# Weaknesses in Cookie Lifecycle



Dawid Czagan
SECURITY INSTRUCTOR
@dawidczagan



#### Overview



Importance of regeneration

Demo

Server-side invalidation

Demo



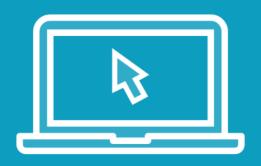
# Importance of Regeneration

- 1. User is logged out: SID=abc
- 2. Attacker learns user's SID
- 3. User logs in: SID=abc
- 4. Attacker can impersonate a user

Make sure SID is regenerated (step 3)



#### Demo



Is my web application vulnerable?



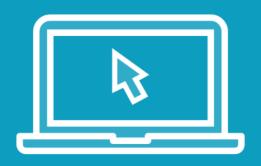
## Server-side Invalidation

- 1. User logs out: SID deleted from browser
- 2. No server-side invalidation
- 3. It's still possible to access user's account

Remember about server-side invalidation



#### Demo



Is my web application vulnerable?



### Summary



Regenerate cookies with sensitive data

Remember about server-side invalidation

