**Feature 01**

**Título: GP|F01|TC01|Prueba de SQL Injection en el Login**

**Escenario: Intentar inyección SQL en el campo de contraseña del login**

* **Método:** POST
* **Endpoint:** /api/Auth/login
* **Headers:**
  + Content-Type: application/json
* **Body:**
* {
* "email": "' OR '1'='1",
* "password": "' OR '1'='1"
* }

**Pasos:**

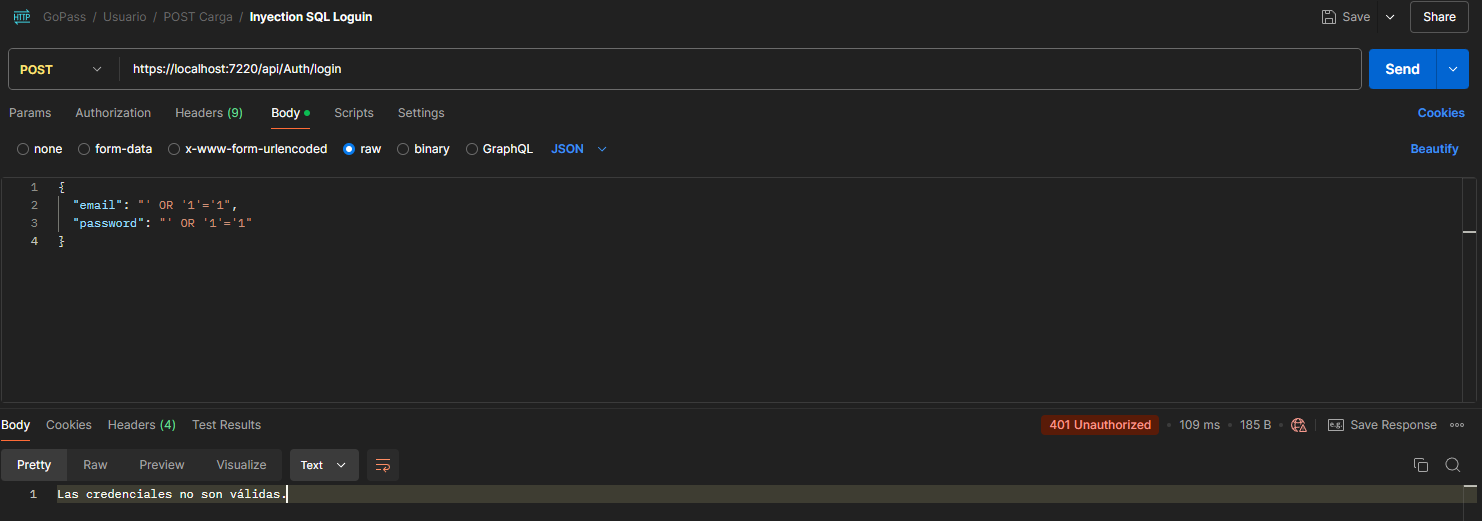
1. Haz una petición POST al endpoint de login con el cuerpo que contiene la inyección SQL en el campo de contraseña.
2. Envía la petición.
3. El sistema no debe permitir el inicio de sesión y que y no debe responder con un código 200 OK.
4. Asegúrate de que la respuesta contenga un código de error 401 Unauthorized o un mensaje de error relacionado con credenciales incorrectas.

**Resultado esperado:**

* El código de estado debe ser 401 Unauthorized.
* El sistema no debe permitir el acceso ni devolver información sensible.
* La base de datos no debe ejecutar la inyección SQL

**Título**: GP|F01|TX01| **Prueba de SQL Injection en el Login**

* **Descripción**: Verificar que el usuario puede actualizar su información personal.
* **Fecha de Ejecución**: 2024-11-04
* **Ejecutor**: Carlos Daniel Jiménez Cálcena
* Estado: Aprobado



**Título: GP|F01|TC02|Prueba de Inyección de comandos en el Login**

**Escenario: Intentar inyección de comandos en los campos del login**

* **Método:** POST
* **Endpoint:** /api/Auth/login
* **Headers:**
  + Content-Type: application/json
* **Body:**
* {
* "email": "email@example.com; ls -la",
* "password": "password; ls -la"
* }

