

日々是Oracle APEX

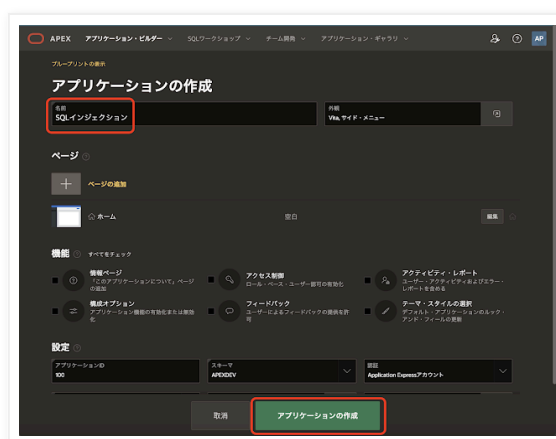
Oracle APEXを使った作業をしていて、気の付いたところを忘れないようにメモをとります。

2021年8月16日月曜日

データベース・セキュリティの活用(3) - テスト用アプリケーションの作成

ワークスペースAPEXDEVにサインインし、テストに使用するアプリケーションを作成します。このアプリケーションには、意図的にSQLインジェクションに脆弱であるSQLを含めます。

アプリケーション作成ウィザードを起動し、空のアプリケーションを作成します。名前はSQLインジェクションとします。アプリケーションの作成を実行します。



アプリケーションが作成されたら、ページ・デザイナーでホーム・ページ(ページ番号1)を開きます。

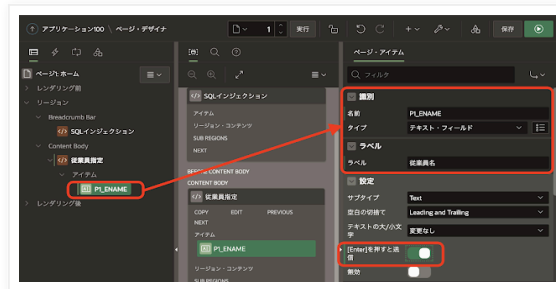


ホーム・ページにリージョンを3つ作成します。左ペインのレンダリング・ビューにあるContent Body上でコンテキスト・メニューを開き、リージョンの作成を実行します。

1つ目のリージョンは、識別の名前を従業員指定、タイプを静的コンテンツとします。



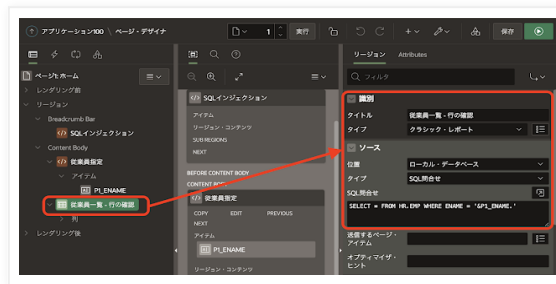
従業員名を入力するページ・アイテムを作成します。Content Body以下のリージョン従業員指定の上でコンテキスト・メニューを開き、**ページ・アイテム**の作成を実行します。識別の名前をP1_ENAME、タイプをテキスト・フィールド、ラベルを従業員名、設定の[Enter]を押すと送信をONにします。



表HR.EMPを一覧するリージョンを作成します。リージョンの作成を実行し、識別のタイトルを従業員一覧 - 行の確認とし、タイプにはクラシック・レポートを選択します。ソースの位置はローカル・データベース、タイプはSQL問合せ、SQL問合せとして以下を記述します。

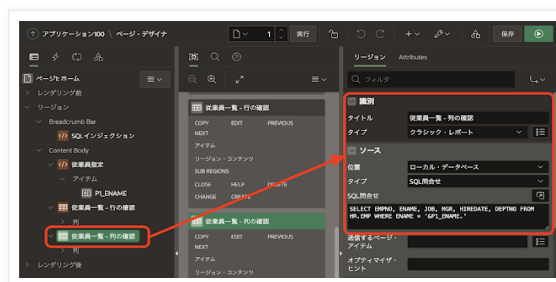
```
SELECT * FROM HR.EMP WHERE ENAME = '&P1_ENAME.'
```

上記のSELECT文は文中に置換文字列&P1_ENAME.を含むため、SQLインジェクションに対して脆弱になっています。正しくはバインド変数:P1_ENAMEを使用します。今回はデータベースのセキュリティ機能の効果を確認するため、あえてこのようにしています。



もうひとつクラシック・レポートのリージョンを作成します。リージョンの作成を実行し、識別のタイトルを従業員一覧 - 列の確認とします。SQL問合せに以下を記述します。検索対象の列からSALおよびCOMMを除外しています。

```
SELECT EMPNO, ENAME, JOB, MGR, HIREDATE, DEPTNO FROM HR.EMP WHERE ENAME = '&P1_ENAME.'
```



