

## 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=VePLHalCZCTopO8c'||pg\_sleep(10)--;

The screenshot displays a web browser window with the 'Request' and 'Response' tabs open. The 'Request' tab shows the raw HTTP request, which includes a cookie with a SQL injection payload: `Cookie: TrackingId=VePLHalCZCTopO8c'||pg_sleep(10)--;`. The 'Response' tab shows the rendered HTML of the page, which is the 'Blind SQL injection with time delays' lab page. The page features a 'Web Security Academy' logo, a 'Solved' badge, and a congratulatory message: 'Congratulations, you solved the lab!'. Below this, there is a 'SHOP' section with a hanger icon and the word 'Lifestyle'. The page also includes a search bar and navigation links for 'Home' and 'My account'.