

# **SERVICENOW PROJECT SUBMISSION**

## **ACCESS CONTROL FOR PROJECT TABLE**

Submitted by

SJ.BENIL au723921104005

T.DHANUSH au723921104013

J.SANTHOSH au723921104044

V.SATHEESH KUMAR au723921104045

**Arjun College of Technology , Coimbatore**

**Anna University Chennai -600 025**

# ACCESS CONTROL FOR PROJECT TABLE

## **Project Overview :**

The goal of this project is to implement a robust access control system for a project table that stores sensitive information related to various projects. The system will ensure that only authorized users can access, modify, or delete project data based on their roles and permissions. This will enhance data security, streamline collaboration, and ensure compliance with organizational policies

## **Objective:**

Assign different levels of access to the project table based on user roles to ensure that users only perform actions that are appropriate for their role.

### **• Example Roles:**

- **Admin:** Full access to create, read, update, delete, and manage user permissions.
- **Project Manager:** Ability to create, update, delete, and assign projects, but no access to manage other users or roles.
- **Team Member:** Limited to reading and commenting on project data.
- **Guest:** View-only access to specific, public project data.

## 1. Implement Granular Permissions

- **Objective:** Fine-tune access to specific operations (e.g., create, read, update, delete) at the project table level based on user role.
- **Example:**
  - Ensure that users with the "Team Member" role can view project details but cannot update or delete project information.
  - Restrict the "Admin" role to only edit user roles and permissions, not project data unless necessary.

## 2. Minimize the Risk of Unauthorized Access

- **Objective:** Protect the project table from unauthorized access by enforcing strict authentication and authorization checks.
- **Example:**
  - Users should not be able to bypass authentication.
  - Implement strong password policies, multi-factor authentication (MFA), or other security mechanisms to prevent unauthorized users from accessing the system.

## 3. Ensure Data Integrity and Protection

- **Objective:** Ensure that users can only modify or delete project data when they are authorized to do so and that their actions are logged for accountability.
- **Example:**

- Project Managers should only be able to edit projects they are associated with or authorized to manage.
- Use validation checks to prevent unauthorized data manipulation.
- Log all access attempts, including changes to project data, for auditing purposes.

### **Access Levels:**

1. Project Manager (PM): Full access (create, read, update, delete)
2. Team Members: Read and update access (task assignments, status updates)
3. Stakeholders: Read-only access (project overview, progress)
4. External Partners: Limited read-only access (specific project details)

### **Access Control Rules:**

1. PM can create, update, and delete projects.
2. Team members can update task assignments and status.
3. Stakeholders can view project overview and progress.
4. External partners can view limited project details.

### **Key Features and concept used:**

1. Regularly review access permissions
2. Use strong passwords and encryption
3. Limit access to sensitive data
4. Monitor audit logs

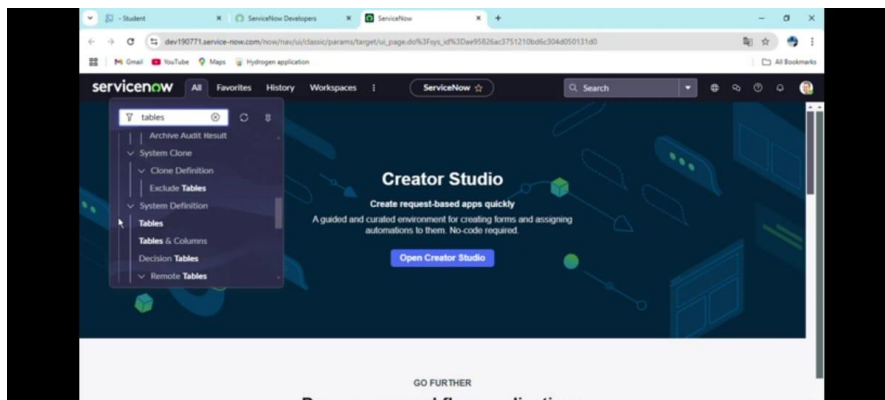
## Detailed Steps To Solution Design :

### Implementation :

**Step 1:** Sign up for a developer account on the ServiceNow Developer site

**Step 2:** Open Instance

**Step 3:** In All >> Tables



**Step 4:** Click >> New

Label	Name	Extends table	Extensible	Updated
Adaptive Authentication Event	adaptive_auth_event	(empty)	false	2024-07-27 14:38:14
Agent Assist Recommendation	agent_assist_recommendation	Application File	false	2024-07-27 14:40:10
Mid Server File	agent_file	(empty)	false	2024-07-27 14:20:54
Record Producer Configuration	alsa_rp_config	Application File	false	2024-07-27 14:44:59
Search Actions	alsa_sl_action	Application File	false	2024-07-27 14:44:58
AI Search ACL Overrides	als_acl_overrides	Application File	false	2024-07-27 13:59:03
AI Search Active Table Ingestion Tracker	als_active_table_ingestion_tracker	(empty)	false	2024-07-27 13:59:01
AI Search Async Genius Result	als_async_genius_result	(empty)	false	2024-07-27 13:59:06
AI Search Async Request	als_async_request	(empty)	false	2024-07-27 13:59:06
AI Search Child Table	als_child_table	Application File	false	2024-07-27 13:59:04
AI Search Configuration Attribute	als_configuration_attribute	(empty)	false	2024-07-27 13:59:00
AI Search Connection	als_connection	(empty)	false	2024-07-27 13:59:06
AI Search Country To Search Language	als_country_to_search_language	Application File	false	2024-07-27 13:59:06

## Step 5: Fill The Details And Click Submit

ServiceNow recommends creating custom tables in scoped applications. To learn more about creating scoped applications, click [here](#).