これで表HR.EMPを一覧するページが完成しました。ページを実行し動作を確認します。

ワークスペースAPEXDEVにサインインしたユーザー(通常はAPEXDEV)にてサインインします。



従業員名に**SCOTT**を入力して**Enter**を押します。SCOTTの情報がそれぞれのクラシック・レポートに1行だけ表示されています。



アプリケーションが従業員名として想定している入力は一単一の従業員名です。別の従業員名を入力しても、レポートに表示されるのは1行のみです。

SQLインジェクションをシミュレートするため、**従業員名**として以下を入力します。

SCOTT' or '1' = '1

レポートには**すべての従業員の情報が一覧**されます。

従業員指定

従業員名
SCOTT' or '1' = '1

従業員一覧 - 行の確認

Empno ↑	Ename	Job	Mgr	Hiredate	Sal	Comm	Deptno
7369	SMITH	CLERK	7902	1980/12/17	800		20
7499	ALLEN	SALESMAN	7698	1981/02/20	1600	300	30
7521	WARD	SALESMAN	7698	1981/02/22	1250	500	30
7566	JONES	MANAGER	7839	1981/04/02	2975		20
7654	MARTIN	SALESMAN	7698	1981/09/28	1250	1400	30
7698	BLAKE	MANAGER	7839	1981/05/01	2850		30
7782	CLARK	MANAGER	7839	1981/06/09	2450		10
7788	SCOTT	ANALYST	7566	1982/12/09	3000		20
7839	KING	PRESIDENT		1981/11/17	5000		10
7844	TURNER	SALESMAN	7698	1981/09/08	1500	0	30
7876	ADAMS	CLERK	7788	1983/01/12	1100		20
7900	JAMES	CLERK	7698	1981/12/03	950		30
7902	FORD	ANALYST	7566	1981/12/03	3000		20
7934	MILLER	CLERK	7782	1982/01/23	1300		10

1 - 14

続いて、従業員名に以下を入力します。

SCOTT' UNION SELECT EMPNO, ENAME || '-' || SAL || '-' || COMM ENAME, JOB, MGR, HIREDATE, DEPTNO FROM HR.EMP WHERE '1'='1

レポートは列SALおよびCOMMを含んでいませんが、列ENAMEにSALおよびCOMMの情報が表示されています。

従業員指定

従業員名
SCOTT' UNION SELECT EMPNO, ENAME || '-' || SAL || '-' || COMM ENAME, JOB, MGR, HIREDATE, DEPTNO FROM HR.EMP WHERE '1'='1

従業員一覧 - 行の確認

レポート - エラー
ORA-01799: 問合せプロックにある結果の列数が正しくありません

従業員一覧 - 列の確認

Empno ↑	Ename	Job	Mgr	Hiredate	Deptno
7369	SMITH - 800 -	CLERK	7902	1980/12/17	20
7499	ALLEN - 1600 - 300	SALESMAN	7698	1981/02/20	30
7521	WARD - 1250 - 500	SALESMAN	7698	1981/02/22	30
7566	JONES - 2975 -	MANAGER	7839	1981/04/02	20
7654	MARTIN - 1250 - 1400	SALESMAN	7698	1981/09/28	30
7698	BLAKE - 2850 -	MANAGER	7839	1981/05/01	30
7782	CLARK - 2450 -	MANAGER	7839	1981/06/09	10
7788	SCOTT	ANALYST	7566	1982/12/09	20
7788	SCOTT - 3000 -	ANALYST	7566	1982/12/09	20
7839	KING - 5000 -	PRESIDENT		1981/11/17	10
7844	TURNER - 1500 - 0	SALESMAN	7698	1981/09/08	30
7876	ADAMS - 1100 -	CLERK	7788	1983/01/12	20
7900	JAMES - 950 -	CLERK	7698	1981/12/03	30
7902	FORD - 3000 -	ANALYST	7566	1981/12/03	20
7934	MILLER - 1300 -	CLERK	7782	1982/01/23	10

