Name: Fatma Essam Elden

ID: 20216077 – S5

**Report2**

How to test in postman:

* **POST /users/login** is open to anyone (no 401 unauthorized).
* **All other** requests require a valid credential (Basic Auth header), due to using a stateless session.
* **Specific /users/\*\* endpoints** are locked to ROLE\_ADMIN only.
* **Any other URL** (user-facing banking APIs) needs the caller to be logged in (and therefore can be accessed by a normal ROLE\_USER).

**So, I fix vulnerabilities in Authentication and Authorization**.