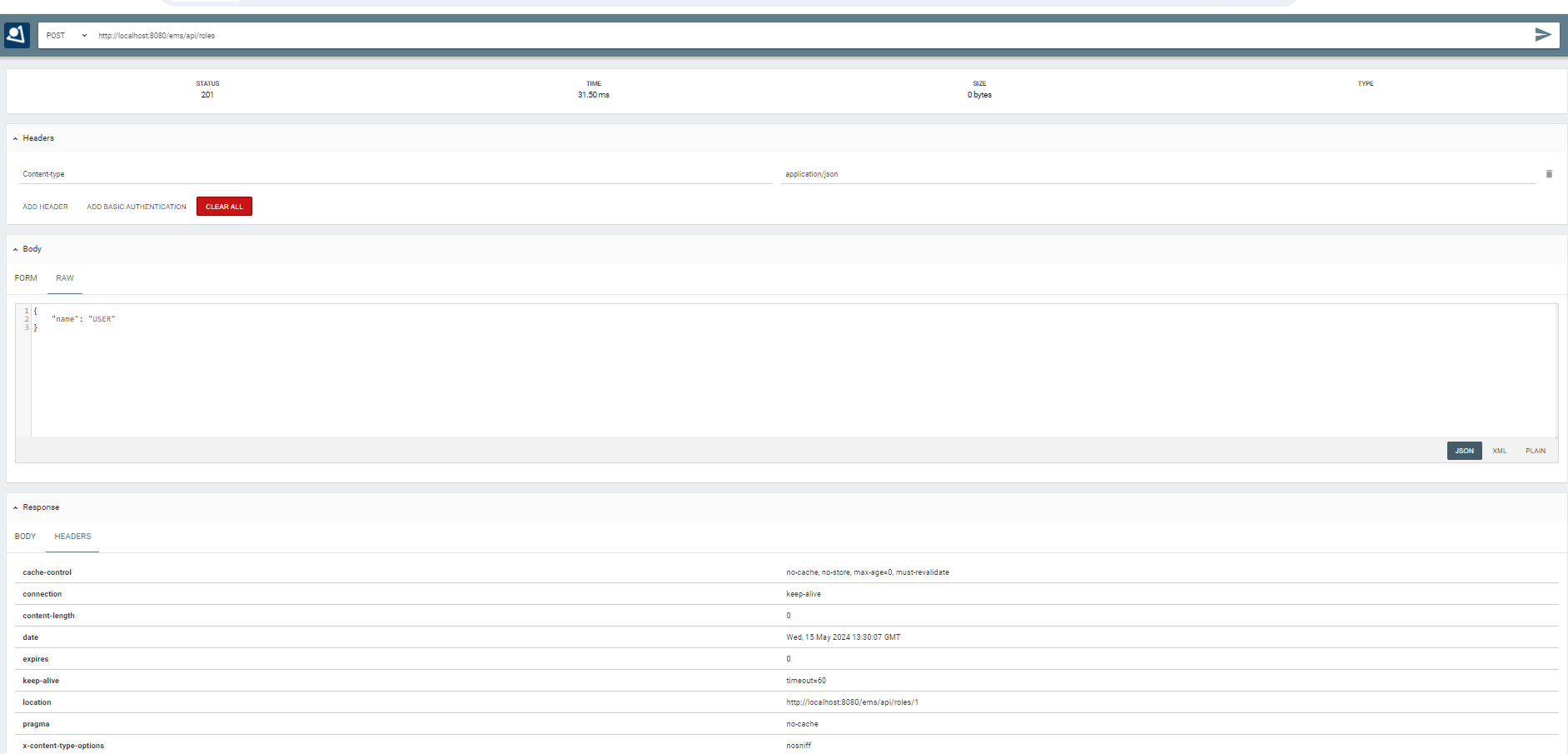
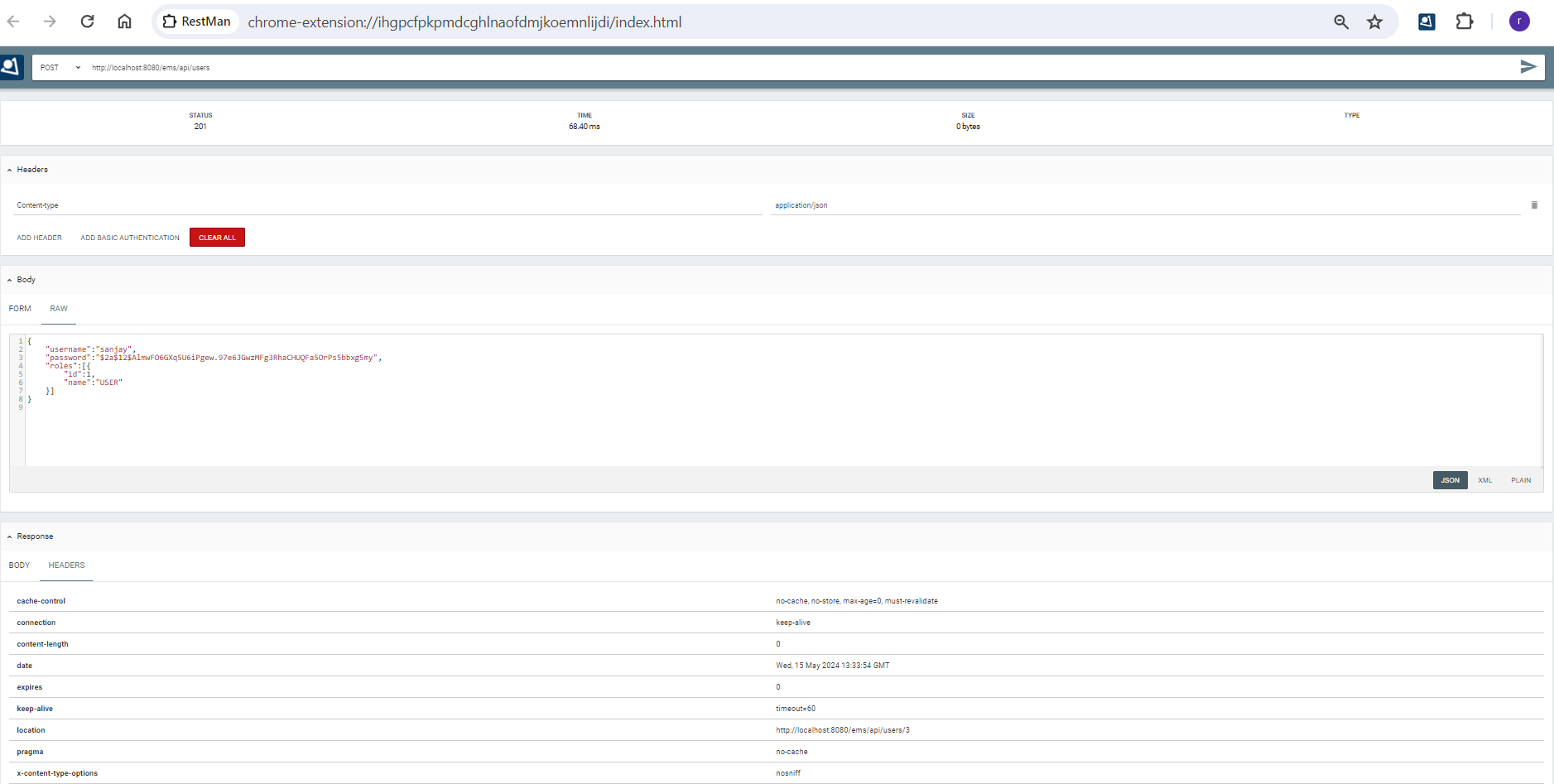
