Lab name: [Source code disclosure via backup files](https://portswigger.net/web-security/information-disclosure/exploiting/lab-infoleak-via-backup-files)

Severity:

Lab description:

* This lab leaks source code through backup files in a hidden directory. Need to find database password that is hardcoded.
* Source code disclosure vulnerability occurs when the application accidentally exposes its server-side code to clients via any backup files.

Impact:

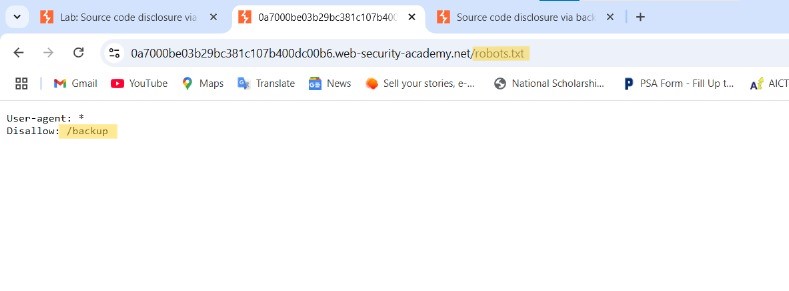
* Attackers can use these temporary backup files to exploit hidden vulnerabilities.
* Attackers or any end users are going to have at least generic knowledge on the application’s structure.
* This source code might sometimes unintentionally expose passwords (in any form) and allow privilege escalation.
* It also can expose sensitive data like financial information or any PII, this eventually leads to account hijacks.
* Business logic can be interrupted, which brings down any organization’s reputation.
* Sometimes, source code can reveal the IP addresses and server names which increases the attacking surface.
* Integrity is highly impacted here. So severity is high.

Recommendations:

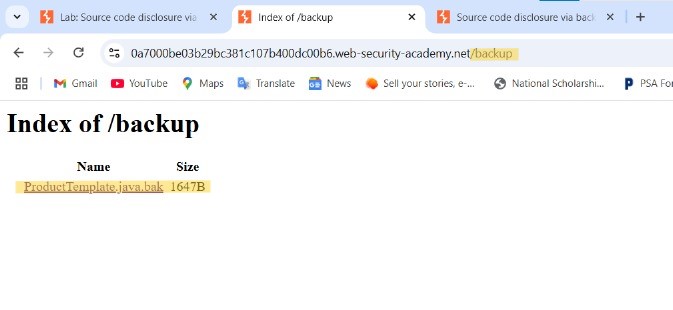
* Disable directory listing in the webserver would stop attackers from accessing the contents of directories and finding files that are meant to be a secret.
* Restrict file permissions in webserver so that source codes or any important file is not visible to any end users.
* Use secure development practices to avoid these kinds of vulnerabilities.
* Place confidential files with credentials and store them separately and the file that clients can interact should be kept in a different directory.

Steps to reproduce:

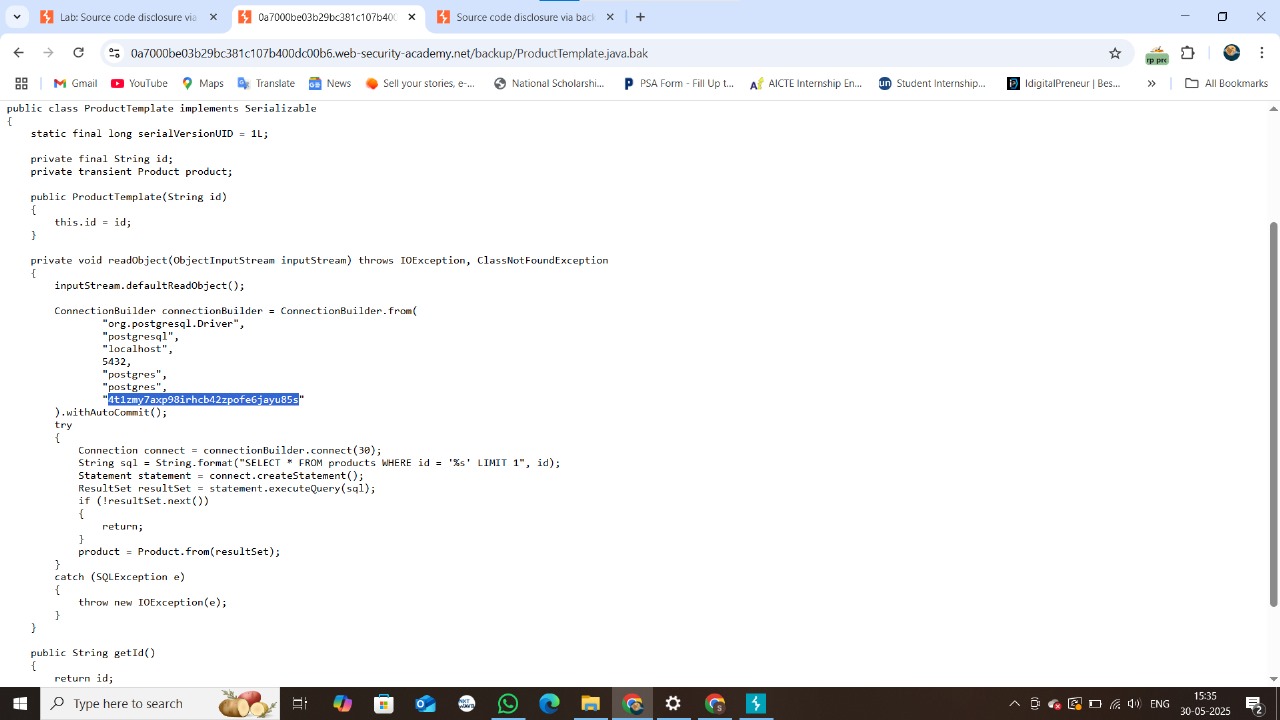
* Access the lab, and in the URL, add */robots.txt* and enter.
* Now we can notice that there is some end point revealed. Now browse the */backup* endpoint.



* Now we can see *ProductTemplate.java.bak* this source code file is exposed.



* After accessing */backup/ProductTemplate.java.bak* and now we will be seeing the hash like string in the readObject method.



* That is the hardcoded password (4t1zmy7axp98irhcb42zpofejayu85s) that is revealed in the source code.
* The lab is done.