



BMTT NHOM7 G2 - sdasdasdsadsa

Mạng máy tính (Đại học Tôn Đức Thắng)



Scan to open on Studocu

**TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM
TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG
KHOA CÔNG NGHỆ THÔNG TIN**



INFORMATION SECURITY ASSIGNMENT

...

Lecturer: **Ms. Huynh Ngoc Tu**

Full Name: **Bành Uyển Nhi -519H0128**

Nguyễn Bảo Khánh - 519H0075

Class: **19H50303**

Course: **23**

THÀNH PHỐ HỒ CHÍ MINH, NĂM 2021

FIRST WORDS

Firstly, I sincerely thanks to Ms. Huynh Ngoc Tu who is my Information Security instructor. During my learning process, I received a lot of useful advices and enthusiastic support from my instructor. Ms. Tu is the person who helps us take a few very little first steps in this course. From what I have learned and from my personal knowledge, I was able enough to finish my Assignment report.

Because of my lack of experience as well as my limited knowledge, this report definitely cannot avoid the incorrectness. I willingly and hopefully to be received some comments from my instructor to make this report become more and more complete.

Lastly, I would like to greet you a good health, success and happiness.

Yours faithfully.

PROFESSOR'S EVALUATION

Tp. Hồ Chí Minh, ngày tháng năm
(kí và ghi họ tên)

CONTENT

EXERCISE 1. Study different privileges and personally choose 4 most important.....4

EXERCISE 2. Study different roles and personally choose 4 most important

EXERCISE 3. Create roles and Redesigning.....8



EXERCISE 4. Reporting your hierarchy

EXERCISE 5. Define your hierarchy roles in OpenMRS.....12

EXERCISE 6. Challenges and Solutions

EXERCISE 1. STUDY DIFFERENT PRIVILEGES IN OPENMRS DEMO AND LIST FOUR OF THEM THAT SEEMS MOST IMPORTANT TO YOU.

1. App:coreapps.systemAdministration:

 App: coreapps.summaryDashboard	Able to access summary dashboards
<input type="checkbox"/> App: coreapps.systemAdministration	Able to access the System Administration page
<input type="checkbox"/> App: formentryapp.forms	Manages implementation-defined forms and attaches them to the UI
 App: referenceapplication.legacyAdmin	Able to access the advanced administration app




Explanation: As we all know, an administrator provides office support to either an individual or team and is vital for smooth-running of a business. Also, administrators are often responsible for office projects and tasks, as well as overseeing the work of junior admin staff. In the worst circumstances, if the attacker is given the privileges to access the administrator page, then the attacker will gain access to an administrative account page. This page might disclose the administrator's password or provide a means of changing it or might provide direct access to privileged functionality.

2. Share metadata

 Schedule Appointments	Ability to schedule new appointments
 Share Metadata	Allows user to export and import metadata
 Squeezing Appointments	Ability to override the constraints and schedule

Explanation: Metadata summarizes basic information about data, which can make it easier to find. For web pages, metadata contains descriptions of the page's contents, as well as keywords linked to the content. If the attacker is given this privilege, this leads to some very serious consequences: blackmail a business or individual, apply for fraudulent loans and credit cards under a person's or business's name, gain unauthorized access to personal online accounts, email phishing, spoofing, vice versa...That is why this privilege is extremely vital.

3. Edit User Passwords

<input type="checkbox"/> Edit Roles	
 Edit User Passwords	Able to change the passwords of users in OpenMRS
 Edit Users	Able to edit users in OpenMRS
 Edit Visits	Able to edit visits

Explanation: Having a privilege to be able to change the passwords of users in OpenMRS is very powerful. That is to say, once you have this privilege, suppose that you are an attacker or an unprofessional staff, you may easily change some or all patient's passwords to get into their account. Until that point happen you probably have controlled all the confidential information of a healthcare system which attacker may use for selling, blackmailing, illegal money transferring, vice versa...

