**Title:** Broken Access Control - Lecture Slide PDF Access
**Reported by:** Ali Shaker Alawami, Bakr Abdulaziz Alrayes
**Course:** Cybersecurity stream
**Instructor / Contact:** Atharva Bhamburkar
**Date discovered:** [2025-10-12]
**Date reported:** [2025-10-15]

Executive summary:

While preparing for our assessment 2 on October 12th, we were reviewing the lecture slides on the academy portal and found that the slides were embedded as images into the page. The slides page also blocked inspection of the page and any interaction other than scrolling up and down or zooming in and out. The page also blocked attempts at printing the page to have the slides as a file indicating that students are not meant to be able to download the slides onto their devices. By using cmd+options+I we were able to bypass the right click restriction on the page and inspect the page. Further investigation of the network calls revealed a direct reference URL to the lecture slides PDF file used to generate those slide images on the page allowing us to view and download the slides as a PDF. The issue indicates insufficient access control or file protection on backend document endpoints, exposing internal course materials that should only be accessible through authorized and contextual UI routes.

**Vulnerability classification / definition:**

**Name:** Broken Access Control — Insecure Direct Object Reference (IDOR) / Missing server-side authorization

**Definition:** Broken access control occurs when an application does not correctly enforce who is allowed to access a resource. This can allow an authenticated or unauthenticated user to access objects (files, records, pages) they should not be able to. A common variant is IDOR: the application references objects by a predictable identifier (for example a sequential numeric ID) and fails to check whether the requesting user is authorized for that specific ID.

**Risk:** Allows unauthorized viewing or downloading of lecture slides. This could undermine copyright and allow the leak of material.

**Affected URLs / resources**

This is not a comprehensive list as its possible with almost all lecture slides pages a student has access to.

- https://[redacted]/api/v1/userData/contents/20251003/1759468944532_Week_2-_Network_Security_&_Traffic_Analysis.pdf

- https://[redacted]/api/v1/userData/contents/20251003/1759469244778_Week-3_Cloud_Security-Securing_the_Cloud.pdf

**Affected systems / components**

- Frontend course content page: Lecture slide viewer and related embedded image logic.
- Backend document storage / file delivery endpoints: The server-side component that returns the PDF or source file for slides.
- Access control layer: Missing authorization checks on document requests.

**How issue was observed:**

1- While studying for Assessment 2 on October 12th, the lecture slides were accessed through the academy portal as part of course preparation.

2- Upon inspecting the course content page, it was noted that the slides appeared as embedded images rather than an interactive file.

3- Using browser developer tools (Network tab), the slide image requests were traced to a single document source.

4- The network inspection revealed a direct link to a PDF file containing all lecture slides.

5- Opening the file's direct URL in a new browser tab allowed full download and offline access to the lecture material outside the portal interface.

**How to reproduce the issue:**

1- Go to a given slide page such as https://[redacted]/course/content-view/47

2- Press on Command+Options+I on Mac (Control+Shift+I on Windows)

3- Go to the Network Tab and refresh the page

4- Click on the element that starts with an ID as shown in Figure 1, then copy the URL

