SCENARIO

The online store's analytics function seems to be vulnerable to blind SQL injection. While no direct feedback from the SQL query is visible, we can leverage conditional time delays to infer valuable information from the system.

**PROCEDURE**

1. Navigate to the primary page and, using Burp Suite, intercept the request holding the TrackingId cookie.
2. Try introducing a delay in the SQL execution using: TrackingId=x'||pg\_sleep(10)--.
3. Observe whether the application's response gets delayed by 10 seconds, indicating successful exploitation.

**PAYLOAD**

TrackingId=x'||pg\_sleep(10)--

**PROOF OF CONCEPT**

**REMEDIATION**

1. Make use of parameterized queries to avert SQL injection risks.
2. Ensure strict validation for all user inputs.
3. Employ an updated web application firewall (WAF) to recognize and block suspicious patterns.
4. Limit the permissions of SQL user accounts.
5. Educate development teams on secure coding practices.