4. Assign System Developer Role

 App: registrationapp.registerPatient	Able to access the register patient app
 Assign System Developer Role	Able to assign System Developer role
 Configure Visits	Able to choose encounter visit handler and
 Delete Cohorts	Able to add a cohort to the system

Explanation: System developers create tools and programs that would fit the requirements of the company. They also know how to look for problems in the system and can fix these problems upon identification. So if attacker has the right to assign System Developer Role to another person, it will be very dangerous because he/she will assign it to a person that aim to harm the organization in order to gain more profits. For this reason, the person has the privilege to assign System Developer Role is very important, because that person can give that vital role to a normal user or even the attacker.

EXERCISE 2: STUDY DIFFERENT ROLES IN OPENMRS DEMO AND NAME FOUR MAIN ROLES THAT HAVE MAXIMUM SET OF PRIVILEGES.

1. System Developer

<input type="checkbox"/> Registration Clerk	Add/Edit/View Patients/User/Appointment	Patient Manager , User Manager
<input type="checkbox"/> Surgeon		Diagnoses Doctor , Ambulance Personnel
<input type="checkbox"/> System Administrator		User Manager
<input checked="" type="checkbox"/> System Developer	Developers of the OpenMRS .. have additional access to change fundamental structure of the database model.	[Has all roles and privileges]
<input type="checkbox"/> System administrator	Add/edit/view User/Roles - Edit/View User Password	

Explanation: As the name says, this role is developers of the OpenMRS system, so it has not only all roles and privileges, but also has additional access to change the fundamental structure of the database model.

2. Privilege Level: Full

<input type="checkbox"/> Physiotherapist	Add/Edit/View Encounter/Physiotherapy Order	Meeting Manager
<input checked="" type="checkbox"/> Privilege Level: Full	A role that has all API privileges	
<input type="checkbox"/> Privilege Level: High	A role that has all API privileges except administrative privileges with security implications	
<input checked="" type="checkbox"/> Provider	All users with the 'Provider' role will appear as options in the default Infopath	
<input type="checkbox"/> Psychologist	Add/Edit/View Encounter/psychology Order	Meeting Manager

Explanation: This is one of the roles with the most privileges along with the **System Developer** role. Because it has privileges with security implications, not many roles inherit it.

3. Privileges Level: High

<input type="checkbox"/> Patient Manager	Add/Edit/View patient	
<input type="checkbox"/> Physiotherapist	Add/Edit/View Encounter/ Physiotherapy Order	Meeting Manager
<input type="checkbox"/> Privilege Level: Full	A role that has all API privileges	
<input type="checkbox"/> Privilege Level: High	A role that has all API privileges except administrative privileges with security implications	
Provider	All users with the 'Provider' role will appear as options in the default Infopath	

Explanation: this role is similar to the Privileges Level: Full role, except privileges with security implications. In contrast to the Privileges Level: Full role, this role is inherited by many roles.

4. Application: Has Super User Privileges

<input type="checkbox"/> Application: Edits Existing Encounters	Gives user the ability to edit patient encounter	Privilege Level: High
<input type="checkbox"/> Application: Enters ADT Events	Enters ADT events	Privilege Level: High
<input type="checkbox"/> Application: Enters Vitals	Enters vitals	Privilege Level: High
<input type="checkbox"/> Application: Has Super User Privileges	Extends the underlying System Developer API role	System Developer , Privilege Level: High
<input type="checkbox"/> Application: Manages Atlas	Can configure whether/how this implementation is displayed on the OpenMRS Atlas	Privilege Level: High
<input type="checkbox"/> Application: Manages Provider Schedules	Gives user ability to add and edit provider schedules	Privilege Level: High

Explanation: this role extends the underlying **System Developer** API role, so it inherits almost all the roles and privileges from System Developer, plus some more from **Privileges Level: High**.

EXERCISE 3. DEFINE THE ABOVE MENTIONED ROLES AND USERS IN OPENMRS AND ATTACH THE SCREENSHOT.

