PortSwigger Lab

Name: Harshali Kasurde

Intern Id: 299

To solve PortSwigger lab need Kali Linux. Open Kali Linux use Firefox and browse PortSwigger then create your account. After creating an account start burpsuite, in burpsuite go to proxy and ON the Intercept. We see the burpsuite chromium, in chromium search PortSwigger you'll get your account. It is the way of connecting to PortSwigger to burpsuite for solving lab.

1. **Lab Name:** SQL Injection – Retrieve Hidden Data (WHERE clause)

2. **Vulnerability Type:** SQL Injection

3. **Summary:**

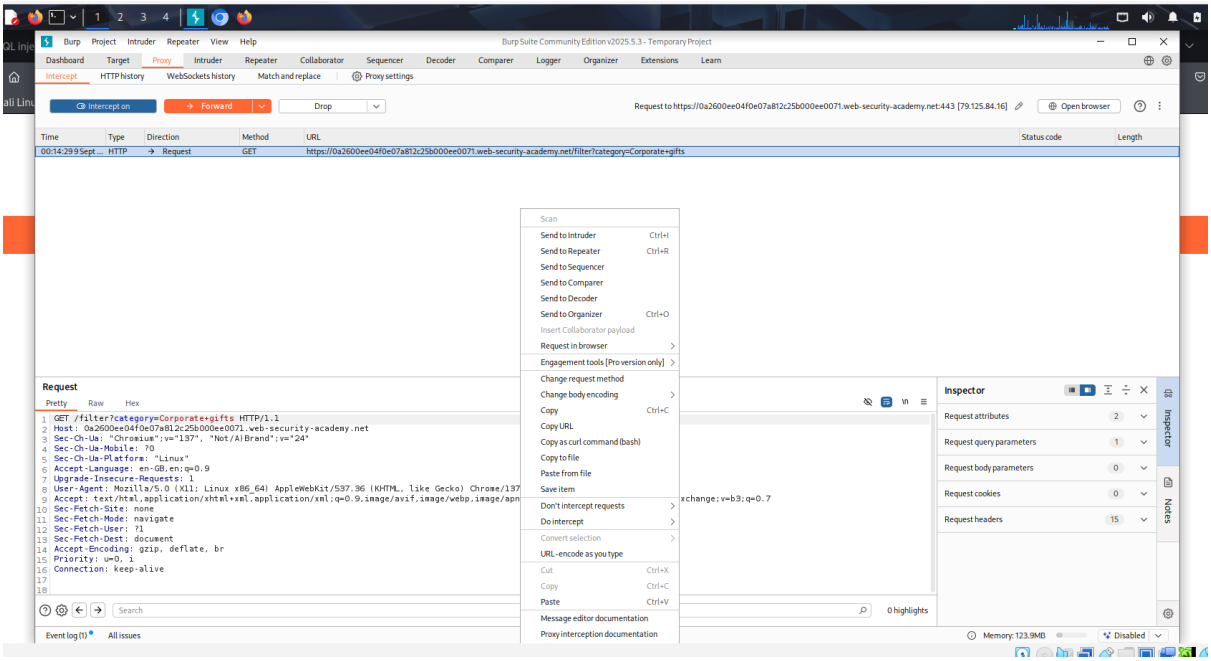
   - The website had a search/filter option (/filter?category=...).
   - Normally, it only showed products that were released (because the backend query had AND released = 1).
   - You injected malicious input (' OR 1=1--) into the category parameter.
   - This changed the query so that the released = 1 condition was bypassed.
   - As a result, the application showed hidden products (unreleased ones).
   - So, in plain meaning:
     "I found a SQL injection bug in the category filter. By adding a payload, I tricked the query to ignore the filter, so it displayed hidden products that should not have been visible."

