Access Control Flaws

Tuesday, October 17, 2017 7:45 AM

Role-based access control scheme:

- Role permission management
- Role assignment

If broken - user able to perform accesses that are not allowed by his/her assigned roles or allow priv escalation to an unauthorized role

LAB

Business Layer Access Control

- Delete your page as Tom by using WebScarab to intercept the ViewProfile request
- Alter the action from ViewProfile to DeleteProfile

Data Layer Access Control

- Login to my profile as Tom
- Launch WebScarab
- Click ViewProfile
- Intercept the request and modify the employee ID to that of another employee

How to bypass a path based access control scheme:

- In a path based access control scheme, an attacker can traverse a path by providing relative path information
- Therefore, an attacker can use relative paths to access files that normally are not directly accessible by anyone, or would other be denied if requested directly

*You can modify the URL in the browser to localhost:8081/WebGoat/main.jsp to take you there without being denied access.

- Alternatively, you can also intercept and modify the web page request to ../main.jsp using WebScarab

*** To complete the challenge click a file to view what directory it would put you in.
Intercept the next request to go back to the parent directory until you end up in the WebGoat folder (../../../../../). Then append (WEB-INF/spring-security.xml)