## **Session hijacking**

## 

## **What is session -**

## **- After Validating user with on basis of username and password, server assign him a string value called \*\*Session ID\*\***

## **- These Session ID's are used to identify USERs.**

## **- After Validating user's credentials a fresh Session ID is assigned to User Every time.**

## **- This Session ID is Stored in Form of Cookies on User's Browser.**

## 

## **What is cookies -**

## **- Cookies are the values which help server to validate requests for each user or session**

## **- Cookies Contain User Identity Details, Personalization, and other information used to identify user and computer on network.**

## 

## **Why session hijacking works -**

## **-> Insecure Session Handling**

## **-> Insecure Session Termination**

## **-> Weak Session ID generation algorithms - linear algo. used such as time or IP address for generating session ID.**

## **-> Unencrypted Session ID's**

## 

## **Types of session hijacking -**

## **- Active - In Active Session Hijacking, Attacker steal Session Cookies from victim's Browser and use those cookies. Also known Application-Level Hijacking.**

## **- Passive - A passive Attack uses sniffers on the network, allowing attacker to obtain info. to log on as a valid user and enjoy the privileges.**

## **Also called Network-Level Hijacking.**

## 

## **Methods to obtain session id -**

## **- Predict Session**

## **- MITM = Man In The Middle Attack**

## **- MITB = Man In The Browser Attack => Hijack Victims Browser - BeEF**

## **- Network Sniffing**

## **- Malware Attack**

## **- XSS = Cross-Site Scripting => Executing Malicious Script to fetch User Cookies, when Victim Browse a Website script executes and Attacker get Session ID.**

## **- Proxy Server => Attacker use their System as a Proxy Server for Victim so that all the traffic pass through their machine, and they can extract juicy info**

## **from requests and responses.**

## 

## **We will use cookie editor extension for practical part.**