**TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP. HỒ CHÍ MINH**

**KHOA ĐÀO TẠO CHẤT LƯỢNG CAO**

**NGÀNH CÔNG NGHỆ THÔNG TIN**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



**BÁO CÁO ĐỒ ÁN**

**BẢO MẬT CƠ SỞ DỮ LIỆU**

**GVHD : Cô LÊ THỊ MINH CHÂU**

**SVTH : PHẠM TUẤN ANH**

**LỶ SAY HỘI**

**MSSV : 15110010**

**15110053**

**LỚP : 15110CL2A**

**Tp. Hồ Chí Minh, tháng 06 năm 2018**

Contents

[1. Phần làm được trên oracle 1](#_Toc516568802)

[1.1. User: 1](#_Toc516568803)

[1.2. Profile: 1](#_Toc516568804)

[1.3. Privilege: 2](#_Toc516568805)

[1.3.1. Quyền hệ thống (System Privilege) 2](#_Toc516568806)

[1.3.2. Quyền đối tượng (Object Privilege) 2](#_Toc516568807)

[1.4. Role 2](#_Toc516568808)

[1.5. Policy 3](#_Toc516568809)

[2. Phần đã cài đặt 6](#_Toc516568810)

[2.1. Giao diện thêm sửa xóa user 6](#_Toc516568811)

[2.2. Giao diện thêm sửa xóa profile 8](#_Toc516568812)

# Phần làm được trên oracle

## User:

* Admin

Người có chức năng quản lý toàn bộ user của trang web với quyền dba. Mọi policy không áp dụng lên Admin.

* User thường

User bị giới hạn quyền, chỉ sử dụng được một số quyền do Admin cấp.

## Profile:

Qui định các giới hạn của tài khoản user: số lần login thất bại, số lượng phiên làm việc mà user có thể sử dụng đồng thời,... Profile của Admin mặc định là default (mọi tài nguyên được sử dụng unlimited)

CREATE PROFILE user\_1 LIMIT

FAILED\_LOGIN\_ATTEMPTS 3 -- số lần cố gắng login thất bại

SESSIONS\_PER\_USER UNLIMITED -- số lượng phiên làm việc mà người dùng có thể sử dụng đồng thời

CPU\_PER\_SESSION UNLIMITED -- Chỉ định giới hạn thời gian CPU cho một phiên

CPU\_PER\_CALL 3000 -- Chỉ định giới hạn thời gian CPU cho một cuộc gọi, thời gian tính bằng phần trăm giây.

CONNECT\_TIME 45 -- thời gian connect cho một session giới hạn trong vòng 45 phút

IDLE\_TIME 5 -- Lượng thời gian nhàn rỗi cho session của user, thời gian tính bằng phút

LOGICAL\_READS\_PER\_SESSION DEFAULT -- Chỉ định số khối dữ liệu được phép đọc trong một phiên, bao gồm các khối đọc từ bộ nhớ và đĩa.

LOGICAL\_READS\_PER\_CALL 1000; -- Chỉ định số khối dữ liệu được phép đọc cho một cuộc gọi để xử lý câu lệnh SQL

## Privilege:

Cho phép thực hiện 1 câu lệnh SQL nào đó hoặc được phép truy xuất đến một đối tượng nào đó như quyền: tạo bảng CREATE TABLE; connect đến cơ sở dữ liệu CREATE SESSION, quyền SELECT trên một bảng cụ thể nào đó, … Có 2 loại quyền:

### Quyền hệ thống (System Privilege)

Thực hiện một tác vụ CSDL cụ thể hoặc quyền thực hiện một loại hành động trên tất cả những đối tượng schema của hệ thống.

