Title: Broken Access Control / Insecure Direct Object Reference (IDOR) — Accenture Academy
Reported by: Ali Shaker Alawami, Bakr Abdulaziz Alrayes
Course: Cybersecurity stream
Instructor / Contact: Atharva Bhamburkar
Date discovered: [2025-10-07]
Date reported: [2025-10-09]

Executive summary:

During a scheduled course exam on Tuesday, October 7th, we observed that certain lecture slide pages and documents remained accessible despite the normal UI control (the slide access button) being disabled at exam start by saving the URL beforehand. Further investigation revealed a broken access control issue: resources intended to be restricted during exams could still be accessed if a previously saved resource link was used, and (separately) modifying an identifier in the resource URL exposed other course pages and documents not intended for our class.

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, test materials, or other documents. This could undermine exam integrity and expose sensitive materials to unauthorized users.

Affected URLs / resources

1- Save slide links that remained accessible durning exam

- https://[redacted].com/course/content-view/45
- https://[redacted].com/course/content-view/46

2- Exposed courses

- https://[redacted].com/course/3/content
- https://[redacted].com/course/4/content

3- Other exposed documents not related to our class (not full list but some examples):

- https://[redacted]/course/content-view/1
- https://[redacted]/course/content-view/10

Affected systems / components

- Web application front end: resource slide viewer page and related links.

- Backend file/document storage and delivery endpoints (API or web handlers that return files).

- Authentication/session management (possible reliance on client-side controls).

- Role/permission logic (course enrollment checks, exam state checks).

How issue was observed:

1- Prior to the exam start, we opened the lecture slide page for my class and saved the browser address (URL).

2- At exam start, the site's **slide access button** became disabled in the UI (intended behavior) but the previously saved URL still allowed the slide page to be loaded in the browser. This suggests the UI block is client-side only and server-side checks are missing.

3- While inspecting the resource URL pattern, we noticed that altering the numeric identifier component in the URL returned other pages and documents which appear to belong to other classes or sections. This indicates that the server returns documents based solely on the provided identifier without verifying whether the requesting user has permission to access that specific document.

How to reproduce the issue:

1- Lecture slide access during exam:

- Access slides hours before exam and save the URL
- Copy URLs and save them
- Paste the URL during the exam

2- Access other class pages

- Modify the number in the middle of the URL marked as [REPLACE ME]

https://[redacted]/course/[REPLACE ME]/content

3- Access other documents not from our class

- Modify the number at the end of the URL marked as [REPLACE ME]

https://[redacted]/course/content-view/[REPLACE ME]

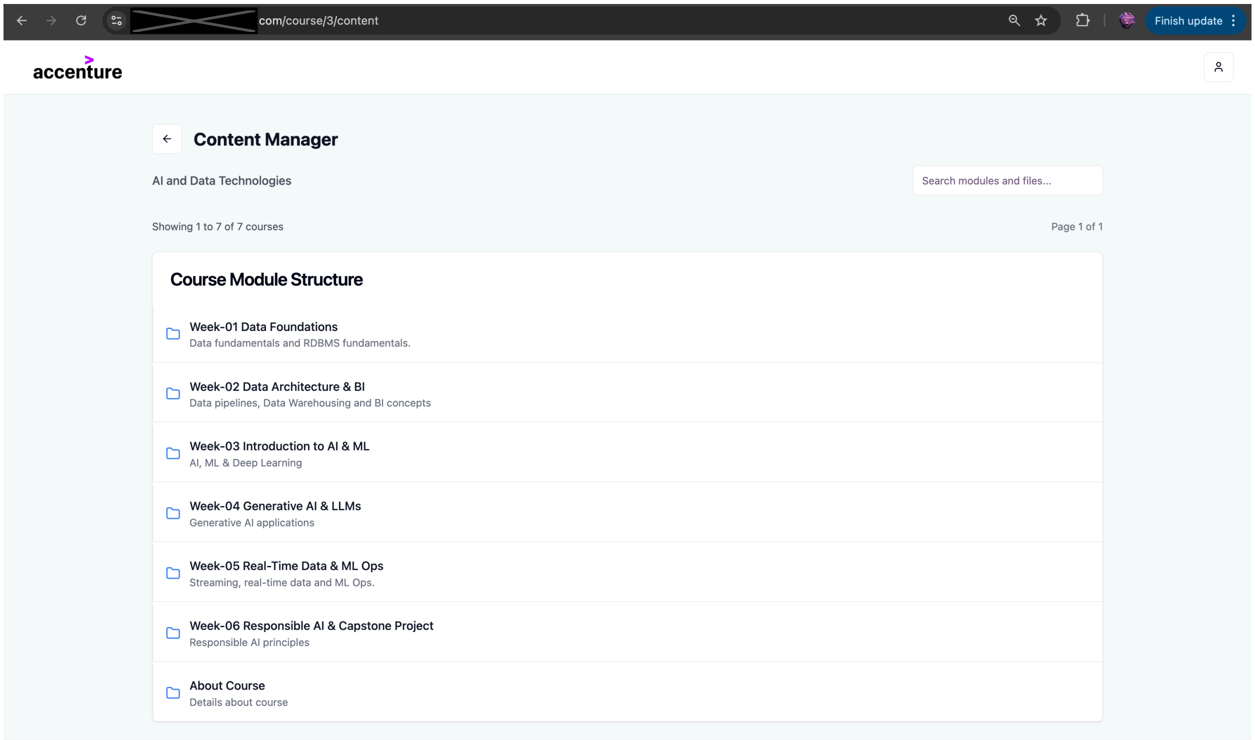
Evidence:

Case 1:

- In order to document the UI button being deactivated leading up to and during the exam and exam must be upcoming. Unfortunately, in order to properly document evidence for this case we must wait till next Tuesday before the exam for the UI slide button to be deactivated again.

Case 2:

- Other class pages



[redacted]com/course/3/content

Content Manager

AI and Data Technologies

Search modules and files...

Showing 1 to 7 of 7 courses

Page 1 of 1

Course Module Structure

Week-01 Data Foundations
Data fundamentals and RDBMS fundamentals.

Week-02 Data Architecture & BI
Data pipelines, Data Warehousing and BI concepts

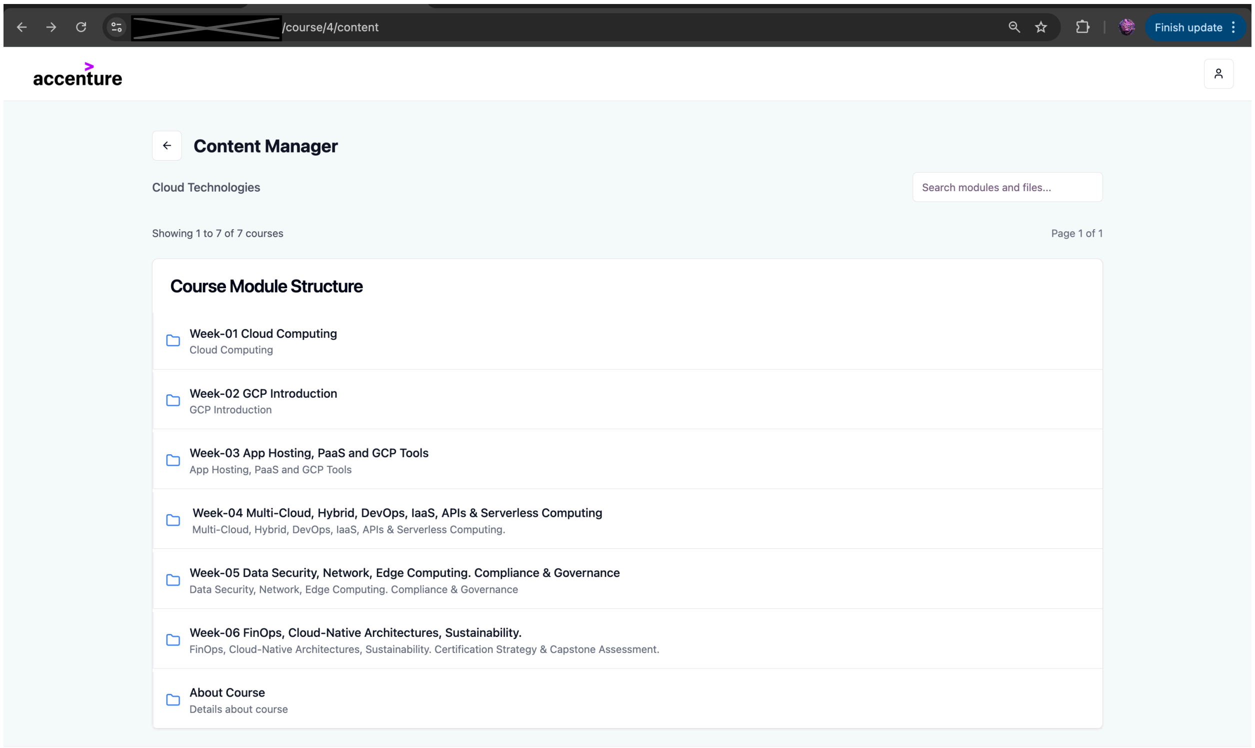
Week-03 Introduction to AI & ML
AI, ML & Deep Learning

Week-04 Generative AI & LLMs
Generative AI applications

Week-05 Real-Time Data & ML Ops
Streaming, real-time data and ML Ops.