1. Create Roles: Data Assistant, Data Manager, Medical Student

Roles	Description	Inherited Roles	Privileges
<input type="checkbox"/> Data Assistant	Edit/View Patients		Edit Patients , View Patients
<input type="checkbox"/> Data Manager	Add/Edit/View Patients		View Patients , Add Patients ...
<input type="checkbox"/> Doctor	Add/Edit/View Patients Add/Edit/View Laboratory Orders Add/Edit/View Encounters Add/Edit/View Visits	Encounters , Staff	Add Visits , View Patients ...
<input type="checkbox"/> Encounters	Add/Edit/View Encounters		View Encounters , Edit Encounters ...
<input type="checkbox"/> Health Secretary	Add/Edit/View Encounters Add/Edit/View Diet Orders	Encounters	Edit Diet Orders , Add Diet Orders ...
<input type="checkbox"/> Medical Students	View Patients		View Patients

2. Create users: Bob, Mary, Erica and assign roles

Username	Given	Family Name	Roles
Bob	Bob		MedicalStudent

Username	Given	Family Name	Roles
Mary	Mary		Data Assistant

Username	Given	Family Name	Roles
Erica	Erica		Data Manager


Search

Name	Gender	User Accounts	Provider Accounts	Action
Super User	M	2	1	
John Smith	M	1	1	
Jane Smith	F	1	1	
Jake Smith	M	1	1	
Julie Smith	F	1	0	
Hoàng Tuấn Vũ	M	1	0	
Lộc	M	1	0	
Thanh	F	1	0	
Bob	M	1	0	
Mary	F	1	0	
Erica	F	1	0	

Showing 1 to 11 of 11 entries

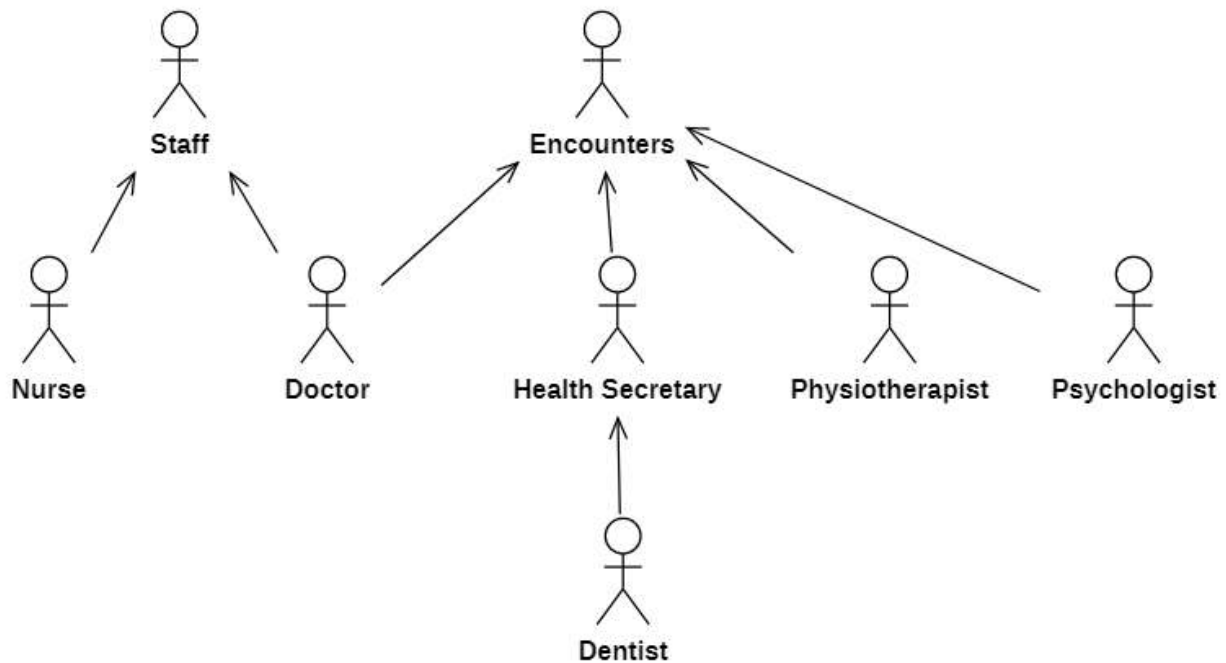
[First](#) [Previous](#) [1](#) [Next](#) [Last](#)