5- Paste the URL in a new tab while logged in

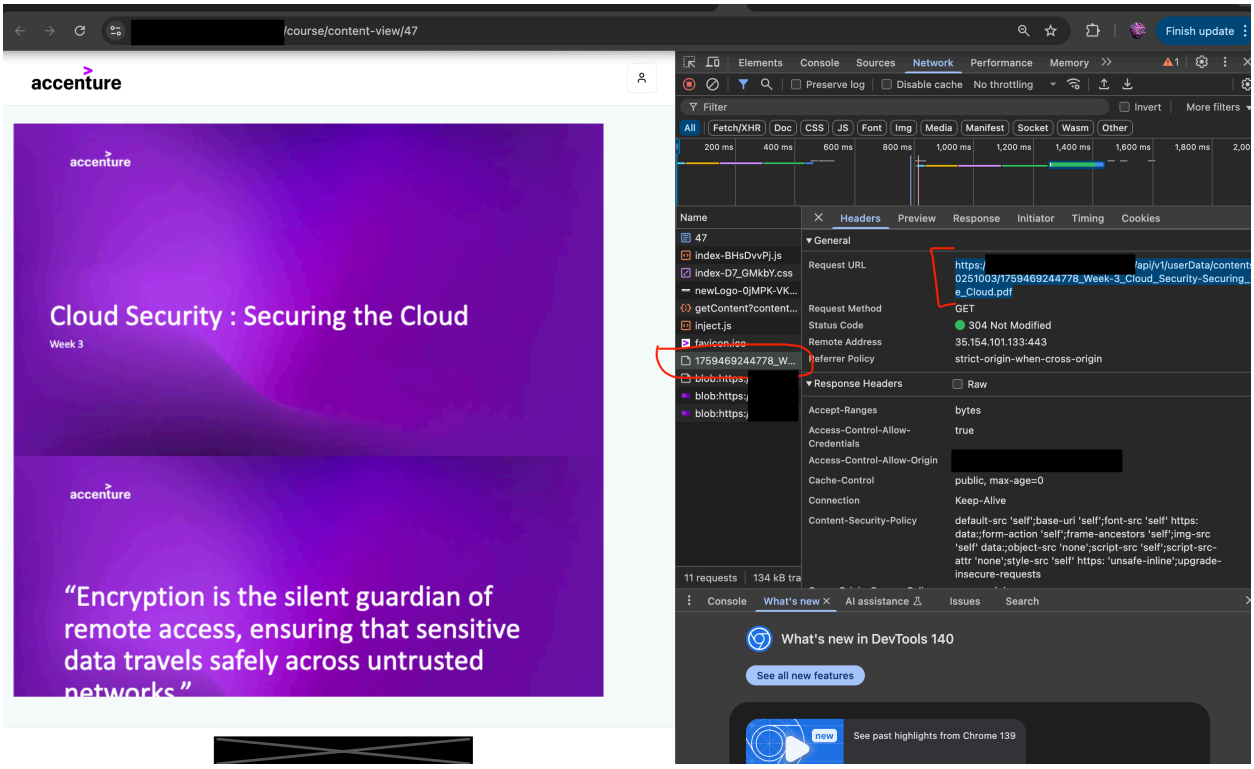
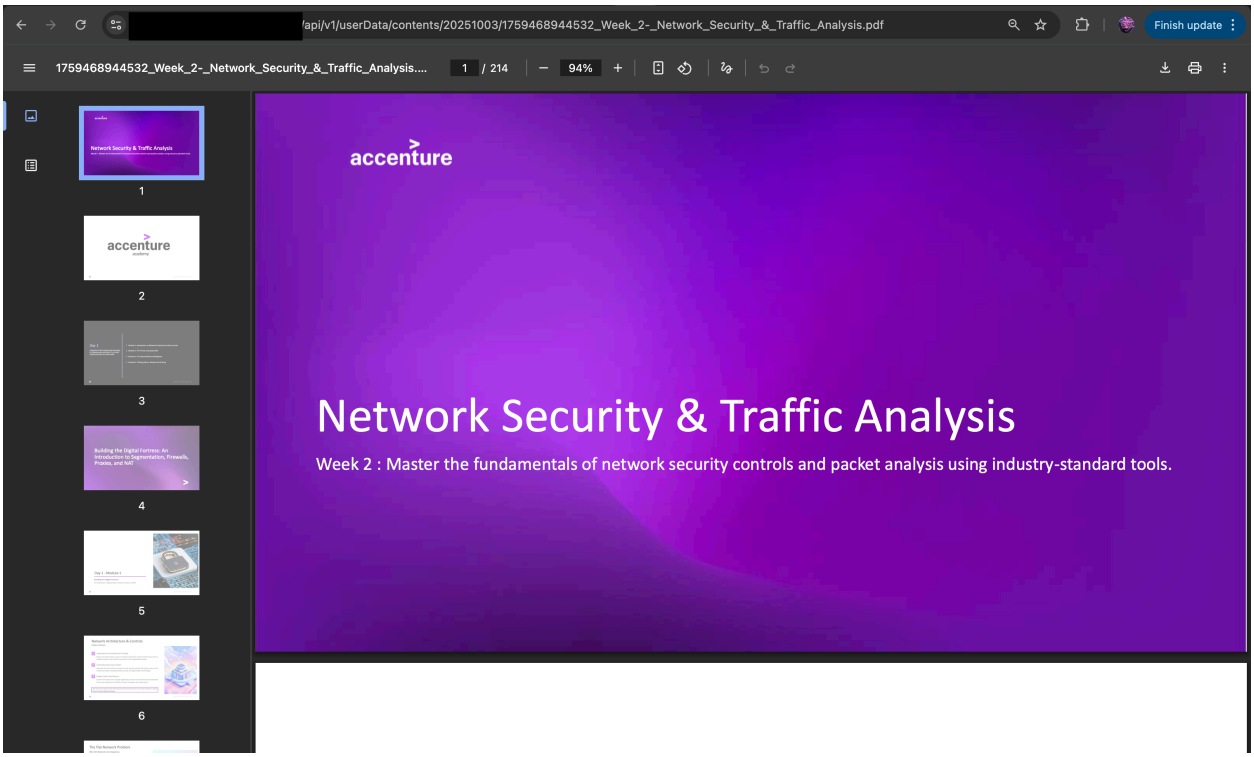



Figure 1

## Evidence:




**Mitigation and Recommendations:**

To mitigate the Broken Access Control vulnerabilities identified we recommend the following:

- Implement strict server-side authorization checks to ensure that only enrolled and authenticated users can access document files.
- Prevent direct linking to file URLs by using secure, time-limited download tokens or indirect resource identifiers.
- Store lecture materials in a secured file repository that validates user permissions for every request.
- Regularly audit and log all document access attempts to identify unauthorized downloads or link sharing.