A table is a collection of records in the database. Each record corresponds to a row in a table, and each field on a record corresponds to a column on that table. Applications use tables and records to manage data and processes. [More info](#)

\* Label: Project  
\* Name: u\_project  
Extends table:

Application: Global  
Create module: ☒  
Create mobile module: ☒  
Add module to menu: Create new  
New menu name: Project

Columns: Controls: Application Access

Table Columns: for text

Dictionary Entries

## Step 6: In All >> Users

Name	Extends table	Extensible	Updated
adaptive_auth_event	(empty)	false	2024-07-27 14:38:14
agent_assist_recommendation	Application File	false	2024-07-27 14:40:10
agent_file	(empty)	false	2024-07-27 14:20:54
aiia_rp_config	Application File	false	2024-07-27 14:44:59
aiia_ui_action	Application File	false	2024-07-27 14:44:58
aiia_ui_overrides	Application File	false	2024-07-27 13:59:03
aiia_active_table_ingestion_tracker	(empty)	false	2024-07-27 13:59:01
aiia_async_pending_result	(empty)	false	2024-07-27 13:59:06
aiia_async_request	(empty)	false	2024-07-27 13:59:06
aiia_child_table	Application File	false	2024-07-27 13:59:04
aiia_configuration_attribute	(empty)	false	2024-07-27 13:59:00
aiia_connection	(empty)	false	2024-07-27 13:59:06
aiia_country_to_search_language	Application File	false	2024-07-27 13:59:06

## Step 7: Click >> New

Create Two Users Product Manager and Employee Management

User ID	Name	Email	Active	Created	Updated
abel.tuter	Abel Tuter	abel.tuter@example.com	true	2012-02-17 19:04:52	2024-11-13 19:37:58
abraham.lincoln	Abraham Lincoln	abraham.lincoln@example.com	true	2013-07-23 17:15:54	2024-11-13 19:38:00
adela.cervantz	Adela Cervantz	adela.cervantz@example.com	true	2012-02-17 19:04:50	2024-11-13 19:37:57
aleen.mottorn	Aleen Mottorn	aleen.mottorn@example.com	true	2012-02-17 19:04:49	2024-11-13 19:37:59
alejandra.prenatt	Alejandra Prenatt	alejandra.prenatt@example.com	true	2012-02-17 19:04:52	2024-11-13 19:37:57
alejandromascal	Alejandro Mascall	alejandromascal@example.com	true	2012-02-17 19:04:52	2024-11-13 19:38:00
alene.rabeck	Alene Rabeck	alene.rabeck@example.com	true	2012-02-17 19:04:53	2024-11-13 19:38:00
alfonso.grigien	Alfonso Grigien	alfonso.grigien@example.com	true	2012-02-17 19:04:51	2024-11-13 19:37:57
alissa.mountjoy	Alissa Mountjoy	alissa.mountjoy@example.com	true	2012-02-17 19:04:52	2024-11-13 19:37:59
alians.schwantz	Alian Schwantz	alians.schwantz@example.com	true	2012-02-17 19:04:53	2024-11-13 19:38:00
allie.pumphrey	Allie Pumphrey	allie.pumphrey@example.com	true	2012-02-17 19:04:52	2024-11-13 19:38:00
alysongillipie	Alyson Gillipie	alysongillipie@example.com	true	2012-02-17 19:04:50	2024-11-13 19:37:57
alva.pennington	Alva Pennington	alva.pennington@example.com	true	2012-02-17 19:04:50	2024-11-13 19:38:01

Step 8: Fill The Details And Click >> Submit

User ID: ProductManagement

First name: Product

Last name: Management

Title:

Department:

Calendar integration: Outlook

Time zone: System (America/Los\_Angeles)

Date format: System (yyyy-MM-dd)

Business phone:

Mobile phone:

Photo: Click to add...