Week-06 Responsible AI & Capstone Project
Responsible AI principles

About Course
Details about course


[redacted]/course/4/content

Content Manager

Cloud Technologies

Showing 1 to 7 of 7 courses

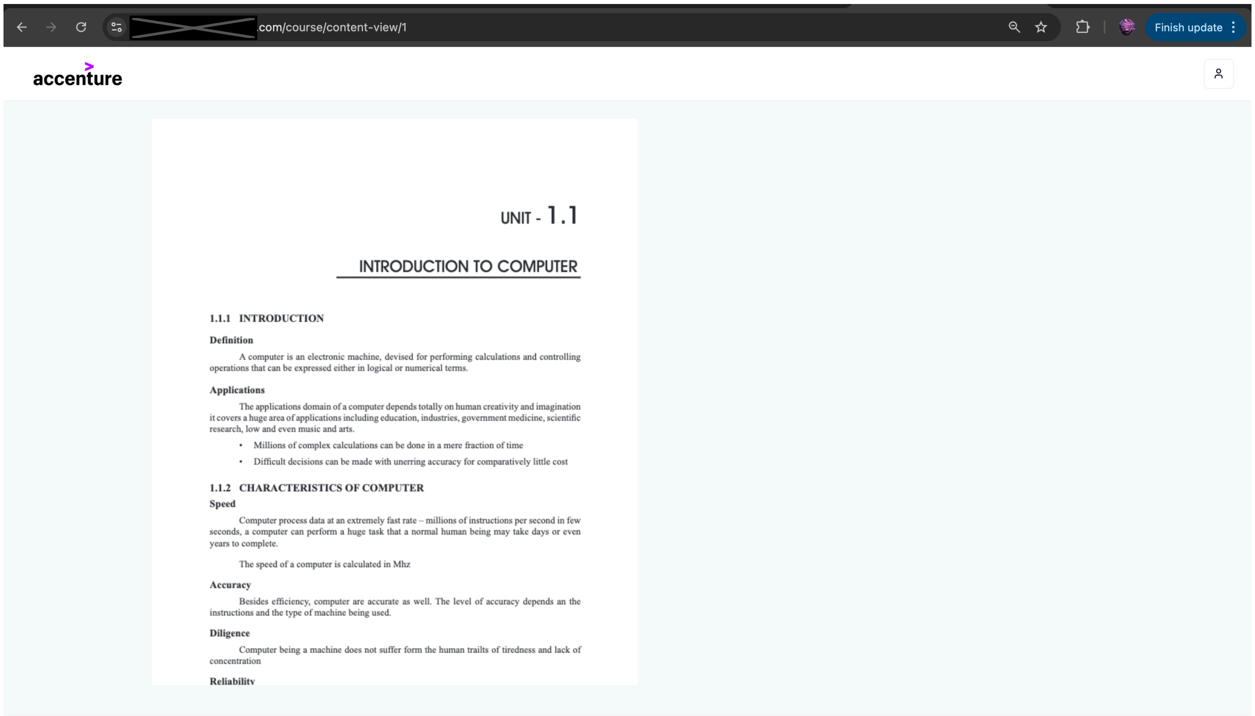
Page 1 of 1

Course Module Structure

- Week-01 Cloud Computing
  Cloud Computing
- Week-02 GCP Introduction
  GCP Introduction
- Week-03 App Hosting, PaaS and GCP Tools
  App Hosting, PaaS and GCP Tools
- Week-04 Multi-Cloud, Hybrid, DevOps, IaaS, APIs & Serverless Computing
  Multi-Cloud, Hybrid, DevOps, IaaS, APIs & Serverless Computing.
- Week-05 Data Security, Network, Edge Computing. Compliance & Governance
  Data Security, Network, Edge Computing. Compliance & Governance
- Week-06 FinOps, Cloud-Native Architectures, Sustainability.
  FinOps, Cloud-Native Architectures, Sustainability. Certification Strategy & Capstone Assessment.
- About Course
  Details about course

Case 3:

- Documents from other classes


[redacted].com/course/content-view/1

UNIT - 1.1

INTRODUCTION TO COMPUTER

1.1.1 INTRODUCTION

Definition

A computer is an electronic machine, devised for performing calculations and controlling operations that can be expressed either in logical or numerical terms.

