

Application Security Assessment**Services Data Sheet****Application Security Assessment**

While testing the application, CyberQ will follow, but not be limited to, the following:

- Unvalidated inputs
- Broken Access control
- Broken Account and Session management
- Cross-site scripting (also referred to as XSS)
- Buffer overflow
- Injection flaws
- Improper error handling.
- Denial of service attacks.
- Remote File inclusion
- Cross Site Request Forgery(CSRF)

Physical and Environmental Review

- Check for Inadequacy of Physical and Environmental controls
- A visit to be conducted at the identified locations to review procedures followed regarding
 - Visitor Handling,
 - Physical Access Control,
 - Security Awareness,
 - Fire Handling Procedures
 - Material movement control, etc.