**Module 11**

**Session Hijacking**

**What is Session Hijacking?**

When ever user log in, server authenticate the user and respond the user with session token. In that session token all type of detail are available about the user. Every session token has limited time.

Session hijacking is a part of web application, in this term we will study that web session can be compromised by attacker by just taking cookie and session token.

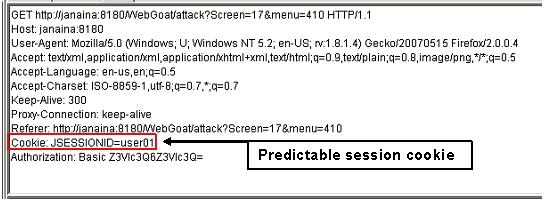
Web session token is given by web server to the client when user log in the page and get authenticate.

Hacker spoof the token and use it to get authentication login in his browser.

**Types of Session Hijacking**

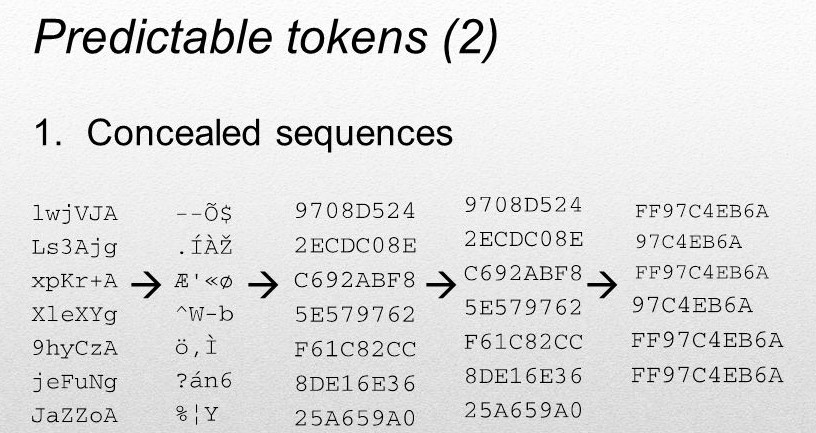
**Predictable session token**

When developer create their own session token which is not in encrypted form, that token may be a predictable for user or hacker.

****

Here we can see that the token carry user serial no which is predictable he can change the token no and got access of another user.