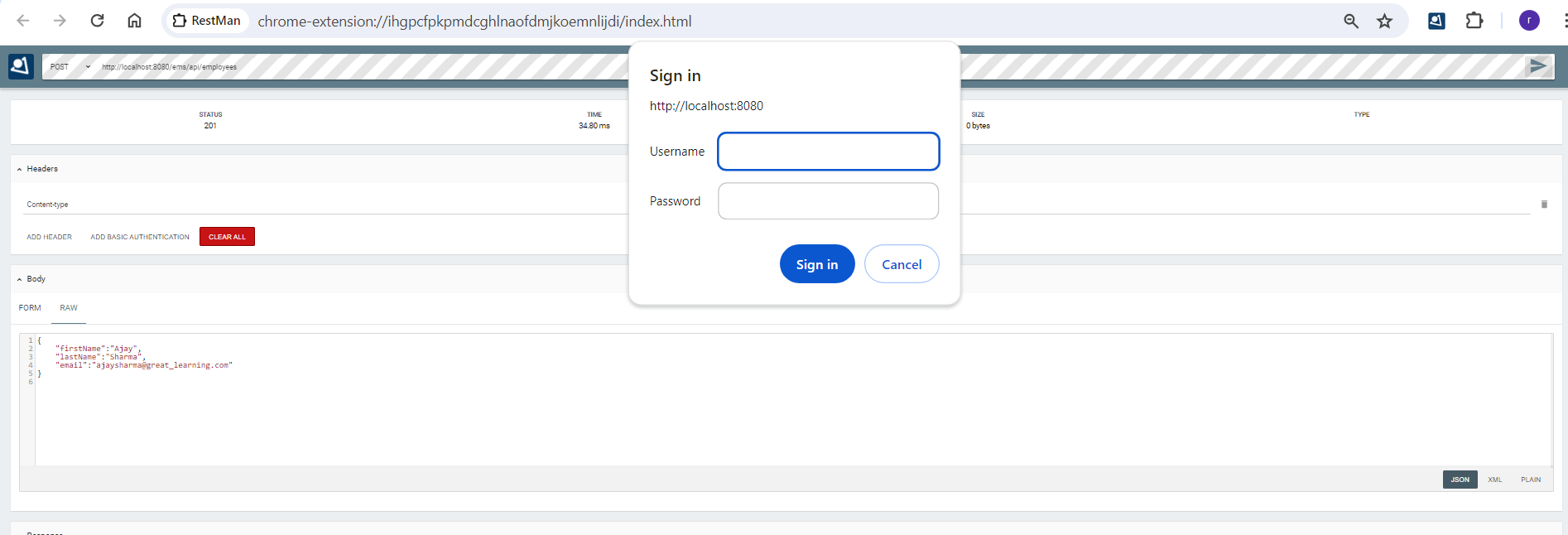
1. Add roles to the database. Endpoint is accessible to all.



