Week4 - Remediation Recommendations

According to the Vulnerabilities discovered in this Report the following are some steps the developers must follow to prevent the privilege escalation, broken access control and IDOR Vulnerabilities

- access by default `access withoud cookies` should always be prevented Unless a resource is intended to be publicly accessible.
- Role-Based Access Control - that means every user's role should be identified in the user's cookie, so that the basic users would only access the basic resources and the admin users would access more critical resources.
- every resource in the platform should be identified, which type of users are able to access this resource and what are the actions they are able to apply in this resource, and before allowing any user to access this resource a robust check mechanism should check if this user is authorized to access this resource or not `that would be happended by check the user's cookie` .
- always in every input field, a Validation and sanitization process should be takes place to prevent injection attacks that could lead to privilege escalation.
- Secure session management practices, including session timeouts and invalidation of sessions on logout.
- **Always** avoid using sequential numeric IDs in URLs. Instead, use secure tokens or UUIDs that do not expose the underlying database structure.
    - As mentioned always perform access control checks on resources based on user roles and permissions
- Implement rate limiting on APIs to prevent brute-force attacks that could exploit IDOR vulnerabilities leading to privilege escalation or broken access control
- Provide training for developers on secure coding practices, particularly regarding access controls.

To show the Presentation summarizing the discovered threads - Click Here.