More example of predictable session token



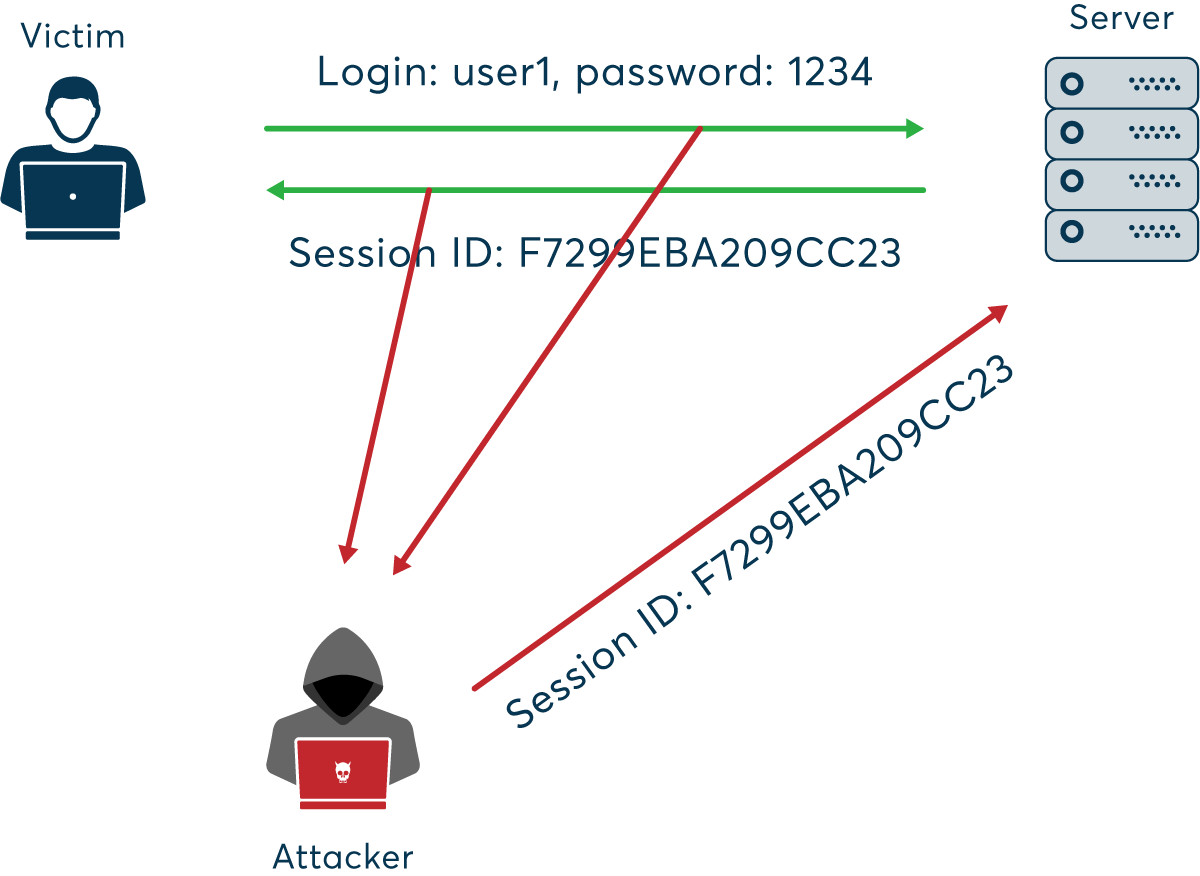
**Session Sniffing**

As we know that sniffing is possible to do,

So session sniffing is also can be done by attacker.

HTTP sniffing is possible but HTTPS sniffing is not possible to sniff, because it is highly encrypted form.

Wireshark can be used to sniff the token



We can use here burp which is best tool for web application testing .

Lets perform session Hijacking.

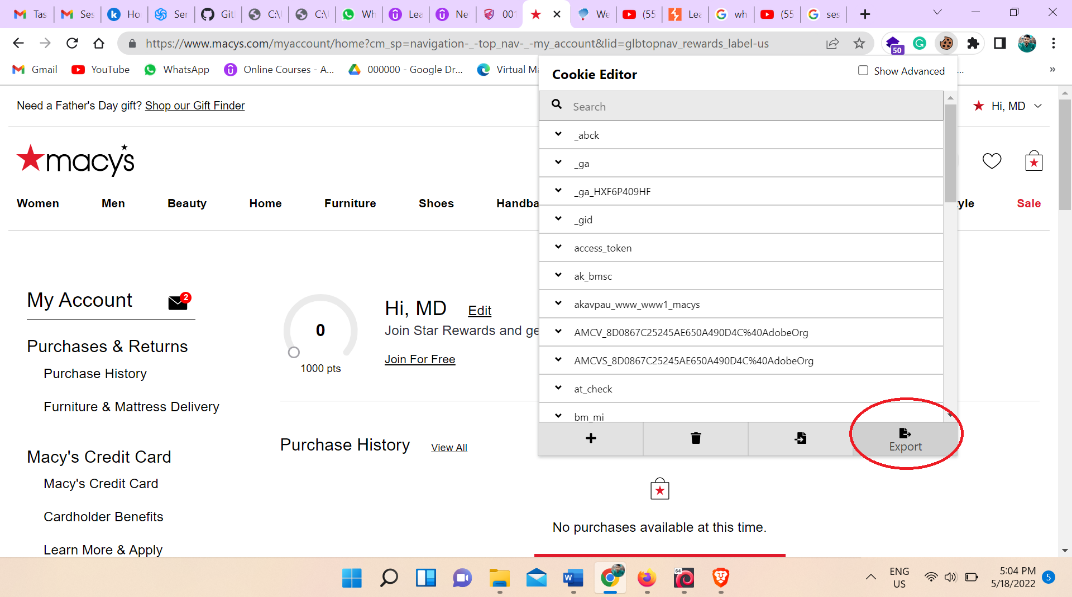
Source :- <https://www.macys.com/account/signin>

We will perform this attack on this website.

