SQLインジェクションの実例を用いたセキュリティ理解の促進

Promoting Security Understanding Through Practical Examples of SQL Injection

村山皓朗 Hiroaki Murayama　白橋響 Hibiki Shirahashi　我妻未唯 Miyu Wagatsuma　末田欣子 Yoshiko Sueda

明星大学　情報学部

School of Information ,Science,Meisei University

1. まえがき

セキュリティの脆弱性を悪用した攻撃の中でも特に代表的な手法であるSQLインジェクションは，データベースへの不正アクセスを可能にし，機密情報の漏洩やシステム破壊といった重大な影響を及ぼす可能性がある．

中高生を対象とし，SQL インジェクションの仕組みや具体的な攻撃手法を理解するとともに，実際に簡単な実践を通じてその危険性を体感してもらうことを目指す．

2. SQLインジェクションについて

SQLインジェクションは，Webアプリケーションのセキュリティ脆弱性を利用して，不正なSQLクエリをデータベースに実行させる攻撃手法．主に，入力フォームやクエリのパラメータを介して，悪意のあるSQL文を挿入し，データベースから機密情報を取得，データを改竄，消去，またはシステムを破壊することが目的である．

通常，Web アプリケーションではユーザからの入力データをSQLクリエに組み込んでデータベースにアクセスする．例えば，以下のようなSQL文が使われることがある．

```
SELECT * FROM users WHERE username = '入力値'
AND password = '入力値';
```

しかし，ここでユーザーが不正な入力を行った場合，SQL 文が意図しない動作をしている．例えば

```
入力値 = 'admin' --
```

これが SQL 文に挿入されるとコメントを意味する「--」が後続のパスワードチェックを無効化し，以下のようなクエリに変わる．

```
SELECT * FROM users WHERE username = 'admin' -
-' AND password = '入力値';
```

結果として，「admin」ユーザの情報がパスワード確認無しで取得されることになる．

3. 環境構築

本稿で使用する環境は以下の通りである．

(a)Oracle VM VirtualBox をインストールし，適切なバージョンを確認する．

(b)Kali Linux の ISO イメージを公式サイトからダウンロードし，仮想マシンを設定．

(c)TryHackMe VPN を使用して，仮想マシンをセキュアに接続．

4. 実施クエリ

表 1.SQL インジェクションの実行結果

実施クエリ	成功/失敗
‘	失敗
‘ ‘	失敗
;%00	失敗
--	失敗
-- -	失敗
“ “	失敗
;	失敗

実施クエリ	成功/失敗
‘ OR ‘1	成功
‘ OR ‘1-- -	成功
“ OR “ ” = “	失敗
“ OR 1 = 1 -- -	失敗
‘ OR ‘ ‘ = ‘	失敗
OR 1=1	失敗

(1) 基本的な SQL インジェクションの実行

入力: ' OR '1' = '1 期待される結果: 全ユーザーの情報が表示される．

解説: このクエリは条件文に常に真となる論理式を挿入することで，認証を突破する．

(2) コメントを用いた認証回避

入力: 'admin' --

期待される結果: "admin"ユーザーの情報が取得される．

解説: コメント記号（--）を利用して，パスワードチェック部分を無効化する．

(3) エラーメッセージの観察

入力: " OR "" = "期待される結果: エラーメッセージが表示される．

解説: 不正な構文によって発生するエラーを観察し，データベースが入力をどのように解釈しているかを学ぶ．

5. まとめ

本プロジェクトでは，SQL インジェクションの基礎を中高生に理解させることを目指し，実践を通じてその危険性を体感してもらう内容を提案した．加えて，エラーメッセージやシステム処理の分析を通じて，セキュリティ設計の重要性についても学びを深めることができる．今後は，他のセキュリティ攻撃手法についても取り上げ，より包括的なセキュリティ教育の実現を目指す．

参考文献

[1] 野溝のみぞう，”7 日間でハッキングをはじめる本”， 株式会社翔泳社 pp.131-139(2024.8)

[2] 石川 朝久，北原 憲，洲崎 俊，オライリー・ジャパン，ハッキング API-Web API を攻撃から守るためのテスト技法”pp.302-307(2023.3)