**EXPERIMENT-7**

**Student’s Name: Kanishk Soni UID: 20BCS9398**

**Section/Group: 707\_WM\_B Subject Code: 20CSP-338**

**Subject Name: WMS Lab Date of performance:27/10/2022**

**Branch: BE CSE Semester:5th**

**Aim:** Implementation of Session hijacking attack on http-enabled website

**Objective:**  To Identify vulnerable session cookies.

**Software/Hardware Requirement:**Burp Suite

**Discussion:** **Session Hijacking:**

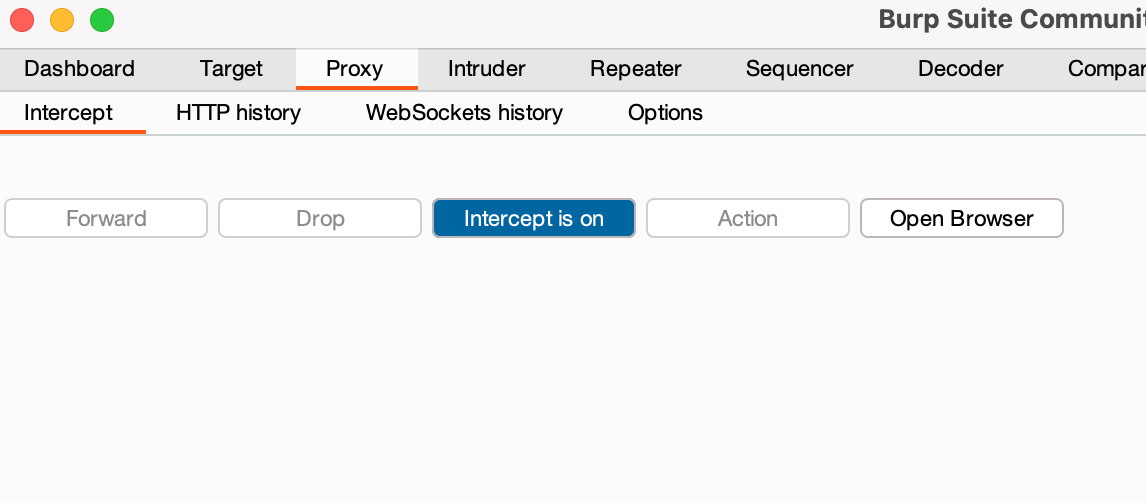
The Session Hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token. Because http communication uses many different TCP connections, the web server needs a method to recognize every user’s connections. The most useful method depends on a token that the Web Server sends to the client browser after a successful client authentication.

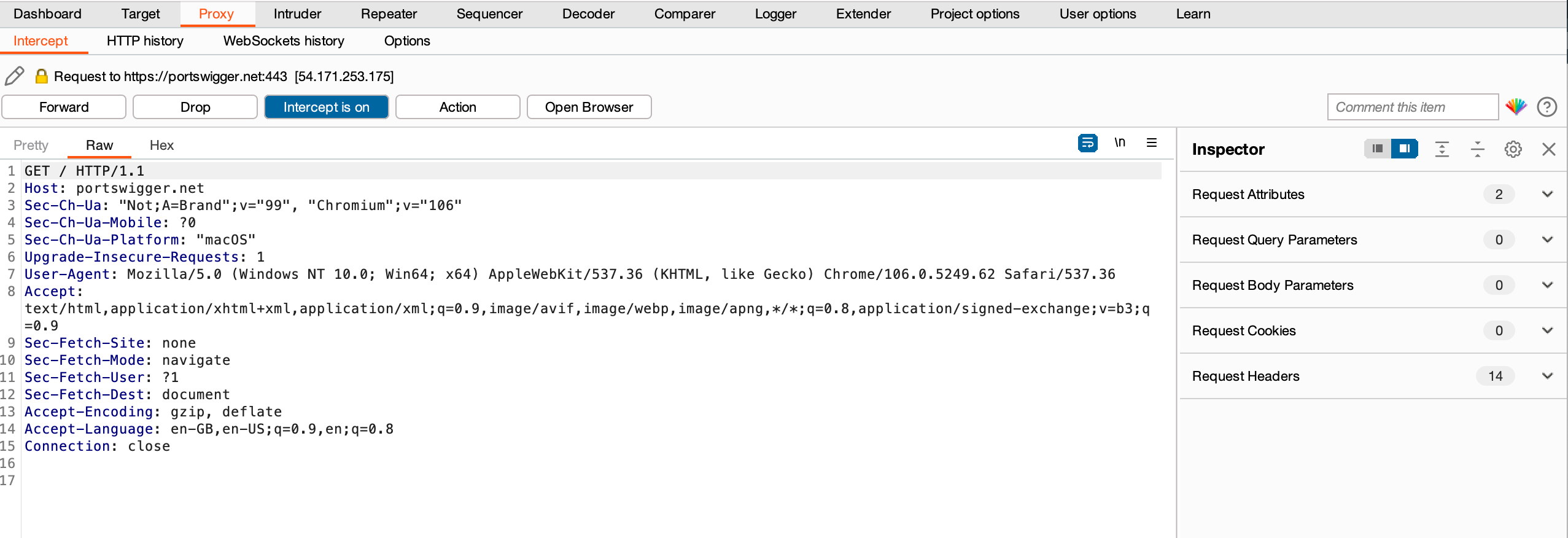
The Session Hijacking attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server.