3. Redesign roles slightly

Roles	Description	Inherited Roles	Privileges
 Authenticated	gained once authentication has been established	Medical Students	Get Concept Datatypes , View Privileg
<input type="checkbox"/> Data Assistant	Edit/View Patients		Edit Patients , View Patients
<input type="checkbox"/> Data Manager	Add/Edit/View Patients	Data Assistant	Edit Patients , View Patients ...
<input type="checkbox"/> Doctor	Add/Edit/View Patients Add/Edit/View Laboratory Orders Add/Edit/View Encounters Add/Edit/View Visits	Encounters , Staff	Add Visits , View Patients ...
<input type="checkbox"/> Encounters	Add/Edit/View Encounters		View Encounters , Edit Encounters ...
<input type="checkbox"/> Health Secretary	Add/Edit/View Encounters Add/Edit/View Diet Orders	Encounters	Edit Diet Orders , Add Diet Orders ...
<input type="checkbox"/> Medical Students	View Patients		View Patients

There is a slightly change in the Inherited Roles column, after redesigning the Data Manager Role has inherited the Edit and View privileges from the Data Assistant role. Because Data Manager inherit privileges from Data Assistant so every privilege that Data Assistant has Data Manager should have too.

EXERCISE 4: REPORT YOUR ROLE HIERARCHY




Role	Inherit	Privilege
Staff		Add/ Edit/ View Patients Add/ Edit/ View Laboratory Orders
Encounters		Add/ Edit/ View Encounters
Nurse	<i>Staff</i>	Add/ Edit/ View Patients Add/ Edit/ View Laboratory Orders Add/ Edit/ View Observations Add/ Edit/ View Reports
Doctor	<i>Staff, Encounters</i>	Add/ Edit/ View Patients Add/ Edit/ View Laboratory Orders Add/ Edit/ View Encounters Add/ Edit/ View Visits
Health Secretary	<i>Encounters</i>	Add/ Edit/ View Encounters Add/ Edit/ View Diet Orders
Physiotherapist	<i>Encounters</i>	Add/ Edit/ View Encounters Add/ Edit/ View Physiotherapy Orders
Psychologist	<i>Encounters</i>	Add/ Edit/ View Encounters Add/ Edit/ View Psychology Orders
Radiologist		Add/ Edit/ View Laboratory Orders Add/ Edit/ View Radiology Orders
Dentist	<i>Health Secretary</i>	Add/ Edit/ View Encounters


		Add/ Edit/ View Diet Orders
Ambulance Personnel		View Patients Add Reports
System Administrator		Add/ Edit/ View Users Add/ Edit User Passwords Add/ Edit/ View Roles
Registration Clerk		Add/ Edit/ View Users Add/ Edit/ View Patients Add/ Edit/ View Appointments

EXERCISE 5: DEFINE YOUR ROLE HIERARCHY IN OPENMRS


Staff:

 Provider	All users with the 'Provider' role will appear as options in the default Infopath	
<input type="checkbox"/> Staff	Add/Edit/View Patients Add/Edit/View Laboratory Orders	View Patients , Add Patients ... [View Patients, Add Patients, View Laboratory Orders, Add Laboratory Orders, Edit Patients, Edit Laboratory Orders]
<input type="checkbox"/> System Administrator	Super users (system administrators) are automatically granted all privileges in the system	Organizational: System Administrator , Privilege Level: Full

Encounters:

<input type="checkbox"/> Application: Uses Capture Vitals App	Uses capture vitals app	Privilege Level: High	App: referenceapplication.vitals
<input type="checkbox"/> Application: Uses Patient Summary	Uses patient summary	Privilege Level: High	App: coreapps.findPatient , App: coreapps.patien
<input type="checkbox"/> Application: Writes Clinical Notes	Writes clinical notes	Privilege Level: High	App: coreapps.findPatient , Task: referenceapplic
 Authenticated	Privileges gained once authentication has been established.		Get Concept Datatypes , View Privileges ...
<input type="checkbox"/> Encounters	Add/Edit/View Encounters		View Encounters , Add Encounters ... View Pa [View Encounters, Add Encounters, Edit Encounters]
<input type="checkbox"/> Medical Students	mary		
<input type="checkbox"/> Organizational: Doctor	Doctor	Application: Records Allergies , Application: Writes Clinical Notes ...	
<input type="checkbox"/> Organizational: Hospital Administrator	Hospital Administrator	Application: Configures Appointment Scheduling , Application: Schedules And Overbooks Appointments ...	
<input type="checkbox"/> Organizational: Nurse	Nurse	Application: Records Allergies , Application: Enters ADT Events ...	
<input type="checkbox"/> Organizational: Registration Clerk	Registration Clerk	Application: Schedules Appointments , Application: Registers Patients ...	
<input type="checkbox"/> Organizational: System Administrator	System Administrator	Application: Configures Forms , Application: Configures Appointment Scheduling ...	
<input type="checkbox"/> Privilege Level: Full	A role that has all API privileges		Delete Diagnoses , Manage Concept Classes ...

