

Name = Aadish Rakesh Chougala

Reg number = 21BCE5296

College = Vellore institute of Technology, Chennai

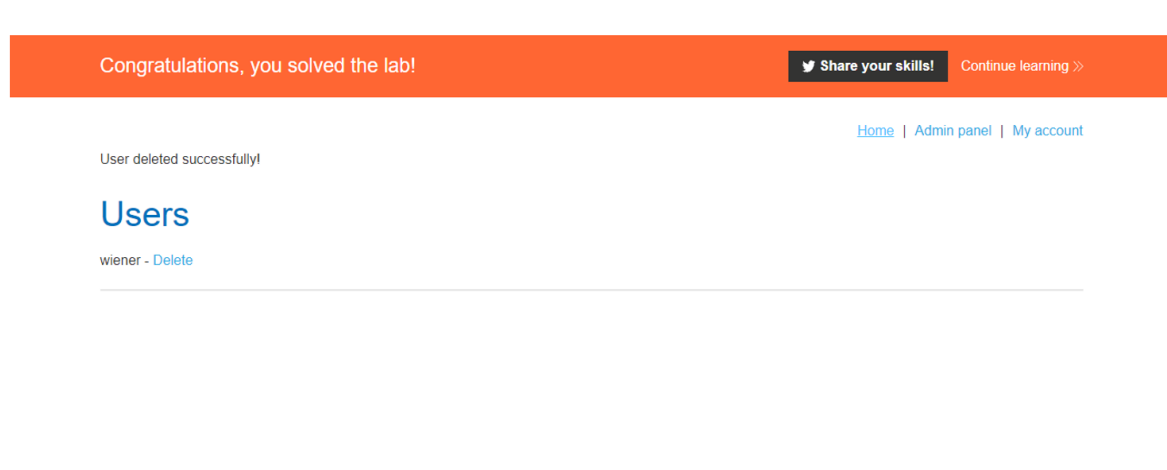
Email = aadishrakesh.chougala2021@vitstudent.ac.in

Assignment 1 = OWASP TOP 5 Vulnerabilities execution

1. Broken Access Control: When a user can actually access a resource or carry out an operation that they are not meant to be able to, there is a broken access control vulnerability.

A hidden field, cookie, or predefined query string parameter are just a few examples of the user-controllable places where some apps retain the user's access privileges or role information once they determine it at login. Based on the supplied value, the program determines further access control decisions.

Users can change the value and obtain access to features they are not supposed to, including administrative functions, making this method essentially insecure.



2. Injection: An attacker's effort to transmit data to an application in a way that modifies the intent of commands sent to an interpreter is

known as injection. The most typical instance of this is SQL injection, where an attacker submits "101 OR 1=1" rather than just "101."

The usual online environment includes several interpreters, including SQL, LDAP, operating systems, XPath, XQuery, Expression Language, and many others. Anything that combines data into a command using a "command interface" is vulnerable. Even XSS is only an HTML injection technique.

