**SCENARIO**

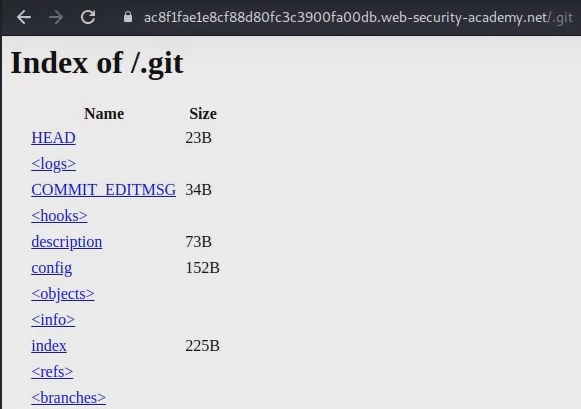
The application's version control history is inadvertently exposed, granting access to the app's historical source code, which might contain hard-coded secrets.

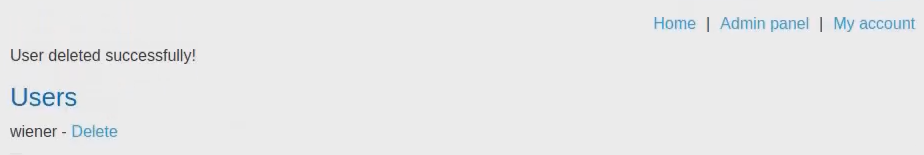
**PROCEDURE**

1. Accessing the /.git path, we discern the lab's Git version control data.
2. Downloading and examining this directory locally, we find previous commits, particularly one which removed a hard-coded admin password.
3. Inspecting the changes of this commit, we can retrieve the previously hardcoded password.

**PAYLOAD**

Access to /.git directory and retrieval of past commits.

**PROOF OF CONCEPT**

****

**REMEDIATION**

1. **Hide .git:** Ensure the .git directory (or other version control directories) is never publicly accessible.
2. **Regular Directory Checks:** Implement automated checks to ensure sensitive directories remain concealed.
3. **Avoid Hardcoded Secrets:** Refrain from hardcoding sensitive information and use environment variables or secure vaults instead.