Nurse:

 Authenticated	Privileges gained once authentication has been established.		Get Concept Datatypes , View Privileges ...
<input type="checkbox"/> Encounters	Add/Edit/View Encounters		View Encounters , Add Encounters ...
<input type="checkbox"/> Medical Students	mary		View Patients
<input type="checkbox"/> Nurse	Add/Edit/View Patients Add/Edit/View Laboratory Orders Add/Edit/View Observations Add/Edit/View Reports	Staff	Add Observations , Add Reports ... [Add Observations, Add Reports, Edit Observations, Edit Reports, View Observations, View Reports]
<input type="checkbox"/> Organizational: Doctor	Doctor	Application: Records Allergies , Application: Writes Clinical Notes ...	
<input type="checkbox"/> Organizational: Hospital Administrator	Hospital Administrator	Application: Configures Appointment Scheduling , Application: Schedules And Overbooks Appointments ...	
<input type="checkbox"/> Organizational: Nurse	Nurse	Application: Records Allergies , Application: Enters ADT Events ...	

Doctor:

<input type="checkbox"/> Application: Writes Clinical Notes	Writes clinical notes	Privilege Level: High	App: coreapps.findPatient , Task: referenceapplic
<input type="checkbox"/> Authenticated	Privileges gained once authentication has been established.		Get Concept Datatypes , View Privileges ...
<input type="checkbox"/> Doctor	Add/Edit/View Patients Add/Edit/View Laboratory Orders Add/Edit/View Encounters Add/Edit/View Visits	Encounters , Staff	Add Visits , View Patients ... [Add Visits, View Patients, Add Patients, View Laboratory Orders, Add Laboratory Orders, View Encounters, Add Encounters, Edit Patients, Edit Laboratory Orders, View Visits, Edit Visits, Edit Encounters]
<input type="checkbox"/> Encounters	Add/Edit/View Encounters		View Encounters , Edit Encounters ...
<input type="checkbox"/> Medical Students	many		View Patients
<input type="checkbox"/> Nurse	Add/Edit/View Patients Add/Edit/View Laboratory Orders Add/Edit/View Observations Add/Edit/View Reports	Staff	Add Observations , Add Reports ...

Health Secretary:

<input type="checkbox"/> Doctor	Patients Add/Edit/View Laboratory Orders Add/Edit/View Encounters Add/Edit/View Visits	Encounters , Staff	Add Visits , View Patients ...
<input type="checkbox"/> Encounters	Add/Edit/View Encounters		View Encounters , Edit Encounters ...
<input type="checkbox"/> Health Secretary	Add/Edit/View Encounters Add/Edit/View Diet Orders	Encounters	Edit Diet Orders , Add Diet Orders ... [Edit Diet Orders, Add Diet Orders, View Diet Orders]
<input type="checkbox"/> Medical Students	many		View Patients
<input type="checkbox"/> Nurse	Add/Edit/View Patients Add/Edit/View Laboratory Orders Add/Edit/View Observations Add/Edit/View Reports	Staff	Add Observations , Add Reports ...

Physiotherapist:

<input type="checkbox"/> Organizational: Hospital Administrator	Hospital Administrator	Application: Configures Appointment Scheduling , Application: Schedules And Overbooks Appointments ...	
<input type="checkbox"/> Organizational: Nurse	Nurse	Application: Records Allergies , Application: Enters ADT Events ...	
<input type="checkbox"/> Organizational: Registration Clerk	Registration Clerk	Application: Schedules Appointments , Application: Registers Patients ...	
<input type="checkbox"/> Organizational: System Administrator	System Administrator	Application: Configures Forms , Application: Configures Appointment Scheduling ...	
<input type="checkbox"/> Physiotherapist	Add/Edit/View Encounters Add/Edit/View Physiotherapy Orders	Encounters	Edit Physiotherapy Orders , View Physiotherapy C [Edit Physiotherapy Orders, View Physiotherapy Orders, Add Physiotherapy Orders] Delete Diagnoses , Manage Concept Classes ...
<input type="checkbox"/> Privilege Level: Full	A role that has all API privileges		
<input type="checkbox"/> Privilege Level: High	A role that has all API privileges except administrative privileges with security implications		Delete Diagnoses , Manage Concept Classes ...

