S. Giridharan
CB.SC.P2CYS23006

Lab: Blind SQL injection with time delays

This lab contains a blind SQL injection vulnerability. The application uses a tracking cookie for analytics, and performs a SQL query containing the value of the submitted cookie.

The results of the SQL query are not returned, and the application does not respond any differently based on whether the query returns any rows or causes an error. However, since the query is executed synchronously, it is possible to trigger conditional time delays to infer information.

To solve the lab, exploit the SQL injection vulnerability to cause a 10 second delay. We can create a 10 second delay using the following payload,

Cookie: TrackingId=VePLHaIcZCTopO8c'||**pg_sleep(10)--;**