Active: ☒

Submit

User ID: EmployeeManagement

First name: Employee

Last name: Management

Title:

Department:

Calendar integration: Outlook

Time zone: System (America/Los\_Angeles)

Date format: System (yyyy-MM-dd)

Business phone:

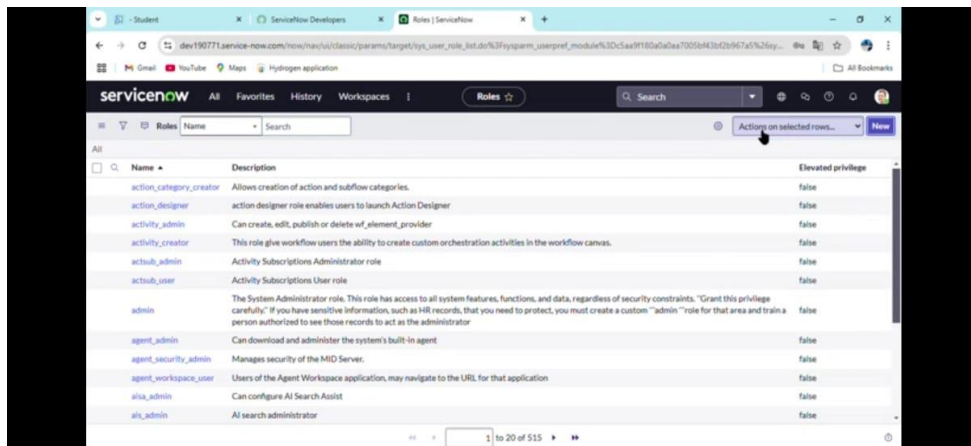
Mobile phone:

Photo: Click to add...