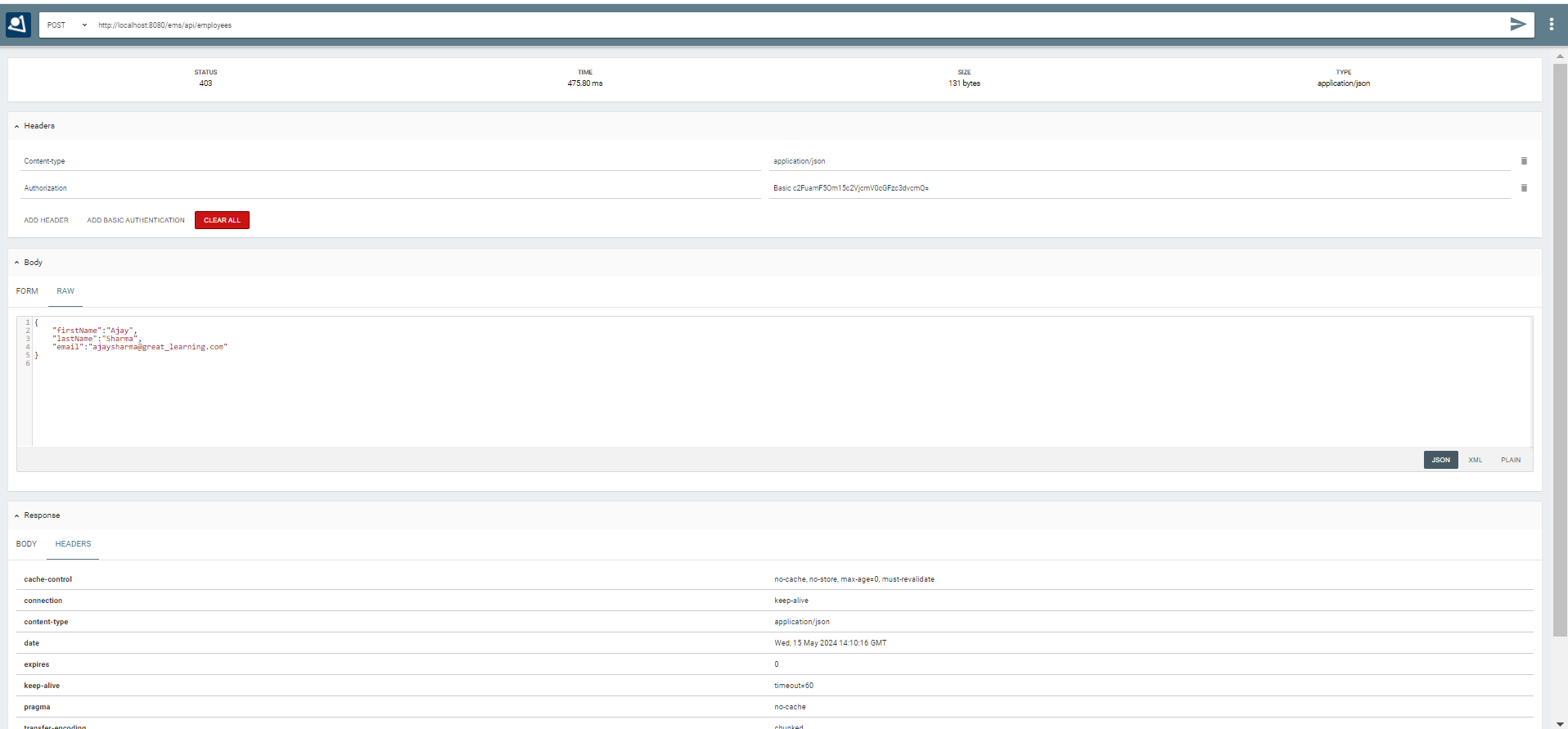
1. Add users with assigned role to database. Endpoint is accessible to all.



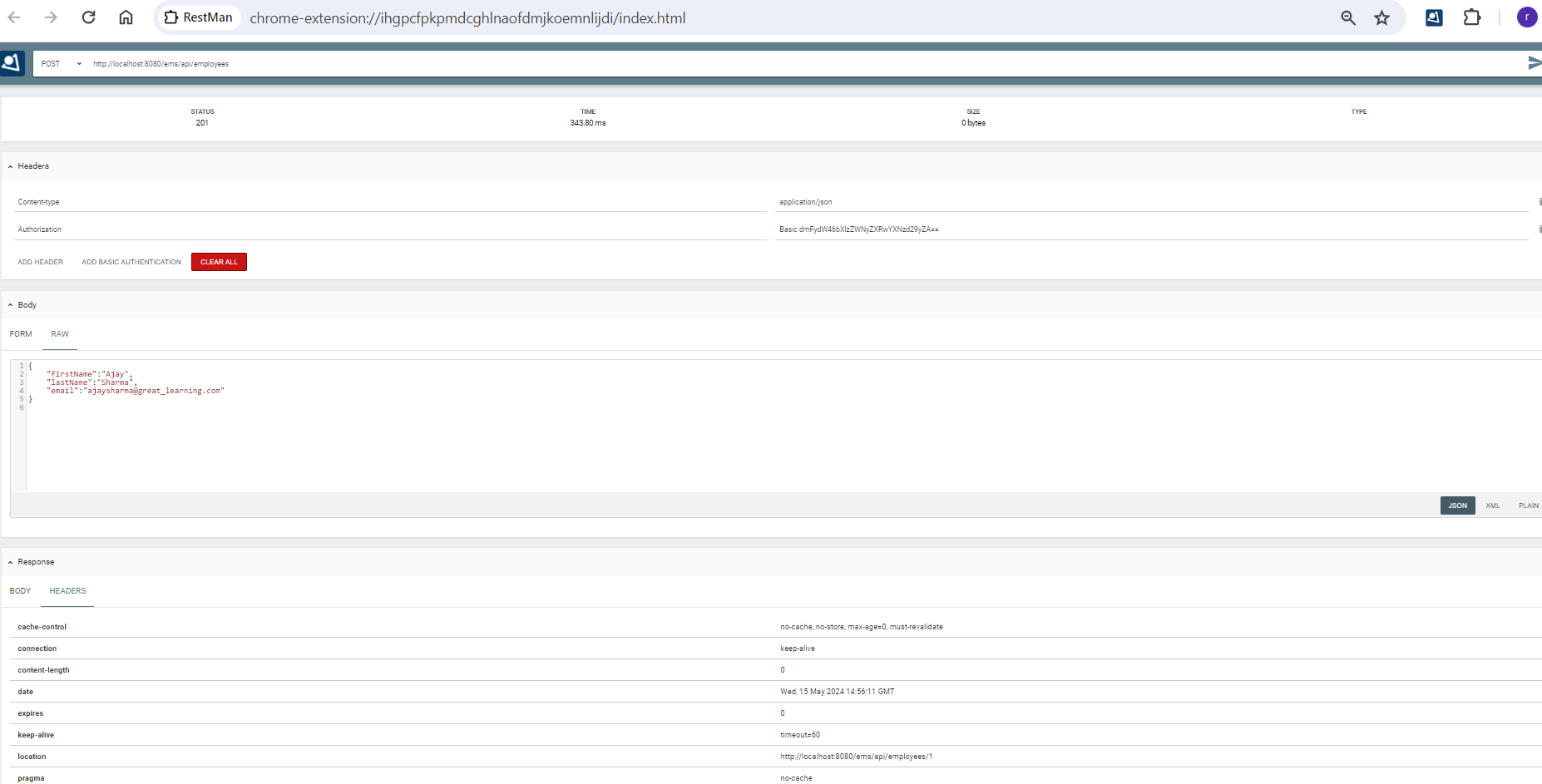
1. save an employee detail. Endpoint is accessible to only role admin. Here in the below snapshot shows