**LAB07 SQL injection and avoiding**

Name Students ID Class

**System environment for developing**

|  |  |  |  |
| --- | --- | --- | --- |
| Resources | Sender(attacker) | Receiver(victim) | Homepage |
| OS |  |  |  |
| IP address |  |  |  |
| URL |  |  |  |
| Web browser |  |  |  |
| CSS language |  |  |  |
| Web server |  |  |  |
| Web application |  |  |  |
| DB server script |  |  |  |
| Others |  |  |  |

[Model A]

1. Search web application database query model for SQL injection test
2. Code full process of web application database query module for SQL injection test
3. Code full process of web application database query module for avoiding SQL injection
4. Explain your test environment of software for test

[Model B]

1. How to prevent and protect SQLI
2. Explain your test environment of software for test

==================================================================

Reference site

<https://www.w3schools.com/sql/sql_injection.asp>

<https://developer.okta.com/blog/2020/06/15/sql-injection-in-php>

<https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/>

<https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/05-Testing_for_SQL_Injection>