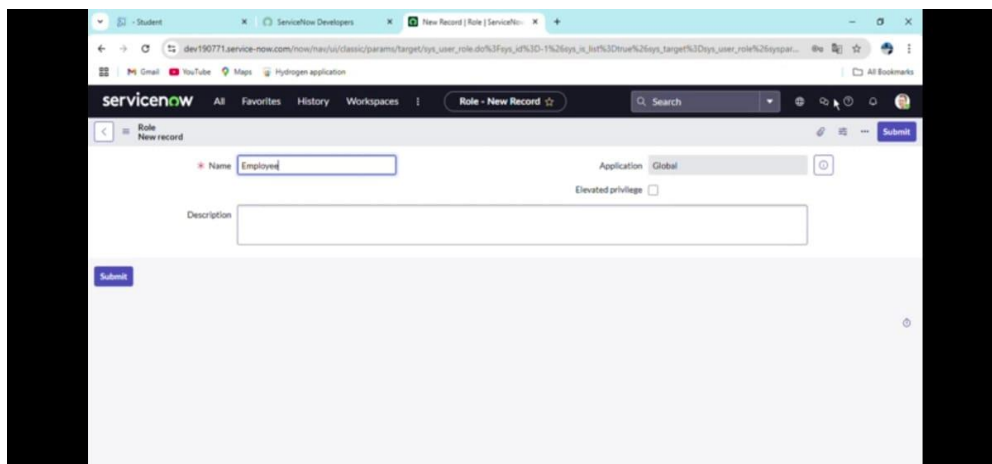
Active: ☒

Submit

Step 9: Open Role >> New

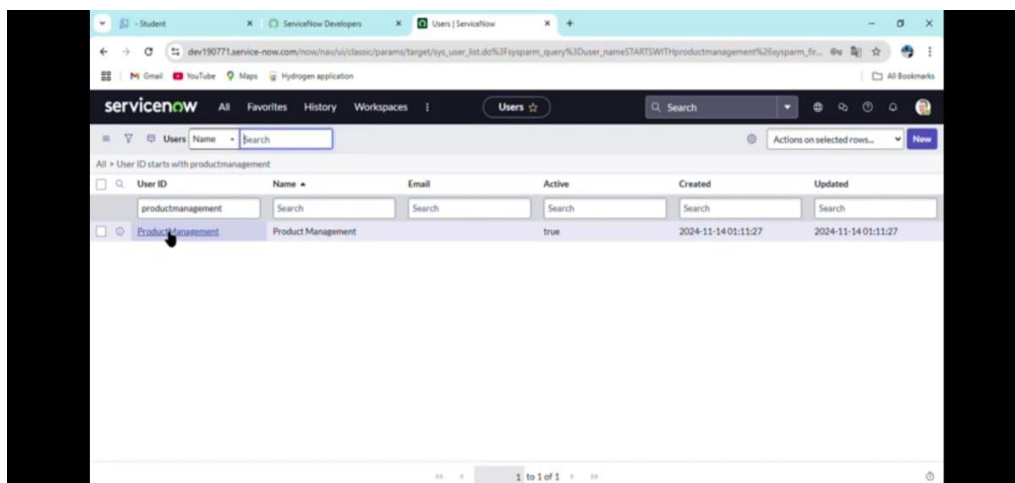


## Step 10: Create Employee Role

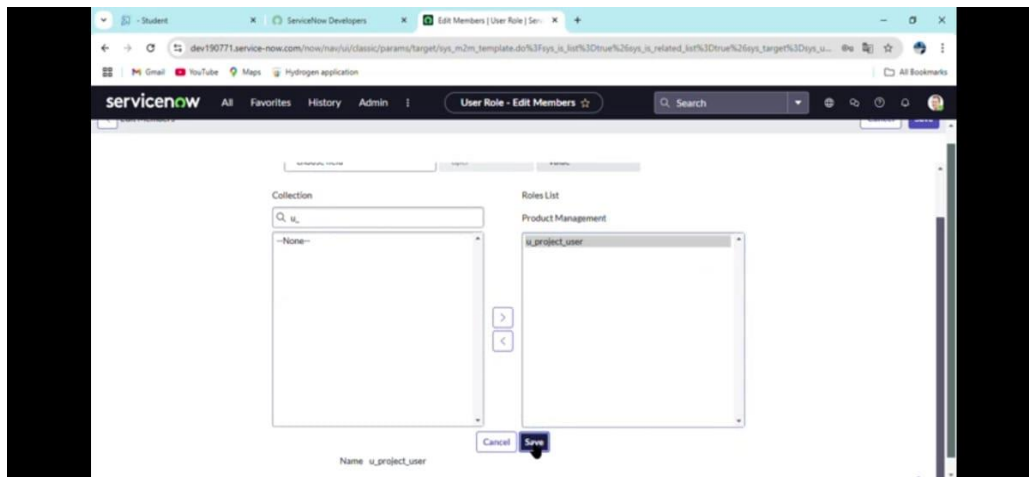


## Step 11: In All >> Users >> Search Product Management

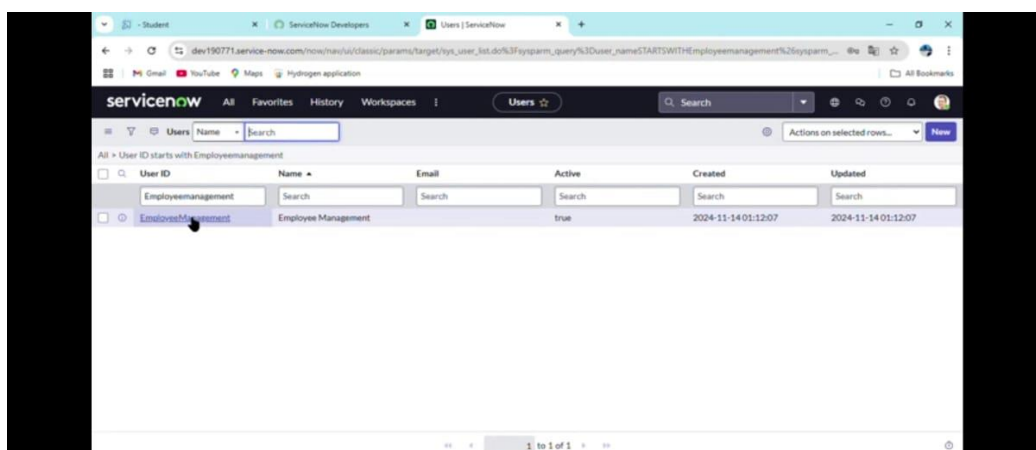
And add Role to it