that the endpoint is accessed without the authorization header and hence it is secured as it prompts for username and password



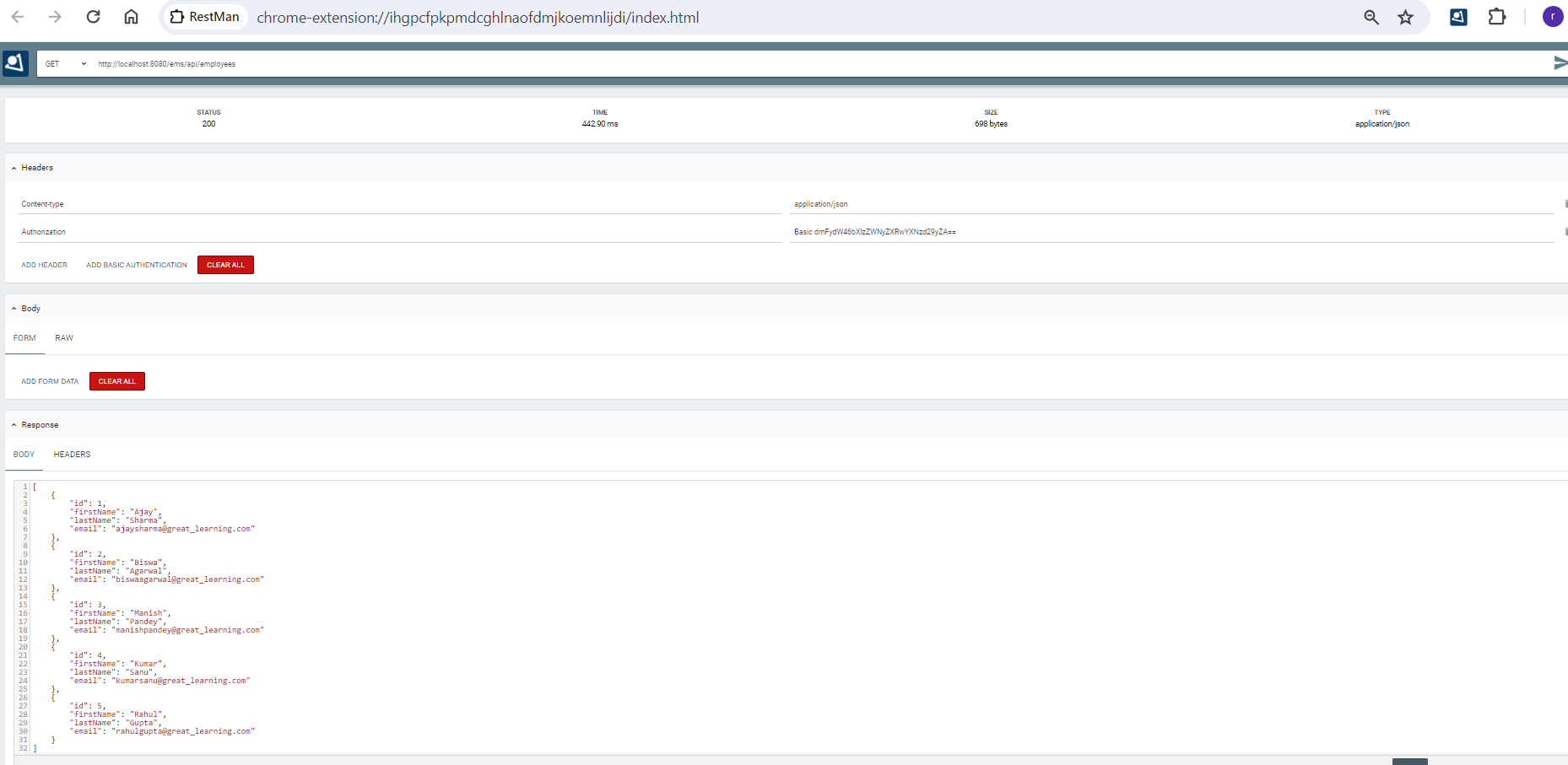
1. Same endpoint as above but with authorization header passed with user having a role