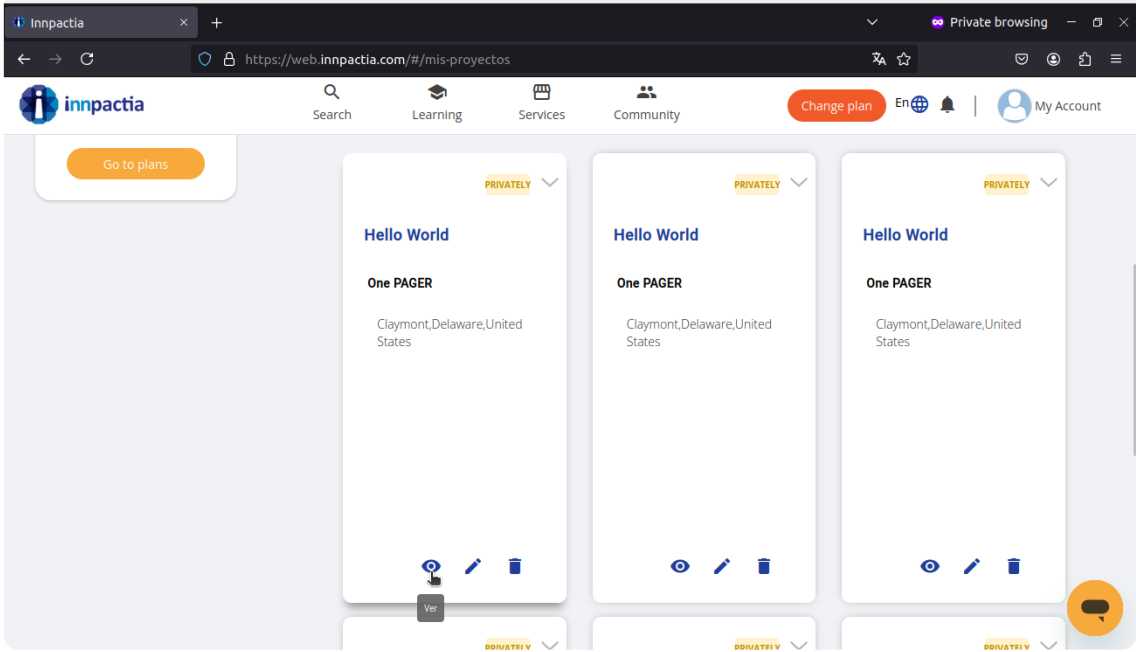
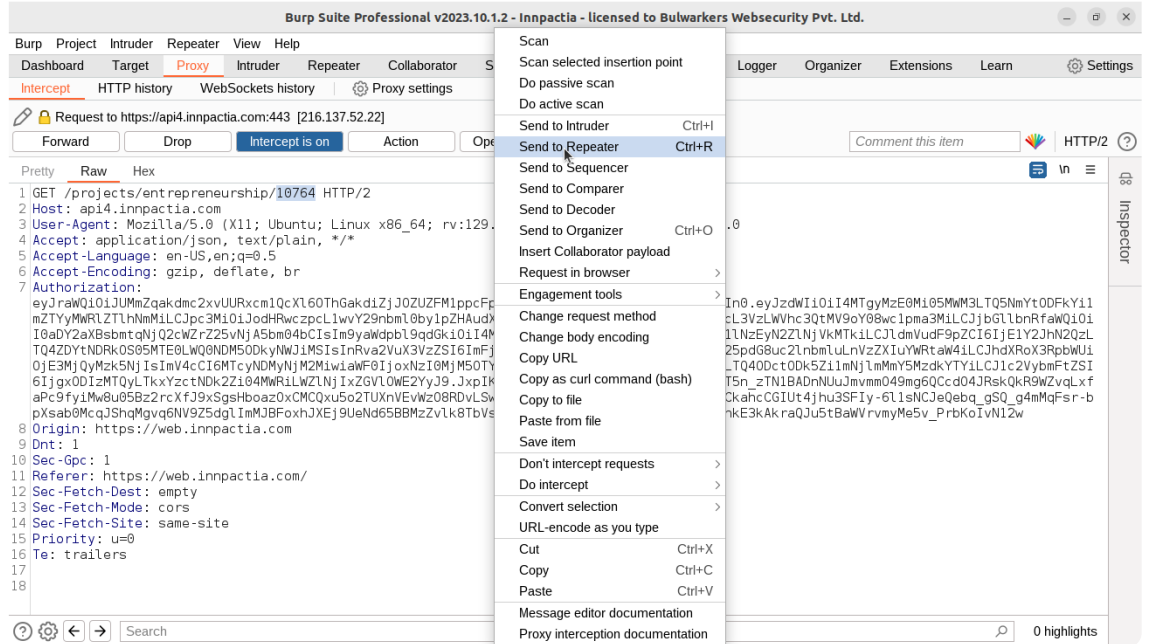


