Sensitive Data Exposure

Web Application Penetration Testing

Lab 1: Source Code disclosure via backup files

Step 1: Open **https://portswigger.net/**

Step 2: Click on academy menu. Scroll down the page and fine "Information disclosure", then find "How to find and exploit information disclosure vulnerabilities" under read more option.

Step 3: Again, scroll down the page and choose "Backup file" option.

Step 4: Append "robots.txt" on the URL and get the directory name. In our case it is backup.

User-agent: *

Disallow: /backup

Step 5: Now remove robots.txt from URL and type backup and then click on file.

Step 6: We will able to get one code from where we can find multiple information like Sever Name, User Name, Password etc.

Note: Sometime instead of password, we may get configuration file, API Token etc.

Reading Material:

Robots.txt file placed in root directory by developer so that search engines like bing, yahoo, google can't crawl specified directory.