BBC
Design + Engineering

# SECURE CODING PRACTICES

**PRINCIPAL SOFTWARE ENGINEER, SECURITY CHAMPION**

ONLINE TECHNOLOGY GROUP

# SOFTWARE SECURITY AND RISK PRINCIPLES

- Confidentiality
- Integrity
- Availability

# SECURE CODING CHECKLIST

- Input validations
- Session management
- Authentication and password management
- Error handling and logging
- Data protection
- Database security

# INPUT VALIDATIONS

- Validate input data on client and server side
- Validate for expected data type, length, range
- Centralised input validation routine
- Pay attention to special characters ( < > ? . & ‘ “ )

# SESSION MANAGEMENT

- Use server or framework's session management controls
- Session timeout period
- No concurrent logins with the same User ID
- Logout

# AUTHENTICATION AND PASSWORD MANAGEMENT

- Authentication must be on server side
- Centralised authentication control
- Use HTTP POST request parameter
- Password management controls

# ERROR HANDLING AND LOGGING

- Do not disclose sensitive data in error responses and in logs
- Implement generic and custom error pages
- Ensure logging contain important log event data e.g. validation, authentication failures
- Restrict access to logs

# DATABASE SECURITY

- User secure credentials for database access
- Use parameterised queries
- Lowest possible level of privilege
- Close connection as soon as possible

# DATA PROTECTION

- Implement least privileges
- Encrypt highly sensitive information (at rest and in transit)
- Do not include sensitive information in HTTP GET request
- Set data retention policy
- Do not reveal backend system or other sensitive information in comments

# GENERAL CODING PRACTICES

- Review and validate third party code/libraries
- Restrict access to privilege/sensitive data
- Always validate input data
- Do not store or disclose sensitive information in logs
- Explicitly close database connections, file connections after use
- Logout functionality should fully terminate the associated session or connection

# CODE ANALYSIS TOOLS

- ECL – Eclipse Emma plugin
- Intellij inspect code
- JaCoCo, Cobertura
- SonarSource – JS analysis
- SonarLint
- ESLint

## THANK YOU

Email – shilpa.danwe@bbc.co.uk
Slack - #shilpadanwe