Broken Authentication: Session Management

Manieren van misbruik

1. **Session Hijacking**
   Het doel hierbij is dat een hacker jouw session ID weet te stelen.
   Dit kan bijvoorbeeld door met cross-site-scripting een stuk code te injecteren die afgaat nadat een gebruiker is ingelogd. Dit stuk code can vervolgens de session ID pakken en opsturen naar de hacker.
2. **Session ID URL Rewriting**
   Het idee hierbij is dat een hacker met behulp van de session ID die opgeslagen is in de URL verder kan gaan met jouw session.
   De URL kan bijvoorbeeld zichtbaar worden voor anderen als je op een onbeveiligde wifi connectie zit.
3. **Session Fixation**
   Deze manier werkt op websites die niet de session ID's vervangen zodra een gebruiker inlogt.
   Het idee is dat een hacker van te voren vaststelt wat de session ID is die de gebruiker heeft als deze inlogt op de website.
   Dit wordt gedaan doordat deze session ID opgeslagen is in de URL van een link die de hacker naar zijn slachtoffer stuurt. Het slachtoffer volgt deze link en logt in op de betreffende website. Hierna kan de hacker verder gaan op de ingelogde session van zijn slachtoffer.

Session Misbruik tegen gaan:

1. **Leg vast hoe lang een session mag duren en wanneer deze stopt.**
   Bijv. als een bepaalde periode van inactiviteit verstreken is, als een tijdsperiode verstreken is of als je uitlogt.
   Probeer deze instelling te matchen aan je gebruikers om zo veiligheid en gemak te optimaliseren.
2. **Vervang en verklaar session ID's en ander tokens direct ongeldig nadat ze gebruikt of afgelopen zijn.**
   Vervang je session ID nadat een gebruikt inlogt, zo voorkom je session fixation.
   Maak session ID's en tokens direct ongeldig om hergebruik door hackers tegen te gaan.
3. **Stop session ID's niet in de URL van je website.**
   Het is te makkelijk voor hackers om dit te misbruiken voor zowel session fixation als session ID URL rewriting. Sla ze op in cookies.

Cookie management in Identity

https://docs.identityserver.io/en/latest/topics/signin.html
https://daanstolp.nl/articles/2018/cookies-tokens-and-session-lifetime-with-identity-server/