4. **Steps:**

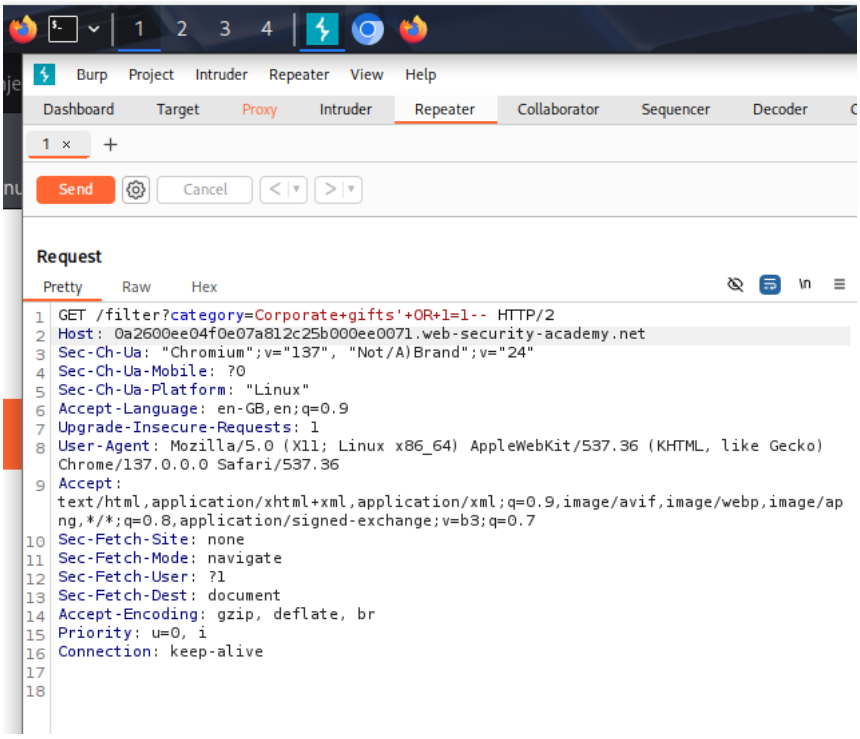
   - Navigated to the products filter page:

https://0a2600ee04f0e07a812c25b000ee0071.web-security-academy.net/filter?category=Corporate+gifts

- Sent the request to **Burp Suite Repeater** for testing.

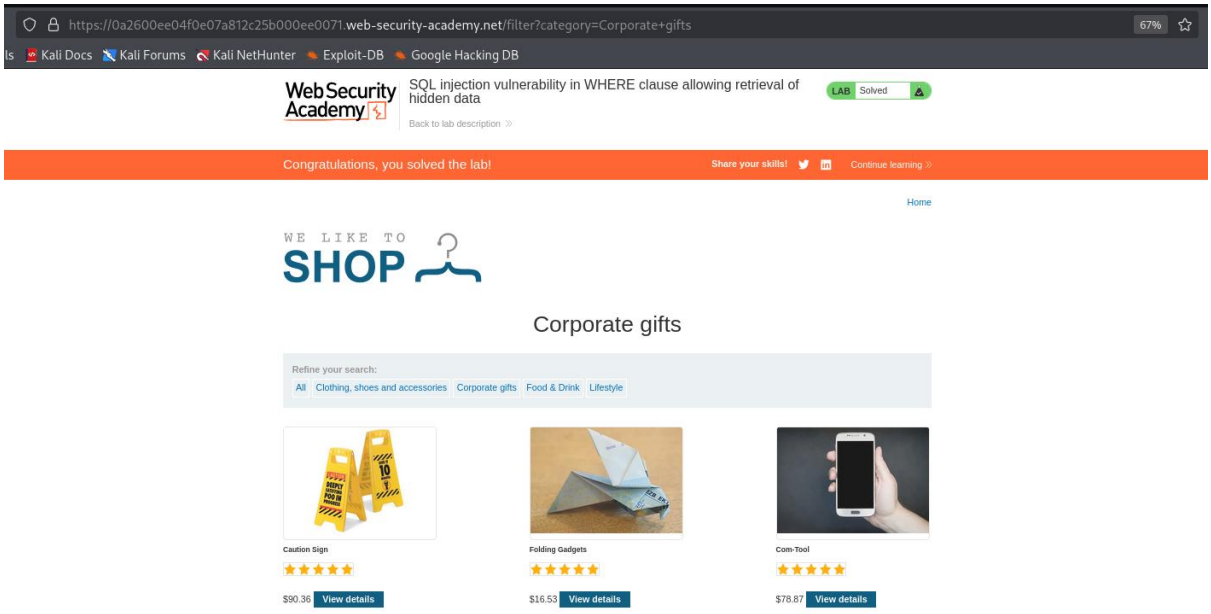


- Modified the category parameter with the payload:
  GET /filter?category=Corporate+gifts'+OR+1=1-- HTTP/1.1



- Sent the request and observed in the response that additional products appeared, including unreleased ones.
- Verified in the browser that the lab was marked as Solved.

5. **Screenshot:**
   https://0a2600ee04f0e07a812c25b000ee0071.web-security-academy.net/filter?category=Corporate+gifts'+OR+1=1--



   Before injection: Only 2 products.

   After injection: Extra products added to the list.

6. **Date Completed:** 07-09-2025