SQL Injection Workout Student Instructions

Introduction

Welcome to the SQL Injection workout! In this workout, you will learn about how malicious actors can bypass vulnerable login pages with an SQL injection attack.

Scenario

The Trojan Cyber Arena is conducting super-secret research on something I can’t tell you about. All I am going to say is that we may or may not have a super-soldier once this research is done. There is a slight problem, though. We lost one of our classified flags that contained some metadata on the research process. The flag was held by our employee of the month (not anymore), Rick, but he forgot his credentials to the member login, and now nobody has access to the metadata. If you could find some way to log into Rick’s account and capture the flag, that would be amazing!

Accessing the Workout

From your student landing page, click the *Enter Workout* button to access UA Little Rock: Classified's Inspect workout automatically.

The Mission

You will need to find the classified flag that is locked behind a login page. Rick forgot his username and password, and the Trojan Cyber Arena hasn’t implemented password recovery for our classified members. You will need to perform an SQL injection in the web form to bypass the authentication mechanism.