Title: Broken Access Control - Unauthenticated API Calls
Reported by: Ali Shaker Alawami
Course: Cybersecurity stream
Instructor / Contact: Atharva Bhamburkar
Date discovered: [2025-10-14]
Date reported: [2025-10-15]

Executive summary:

While inspecting the network calls to find the lecture slides PDF URL (from the report: Broken Access Control - Lecture Slide PDF Access) I read the the javascript in the page and found several API calls made by the page. Further investigation revealed that my student account was able to call the modify the API calls and get successful responses. One of the API calls allowed access to sensitive information including first names, last names, phone numbers, email addresses, candidate IDs, and role IDs of all registered users, not just the authenticated account, to be revealed. This occurs due to missing authorization checks at the backend level, enabling ordinary student accounts to enumerate user data. The issue constitutes a major Broken Access Control / Data Exposure vulnerability, risking privacy violations and potential misuse of personally identifiable information (PII).

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: Exposes personally identifiable information (PII) of all registered users, violating privacy and potentially enabling targeted phishing or social engineering attacks. Represents a critical data exposure and privacy breach.

Affected URLs / resources

https://[redacted].com/api/v1/user/[USER_ID]

Where [USER_ID] is replaced by any ID form 1 to 141

Affected systems / components

- Backend API layer: Endpoints responsible for retrieving user profile and account data.

- Access control and authorization checks: Fails to enforce user-level restrictions, returning all user records regardless of requester role.
- Frontend JavaScript code: Makes unrestricted API calls exposing endpoint URLs in client-side scripts.

How issue was observed:

1. While analyzing the homepage of the academy portal for the calls happening to find the lecture slide PDF file links by inspecting the page's JavaScript source revealed multiple API endpoints being called to retrieve user data.
2. These API calls were tested individually through the browser.
3. It was found that the API returned detailed account data not only for the authenticated user but for any valid account ID provided.

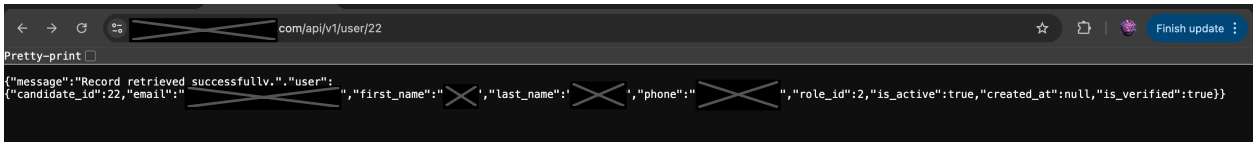
How to reproduce the issue:

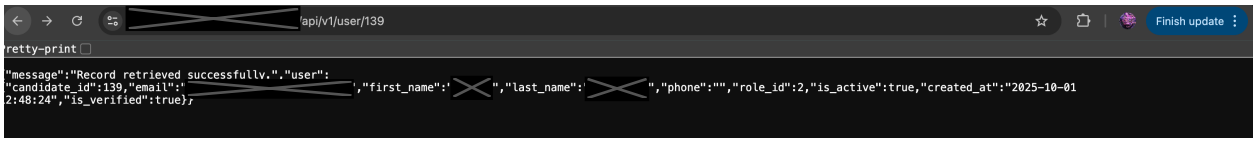
Copy the following URL to the API

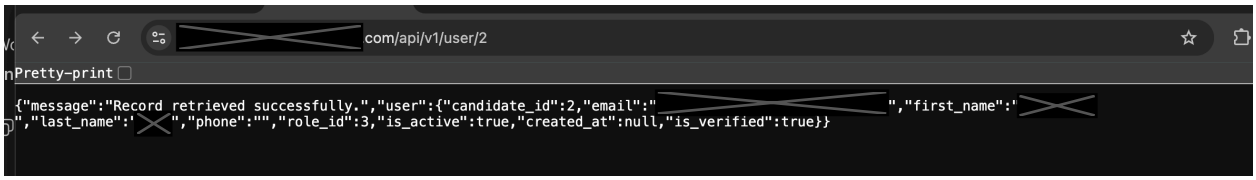
https://[redacted]/api/v1/user/[USER_ID]

And replace [USER_ID] with the desired valid ID (from 1 to 141 as of now)

Evidence:







Mitigation and Recommendations:

- Enforce role-based access control (RBAC) and object-level authorization on all API endpoints such that each request to retrieve user information must verify that the requester has legitimate access rights to that specific data record.
- Implement rate limiting and monitoring to detect enumeration or mass data retrieval attempts.
- Log and monitor all API call attempts and look for any request patterns or timings