

Lab: SQL injection vulnerability allowing login bypass - PortSwigger

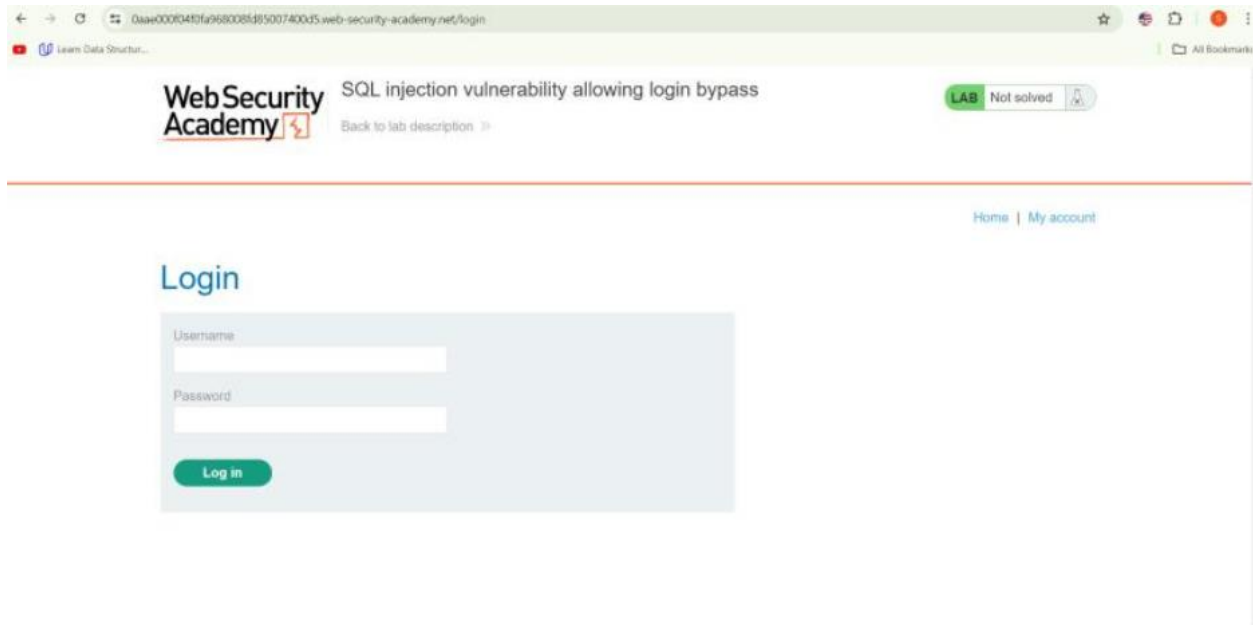
Identified and exploited a SQL injection vulnerability in a web application's login authentication process. Demonstrated how an attacker could bypass password verification using SQL comment sequences, gaining unauthorized access to administrative privileges.

Solution Implemented and Showcased in Screenshots:

Used Burp Suite to intercept and modify the login request.

Modified the username parameter, giving it the value: administrator'--

Before:



After:

The screenshot shows a web browser window with the address bar displaying a URL from web-security-academy.net. The page header includes the Web Security Academy logo, the lab title "SQL injection vulnerability allowing login bypass", a "Back to lab description" link, and a "LAB Not solved" status indicator. A navigation bar at the top right contains links for "Home" and "My account". The main content area features a "Login" section with a light blue background. This section contains two input fields: "Username" and "Password", followed by a green "Log in" button.

Web Security Academy

SQL injection vulnerability allowing login bypass

LAB Not solved

Back to lab description

Home | My account

Login

Username

Password

Log in