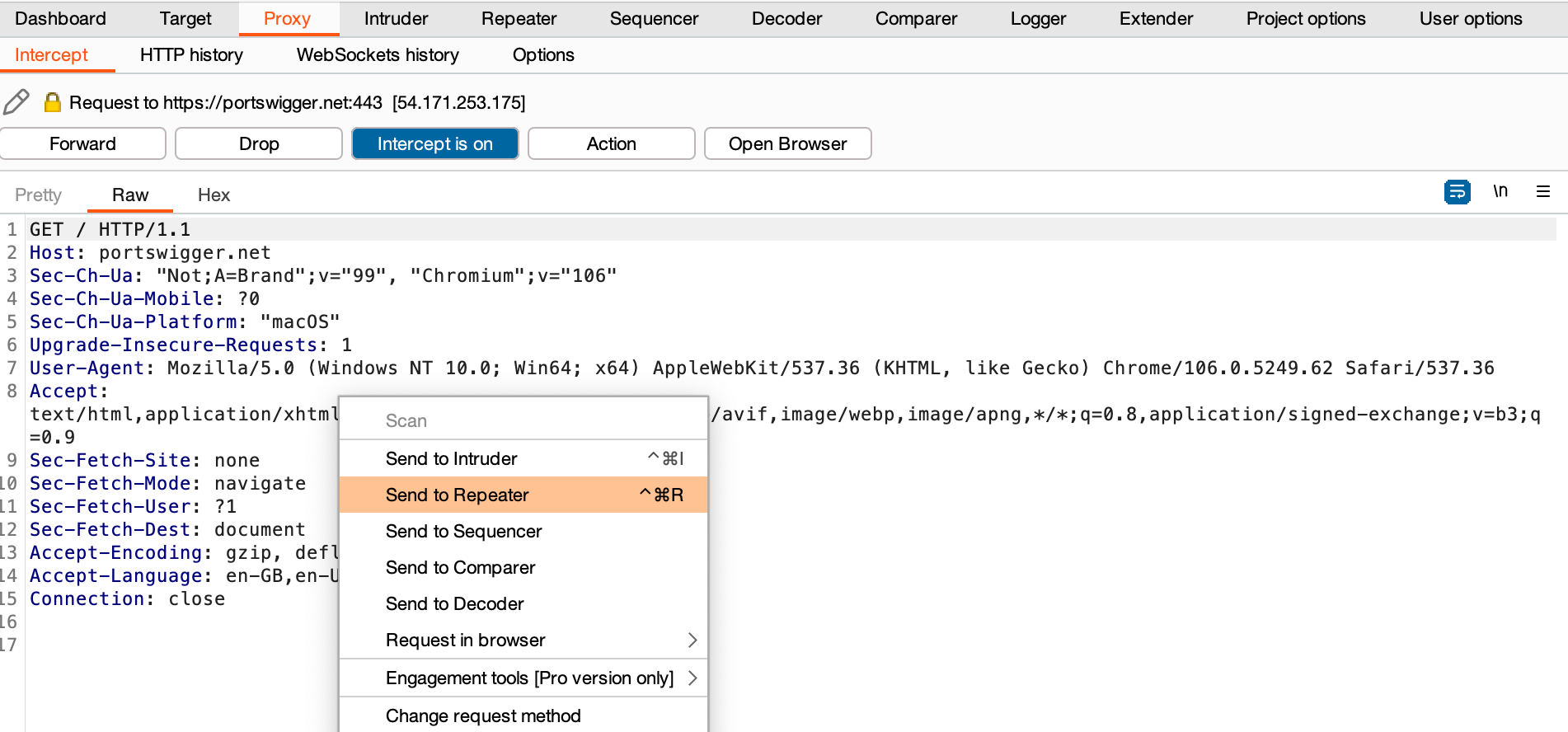
The session token could be compromised in different ways; the most common are:

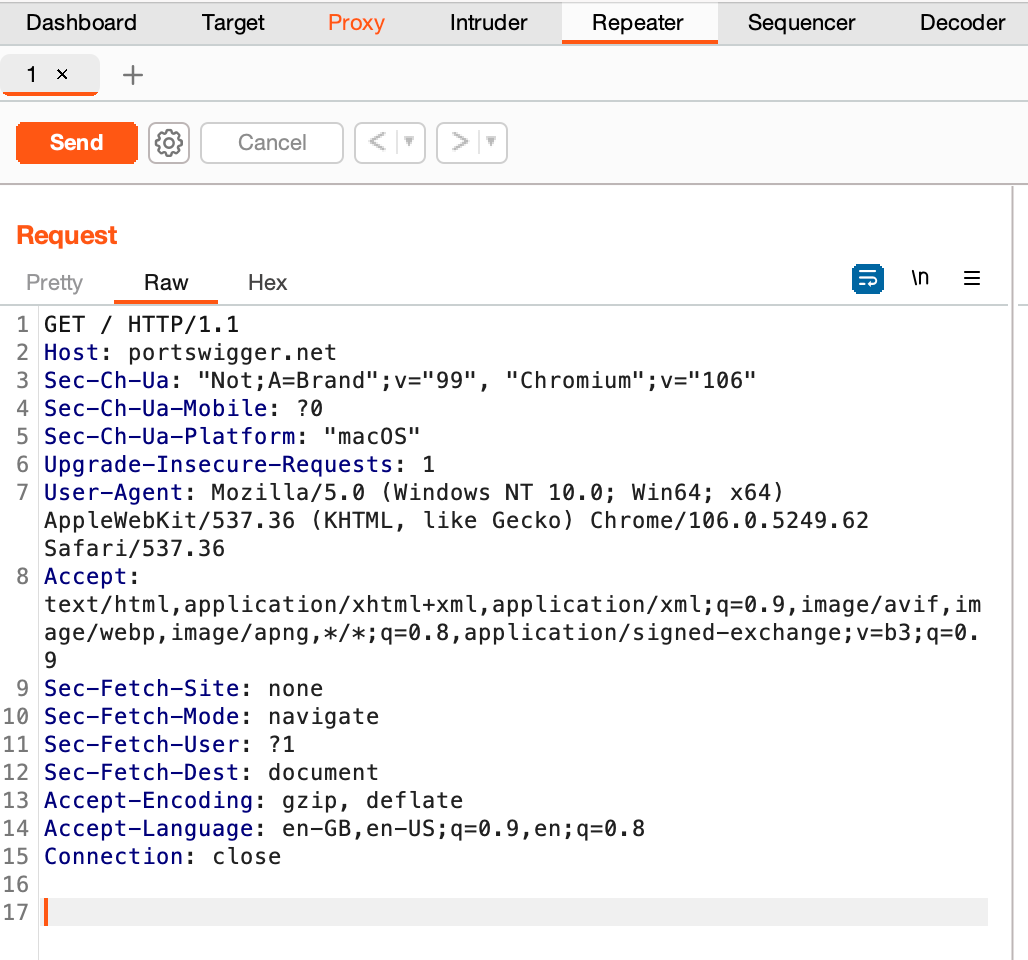
* Predictable session token;
* Session Sniffing;
* Client-side attacks (XSS, malicious JavaScript Codes, Trojans, etc);
* [Man-in-the-middle attack](https://owasp.org/www-community/attacks/Man-in-the-middle_attack)
* [Man-in-the-browser attack](https://owasp.org/www-community/attacks/Man-in-the-browser_attack)

**Steps/Method/Coding:**



After visiting [https://portswigger.net](https://portswigger.net,)  






**Learning Outcomes:**

1. In the above experiment we have learnt that using session hijacking attack how the token session can be manipulated.