other than admin. We can see the request status is forbidden.



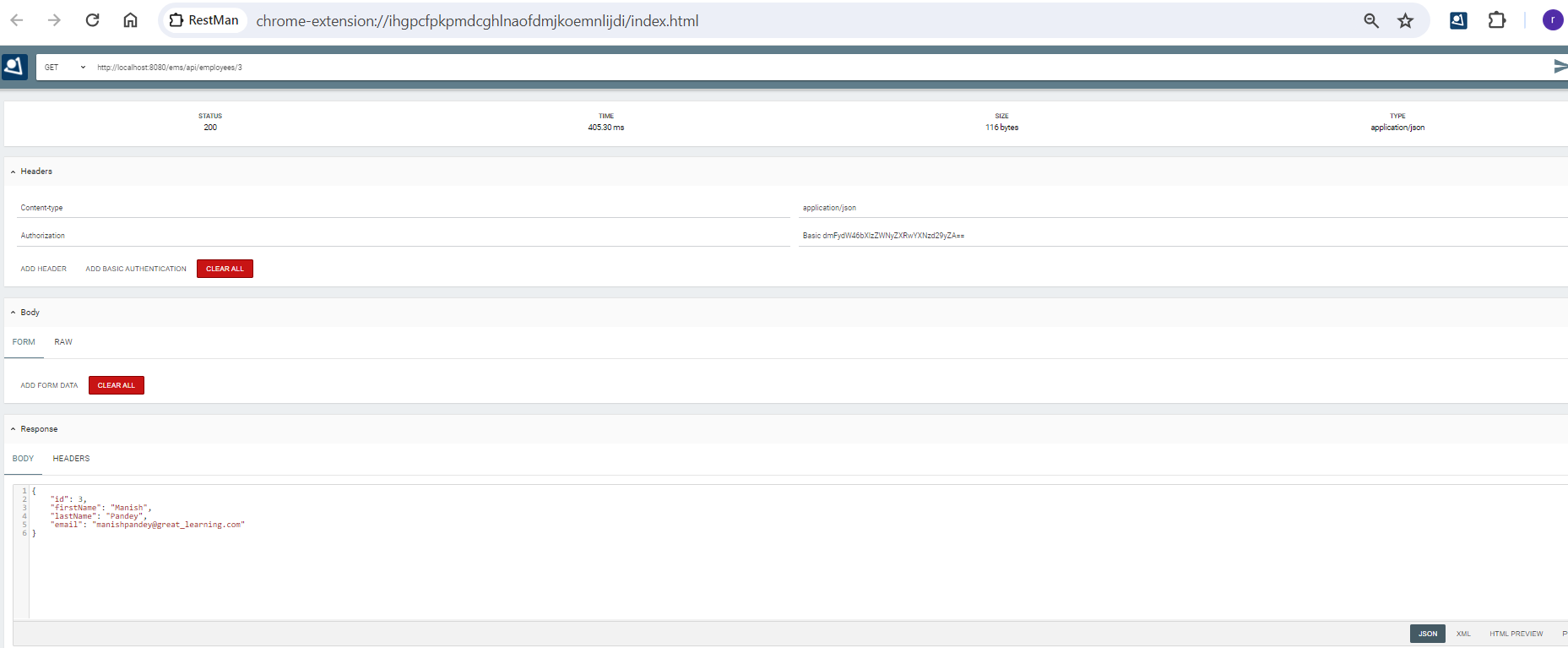
1. Same as above but now with a valid user with role admin is sent in authorization header. Request status is 201 and employee details are saved to database.



