Web Application
ASSESSMENT CHECKLIST

INFORMATION GATHERING:

- Manual application discovery
- Automated discovery
- Harvesting public information

SESSION MANAGEMENT:

- Session fixation
- Weak session token quality
- Weak session token management
- Weak logout
- Cross-site request forgery
- Weak CORS
- Session token protection
- No session timeout
- Session encryption (SSL/TLS)

AUTHENTICATION:

- Password strength enforcement
- Authentication bypass
- Unauthenticated URL access
- Password brute force
- Default account

AUTHORIZATION:

- Insecure authorization design
- Only client side authorization
- Variable manipulation
- Direct access to resources

CLIENT SIDE ATTACKS:

- Reflected XSS
- Stored XSS
- DOM based XSS
- Wrong content-type
- HTTP header injection
- Malicious URL redirect
- Clickjacking

SERVER SIDE ATTACKS:

- LFI
- RFI
- XML External Entity injection
- OS command injection
- SQL injection
- Malicious file upload

BUSINESS LOGIC ATTACKS:

- Malware upload
- Enabling debug mode
- User lockout
- Weak process design

INFORMATION DISCLOSURE:

- Backup files
- Leaking stack-traces
- Comments
- Path disclosure
- Directory listing
- Credentials sent to the browser