine Liste vor, in der alle `SHA-1`-Hashes der Passwörter liegen.

  Zur Kontrolle:

  ```
  SHA1('Luebeck') = 5c5765aa7224eab733473471dd6abcb9d15d5e18
  ```

- Bereiten Sie ein Programm für Aufgabe 3 vor. Das Programm sollte einen HTTP-GET-Request verschicken und die Antwort empfangen können. Außerdem sollten Sie feststellen können, ob die Antwort einen bestimmten String enthält, da Sie nur den Quelltext der Webseite als Antwort bekommen.

  Sie finden im Moodle einige Programmiervorlagen, die bereits die obige Hashfunktion und eine Methode für HTTP-Requests enthalten, sodass Sie nicht sämtliche Funktionen selbst implementieren und testen müssen.

- Informieren Sie sich über die folgenden Datenbank- und SQL-Techniken, um mit diesen im Praktikum gut umgehen zu können:
  - Klassische Abfragesyntax: `SELECT ... FROM ... WHERE ... [ LIKE / AND / OR ]`
  - Weitere Befehle: `UNION`, `CONCAT`, `SUBSTRING`, `ASCII`
  - Struktur der Datenbank `information_schema`

Ein einfaches interaktives Tutorial zum Erlernen der grundlegenden Abfragesyntax findet sich beispielsweise unter `https://sqlbolt.com/`.

Aufgabe 2 Kontodaten stehlen ohne Login

Da Sie demnächst eine größere Anschaffung tätigen möchten, aber gerade kein Bankkonto zur Verfügung haben, hätten Sie gern Alice' Kontonummer. Diese durch Auszuprobieren zu erraten ist allerdings keine Option: Erstens ist sie recht lang, und zweitens sind die Banken sehr vorsichtig, und reduzieren bei jeder Falscheingabe Ihre Bonität[1]. Aber Sie haben Glück – Alice ist in einem dubiosen Webshop angemeldet, der offenbar anfällig für SQL-Injections ist. Leider haben Sie selbst dort keinen Account, das sollte Sie jedoch nicht aufhalten.

1. Testen Sie die verwundbare Suchfunktion im Webshop mit verschiedenen Eingaben und versuchen Sie erste Injections.

   Hinweise:

   - Achten Sie darauf, dass hinter dem Kommentar-Befehl „`--`“ zum Auskommentieren des restlichen Query ein Leerzeichen steht. Falls Sie direkt mit der URL arbeiten, können Sie das durch ein Pluszeichen (+) am Ende erreichen, oder indem sie immer ein Leerzeichen und einen Buchstaben anhängen (z.B. „ `a`“).
   - Der Webshop zeigt das Ergebnis eines Query nur an, wenn es eine bestimmte Anzahl von Spalten hat. Versuchen Sie also zuerst die Anzahl der Spalten zu erraten, indem Sie ein `UNION SELECT` mit konstanten Werten machen (Beispiel für zwei Spalten):

     ```
     ... UNION SELECT 1,2 -- a
     ```

     Füllen Sie entsprechend die später nicht von Ihnen genutzten Spalten mit `NULL` auf. Bei einem Query mit zwei Spalten wäre dies beispielsweise:

     ```
     ... UNION SELECT password,NULL FROM users -- a
     ```

2. Finden Sie mithilfe von `information_schema` heraus, wie die Datenbank heißt und welche Tabellen es gibt. Wenn Sie wissen, welche Tabelle Ihr Ziel ist, sollten Sie in Erfahrung bringen wie die Spalten der Tabelle heißen.
3. Entlocken Sie der Datenbank die Kontonummer von Alice.

◀ 150 / 30

Aufgabe 3 Blind SQL Injection

Leider haben Sie eines ihrer Passwörter vergessen. Sie wissen aber noch ihren Nutzernamen *student*, und wo sie das Passwort zum letzten Mal verwendet haben: Auf einer Website zur Reservierung von Kino-Sitzen. Zum Glück ist auf der Kino-Website eine SQL-Injection möglich. Nutzen Sie die vorhandene Lücke, um Ihre eigenen Login-Daten herauszufinden.

1. Testen Sie die Seite mit verschiedenen Eingaben und beobachten Sie, wie sich die Seite verhält.
2. Mit Hilfe der Abfrage `<freie Platznummer>' AND <frage>` können Sie der Datenbank true/false Fragen stellen. Nutzen Sie diese Eigenschaft, um das erste Zeichen des ersten Eintrags der `TABLE_NAME`-Spalte in der `information_schema.TABLES`-Tabelle zu erraten.

   Hinweis: Testen Sie Ihr Query (oder Teile davon) zuerst mit den schon bekannten Tabellen aus Aufgabe 2.

3. Passen Sie Ihr Programm aus Aufgabe 1 so an, dass Sie automatisiert den Namen und die Struktur der Benutzertabelle, und zum Schluss das komplette Passwort auslesen können (zeichenweise). Es handelt sich hierbei um einen `SHA1`-Hash. Vergleichen Sie den Hash mit dem von Ihnen vorberechneten Wörterbuch, um das Passwort herauszufinden, und geben Sie es anschließend auf dem Praktikumsserver ein.

◀ 150 / 30

[1] Was in unserem Fall einem ordentlichen Punktabzug entspricht.

Aufgabe 4 Angriffe automatisieren mit *SQLMap* (freiwillig)

Nach der ganzen Handarbeit sollen Sie jetzt noch ein Tool kennen lernen, das Ihnen die Arbeit erleichtern kann. Mit *SQLMap*[2] können Sie Webseiten automatisiert auf Verwundbarkeit durch SQL-Injection-Angriffe überprüfen.

1. Folgen Sie den Anweisungen zur Installation von SQLMap.
2. Informieren Sie sich mit `man sqlmap` über die Benutzung des Programms.
3. Gehen Sie auf die Webseite. Sie finden dort ein kleines Gästebuch, in das Sie unbedingt etwas posten möchten – leider haben Sie schon wieder Ihr Passwort vergessen. Nutzen Sie *SQLMap* und das Wörterbuch, um Ihr Passwort herauszubekommen, und schreiben Sie einen netten Gästebucheintrag. Geben Sie das gefundene Passwort anschließend auf dem Praktikumsserver ein.

◁ 150 / 30

[2] `https://github.com/sqlmapproject/sqlmap`