

```
                                sql_injection_demo
REM This script demonstrates a simple example of sql injection using the HR demo
schema
```

```
connect hr
```

```
set serveroutput on
set echo on
```

```
-- Procedure that retrieves user phone numbers
```

```
pause
```

```
create or replace
```

```
procedure get_phone (p_email varchar2 default null)
```

```
as
```

```
type cv_emptyt is ref cursor;
```

```
cv cv_emptyt;
```

```
v_phone employees.phone_number%type;
```

```
v_stmt varchar2(400);
```

```
begin
```

```
    v_stmt := 'select phone_number from employees where email = '''
              || p_email || ''';
```

```
    dbms_output.put_line('sql statement: ' || v_stmt);
```

```
    open cv for v_stmt;
```

```
    loop
```

```
        fetch cv into v_phone;
```

```
        exit when cv%notfound;
```

```
        dbms_output.put_line('phone: ' || v_phone);
```

```
    end loop;
```

```
    close cv;
```

```
exception when others then
```

```
    dbms_output.put_line(sqlerrm);
```

```
    dbms_output.put_line('sql statement: ' || v_stmt);
```

```
end;
```

```
/
```

```
-- Retrieve phone number for a known user
```

```
pause
```

```
exec get_phone('DGRANT');
```

```
-- Let's try some sql injection
```

```
pause
```

```
exec get_phone('x' union select username from all_users where 'x'='x');
```

```
-- How can we change the procedure to prevent sqli?
```

```
pause
```

```
create or replace
```

```
procedure get_phone (p_email varchar2 default null)
```

```
as
```

```
begin
```

```
for i in
```

```
    (select phone_number
```

```
      from employees
```

```
      where email = p_email)
```

```
    loop
```

```
        dbms_output.put_line('phone: ' || i.phone_number);
```

```
    end loop;
```

```
end;
```

```
/
```

## sql\_injection\_demo

```
-- Let's try user DGRANT again
```

```
pause
```

```
exec get_phone('DGRANT');
```

```
-- Has the injection been prevented?
```

```
pause
```

```
exec get_phone('x' union select username from all_users where 'x'='x');
```