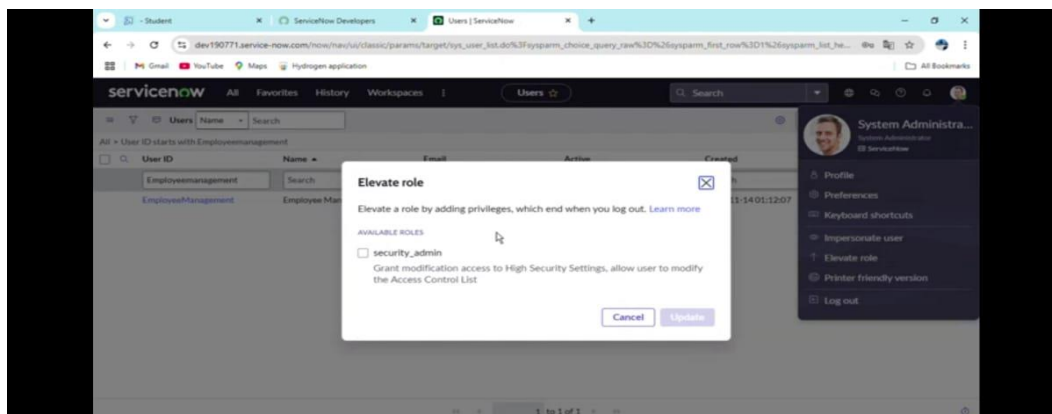




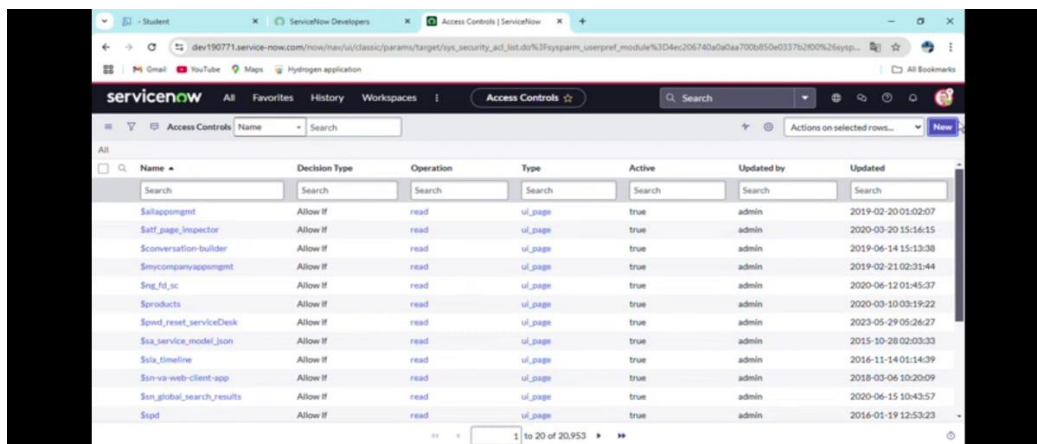
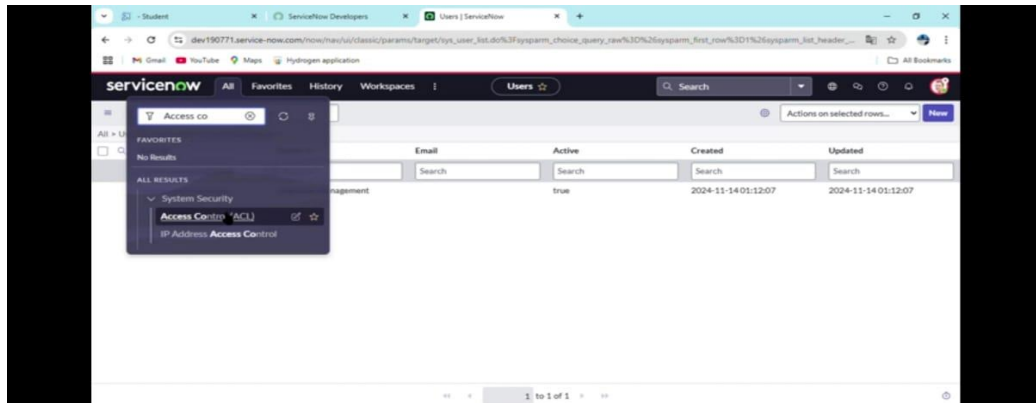
**Step 12:** In All >> Users >> Search Employee Management  
And add Role to it



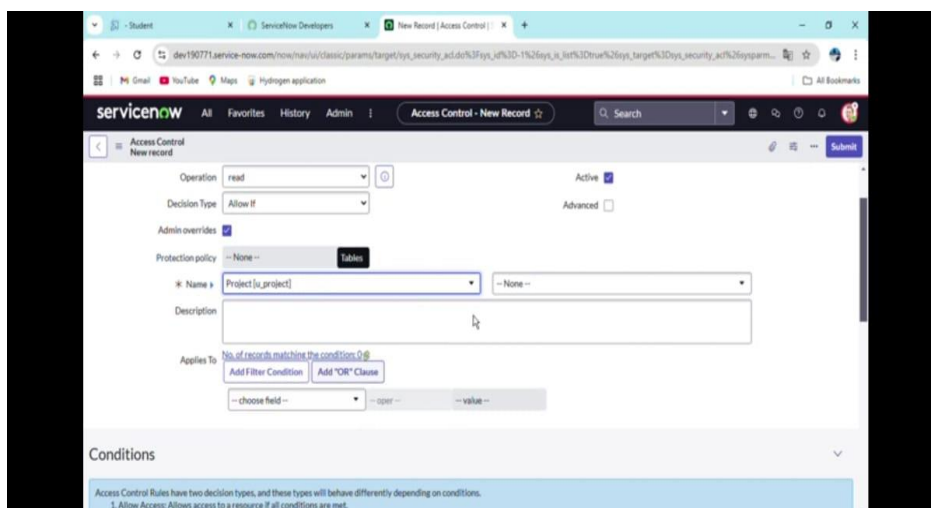
**Step 13:** Click on the Profile avatar >> Elevate Role  
>> Grant the high security