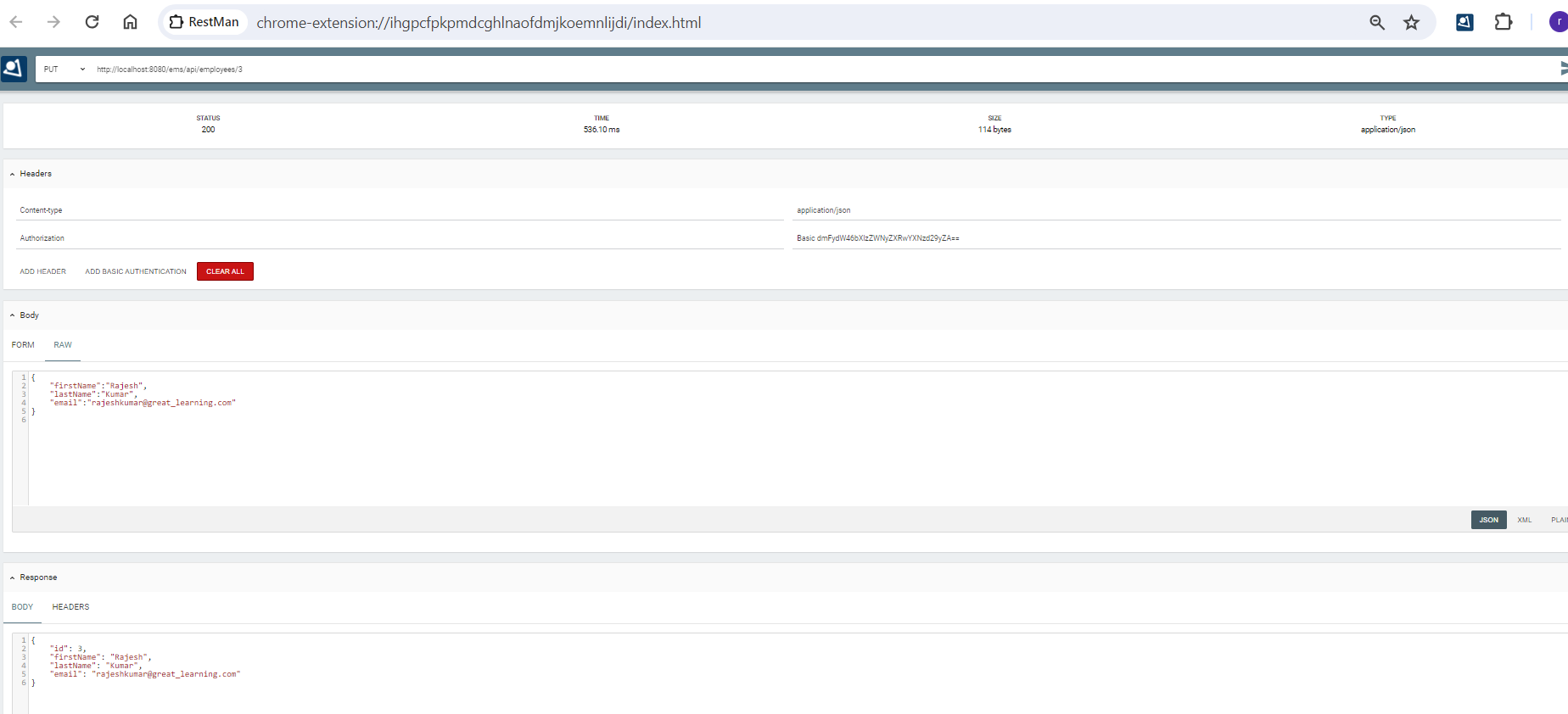
1. Get all employees in database.



