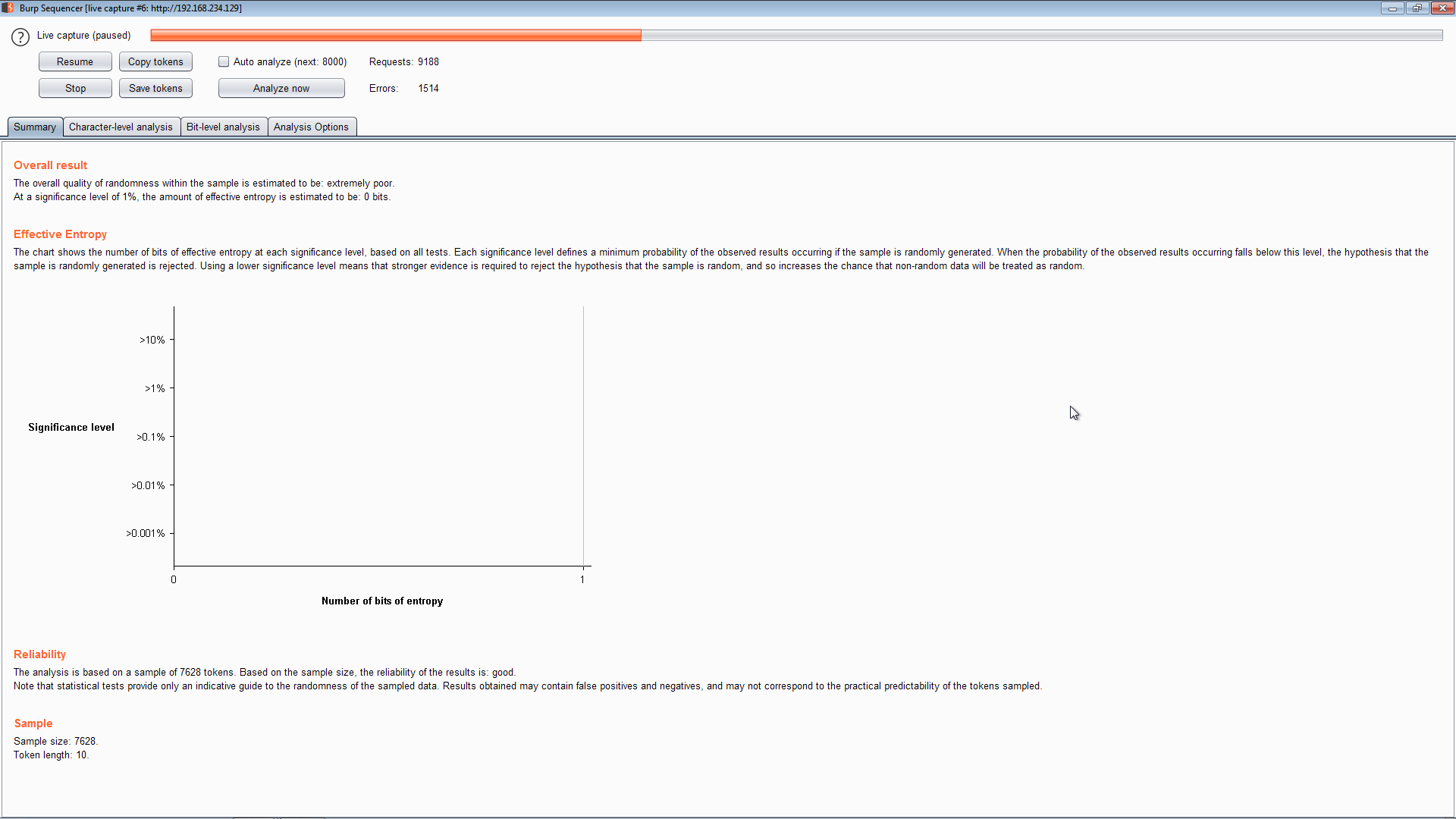
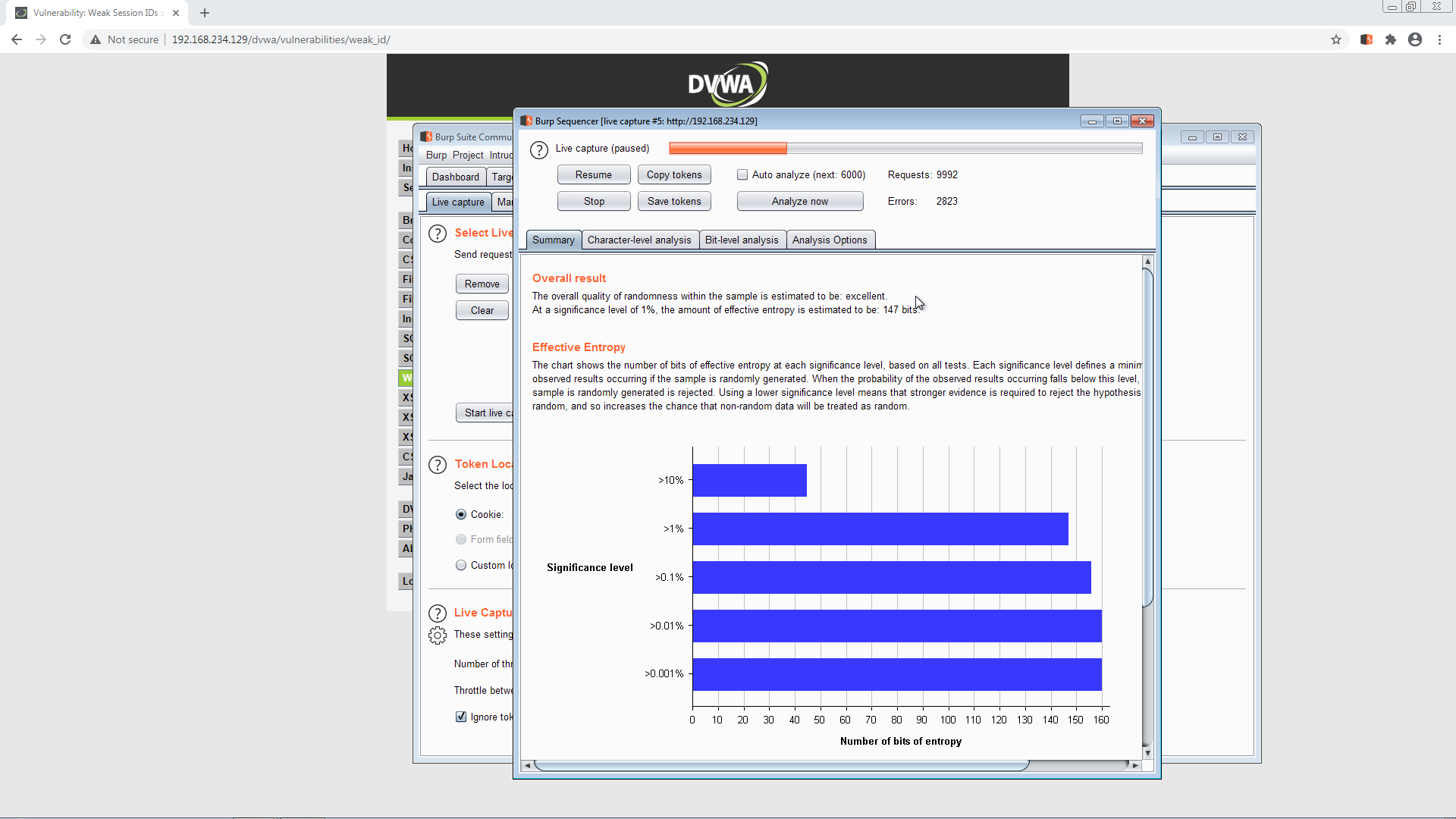
|  |  |
| --- | --- |
| Class & Module | IAW301  Lab 22: Weak Session Cookie analysis |
| Name | Nguyễn Đức Kiên |
| IC No. | HE141763 |
| Date & Time | November 3, 2020 |

