# Lern- und Arbeitsauftrag *LA\_183\_05\_SQLInjection.docx*

|  |  |
| --- | --- |
| Titel | SQL Injection |
| Modul | 183 Informatiker/in EFZ |
| Autor / Version | Birgit Rieder / V1.0 |
| Hilfsmittel: | PR\_183\_InterpreterInjection |
| Nachweis |  |
| Sozialform | Einzelarbeit / Partnerarbeit |
| Leistungsziele | 2.2, 4.1, 4.2 |

## Ausgangslage

Sie haben den Auftrag, die Webapplikation der BBB Insecure App sicherheitstechnisch zu untersuchen und Sicherheitslücken zu schliessen.

### Ein Bild, das Werkzeug, medizinische Ausrüstung enthält. Automatisch generierte Beschreibung

Bild von OpenClipart-Vectors auf Pixabay

### Aufgabe 1: Injection verstehen

1. Erarbeiten Sie sich anhand der Präsentation das notwendige Wissen über SQL Injection.
2. Absolvieren Sie die Hacksplaining Lektion zu SQL-Injection: <https://www.hacksplaining.com/lessons>.

### Aufgabe 2: Sicherheitslücke finden

Bei einer SQL-Injection kann ein Angreifer die SQL-Befehle manipulieren (ändern), die an die Datenbank übergeben werden.

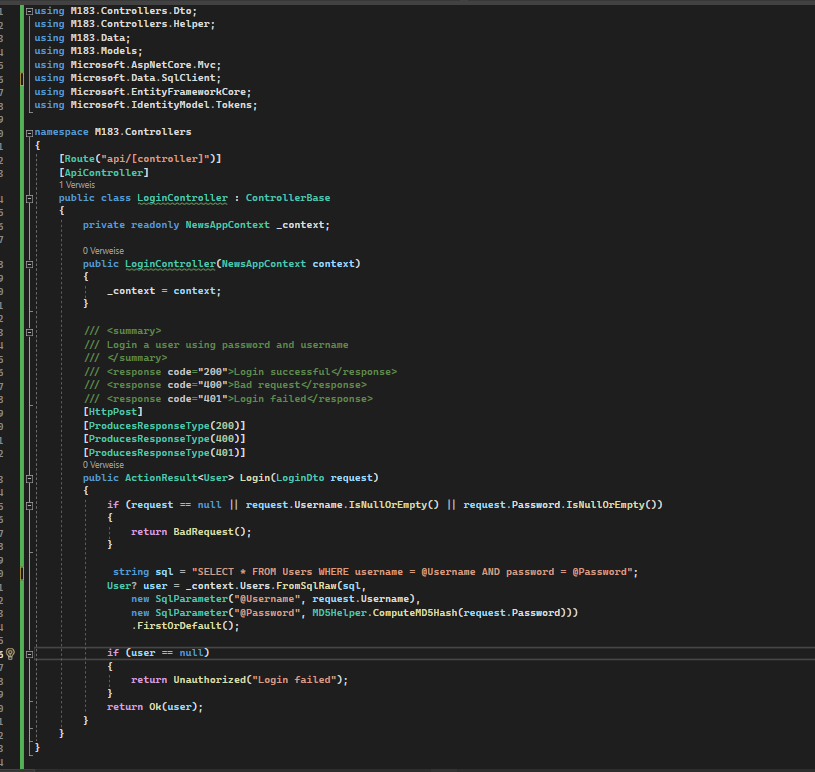
1. Wo finden Sie SQL-Code in der InsecureApp? Ein Bild, das Text, Screenshot, Software enthält.

   Automatisch generierte Beschreibung  
     
   Hier im Logincontroller sieht man den string sql, welcher einen SQL befehl beinhaltet
2. Was ist die Aufgabe dieses Codes?  
   Der Code geht in die Datenbank zur Tabelle Users und schaut dort, ob es einen User mit dem gewählten username gibt und ob dieser mit dem Hashwert, des Passworts übereinstimmt.
3. Kreieren Sie einen Angriff: Versuchen Sie sich als administrator einzuloggen. Ohne das Passwort zu kennen oder zu raten. Dazu braucht es etwas Phantasie. Oder Ideen aus dem Cheat Sheet (s. zusätzliche Angaben zum Auftrag). Machen Sie sich Zeichen wie String-Ende oder Kommentar zu Nutze.  
   Ein Bild, das Text, Screenshot, Schrift, Zahl enthält.

   Automatisch generierte Beschreibung  
   Indem man als Username «administrator ‘—"nimmt, erhält man zugriff mit jedem beliebigen password. Denn wenn man nach dem namen administrator noch «’—» eingibt, wird der restliche teil der SQL abfrage als kommentar behanfelt, wodurch die Passwortumfrage umgangen wird.

### Aufgabe 3: Sicherheitslücke beheben

Schliessen Sie diese Sicherheitslücke, so dass Benutzer:innen den SQL-Befehl nicht mehr manipulieren können.



Ein Bild, das Text, Screenshot, Schrift, Zahl enthält.

Automatisch generierte Beschreibung  
Ich habe den Code verbessert, um die Sicherheit zu erhöhen. Mit SqlParameter schützen wir vor SQL-Injektionen, indem wir Benutzereingaben sicher in die SQL-Abfrage einbinden. Dadurch wird die Anwendung robuster gegen Angriffe.

## Gütekriterien

Der Lern- und Arbeitsauftrag ist erfüllt, wenn …

* Sie die Hacksplaining-Lektion durchgearbeitet haben.
* Sie einen erfolgreichen Angriff auf das Login vorgenommen haben
* Sie die Sicherheitslücke in der InsecureApp geschlossen haben.

## Zusätzliche Angaben zum Auftrag

Unter <https://www.invicti.com/blog/web-security/sql-injection-cheat-sheet/> finden Sie weitere Techniken für Angriffe mit SQL-Injection.

## Mögliche Erweiterungsaufträge

-