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

We can’t categorize this as IDOR, as this requires user 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 modified to <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

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.

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, since 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.