Một user có thể cấp 1 quyền hệ thống cho user khác nếu có một trong các điều kiện sau:

* Đã được cấp quyền hệ thống đó với tùy chọn **WITH ADMIN OPTION**
* Có quyền **GRANT ANY PRIVILEGE**

GRANT CREATE PROFILE, ALTER PROFILE, DROP PROFILE,

CREATE ROLE, ALTER ANY ROLE, DROP ANY ROLE, GRANT ANY ROLE,

CREATE SESSION, CREATE ANY TABLE, ALTER ANY TABLE, DROP ANY TABLE,

SELECT ANY TABLE, DELETE ANY TABLE, INSERT ANY TABLE, UPDATE ANY TABLE,

CREATE TABLE, CREATE USER, ALTER USER, DROP USER

TO user\_test\_01 WITH ADMIN OPTION;

### Quyền đối tượng (Object Privilege)

Thực hiện một thao tác cụ thể lên một schema object cụ thể.

Một user có thể cấp 1 quyền đối tượng cho user khác nếu có một trong các điều kiện sau:

* Có tất cả mọi quyền đối tượng trên tất cả các đối tượng thuộc schema của mình, ngoài ra còn có thể cấp bất kì quyền đối tượng nào thuộc schema của mình cho bất cứ user nào khác.
* Có quyền **GRANT ANY OBJECT PRIVILEGE**
* Được cấp quyền đối tượng đó với tùy chọn **WITH GRANT OPTION**

GRANT SELECT, INSERT, UPDATE, DELETE ON QUANLYUSER TO user\_test\_01 WITH GRANT OPTION;

## Role

Là một tập hợp các quyền và cả các role khác. Role có thể được gán cho các user hoặc các role khác.

Một user có thể cấp role cho user khác nếu có một trong các điều kiện sau:

* User đã tạo ra role đó
* Đã được cấp role đó với tùy chọn WITH ADMIN OPTION
* Được cấp quyền GRANT ANY ROLE

CREATE ROLE ROLE1; -- Tạo role

GRANT CREATE SESSION, ALTER PROFILE TO ROLE1; -- Cấp quyền cho role vừa tạo

GRANT SELECT, UPDATE ON QUANLYUSER TO ROLE1

GRANT USER\_ROLE1 TO user\_test\_02; -- Cấp role vừa tạo cho user

## Policy

Admin tạo một policy để user chỉ có thể xem được chính thông tin của user đó mà không được phép xem thông tin của user khác

Tạo function:

create or replace FUNCTION FUNCTION\_USER\_CHI\_DUOC\_XEM\_THONG\_TIN\_CUA\_MINH

(p\_schema IN VARCHAR2, p\_object IN VARCHAR2)

RETURN VARCHAR2

AS

BEGIN

RETURN ‘upper(USERNAME) = upper(user)’;

END;

- Thêm policy:

BEGIN

DBMS\_RLS.add\_policy

(object\_schema => 'ADMIN',

object\_name => USERS,

policy\_name => POLICY\_USER\_CHI\_DUOC\_XEM\_CHINH\_SUA\_THONG\_TIN\_CUA\_MINH',

policy\_function => 'FUNCTION\_USER\_CHI\_DUOC\_XEM\_THONG\_TIN\_CUA\_MINH',

statement\_types => 'SELECT, UPDATE');

END;

1. **Các Table**

**1. Table quản lý quyền**

SELECT d.GRANTEE, d.PRIVILEGE, d.ADMIN\_OPTION, u.USERNAME

from user\_sys\_privs u FULL OUTER JOIN dba\_sys\_privs d ON u.PRIVILEGE=d.PRIVILEGE

WHERE d.GRANTEE NOT IN ('SYS','SYSTEM','DV\_REALM\_OWNER','EM\_EXPRESS\_ALL','DV\_REALM\_RESOURCE','EXP\_FULL\_DATABASE',

'GSMADMIN\_ROLE','GSMUSER','IMP\_FULL\_DATABASE','DVSYS','DV\_ACCTMGR','EM\_EXPRESS\_BASIC','GGSYS','GSMADMIN\_INTERNAL',