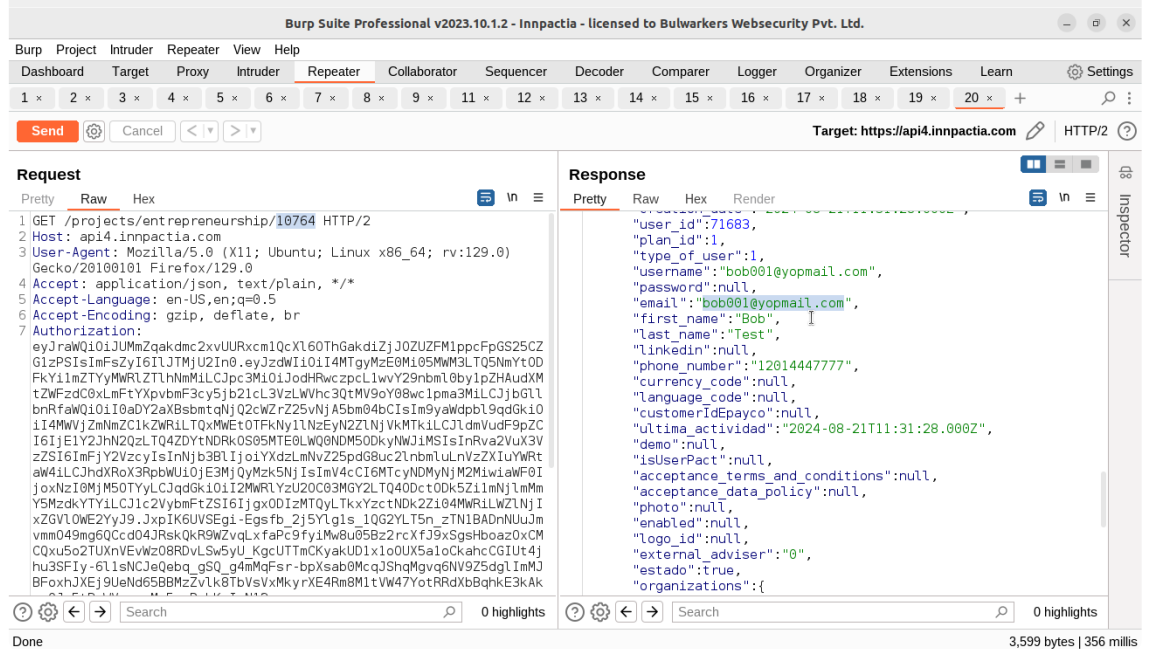
[Innpactia] Unauthorised access to view information of any user (20556)

Severity	High
Security Control	Authorization
Vulnerability	Missing Authorization [CWE-862]
Finding Description	Application has functionality for the user to view information. It does not have implement authorization check for "project_id" parameter which allows user to view information of any user by replacing "project_id" parameter.
Method of Identification	Manual
Affected Resources	https://api4.innpactia.com/projects/entrepreneurship/10764
Affected Parameter	project_id

Evidence	Step 1: Let's say we have two users. User 1: Alice - Victim User 1: Bob - Attacker Login to the application with user "Bob". Navigate to "Mis Projectors" and click on "View" button.  Step 2: Intercept the following request using Burp Suite and observe the "project_id" parameter. Send the request to Repeater.
----------	---



Step 3: Now, click on the send button and observe the response to of the original request.



Step 4: Here, change the "project_id" parameter value and click on the send button and observe the response.