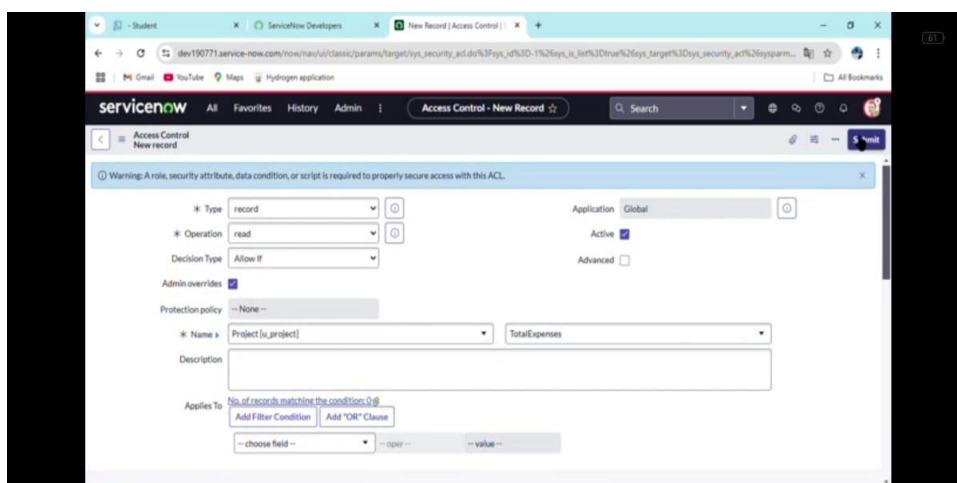
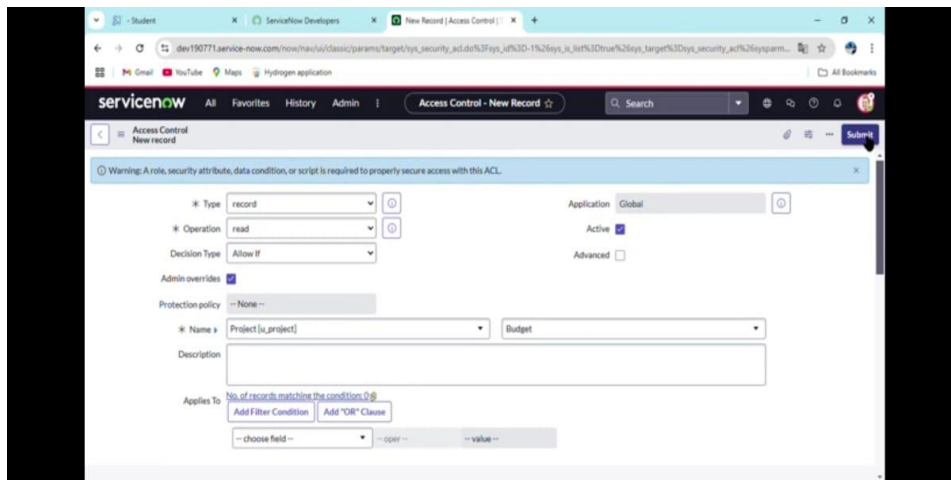


