# Họ và tên: Trần Minh Triết

# MSSV: SE172241

# Class: IA1702

# Question:

1. **What distinguishes Time-Based SQL Injection from other SQL injection techniques? Explain how an attacker can use time delays in SQL queries to extract information from a database, and why this method is particularly useful when dealing with blind SQL injection scenarios where no data is returned in the web application's responses.**

* Time-Based SQL Injection is a type of SQL injection technique that exploits database vulnerabilities by introducing time delays in SQL queries.
* Attackers can use time delays by injecting specific SQL statements that force the database to wait for a specified period before responding.
* This technique is particularly useful in blind SQL injection scenarios where the application doesn't display database information directly. Since the attacker can't see the data in the web application's responses, they leverage time delays to indirectly extract information.

1. **Describe the process of executing a Time-Based SQL Injection attack on a vulnerable web application. What are the key steps in crafting a SQL query that causes a deliberate delay in the database response.**

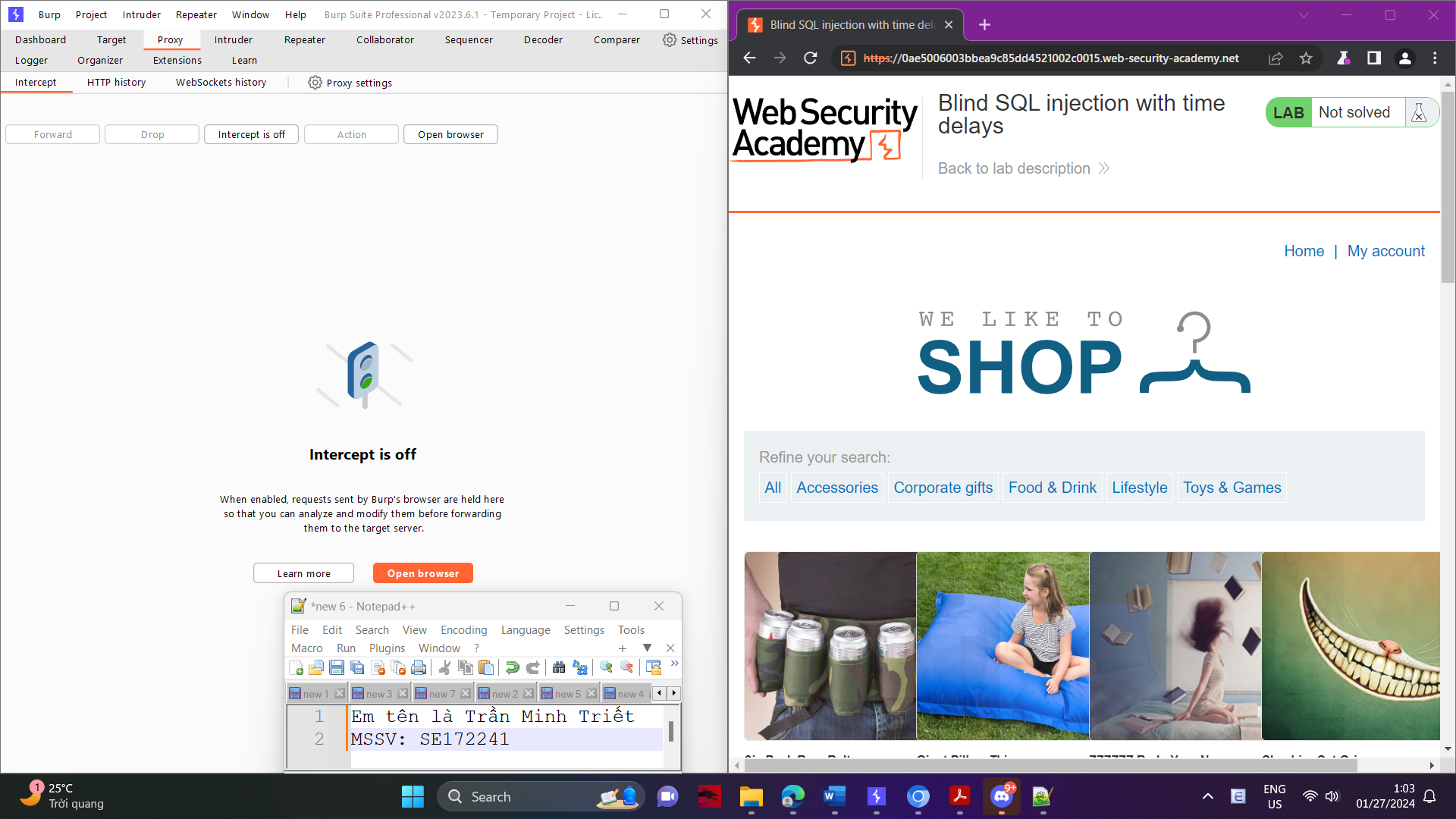
Executing a Time-Based SQL Injection attack involves injecting malicious SQL statements into user inputs, exploiting vulnerabilities in the web application's database.

