Securing Authentication, Sessions and Access Cont.

- **Access Control:** Fine-grained logic to determine R/W permissions per user or object.
- Determines if a user is authorized to perform an action
- Often implemented as roles
- Avoid assumptions as to how users might interact with the application

https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

Safe-handling input data across boundaries

- Stored procedures, parameterized queries for SQL Injection
- Validation at each boundary / input point
- Whitelist/blacklist
- Sanitization
- Challenges of expressive languages on the web