## Step 14: In All>> Search & Open ACL >> New

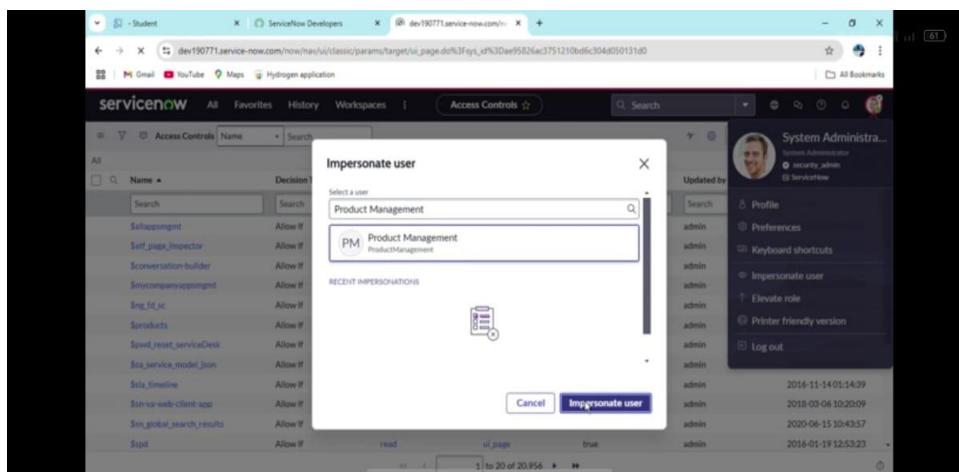


## Step 15: Fill the details below and Create Read Operation Table Level ACL(none) on Employee role >> Save

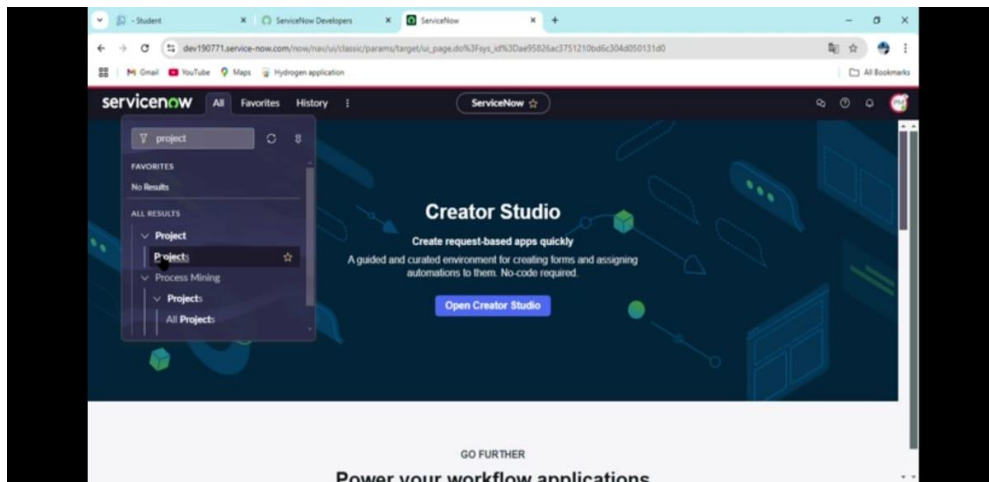




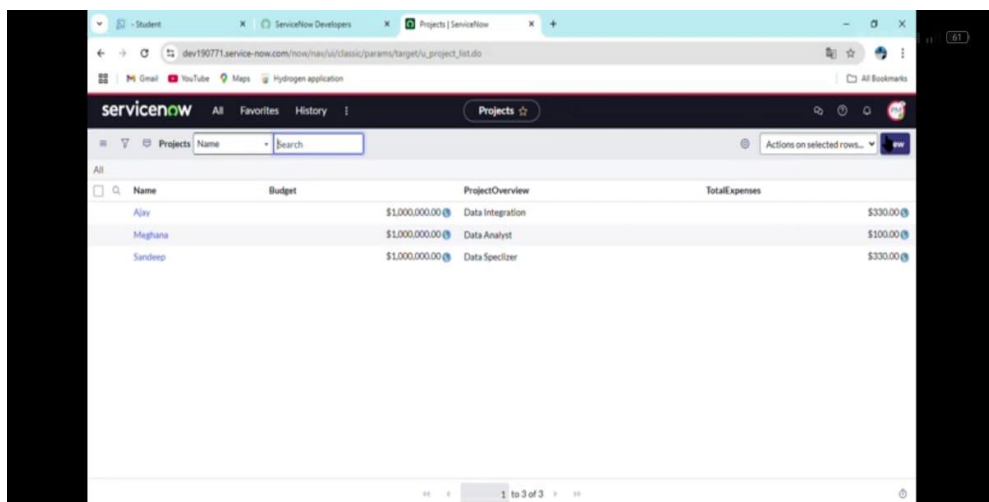
## Step 16: Impersonate User >> Product Management



## Step 17: All>>Project>>New



**Step 18:** Create 3 Records with any details



## **Testing and Validation:**

### **Test User Authentication**

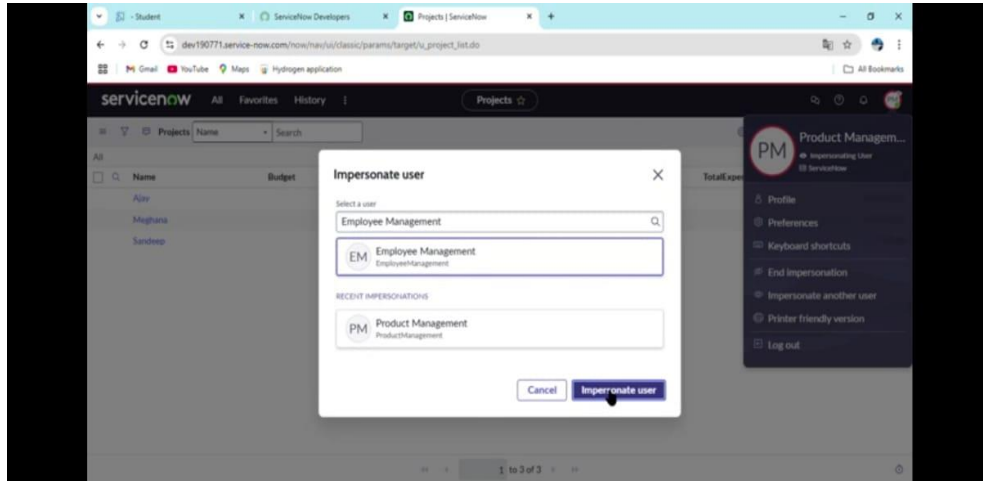
- Ensure that users can only access the project table after successful authentication (e.g., login with username and password).
- Test invalid login attempts and ensure that users cannot access the table without proper credentials.
- Verify session expiration behavior (if applicable).

### **Validation:**

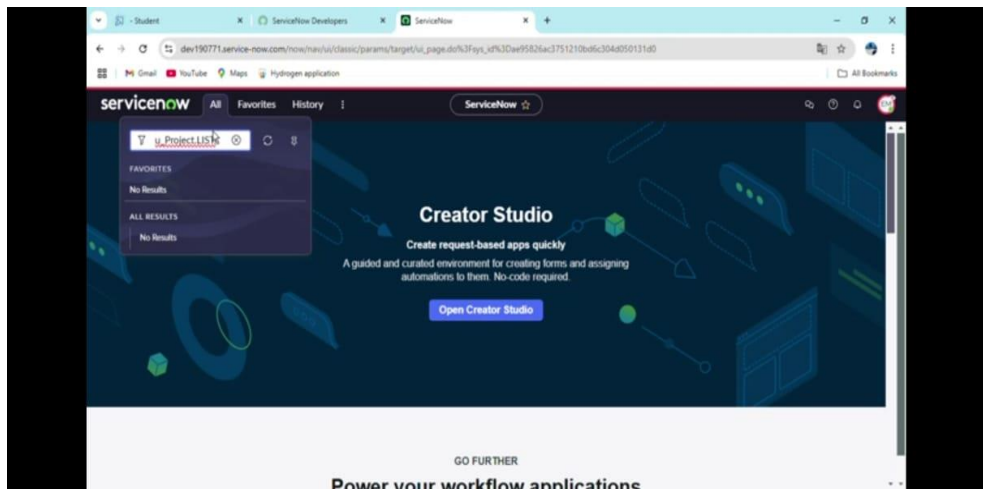
When testing and validating access control for a project table, the goal is to ensure that only authorized users can access, modify, or manage the project table data according to defined roles and permissions. Proper access control testing helps protect sensitive data and ensures that users' actions are consistent with their designated permissions.