'JAVADEBUGPRIV','MDSYS','LBACSYS','OEM\_ADVISOR','OLAP\_DBA','OJVMSYS','OLAP\_USER','OUTLN','ORDSYS','RECOVERY\_CATALOG\_OWNER',

'SCHEDULER\_ADMIN','WMSYS','XDB','XS\_CONNECT','AQ\_ADMINISTRATOR\_ROLE','APPQOSSYS','OEM\_MONITOR','DATAPUMP\_IMP\_FULL\_DATABASE',

'SPATIAL\_CSW\_ADMIN\_USR','SYSBACKUP','SYSDG','SYSKM','RECOVERY\_CATALOG\_OWNER\_VPD','RESOURCE','SI\_INFORMTN\_SCHEMA','CTXSYS',

'SYSRAC','DATAPUMP\_EXP\_FULL\_DATABASE')

ORDER BY d.GRANTEE;

**2. Table quản lý role**

SELECT U.USERNAME, S.PROFILE, U.ACCOUNT\_STATUS, S.RESOURCE\_NAME

FROM DBA\_USERS U LEFT OUTER JOIN DBA\_PROFILES S ON S.PROFILE = U.PROFILE

WHERE U.USERNAME NOT IN ('ANONYMOUS','APPQOSSYS','APPQOSSYS','APPQOSSYS','DBSFWUSER','DBSNMP','DIP','DVF','DVSYS','GGSYS','GSMADMIN\_INTERNAL',

'GSMCATUSER','GSMUSER','LBACSYS','MDDATA','MDSYS','OJVMSYS','OLAPSYS','ORACLE\_OCM','ORDDATA','ORDPLUGINS','WMSYS','XDB','XS$NULL','CTXSYS',

'OUTLN','ORDSYS','REMOTE\_SCHEDULER\_AGENT','SYSTEM','SYSKM','SYSRAC','AUDSYS','PDBADMIN','SYS$UMF','SYSBACKUP','SYS','SYSDG')

ORDER BY USERNAME;

**3. Table quản lý profile**

Select a.grantee User\_name, a.granted\_role role, b.privilege from DBA\_ROLE\_PRIVS a, DBA\_SYS\_PRIVS b where

a.granted\_role=b.grantee and a.GRANTED\_ROLE NOT IN ('SYS','IMP\_FULL\_DATABASE','EXP\_FULL\_DATABASE','CONNECT','DATAPUMP\_IMP\_FULL\_DATABASE',

