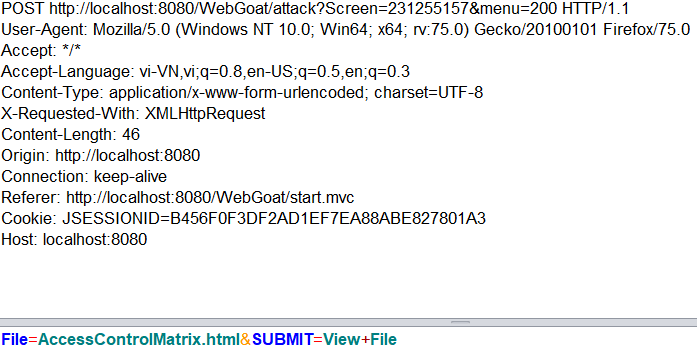
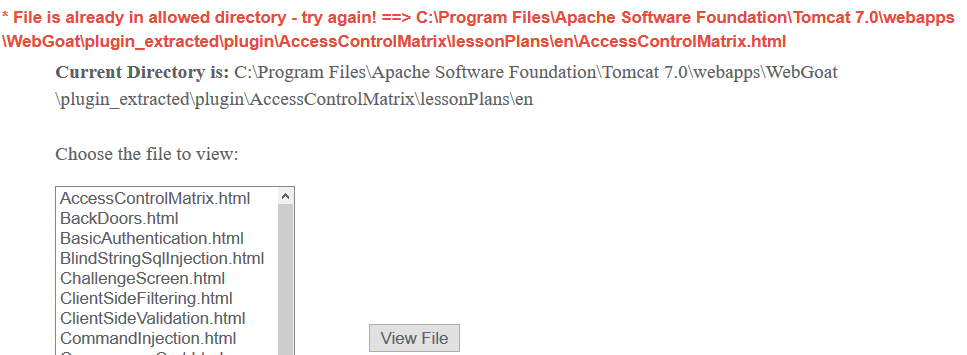
**Kịch bản:** Giả sử Role Guest có thể truy cập toàn bộ files trong thư mục lessonPlans/en, nhưng lợi dụng khả năng truy cập files và lỗ hỏng Role Access, Hacker sẽ cố gắng dùng các lệnh ../ để lùi thư mục và truy cập vào các tài nguyên mà chúng cần

**Mục tiêu Lab:** Xem nội dung file WEB-INF/spring-security.xml

**Tiến hành:**

**1. Xem cấu trúc Request và Response:**





**2. Xác định thư mục WEB-INF:** Nằm ở thư mục Root (WebGoat)

**3. Xác định cấu trúc đường dẫn:**

WebGoat/plugin\_extracted/plugin/MultiLevelLogin2/lessonPlans/en/MultiLevelLogin2.html

Như Path trên và Request gửi đi ta có thể xác định cấu trúc thuật toán sẽ là theo Path

…/en/FileNameFromRequest

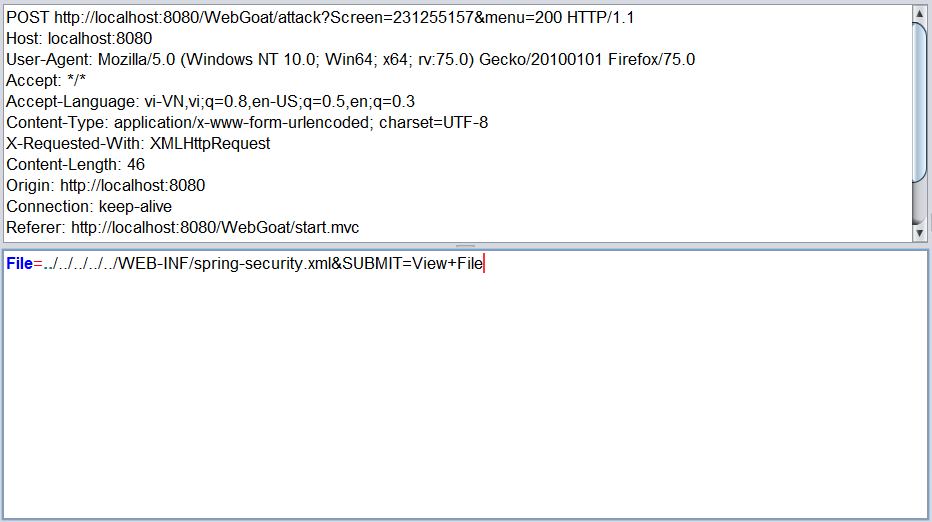
**4. Giải quyết:**

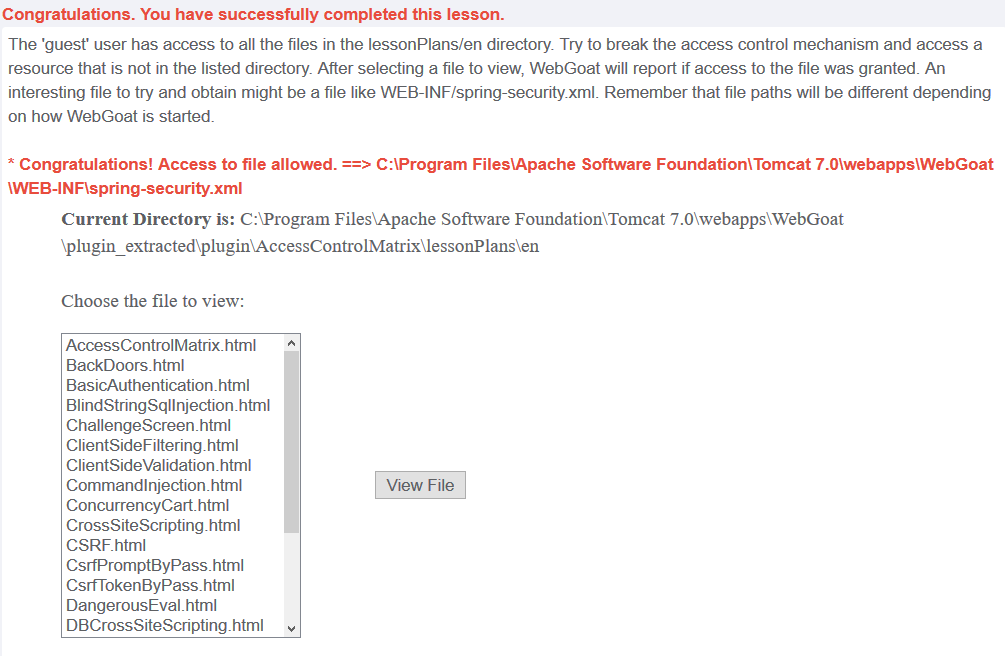
Theo cách thực thi ở trên ta có thể dùng .. để lùi file lại cho đến thư mục WebGoat và tiền hành truy cập vào WEB-INF/spring-security.xml

WebGoat**/plugin\_extracted/plugin/MultiLevelLogin2/lessonPlans/en/MultiLevelLogin2.html**

Ta sẽ thay thế thành:../../../../../WEB-INF/spring-security.xml

**5. Kết quả:**

****

****