**Vulnerability Assessment and Penetration Testing Report**

**Information Disclosure via Backup Files (PortSwigger Lab)**

*Executive Summary*

Objective: To assess the resilience of the web application against information disclosure vulnerabilities.

Key findings: A publicly accessible backup file was discovered at the /backup endpoint (referenced in robots.txt) of the web application which expose the credentials of the database. This can lead to data breaches and identification and exploitation of additional vulnerabilities.

Risk Level: Critical

Impact: Unauthorized access to sensitive information and potential for further exploitation.

Recommendations: Implement strict access controls, remove backup files from publicly accessible endpoints, establish secure development practices.

*Introduction*

Scope: Evaluate the web application for vulnerabilities related to information disclosure.

Testing Period: 25 April 2025 8:22pm

*Methodology*

Reconnaissance: Accessed Robots.txt to find directories with indexing dis-allowed.

Testing Tools: Manual Testing to find exposed backup files and try to access their contents.

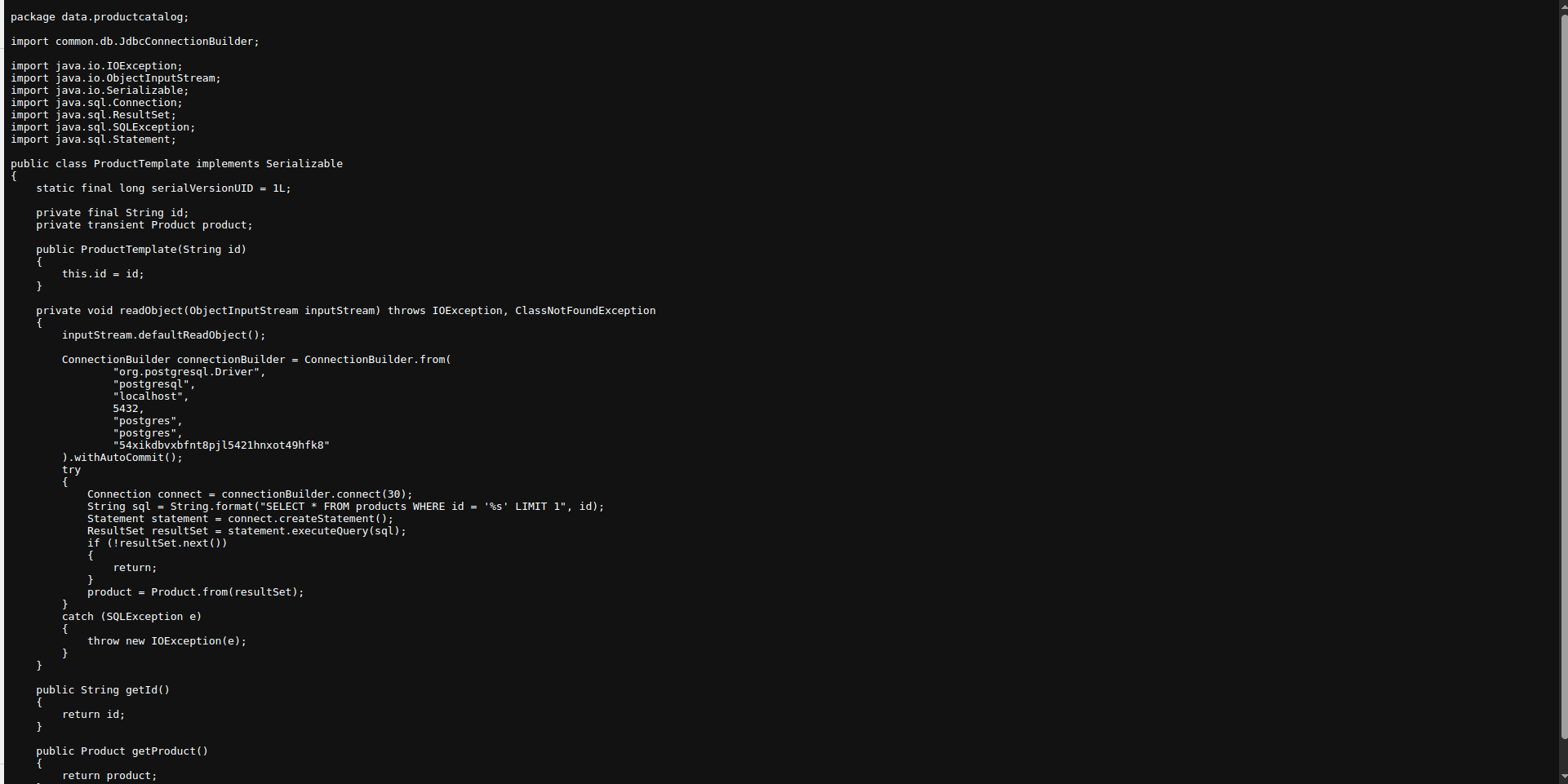
Analysis: Reviewed the contents of the exposed backup file.

*Findings*

Vulnerability: Exposed backup file.

* Description: A backup file containing the database credentials was accessible without authentication.
* Location: <https://portswiggerlab.com/ProductTemplate.java.bak>
* Impact: Exposure of potential credentials of the database.
* Evidence: Accessing the file revealed the credentials of the postgres database

|  |  |
| --- | --- |
| Username | Password |
| postgres | 54xikdbvxbfnt8pjl5421hnxot49hfk8 |



*Risk Rating*

|  |  |  |
| --- | --- | --- |
| *Likelihood* | *Impact* | *Overall Risk* |
| *High* | *Critical* | *Critical* |

*Recommendation*

* Immediately remove all backup files from public access.
* Enforce strict access control policies on server directories.
* Implement automatic backup file cleaning post-deployment.
* Conduct regular security audits to catch such misconfigurations early.

*Conclusion*

The exposed backup file vulnerability poses a critical threat. Immediate remediation is necessary to prevent serious data breaches and system compromise.