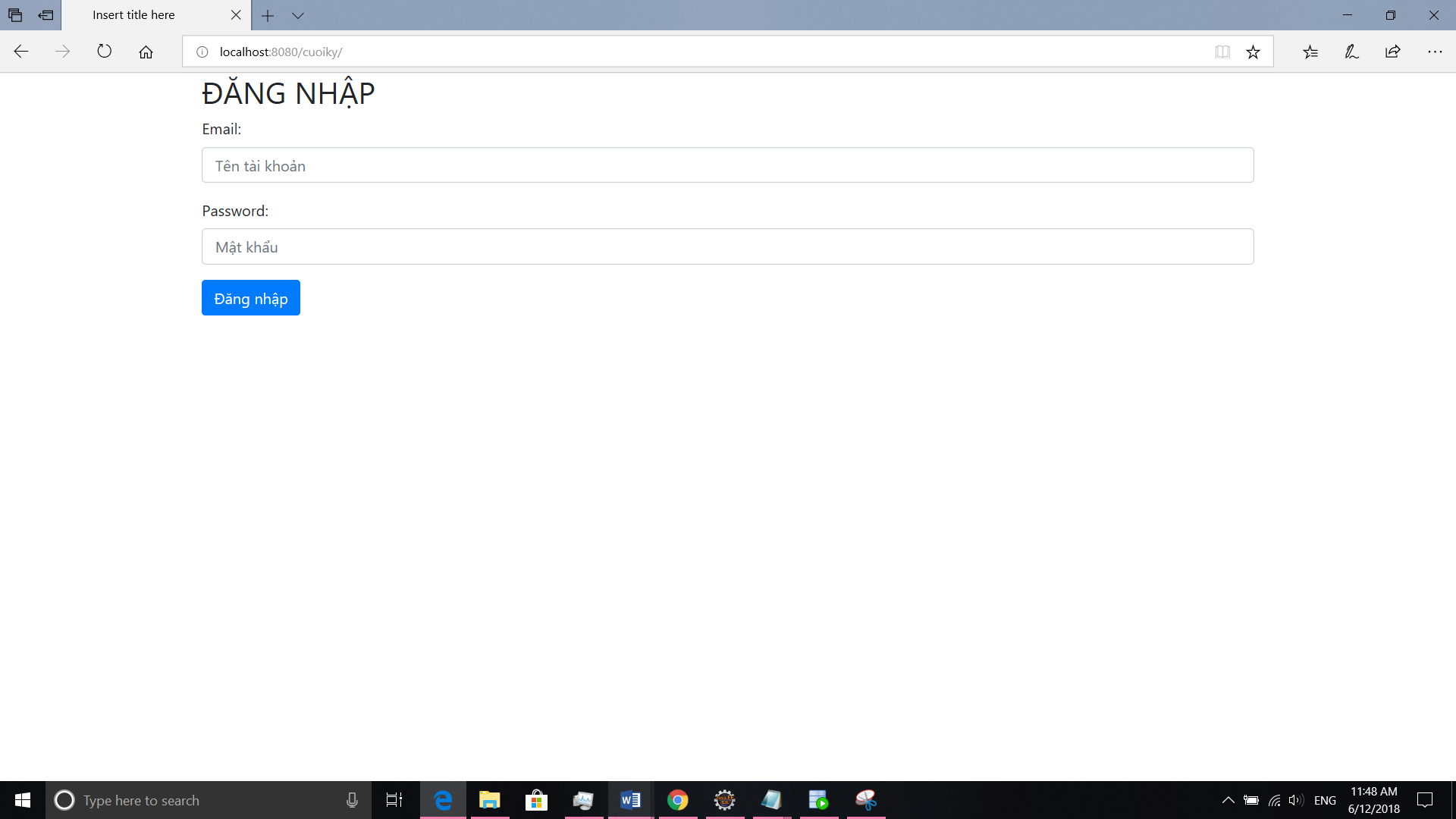
'IMP\_FULL\_DATABASE','EM\_EXPRESS\_ALL','AQ\_ADMINISTRATOR\_ROLE','RESOURCE','OLAP\_DBA','CTXAPP')

ORDER BY a.GRANTEE DESC;

