

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 :

Ensure authorized personnel have access to project information while maintaining confidentiality, integrity, and security.

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.

Best Practices:

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

4. Monitor audit logs

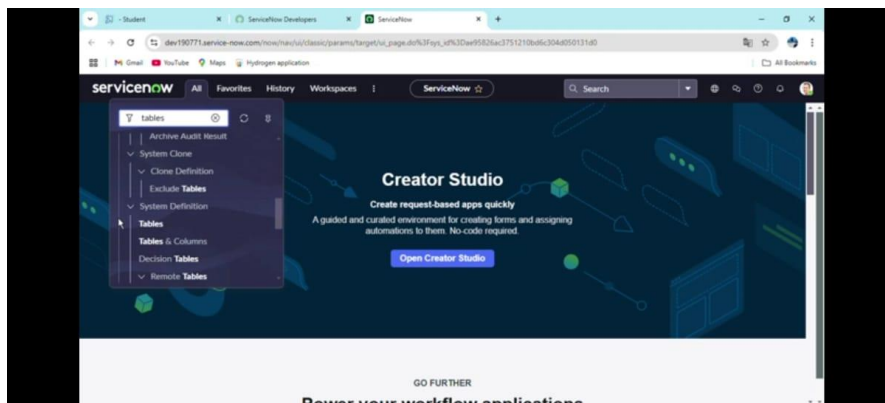
Detailed Steps To Solution Design :

Implementation :

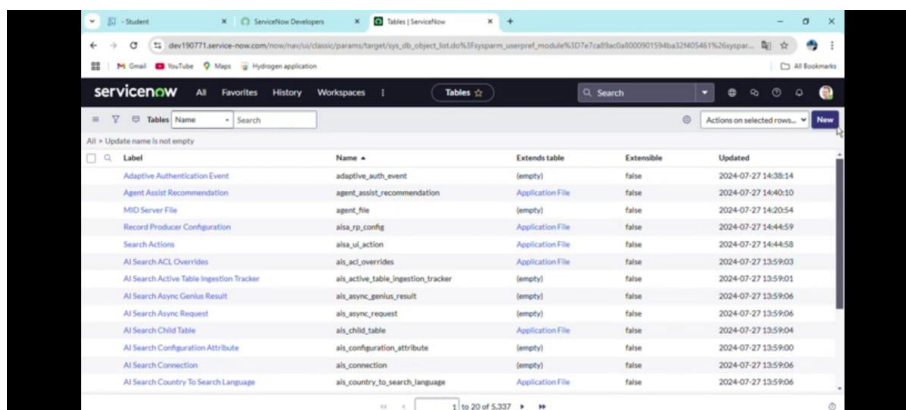
Step 1: Sign up for a developer account on the ServiceNow Developer site