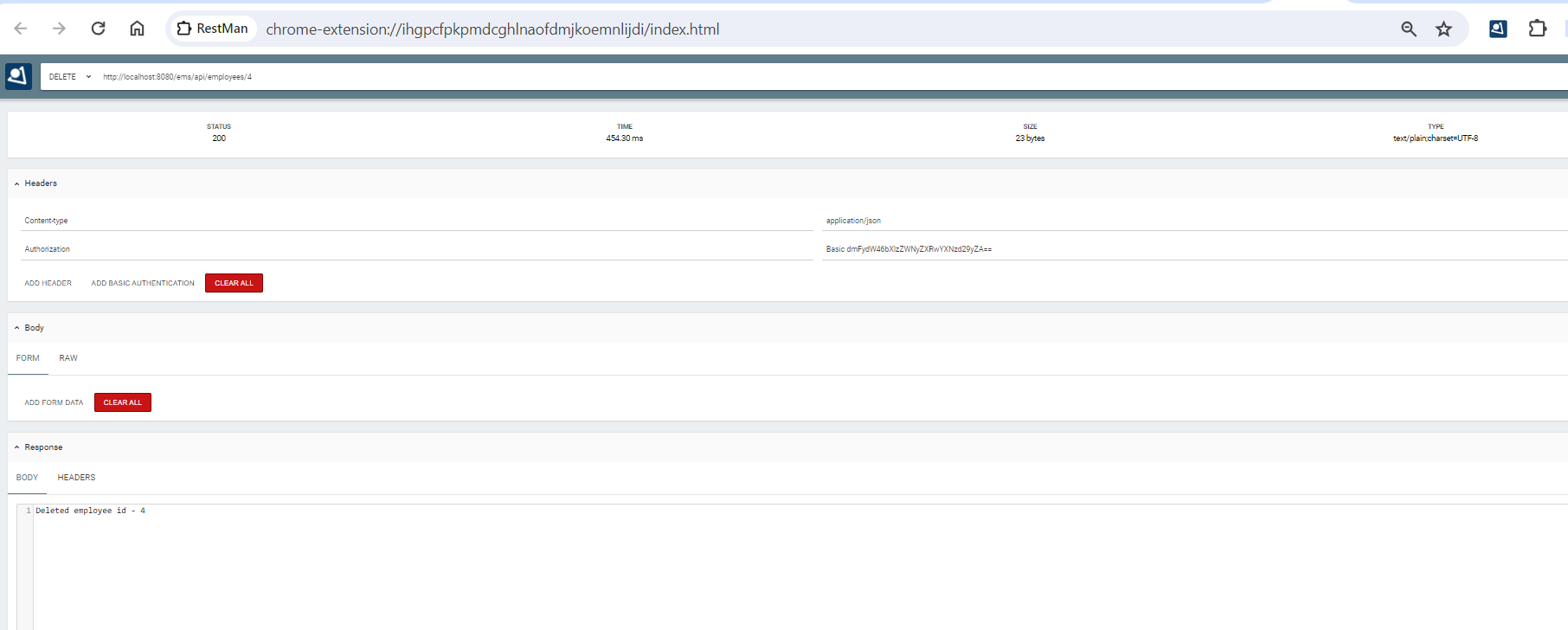
1. Get employee by id.