We wil take help of cookie editor extension, first add it to the browser like chrome and firefox.

Lets create an account and get sign in on the given website.

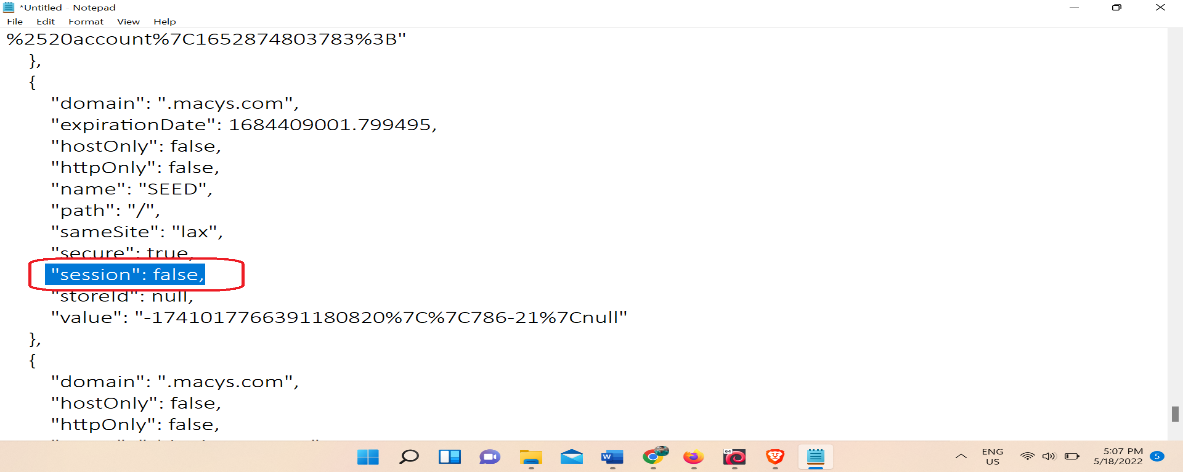
Than export the session from cookie editor extension.

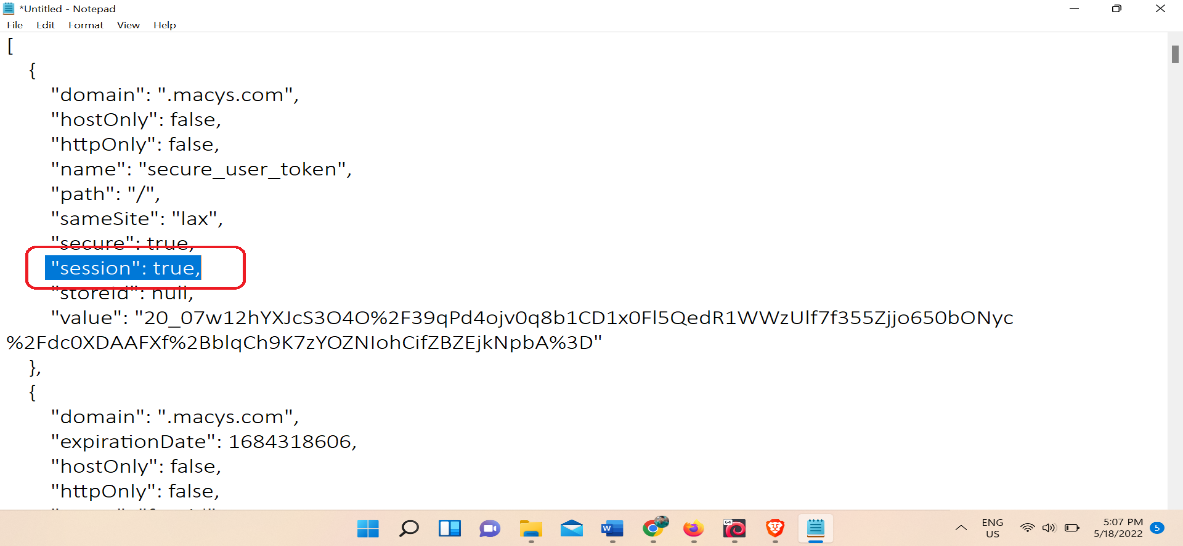


Than open text editor and paste the cookie.