Step 2: Open Instance

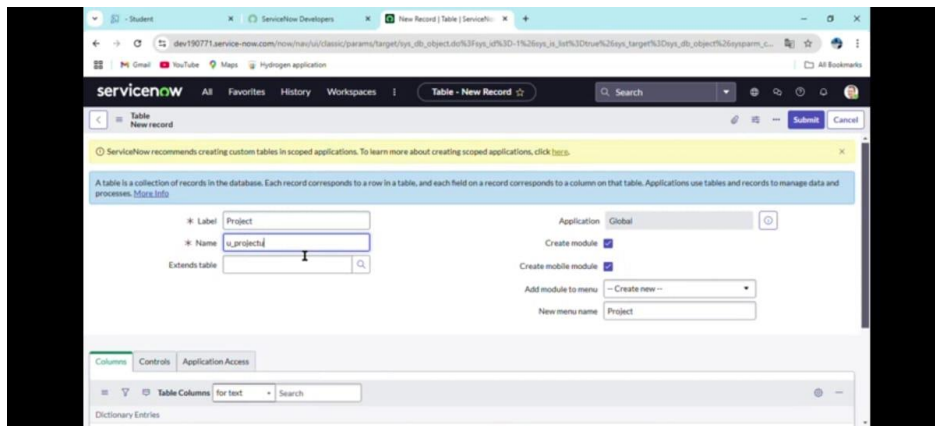
Step 3: In All >> Tables



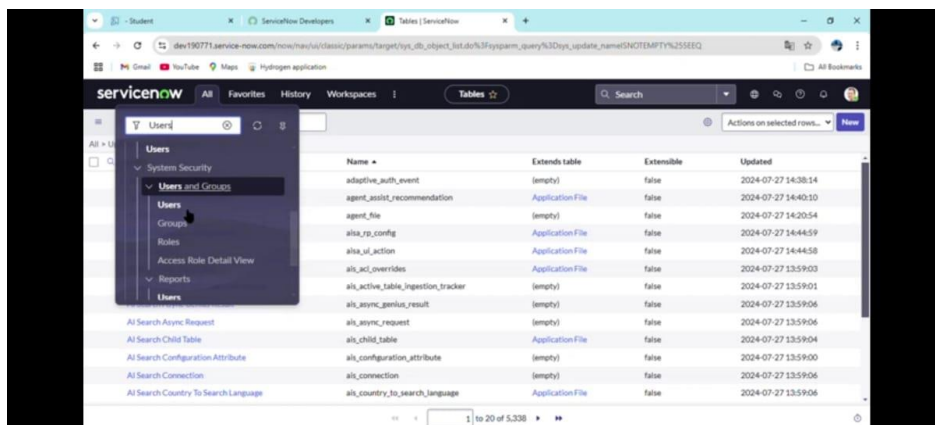
Step 4: Click >> New



Step 5: Fill The Details And Click Submit

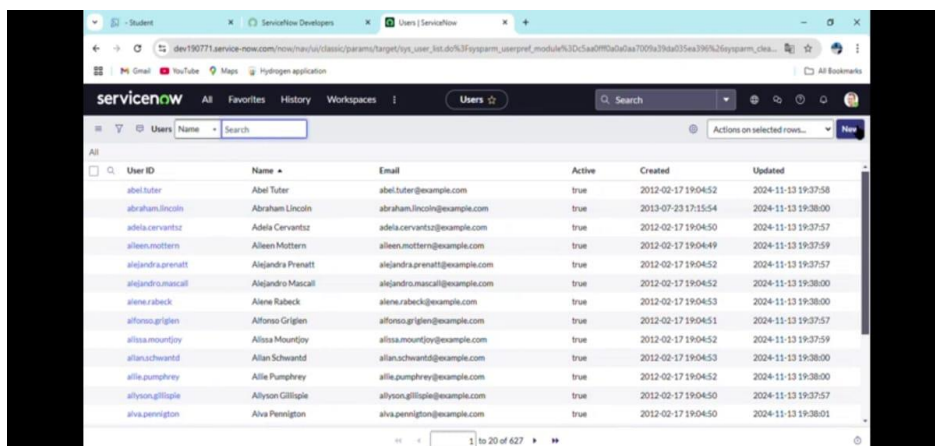


Step 6: In All >> Users

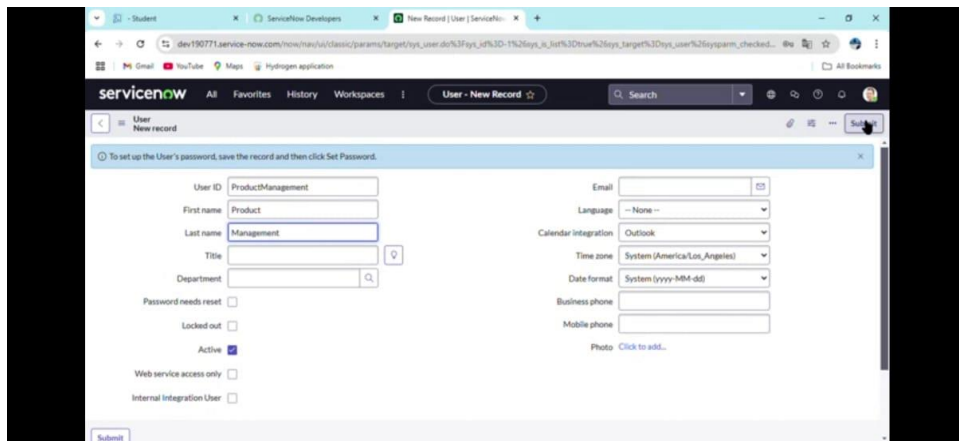


Step 7: Click >> New

Create Two Users Product Manager and Employee Management

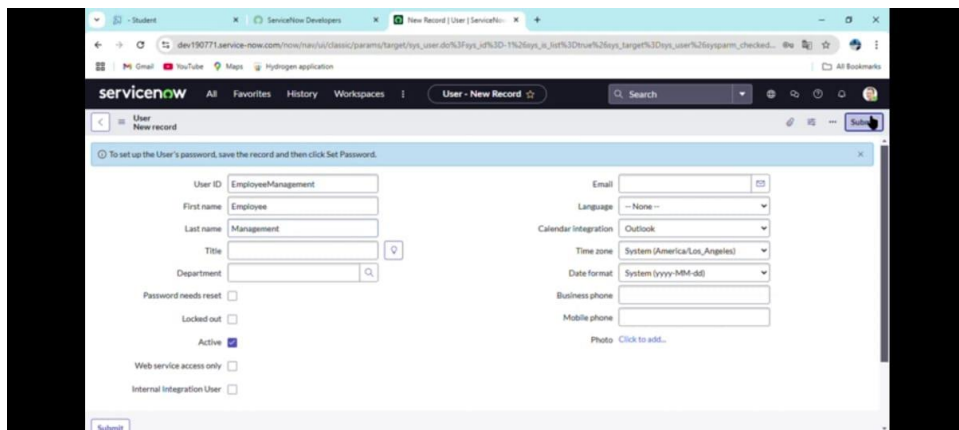


Step 8: Fill The Details And Click >> Submit



ServiceNow User - New Record form. The form is titled "User - New Record" and includes a "Submit" button. The form fields are:

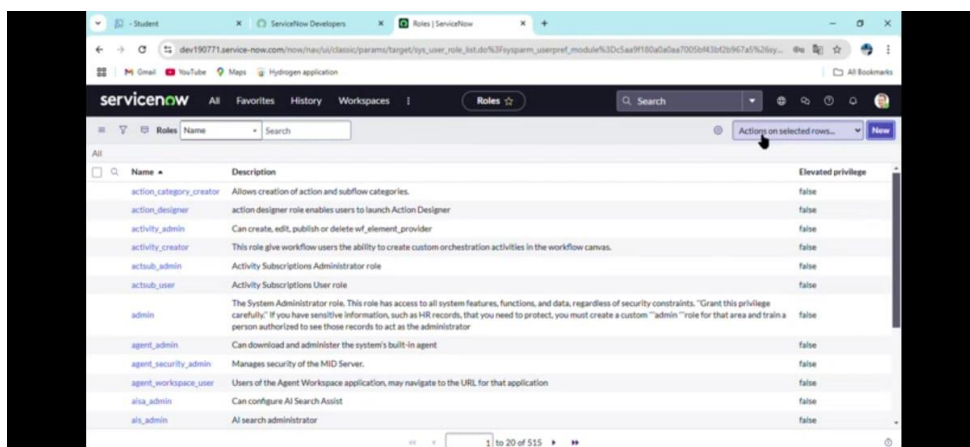
- User ID: ProductManagement
- First name: Product
- Last name: Management
- Title: (empty)
- Department: (empty)
- Password needs reset: ☐
- Locked out: ☐
- Active: ☒
- Web service access only: ☐
- Internal Integration User: ☐
- Email: (empty)
- Language: None
- Calendar integration: Outlook
- Time zone: System (America/Los Angeles)
- Date format: System (yyyy-MM-dd)
- Business phone: (empty)
- Mobile phone: (empty)
- Photo: Click to add...



ServiceNow User - New Record form. The form is titled "User - New Record" and includes a "Submit" button. The form fields are:

- User ID: EmployeeManagement
- First name: Employee
- Last name: Management
- Title: (empty)
- Department: (empty)
- Password needs reset: ☐
- Locked out: ☐
- Active: ☒
- Web service access only: ☐
- Internal Integration User: ☐
- Email: (empty)
- Language: None
- Calendar integration: Outlook
- Time zone: System (America/Los Angeles)
- Date format: System (yyyy-MM-dd)
- Business phone: (empty)
- Mobile phone: (empty)
- Photo: Click to add...

Step 9: Open Role >> New



ServiceNow Roles page. The page shows a list of roles with columns for Name, Description, and Elevated privilege. The 'New' button is highlighted in the top right corner.