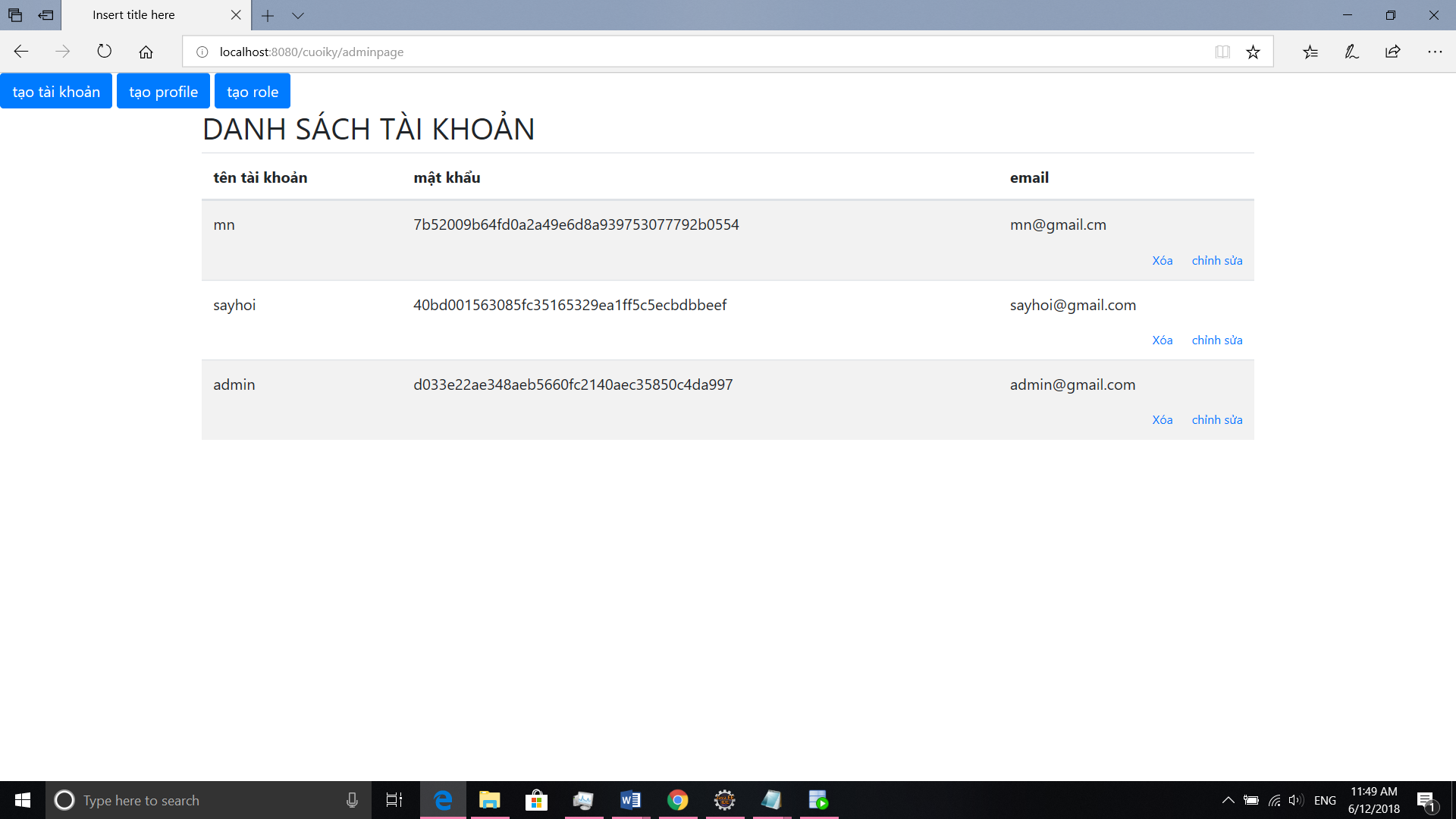
# Phần đã cài đặt

## Giao diện thêm sửa xóa user

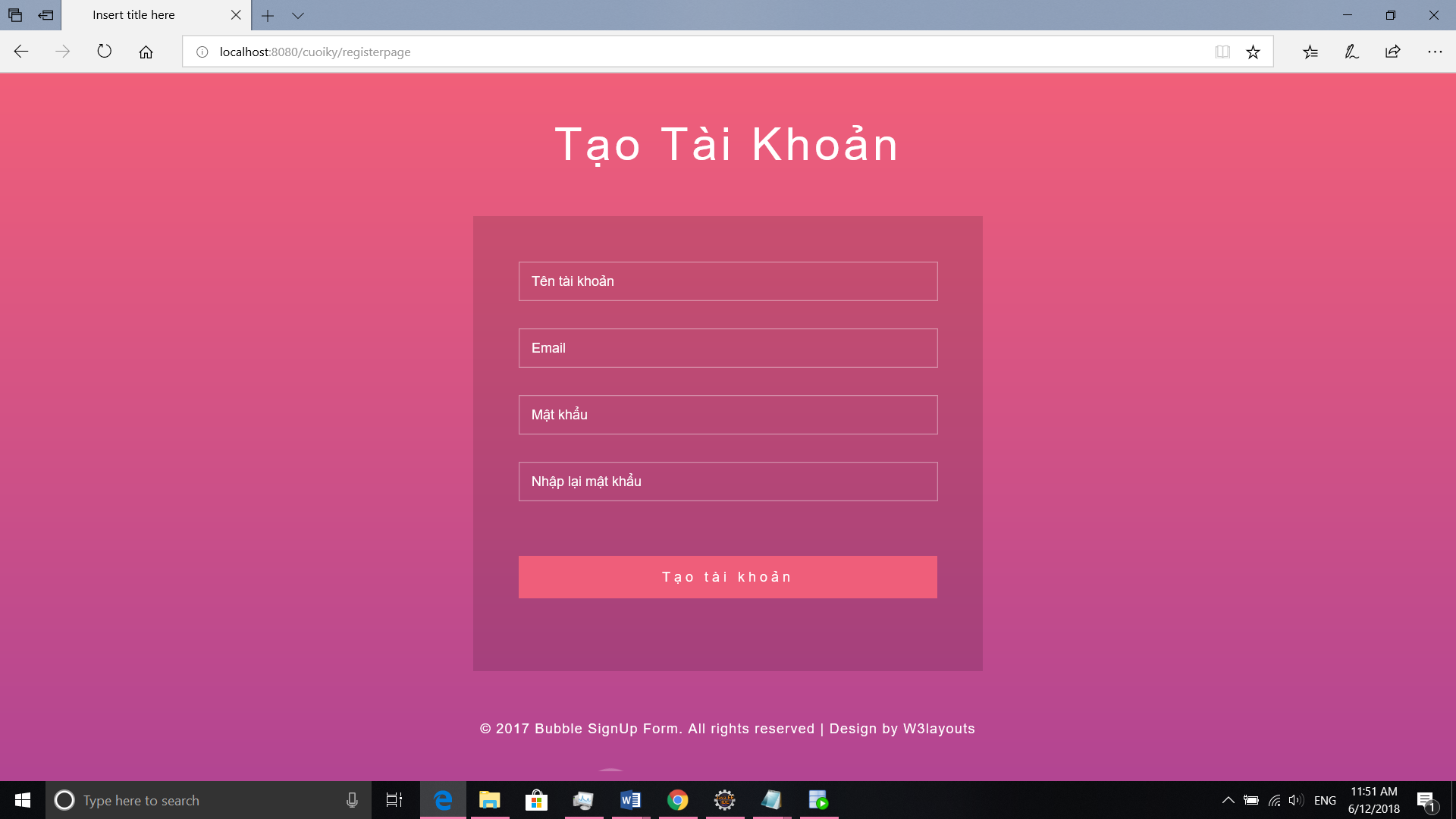
* Màn hình đăng nhập



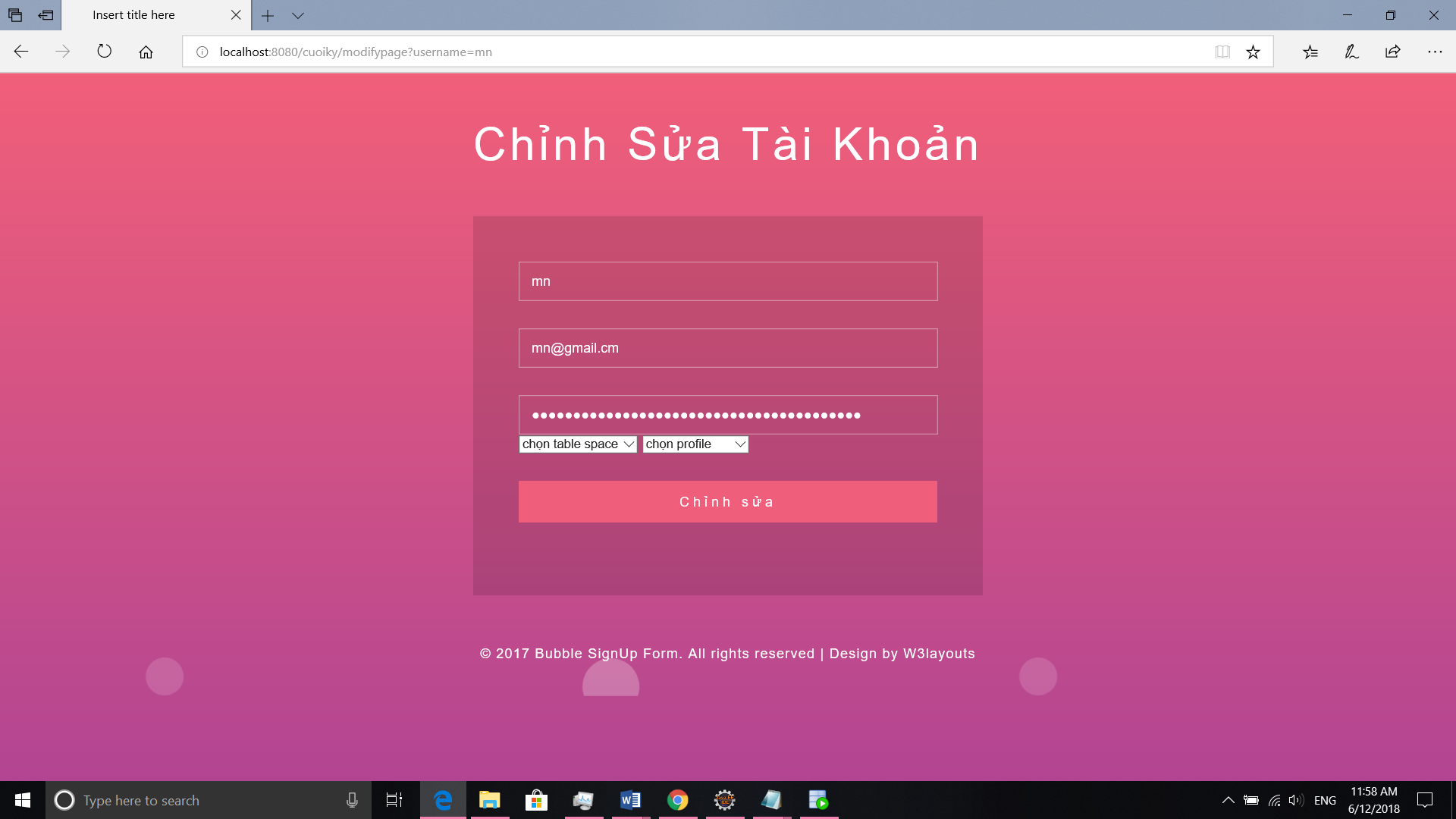
* Giao diện hiện thị danh sách tài khoảng
* Thông tin tài khoản user gồm tên tài khoản, email, mật khẩu (đã mã hóa mã sha1)



* Giao diện tạo tài khoản cho user
* Thông tin tài khoản cũng như trên: tên đăng nhập, email, và mật khẩu



* Giao diện chỉnh sửa tài khoản
* Chỉ thay đổi profile và tablespace của tài khoản



## Giao diện thêm sửa xóa profile

* Giao diện thao tác với profile
* Đâu tiên hiển thị danh sách profile cùng các thông số
* Kế bên có chữ chỉnh sửa và xóa để thực hiện sửa và xóa
* Form dưới để tạo profile mới
* Những thông số không được nhập sẽ lấy giá trị mặc định unlimited (trừ tên)

