Bug Report

Title:
Unauthorized Access to Student CGPA Graphs via Direct URL Manipulation

Reported On:
29-April-2025

Environment:

- URL: https://cms.must.edu.pk:8082/Chartlet/MUSTFA21-BIT-064AJK/FanG_Chartlet_Chartlet3.Jpeg?133903561480798606
- Browser: All modern browsers (Chrome, Firefox, Edge tested)

Severity:
Medium (Information Disclosure)

Priority:
High (Needs Fix)

Description:
The CMS portal at MUST University exposes student CGPA graphs through a predictable URL pattern. By manually changing the **Roll Number** in the URL (e.g., modifying `FA21-BIT-064` to `FA21-BIT-063`), anyone can access other students' academic performance graphs without authentication or authorization.
Although it does not allow full profile access, this information leakage violates student data privacy policies.

Steps to Reproduce:

1. Open the following URL:
   `https://cms.must.edu.pk:8082/Chartlet/MUSTFA21-BIT-064AJK/FanG_Chartlet_Chartlet3.Jpeg?133903561480798606`
2. Change the roll number in the URL manually (e.g., `FA21-BIT-063`, `FA21-BIT-062`, etc.).
3. Hit Enter.
4. Observe that CGPA graphs of other students load without any authentication.

Expected Behavior:
Access to student CGPA graphs should be restricted. Users should only be able to see their own graphs after successful authentication.

Actual Behavior:
Student CGPA graphs are accessible publicly by simply modifying the roll number in the URL.

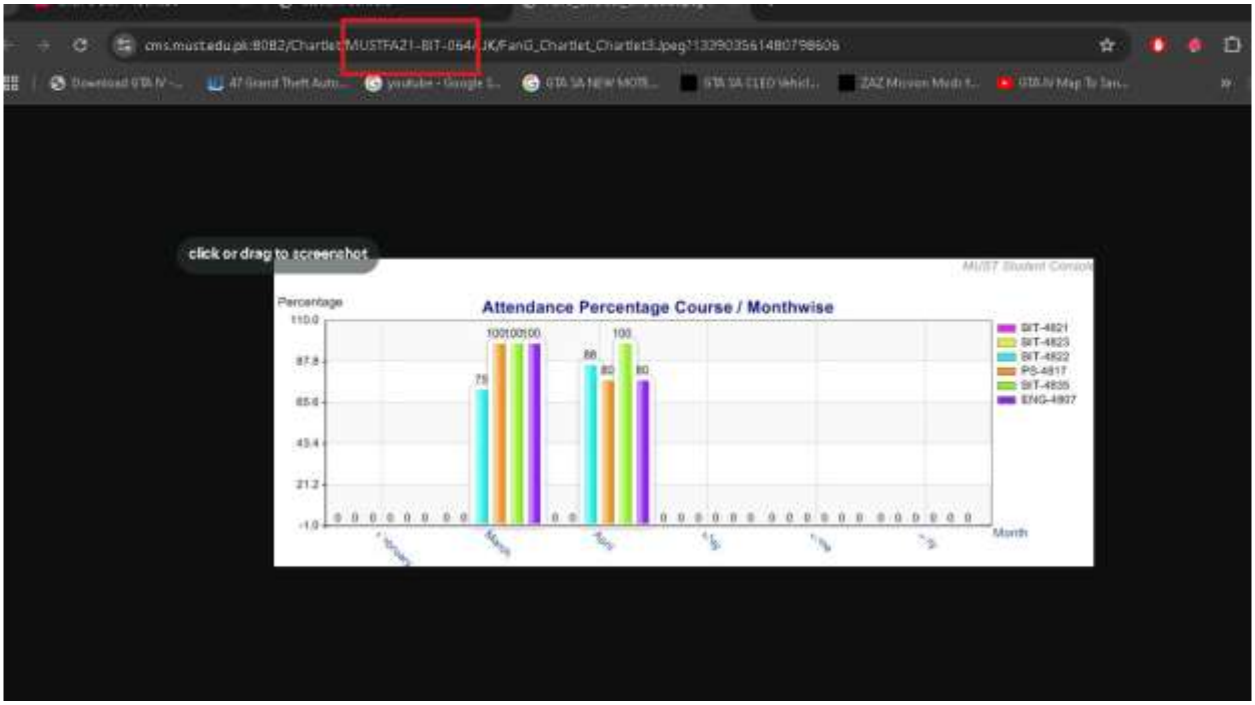
Impact:

- Student privacy violation
- Potential misuse of academic records
- Data Protection non-compliance risk

Recommended Fix:

- Implement authorization checks before serving the chart image.
- Serve dynamic charts after validating logged-in user identity, rather than exposing static images via direct URLs.
- Expire direct links after short time intervals (using tokens).

Attachments:



cms.must.edu.pk:8082/Chartlet/MUSTFA21-BIT-0644JK/FanG_Chartlet_Chartlet3.jpeg?133903561480798606