Name	Description	Elevated privilege
action_category_creator	Allows creation of action and subflow categories.	false
action_designer	action designer role enables users to launch Action Designer	false
activity_admin	Can create, edit, publish or delete wf_element_provider	false
activity_creator	This role give workflow users the ability to create custom orchestration activities in the workflow canvas.	false
actsub_admin	Activity Subscriptions Administrator role	false
actsub_user	Activity Subscriptions User role	false
admin	The System Administrator role. This role has access to all system features, functions, and data, regardless of security constraints. "Grant this privilege carefully" if you have sensitive information, such as HR records, that you need to protect, you must create a custom "admin" role for that area and train a person authorized to see those records to act as the administrator	false
agent_admin	Can download and administer the system's built-in agent	false
agent_security_admin	Manages security of the MID Server.	false
agent_workspace_user	Users of the Agent Workspace application, may navigate to the URL, for that application	false
aisa_admin	Can configure AI Search Assist	false
ais_admin	AI search administrator	false

Step 10: Create Employee Role

Role - New Record

Name:

Application:

Elevated privilege: ☐

Description:

Submit

Step 11: In All >> Users >> Search Product Management And add Role to it

Users

Search:

User ID	Name	Email	Active	Created	Updated
productmanagement	Product Management		true	2024-11-14 01:11:27	2024-11-14 01:11:27

User Role - Edit Members

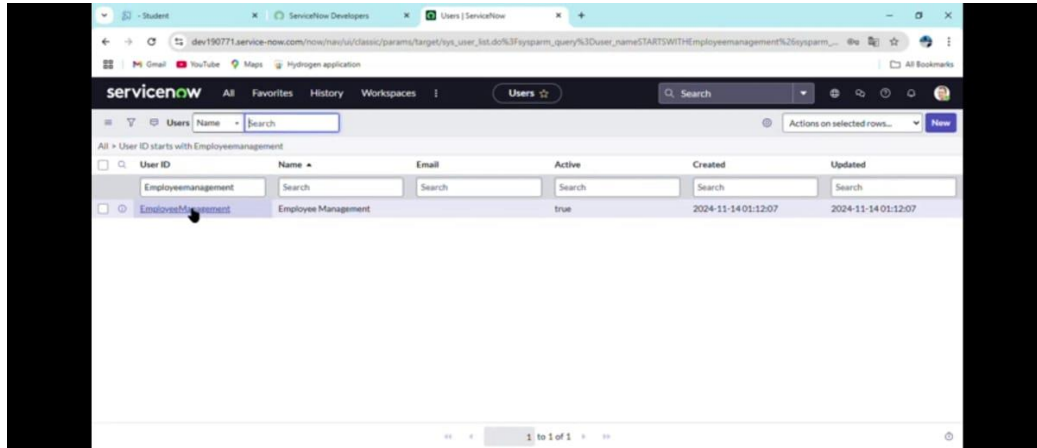
Collection:

Roles List: Product Management

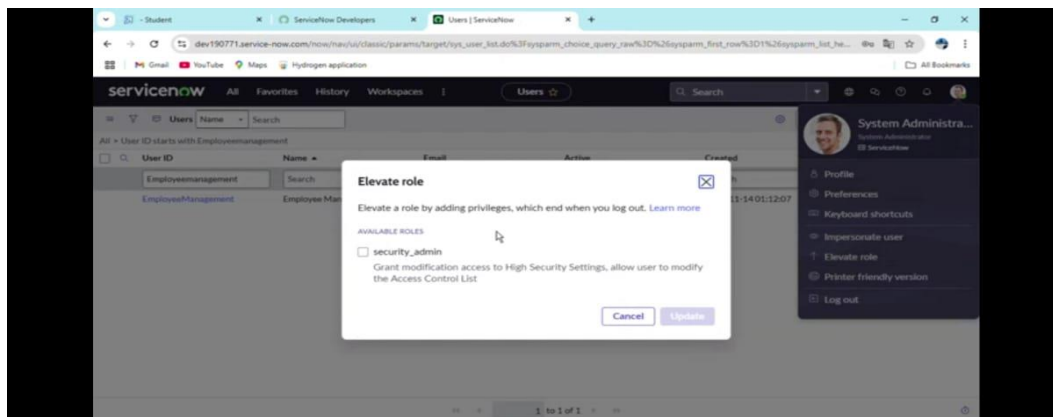
Cancel Save

Name: u_project_user

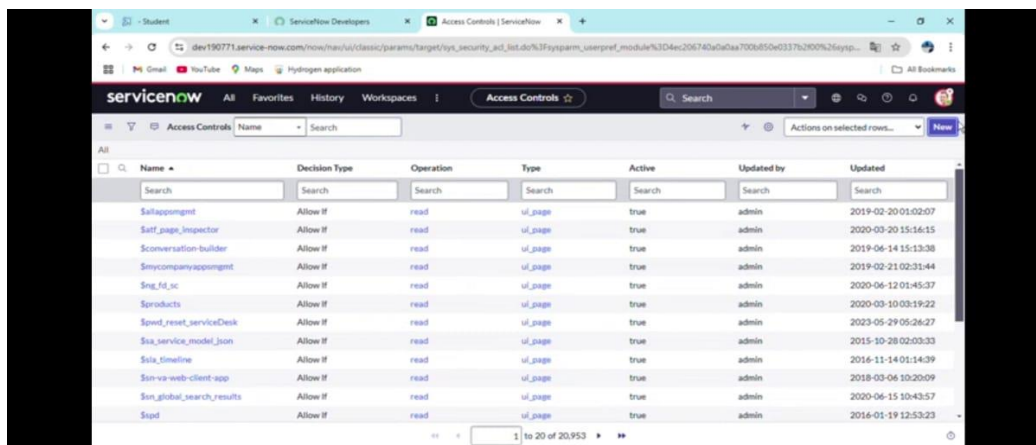
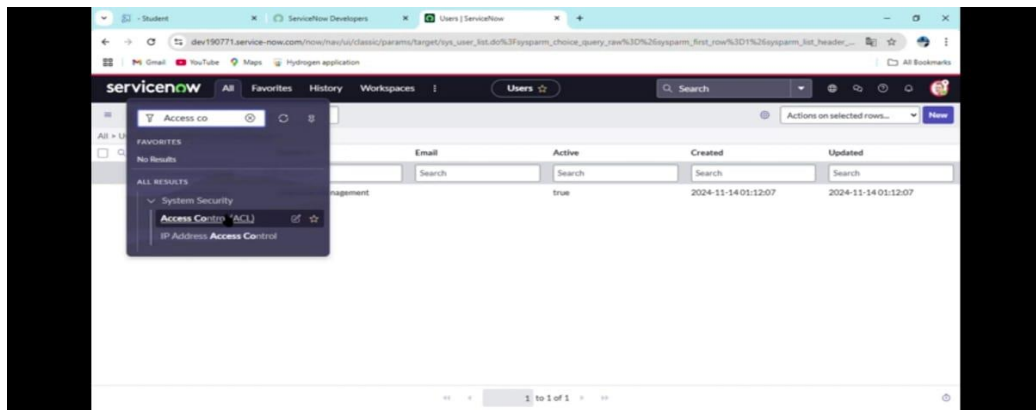
Step 12: In All >> Users >> Search Employee Management
And add Role to it



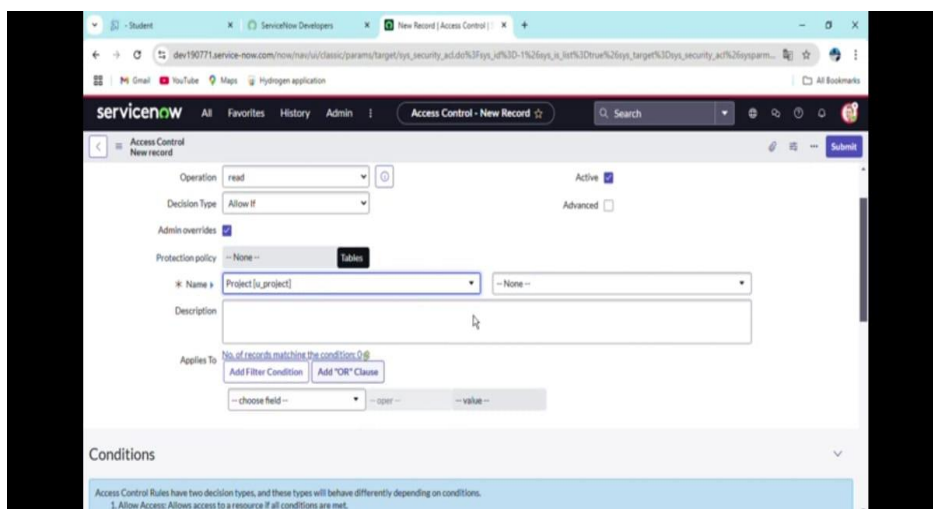
Step 13: Click on the Profile avatar >> Elevate Role
>> Grant the high security

