This is one of odd finding I came across while testing an application.

Broken Access Control / Lack of access control / IDOR with authentication

Consider <https://pentest.test-env.com> is the URL of the app.

With proper authentication, I have navigated to *my profile* page from the *settings*

There I observed that URL is displayed as <https://pentest.test-env.com/user/Profile/11>

There is a numerical value 11 at the end of the URL that represents the user profile number

So, I have decided to Brute-force / fuzz this, starting from 1 to 1000.

Also, there is no rate limiting and anti-automation implemented to stop this fuzzing *(Yet this is another vulnerability found while fuzzing the URL)*

I got success for most of the responses with status code 200 OK, all those successful responses have valid user profile page.

I was able to harvest the email ID all the users who has been using this application, the password value is displayed as \*\*\*\*\*\*\*\* by default, it was hard to crack it.

As we know, the corporate Email ID are highly helpful in social engineering attacking and we can perform internal phishing attack using this.

We can possibility find similar kind of vulnerabilities in other applications, that may contain highly sensitive data of the user (PII, Medical / health information, etc)