Psychologist:

<input type="checkbox"/> Privilege Level: High	except administrative privileges with security implications		Delete Diagnoses , Manage Concept Classes ...
Provider	All users with the 'Provider' role will appear as options in the default Infopath		
<input type="checkbox"/> Psychologist	Add/Edit/View Encounters Add/Edit/View Psychology Orders	Encounters	View Psychology Orders , Add Psychology Orders [View Psychology Orders, Add Psychology Orders, Edit Psychology Orders]
<input type="checkbox"/> Staff	Add/Edit/View Patients Add/Edit/View Laboratory Orders		View Patients , Add Patients ...
	Super users (system administrators)		

Radiologist:

Provider	All users with the 'Provider' role will appear as options in the default Infopath		
<input type="checkbox"/> Psychologist	Add/Edit/View Encounters Add/Edit/View Psychology Orders	Encounters	View Psychology Orders , Add Psychology Orders
<input type="checkbox"/> Radiologist	Add/Edit/View Laboratory Orders Add/Edit/View Radiology Orders		View Laboratory Orders , Add Laboratory Orders [View Laboratory Orders, Add Laboratory Orders, View Radiology Orders, Edit Radiology Orders, Edit Laboratory Orders, Add Radiology Orders]
<input type="checkbox"/> Registration Clerk	Add/Edit/View Users Add/Edit/View Patients Add/Edit/View Appointments		Add Users , View Patients ...
<input type="checkbox"/> Staff	Add/Edit/View Patients Add/Edit/View Laboratory Orders		View Patients , Add Patients ...
	Add/Edit/View		

Dentist:

<input type="checkbox"/> Application: Uses Capture Vitals App	Uses capture vitals app	Privilege Level: High	App: referenceapplication.vitals
<input type="checkbox"/> Application: Uses Patient Summary	Uses patient summary	Privilege Level: High	App: coreapps.findPatient , App: coreapps.patien
<input type="checkbox"/> Application: Writes Clinical Notes	Writes clinical notes	Privilege Level: High	App: coreapps.findPatient , Task: referenceapplic
Authenticated	Privileges gained once authentication has been established.		Get Concept Datatypes , View Privileges ...
<input type="checkbox"/> Dentist	Add/Edit/View Encounters Add/Edit/View Diet Orders	Health Secretary	Edit Diet Orders , Add Diet Orders ... [Edit Diet Orders, Add Diet Orders, View Diet Orders]
<input type="checkbox"/> Doctor	Add/Edit/View Patients Add/Edit/View Laboratory Orders	Encounters , Staff	Add Visits , View Patients ...
<input type="checkbox"/> Encounters	Add/Edit/View Encounters		View Encounters , Edit Encounters ...

Ambulance Personnel:

Current Roles			
Role	Description	Inherited Roles	Privileges
<input checked="" type="checkbox"/> Ambulance Personnel	View Patients Add Reports		Add Reports , View Patients
<input checked="" type="checkbox"/> Anonymous	Privileges for non-authenticated users.		Add Laboratory Orders , Manage Concept Classes
<input type="checkbox"/> Application: Administers System	Administers system Gives user the ability to add and edit appointment types	Application: Configures Appointment Scheduling , Doctor ...	Task: coreapps.deletePatientProgram , Task: core...
<input type="checkbox"/> Application: Configures Appointment Scheduling	Manages forms and attaches them to the UI	Privilege Level: High	App: appointmentschedulingui.appointmentTypes
<input type="checkbox"/> Application: Configures Forms	Manages forms and attaches them to the UI	Privilege Level: High	App: coreapps.configuremetadata , App: forment
<input type="checkbox"/> Application: Configures Metadata	Gives user the ability to edit patient encounter	Privilege Level: High	App: coreapps.configuremetadata
<input type="checkbox"/> Application: Edits Existing Encounters	Enters ADT events	Privilege Level: High	Task: emr.patient.encounter.edit , Task: emr.pat
<input type="checkbox"/> Application: Enters ADT Events	Enters vitals	Privilege Level: High	Task: coreapps.createVisit , Task: referenceapplic
<input type="checkbox"/> Application: Enters Vitals			App: coreapps.findPatient , App: coreapps.active