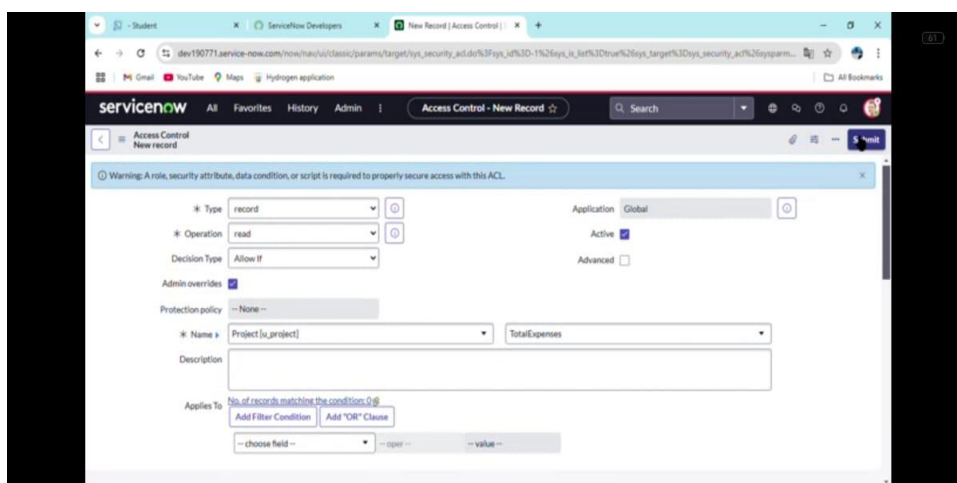
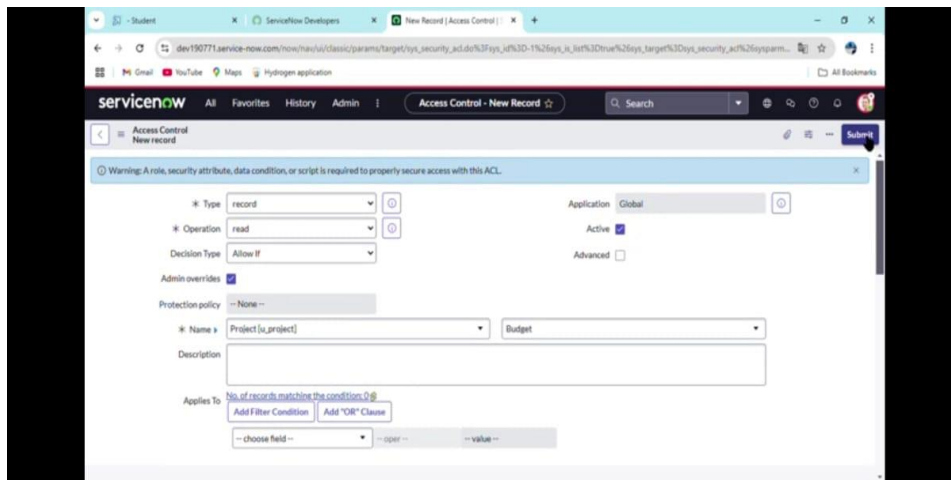


Step 14: In All >> Search & Open ACL >> New

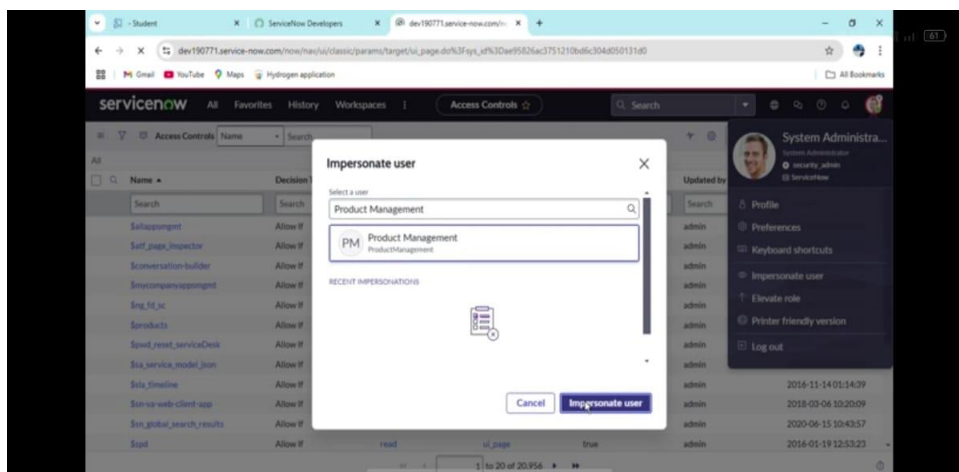


Step 15: Fill the details below and Create Read Operation Table Level ACL(none) on Employee role >> Save