#### Exercise 1.1 Medium Security



**Exercise 1.2 Impossible Security**



2, Comment về phương pháp generate dvwaSession của 3 mức độ (Medium, High, Impossible). Và phương pháp đó có đảm bảo tính random hay không.

Vd.: Low - Ở mực security low. DVWA generate dvwaSession bằng cách lấy session trước đó cộng thêm 1.

Phương pháp này không an toàn.

Medium: ở mức này session đã dùng hàm date.Now() để generate cookie từ ngày hiện tại sang giây, nhìn có vẻ phức tạp nhưng khi đã biết thì lại khá dễ đoán.

🡪 Phương pháp không an toàn.

High: mức này cookie đã được generate bằng md5 hash function, khi decode ra ta sẽ có id ở dạng số tự nhiên như “2, 3, 4…”

🡪 tuy nhiên phương pháp này theo em đã đủ an toàn với các user ở tầm thấp với chuyên môn an toàn thông tin không quá cao.

Impossible: sau khi check source code ta thấy session này sử dụng ham st.rand() với time() được lấy từ thời điểm hiện tại bao gồm ngày tháng năm giờ phút giây khá phức tạp, time() được cộng thêm 3600 để tăng độ phức tạp, sau đó được mã hóa tiếp bằng hàm sha1(), gần như rất rất khó để decode

🡪 phương pháp này đảm bảo tính random và an toàn cần thiết để giữ cookie bảo mật.

3, Tại sao Session lại cần phải random.

- Một khi đã có được cookie, người tấn công có thể truy cập vào tài khoản người dùng một cách dễ dàng mà không cần phải qua các bước authenticate như điền tên đăng nhập và mật khẩu, vì chức năng chính của cookie là để lưu trữ các phiên đăng nhập, do đó việc random session là rất cần thiết để tránh việc bị tấn công.