Session Fixation

كتير بنسمع عن "session fixation" وده نوع من الهجمات اللي بيستغل فيها الهاكرز طريقة هندلتك للـ sessions. الفكرة ببساطة إن الهاكر يحاول يثبت session ID معين للضحية. وبعد ما الضحية يعمل login، الهاكر بيستخدم نفس الـ session ID علشان يدخل على الاكونت بتاعه من غير ما يطلب منه باسورد تاني.

### **طب إزاي الهجمة بتحصل؟**

1. الهاكر بيبدأ بإنه يروح على ويب سايت وياخد session ID. أحيانًا ممكن الهاكر يكون هو اللي بيحدد الـ ID ده بنفسه أو ياخده من الـ application .
2. الهاكر ممكن يبعت للضحية لينك فيه الـ session ID اللي هو جهزه وأول ما الضحية يدخل على اللينك ويعمل login، الـ application بيستخدم نفس الـ session ID اللي الهاكر جهزه.
3. بعد ما الضحية يعمل login بنفس الـ session ID، الهاكر يقدر يستخدمه عشان يوصل لنفس الـ session، وبالتالي يقدر يدخل على حساب الضحية ويعمل أي حاجه هو عايزها باسم الضحية.

### **تعالى نوضح اكتر بمثال عملي**

تخيل إن في تطبيق بيسمح انك تبعت الـ session ID في اللينك. الهاكر ممكن يبعت لينك للضحية بشكل "https://example.com/login.php?SESSIONID=123456". لما الضحية يدخل على اللينك ده ويعمل login، الapplication مش بيغير الـ session ID وبيستخدم نفس الid اللي في اللينك. هنا الهاكر يقدر يدخل بنفس الاكونت لأنه عنده نفس الـ session ID.

### **طب ازاي نحمي نفسنا من الهجمة دي**

علشان تمنع session fixation، لازم تعمل حاجات زي:

* **تجدد الـ Session ID بعد كل** login: أول ما الuser يعمل login، بنعمل regenerate للـ session ID باستخدام session()->regenerate() علشان نتأكد إنه محدش يقدر يستخدم ID قديم.
* **تستخدم Secure و HttpOnly Cookies**: علشان نضمن إن الـ session cookies مش بتتسرق أو تتعدل من الـ browser .