**Pasos:**

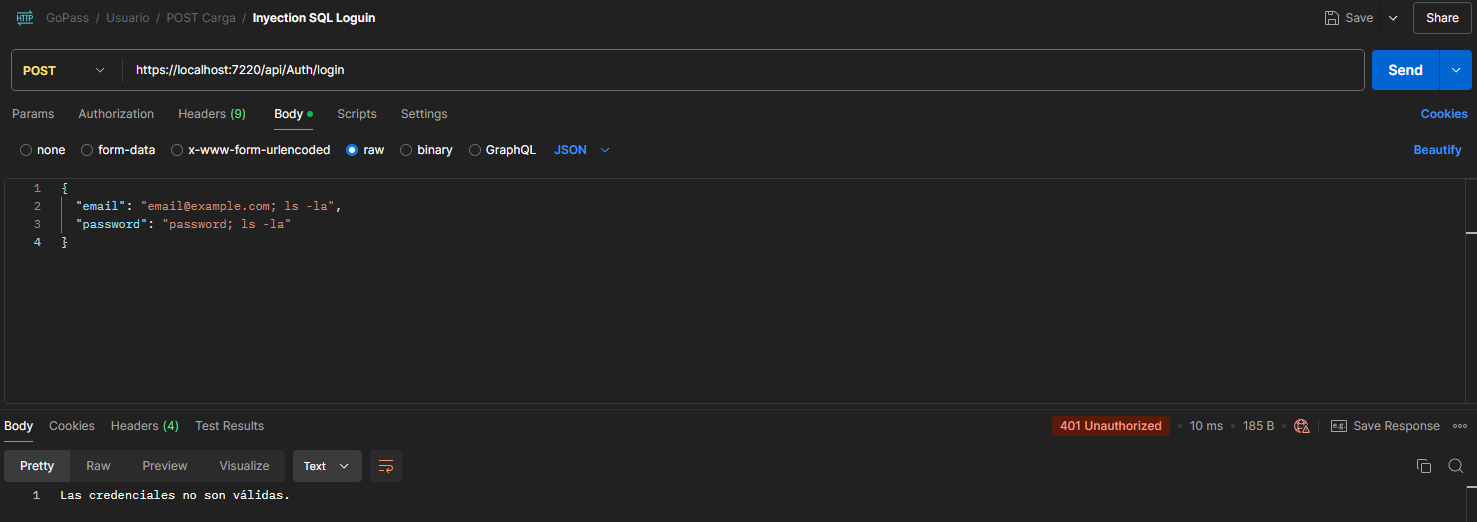
1. Haz una petición POST al endpoint de login con el cuerpo que contiene la inyección de comandos en el campo de email y de contraseña.
2. Envía la petición.
3. El sistema no debe permitir el inicio de sesión y que y no debe responder con un código 200 OK.

**Resultado esperado:**

* El código de estado debe ser 401 Unauthorized.
* El sistema no debe permitir el acceso ni devolver información sensible.
* La base de datos no debe ejecutar la inyección de comandos

**Título**: GP|F01|TX02| **Prueba de Inyección de comandos en el Login**

* **Descripción**: Verificar que el usuario puede actualizar su información personal.
* **Fecha de Ejecución**: 2024-11-04
* **Ejecutor**: Carlos Daniel Jiménez Cálcena
* Estado: Aprobado



**Título: GP|F01|TC03|Prueba de Inyección de scripts XSS en el Login**

**Escenario: Intentar inyección de comandos en los campos del login**

* **Método:** POST
* **Endpoint:** /api/Auth/login
* **Headers:**
  + Content-Type: application/json
* **Body:**
* {
* "email": "<script>alert('XSS')</script>",
* "password": "<script>alert('XSS')</script>"
* }