1 - 15

SQLインジェクションを確認するページは出来上がりました。

表HR.EMPを編集する対話グリッドのページを作成します。ページの作成を実行し、ページ作成ウィザードを起動します。



フォームを選択します。



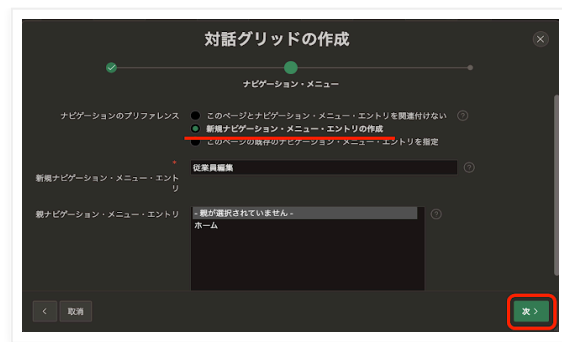
編集可能対話グリッドを選択します。



ページ名を従業員編集として、次へ進みます。

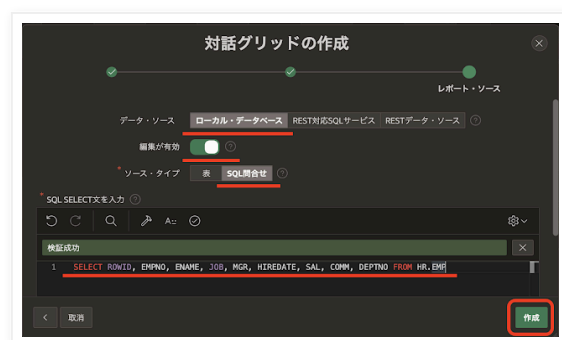


ナビゲーションのプリファレンスとして、新規ナビゲーション・メニュー・エントリの作成を選びます。次へ進みます。



データ・ソースをローカル・データベース、編集が有効をONとします。ソース・タイプとしてSQL問合せを選択し、SQL問合せとして以下のSQLを記述します。作成をクリックします。

```
SELECT ROWID, EMPNO, ENAME, JOB, MGR, HIREDATE, SAL, COMM, DEPTNO FROM HR.EMP
```



作成したページを実行すると、以下になります。従業員の挿入、更新、削除といった操作を行えます。

Empno	Ename	Job	Mgr	Hiredate	Sal	Comm	Deptno
7839	KING	PRESIDENT		1981/11/17	5000		10
7838	BLAKE	MANAGER	7839	1981/05/01	2850		30
7782	CLARK	MANAGER	7839	1981/06/09	2450		10
7566	JONES	MANAGER	7839	1981/04/02	2975		20
7788	SCOTT	ANALYST	7566	1982/12/09	3000		20
7502	FORD	ANALYST	7566	1981/12/03	3000		20
7369	SMITH	CLERK	7502	1980/12/17	800		20
7499	ALLEN	SALESMAN	7566	1981/02/20	1600	300	30
7521	WARD	SALESMAN	7566	1981/02/22	1250	500	30
7654	MARTIN	SALESMAN	7566	1981/03/28	1250	1400	30
7844	TURNER	SALESMAN	7566	1981/09/08	1500	0	30
7676	ADAMS	CLERK	7788	1983/01/12	1100		20
7900	JAMES	CLERK	7566	1981/12/03	950		30
7934	MILLER	CLERK	7782	1982/01/23	1300		10

対話グリッドのページをもう一枚作成します。操作の流れは同じなので、異なる部分だけを示します。ページ作成ウィザードを起動し、編集可能对話グリッドを選択します。

ページ名は部分編集とします。



SQL問合せからは列SALおよびCOMMを除いた以下のSQLを、SQL問合せとして記述します。作成をクリックします。

SELECT ROWID, EMPNO, ENAME, JOB, MGR, HIREDATE, DEPTNO FROM HR.EMP



作成されたページは以下になります。列SAL(Sal)とCOMM(Comm)が除かれています。

Empno	Ename	Job	Mgr	Histartdate	Deptno
7839	KING	PRESIDENT		1981/11/17	10
7836	BLAKE	MANAGER	7839	1981/05/01	30
7782	CLARK	MANAGER	7839	1981/06/09	10
7566	JONES	MANAGER	7839	1981/04/02	20
7788	SCOTT	ANALYST	7566	1982/07/09	20
7502	FORD	ANALYST	7566	1981/12/03	20
7569	SMITH	CLERK	7502	1980/12/07	20
7698	ALLEN	SALESMAN	7698	1981/02/20	30
7621	WARD	SALESMAN	7698	1981/02/22	30
7654	MARTIN	SALESMAN	7698	1981/09/28	30
7644	TURNER	SALESMAN	7698	1981/09/08	30
7676	ADAMS	CLERK	7788	1983/01/12	20
7800	JAMES	CLERK	7698	1981/12/03	30
7834	MILLER	CLERK	7782	1982/01/03	10

以上でテストに使用するアプリケーションが完成しました。

アプリケーションのエクスポートは以下に置いています。
<https://github.com/ujnak/apexapps/blob/master/exports/sqlinjection-for-seminar.sql>

続く

Yuji N. 時刻: 17:49

共有

ウェブ バージョンを表示

自己紹介

Yuji N.

日本オラクル株式会社に勤務していて、Oracle APEXのGroundbreaker Advocateを拝命しました。こちらの記事につきましては、免責事項の参照をお願いいたします。

詳細プロフィールを表示