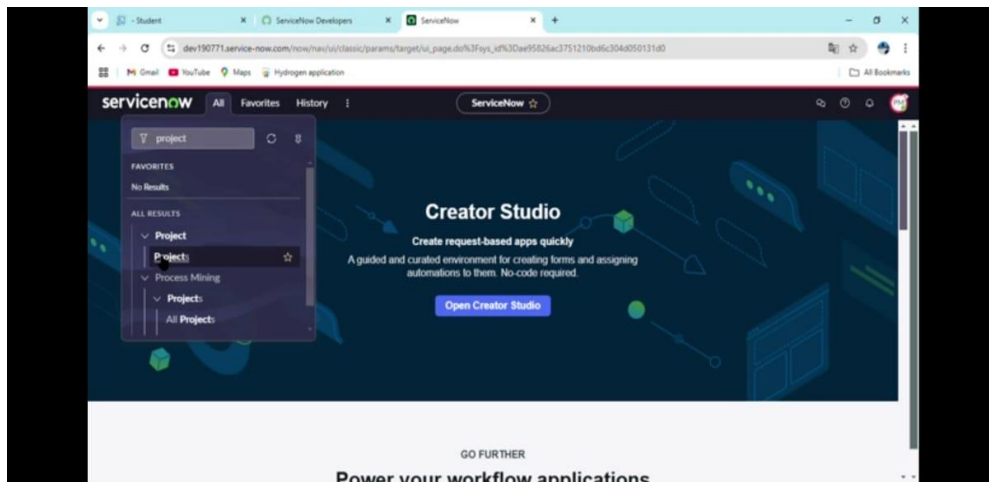




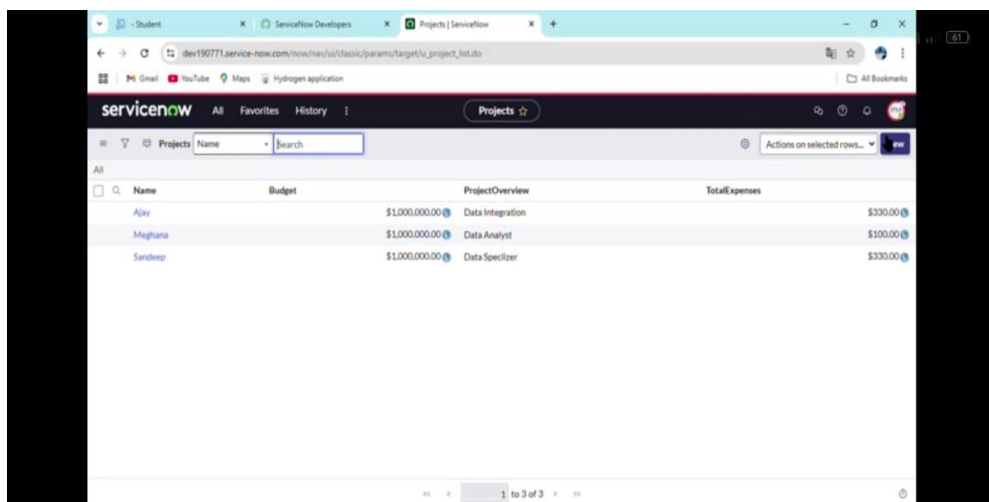
Step 16: Impersonate User >> Product Management



