**SCENARIO**

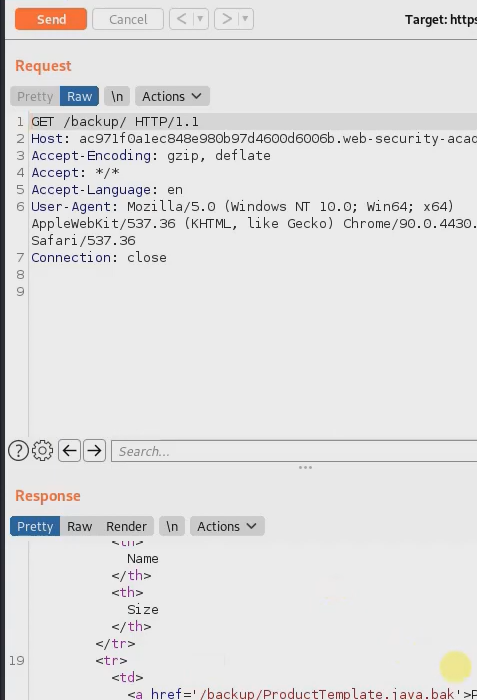
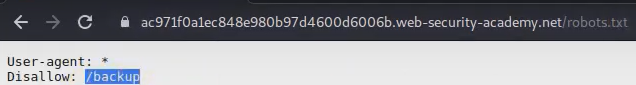
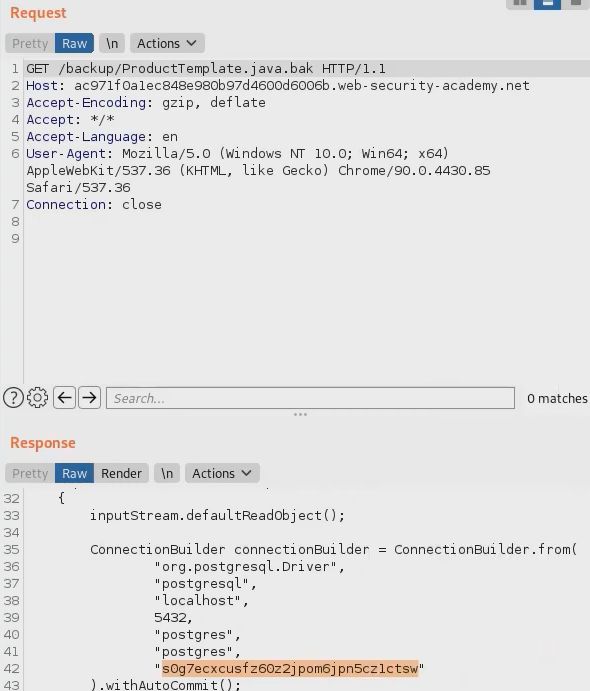
Backup files in a concealed directory of the application unveil the application's source code. This breach can expose sensitive hardcoded details.

**PROCEDURE**

1. Navigate to /robots.txt, uncovering the /backup directory.
2. Accessing this directory, we find backup files such as ProductTemplate.java.bak.
3. Inspecting the source code in this backup reveals a hardcoded database password.

**PAYLOAD**

Access to /backup/ProductTemplate.java.bak

**PROOF OF CONCEPT  
  
  
  
REMEDIATION**

1. **Avoid Public Backups:** Ensure backup files are never stored in publicly accessible directories.
2. **Robots.txt Discretion:** Avoid disclosing sensitive directories in robots.txt.
3. **Regularly Audit Web Directories:** Regular scans should be carried out to spot and clean any unintentionally exposed files.