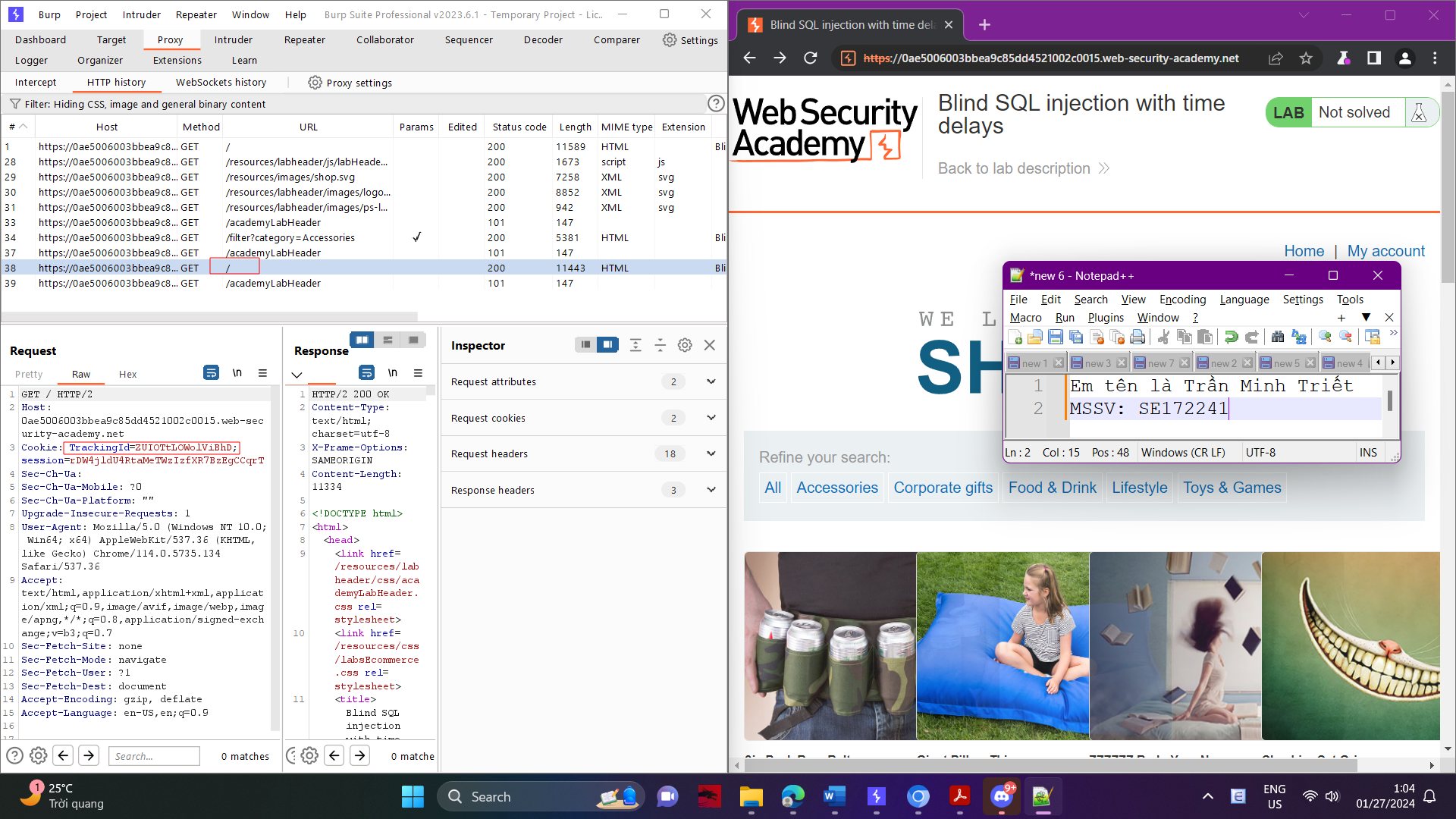
Key Step:

* **Identify Vulnerable Parameter**: Locate a user-input field vulnerable to SQL injection on the web application, such as a search box or login form.
* **Inject Time Delay**: Craft a malicious SQL query by injecting a time-delay function.
* **Observe Response Time**: Submit the manipulated input and observe the web application's response time.
* **Iterate and Extract Information**: Refine the injected queries to extract specific information about the database.

**Lab 10: Blind SQL injection with time delays**

Visit the front page of the shop, and use Burp Suite to intercept and modify the request containing the TrackingId cookie.





Modify the TrackingId cookie, changing it to:

'||pg\_sleep(10)—

