الsession معروف انها الinteraction بين الcomputer والuser زى الlogin session
او بين two devices

الsession hijacking
فى حاجة عندنا اسمها session hijacking devices .. ديه عبارة عن server or client بتبقبل
الاجهزة الى مش مفروض انها تكون موجودة فى ال session على انها اجهزة متاح انها تكون موجودة
وبتبقى حاجة legal .. حاجة شرعية
ال session hijacking ليه انواع .. مثال :
الPredictable token
وده بعد ما عملية الlogin تتم الattacker بيدخل ياخد شوية بيانات بأستخدام two techniques
الsniffing tool و brute force

الCountermeasures for session hijacking

فى عندنا Basic Counter Measures و Advanced Counter Measures
هنتكلم الاول عن Basic Counter Measures
==========

- فى الpasswords والvalidations الى عندنا لازم نستخدم حروف وارقام و special characters

- لازم نعمل regenerate للsession id لما ننتقل from secured to unsecured content

- نستخدم session timeout. زى المواقع الى لما بيلاقى مفيش بينك وبينها interaction لمدة ربع ساعة
مثلا بيقولك your session terminated وان انت لازم تعمل login من جديد

- نستخدم الSSL الى هو Secure Sockets Layer وطرق تانية عشان
نعمل encryption للsession ID

- الافضل اننا نستخدم VPN الى هيا virtual private network عن الpublic network وده عشان
نحمى الsystem بتاعنا من الsnooping الى هو التجسس .. وبتكون بين two or more devices

- ونستخدم الPOST method بدل الGET method وساعتها هنقدر نمنع انه يتعمل rewrite للل
URL