**Pasos:**

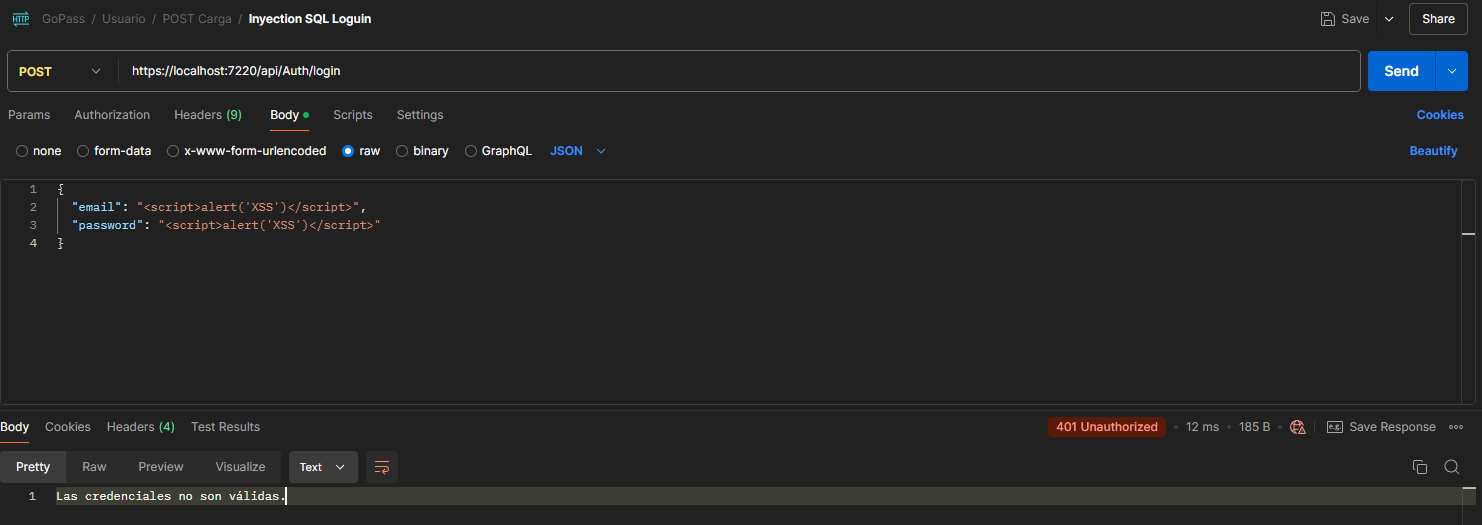
1. Haz una petición POST al endpoint de login con el cuerpo que contiene la inyección de scripts XSS en los campos de email y de contraseña.
2. Envía la petición.
3. El sistema no debe permitir el inicio de sesión y que y no debe responder con un código 200 OK.

**Resultado esperado:**

* El código de estado debe ser 401 Unauthorized.
* El sistema no debe permitir el acceso ni devolver información sensible.
* La base de datos no debe ejecutar la inyección de Scripts XSS

**Título**: GP|F01|TX03| **Prueba de Inyección de scripts XSS en el Login**

* **Descripción**: Verificar que el usuario puede actualizar su información personal.
* **Fecha de Ejecución**: 2024-11-04
* **Ejecutor**: Carlos Daniel Jiménez Cálcena
* Estado: Aprobado



**Título: GP|F01|TC04|Prueba de fuerza bruta de contraseña**

**Escenario: Intentar Prueba de fuerza bruta de contraseña**

**Método:** POST

* **Endpoint:** /api/Auth/login
* **Headers:**
  + Content-Type: application/json
* **Body:**
* {
* "email": "email@example.com",
* "password": "*{{password}}*"
* }

**Pasos:**

1. Haz una petición POST al endpoint de login con el cuerpo que contiene la un mail de ejemplo y una contraseña variable en distintos pedidos
2. Envía la petición.
3. El sistema no debe permitir el inicio de sesión y que y no debe responder con un código 200 OK.

**Resultado esperado:**

* El código de estado debe ser 401 Unauthorized.
* El sistema no debe permitir el acceso ni devolver información sensible.
* La base de datos no debe permitir el ingreso con la prueba de fuerza bruta de contraseña

**Título**: GP|F01|TX05| **Prueba de fuerza bruta de contraseña**

* **Descripción**: Verificar que el usuario puede actualizar su información personal.
* **Fecha de Ejecución**: 2024-11-04
* **Ejecutor**: Carlos Daniel Jiménez Cálcena
* Estado: Aprobado