## Result:

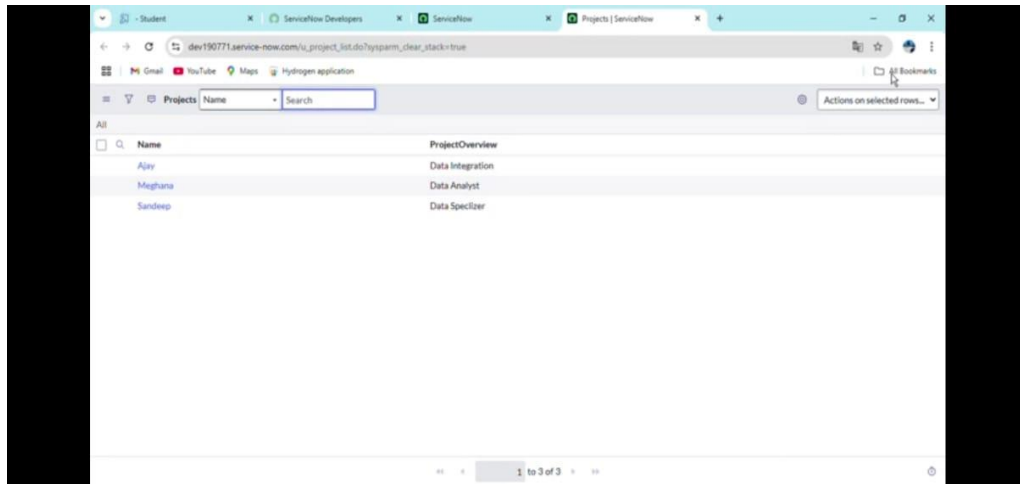
### Step 1: Impersonate User >> Employee Management



### Step 2: All >> u\_project.LIST

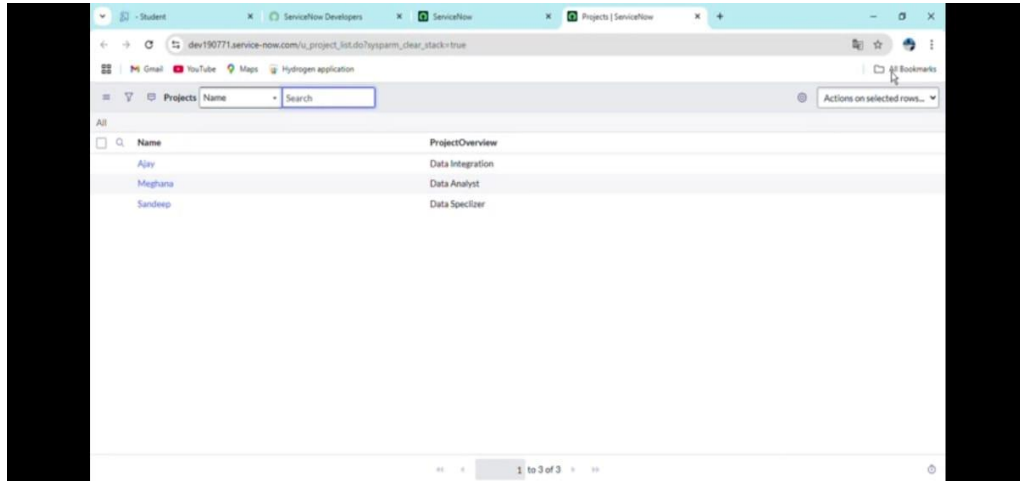


## Step 3:



In the figure above, we can ensure that some fields(Budget,Total Expenses) visibility is restricted for employees on the Project table

## OUTPUT:



The screenshot displays a web browser window with multiple tabs. The active tab is titled 'Projects | ServiceNow'. The address bar shows the URL 'dev190771.service-now.com/ui\_project\_list.do?sysparm\_clear\_stack=true'. Below the browser window, a table is visible with the following structure:

Name	ProjectOverview
Ajay	Data Integration
Meghana	Data Analyst
Sandeep	Data Specifier

The table is part of a larger application interface. At the top, there is a search bar with the placeholder text 'Name' and a 'Search' button. To the right of the search bar, there is a dropdown menu labeled 'Actions on selected rows...'. At the bottom of the table, there is a pagination bar showing '1 to 3 of 3'.

**Conclusion:** Implementing access control for a project table ensures the security, integrity, and confidentiality of project data. By assigning roles and permissions, project managers Thus The Project “Access control for project Table” has been implemented successfully