Step 17: All>>Project>>New

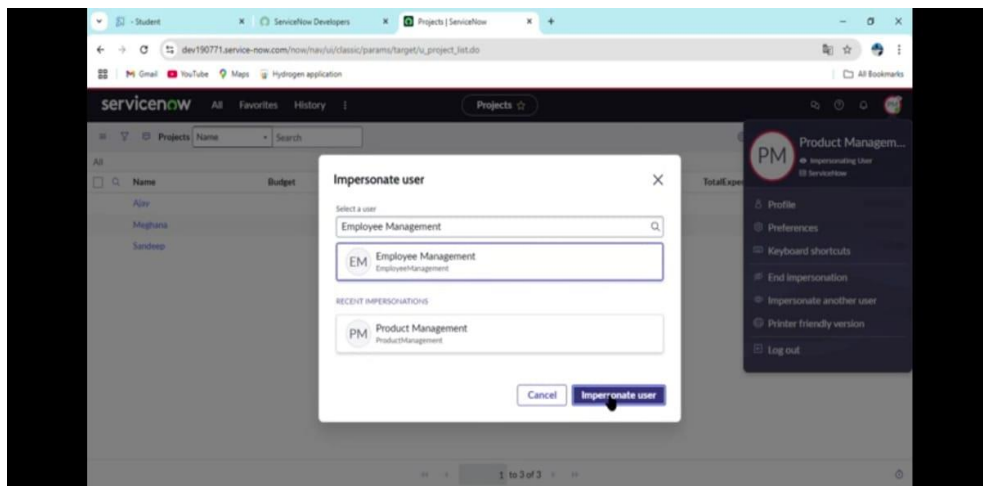


Step 18: Create 3 Records with any details

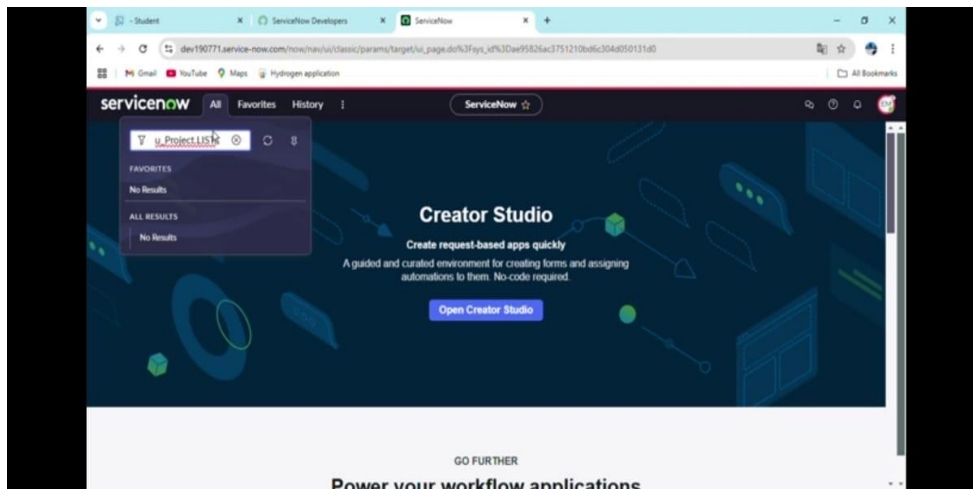


Result:

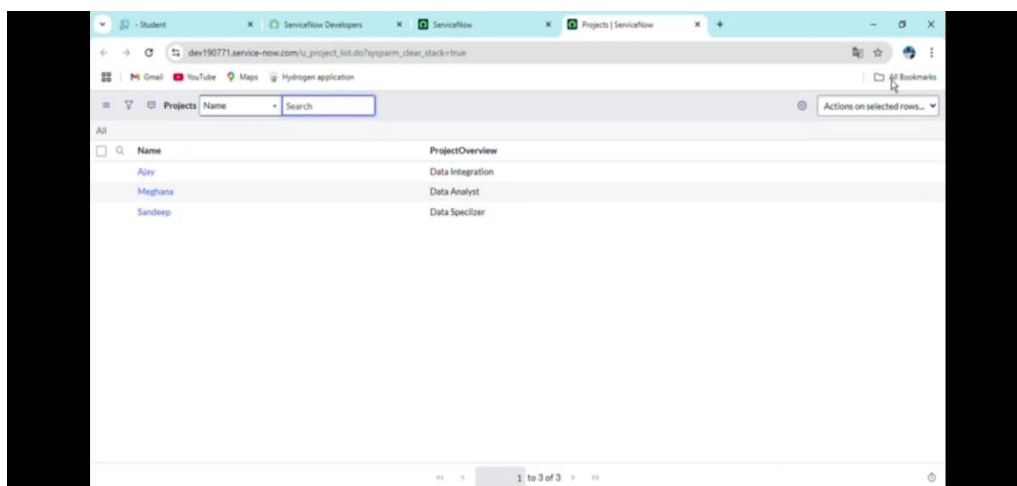
Step 1: Impersonate User >> Employee Management



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

Conclusion:Thus The Project “Access control for project Table has been implemented successfully