Tìm hiểu về SQL Injection: <https://www.w3schools.com/sql/sql_injection.asp>

https://vi.wikipedia.org/wiki/SQL\_injection

Hướng dẫn cài đặt DVWA trên Ubuntu: <https://www.shellvoide.com/hacks/setup-hacking-environment-install-dvwa-application-on-linux>

Tìm hiểu về giao thức http (GET&POST): <https://www.codehub.vn/Khac-Biet-Giua-Phuong-Thuc-POST-va-GET>

Top 10 OWASP 2017: <https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf>

Các dạng tấn công SQL Injection: <https://www.jamviet.com/2015/07/sql-injection-la-gi-tim-hieu-cach-thuc-tan-cong-sql-injection.html>

<https://vi.wikipedia.org/wiki/SQL_injection>

Tham khảo cách tấn công SQL Injection bằng câu truy vấn luôn trả về TRUE: <http://sqlfiddle.com/#!9/3691b3/9>

Khung bên trái ta tạo bảng có: id, email. Password

CREATE TABLE `users` (

`id` INT NOT NULL AUTO\_INCREMENT,

`email` VARCHAR(100) NULL,

`password` VARCHAR(50) NULL,

PRIMARY KEY (`id`)

);

INSERT INTO `users` (`email`, `password`) VALUES ('thanhvan123@gmail.com', md5('thanhvan2807'));

INSERT INTO `users` (`email`, `password`) VALUES ('testing@gmail.com', md5('testing123'));

Bên phải nhập câu truy vấn để kết quả trả về luôn đúng, trong trường hợp này, ta nhập câu truy vấn sau:

SELECT \* FROM users WHERE email = “nhapgicungduoc” OR 1 = 1 – ‘;

Kết quả trả về là thông tin id, email, password đã được mã hóa của bảng users