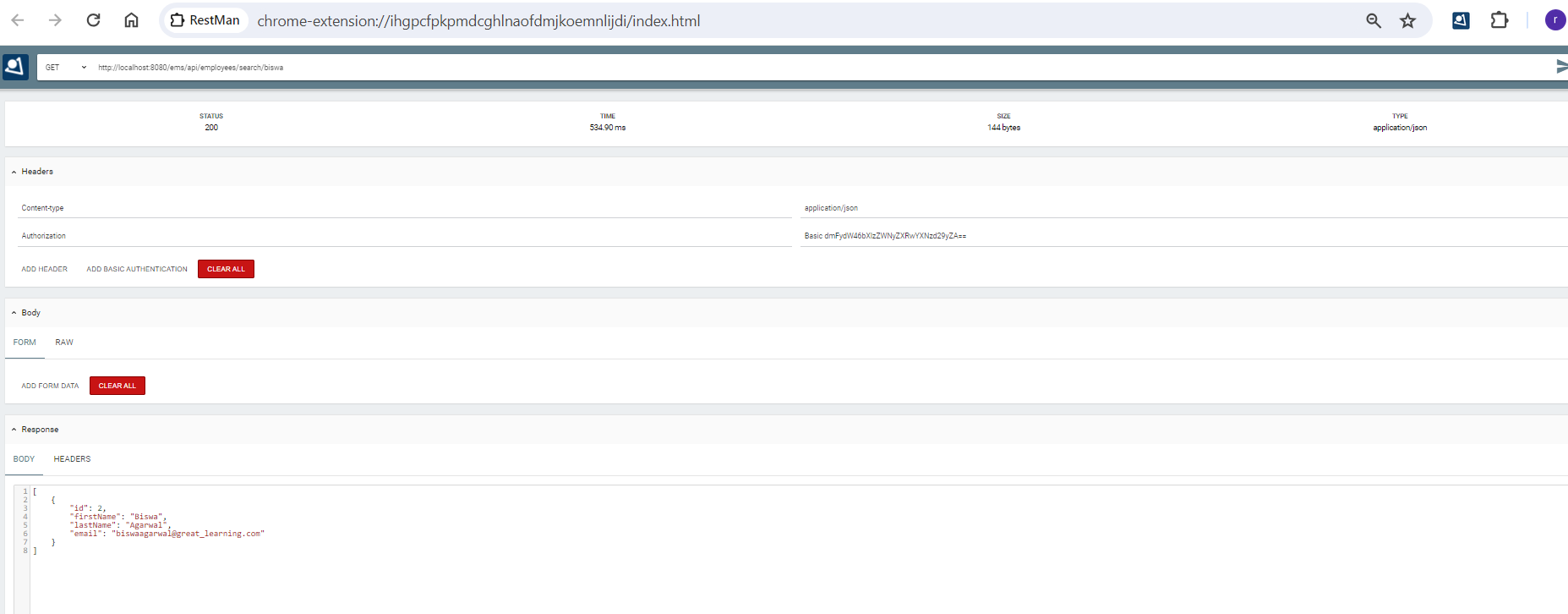
1. Update employee with a given id.



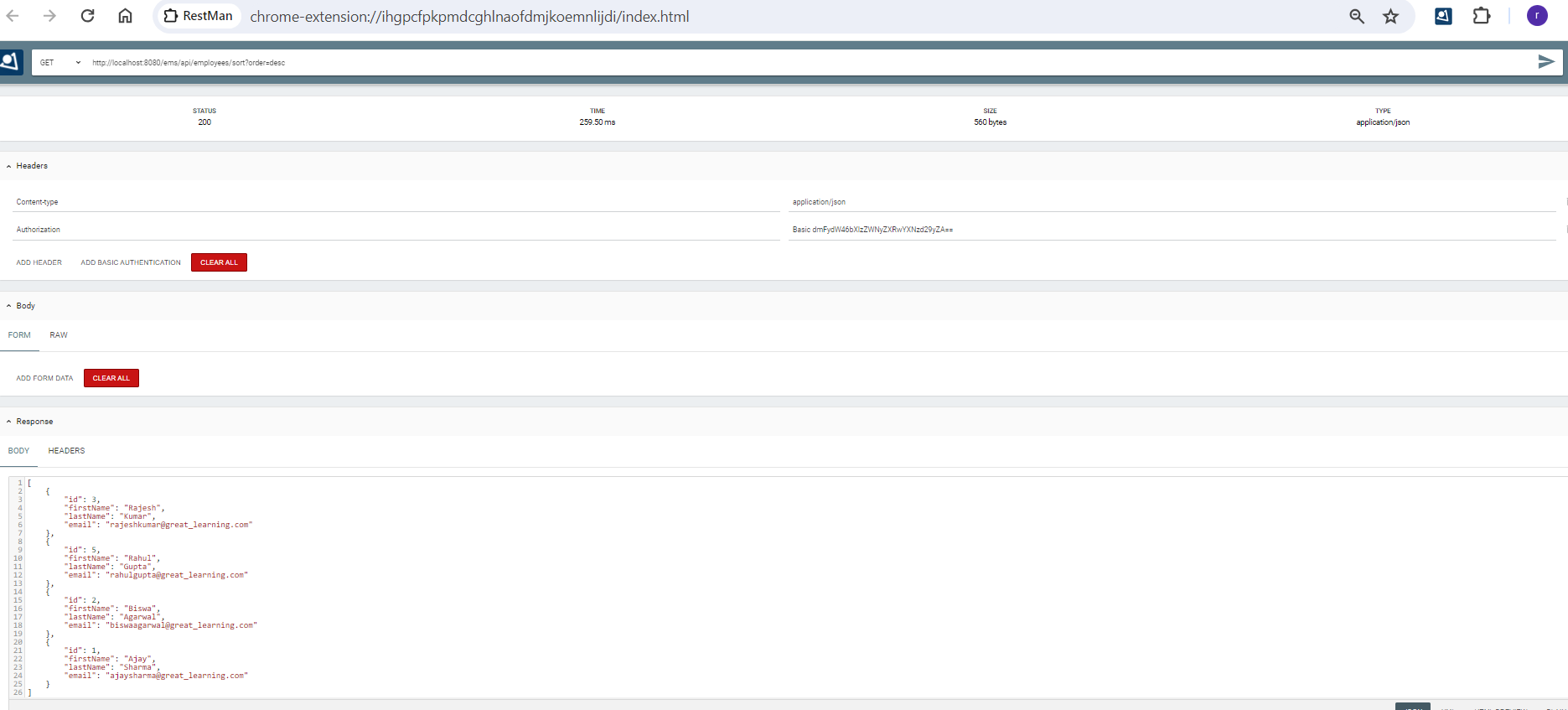
1. Delete employee by id.



1. Search employee with given firstname



1. Sort all employees in desc order.



1. Sort all employees in asc order