System Administrator:

<input type="checkbox"/> Radiologist	Urgent Add/Edit/View Laboratory Orders Add/Edit/View Radiology Orders		View Laboratory Orders , Add Laboratory Orders
<input type="checkbox"/> Registration Clerk	Add/Edit/View Users Add/Edit/View Patients Add/Edit/View Appointments		Add Users , View Patients ...
<input type="checkbox"/> Staff	Add/Edit/View Patients Add/Edit/View Laboratory Orders		View Patients , Add Patients ...
<input checked="" type="checkbox"/> System Administrator	Add/Edit/View Users Add/Edit User Passwords Add/Edit/View Roles		Add Users , Add Roles ... [Add Users, Add Roles, Add User Passwords, Edit Users, View Roles, Edit Roles, View Users, Edit User Passwords]
<input checked="" type="checkbox"/> System Developer	Developers of the OpenMRS ... have additional access to change fundamental structure of the database model.	[Has all roles and privileges]	

Registration Clerk:

<input type="checkbox"/> Psychologist	Add/Edit/View Psychology Orders	Encounters	View Psychology Orders , Add Psychology Orders
<input type="checkbox"/> Radiologist	Add/Edit/View Laboratory Orders Add/Edit/View Radiology Orders		View Laboratory Orders , Add Laboratory Orders
<input checked="" type="checkbox"/> Registration Clerk	Add/Edit/View Users Add/Edit/View Patients Add/Edit/View Appointments		Add Users , View Patients ... [Add Users, View Patients, Add Patients, Edit Users, Edit Patients, Add Appointments, View Appointments, View Users, Edit Appointments]
<input type="checkbox"/> Staff	Add/Edit/View Patients Add/Edit/View Laboratory Orders		View Patients , Add Patients ...
<input type="checkbox"/> System Administrator	Add/Edit/View Users Add/Edit User Passwords Add/Edit/View Roles		Add Users , Add Roles ...
<input checked="" type="checkbox"/> System Developer	Developers of the OpenMRS ... have additional access to change fundamental structure of the database model.	[Has all roles and privileges]	

EXERCISE 6.

WHAT ARE THE CHALLENGES YOU ENCOUNTER WHILE WORKING WITH ACCESS CONTROL MODEL IN OPENMRS?

- Firstly, because this is a Role-based access control healthcare system so every privilege and role is define detailly which create an enormous list for user to working with. Therefore, this requires a certain amount of knowledge about role and privileges.
- Secondly, you can restrict access to certain actions in your system but not to certain data.
- Thirdly, it is hard to manage and maintain. Very often, administrators will keep adding roles to users but never remove them. You end up with users that dozens if not hundreds of roles and permissions.
- Fourthly, it relies on custom code within application layers (API, apps, DB...) to implement finer-grained controls.
- Finally, about the setting up, not all the configuration can fit the requirement of the application. That is to say there are about 20-30% of users cannot install the application to their devices and it is hard to find a page where guide to fix the configuration problem, mostly nowhere.

WHAT ARE YOUR SUGGESTIONS FOR IMPROVING THE ACCESS CONTROL MODEL OF OPENMRS?

- As mentioned in the previous challenge above, we have an enormous number of roles and privileges is assigned to a number of users. If we need to create a new role for a new type of user, we may assign the wrong privilege, causing overlapping privilege, leading to a security hole.
- Similarly, old users may change jobs or responsibilities, then their user level needs to be changed, otherwise, it will cause security problems. In general, it has a ton of roles and privileges, making it difficult to use, dependent on manual input and

monitoring, as well as the need for constant maintenance. It's one of the things that needs to be improved.