Applications

The applications domain of a computer depends totally on human creativity and imagination it covers a huge area of applications including education, industries, government medicine, scientific research, low and even music and arts.

- Millions of complex calculations can be done in a mere fraction of time
- Difficult decisions can be made with unerring accuracy for comparatively little cost

1.1.2 CHARACTERISTICS OF COMPUTER

Speed

Computer process data at an extremely fast rate – millions of instructions per second in few seconds, a computer can perform a huge task that a normal human being may take days or even years to complete.

The speed of a computer is calculated in Mhz

Accuracy

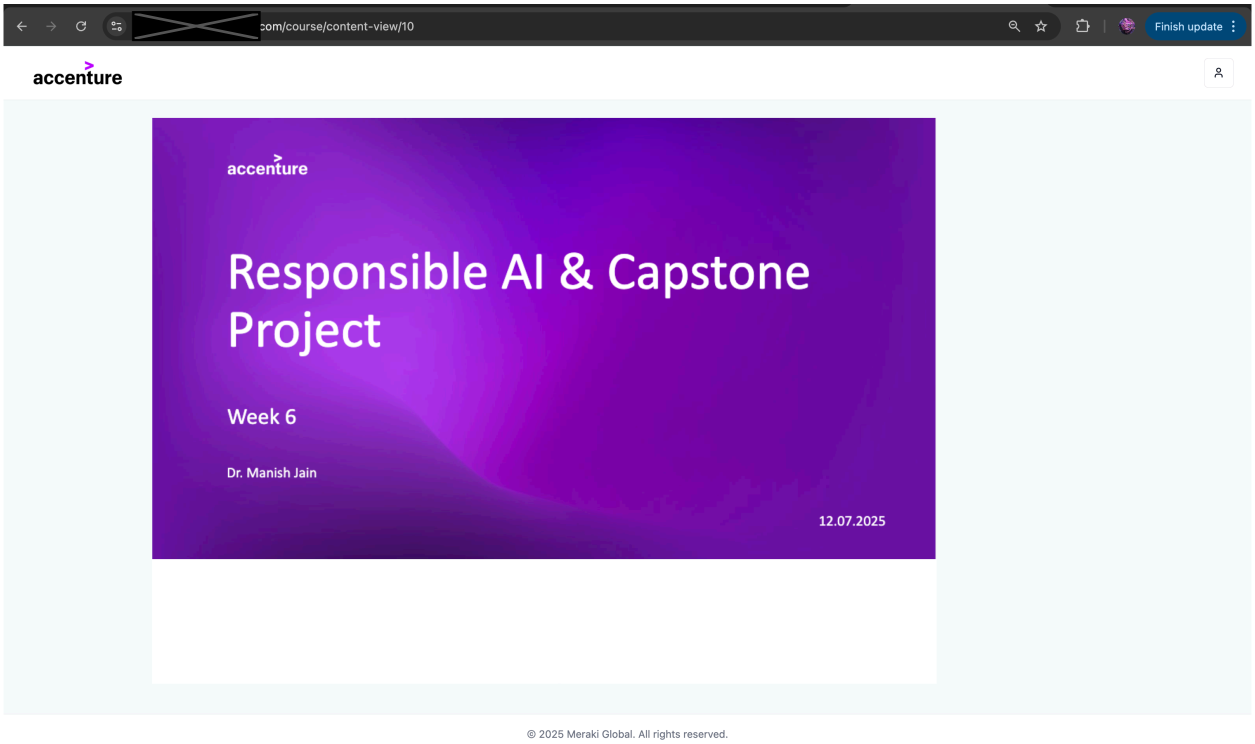
Besides efficiency, computer are accurate as well. The level of accuracy depends an the instructions and the type of machine being used.

Diligence

Computer being a machine does not suffer form the human trailts of tiredness and lack of concentration

Reliability

[redacted]



[redacted]com/course/content-view/10

accenture

accenture

Responsible AI & Capstone Project

Week 6

Dr. Manish Jain

12.07.2025

© 2025 Meraki Global. All rights reserved.

Mitigation and Recommendations:

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

- Implementing server-side authorization checks where every request to course content or resources should verify that the student is enrolled in the corresponding course, and has permission to view the content at that time rather than rely on disabling UI buttons.

- Use indirect or opaque resource identifiers to make URLs less predictable and harder to guess

  Example: /course/content-view/4f3b2c9a-91a1-4b76-9b60-91ea1fdd07b3

- Enforce least privilege and segregation by separating course content per cohort/stream at the backend, not just at the UI layer.

- Log and monitor all access attempts and looking for any request patterns or timings