Make the session true from all the place.

As it is show below image.





Open Another browser and go to the log in page of same webite.

Open the cookie editor delete all the cookie and click on import and paste here edited token text.

Than refresh the page. We can see user account get logged in.

**Know lets see it by manually.**

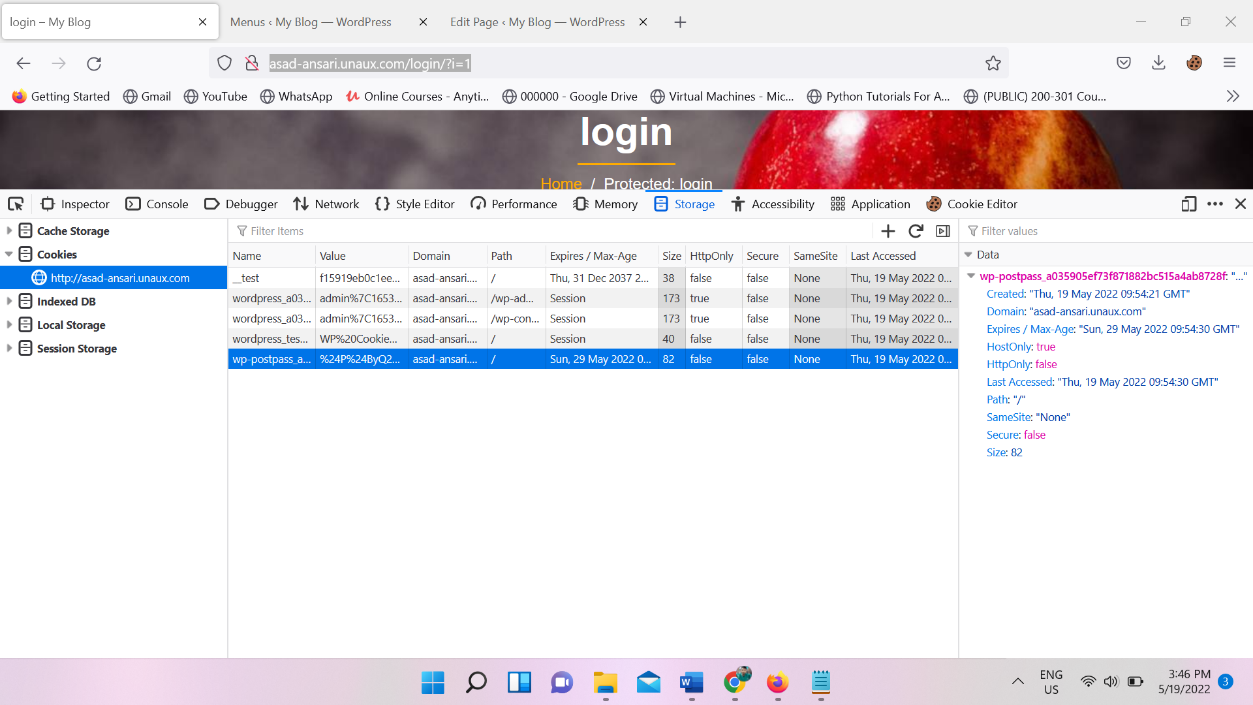
Lets perform it on another website

Source :- <http://asad-ansari.unaux.com/>

**Created by me and Onkar(our digital marketing team member).**

Go to the log in page and log in with password than go to the inspect of web page copy the all cookie.

Open the same link on different browser and create the cookie of same name and paste the same token.



We can see it on above pic.

And refresh the page we can see, we are logged in.

One more website is vulnerable we can try here, But severity is nothing.

Site:- <https://www.bigbasket.com/>

It is vulnerable and it is live website………

Try all the process what ever is taught on above.

Another website is vulnerable is shop clue

Site:- <https://bazaar.shopclues.com/>

**Mitigation**

Always use HTPPS with SSL service.