Security Testing Field Guide 9AAD135248
Quality Assurance & Test - Standards & Practices

<table>
<thead>
<tr>
<th>Department</th>
<th>GF-IS ADM Applications Performance &amp; Excellence (APE)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approver</td>
<td>Giulio Bitella, Global Department Manager</td>
</tr>
<tr>
<td>Owner</td>
<td>Anna Pietras, Quality Assurance Lead (QA)</td>
</tr>
</tbody>
</table>
Field guide to Non-functional testing: Security testing in ABB

Security is a key element that should be considered throughout the application development lifecycle, especially when it is designed to deal with critical business data and resources. Security must be considered and tested throughout the project lifecycle of any application. Security testing ensures that the system under test is capable of protecting the data and maintaining its functionality.

Security Testing is type of non-functional testing (white box or black box) that is done to check whether the application or the product is secured or not. Usually it is an authorized simulated attack on a system/server/application/device that looks for security weaknesses, potentially gaining access to the system’s features and data.

Link to Security Services intranet page

---

**AFTER READING IT**

Understand why application security is important and how to engage InfoSec teams to verify security of your application.

---

**WHEN IS IT USED**

Delivery phase

---

**WHO PREPARES IT**

IS Quality Assurance Lead with support from:
- Project Manager
- Scrum Development team

---

**HOW TO DO IT:**

In ABB we should consider security testing as integral part of overall testing process for applications developed internally or bought from the third party vendors. All applications should be mandatory scanned by automatic scanners and penetration testing should be performed by designated teams from Information Security.

1. All applications should have obligatory security testing as part of overall testing strategy. Security requirements must be included in non-functional requirements specification or in the project backlog.
2. Development teams should perform manual security testing (e.g. using Burp Suite) and perform vulnerability scanning using Qualys tools. Only combination of manual testing and automatic security scans will reduce number of potential vulnerabilities.
3. To get access to Qualys please contact Web Application Scanning (WAS) team. You can integrate your continuous integration environment with Qualys and run vulnerabilities scans as part of your CI/CD process. Alternatively, you can request ad-hoc scanning requests of your test, stage or prod environment (here).
4. You will get a technical report that includes information how to fix vulnerabilities the application owner to remediate the existing vulnerabilities. When vulnerabilities are fixed by development team your application will be scanned again.
5. When the above is done you should additionally perform manual penetration testing. This type of testing is done at the end of the development process. It should be performed on final version of the code to be implemented into production environment. Please contact in advance Security Resilience Testing Services (SRTS) team by ticket in ServiceNow. After testing is done SRTS will present you with a detailed report of all findings/observations. This will be organized by criticality level and contain all the technical data on how the test was performed, each vulnerability found, and the recommended remediation actions.
Six security concepts:

SIX IMPORTANT SECURITY CONCEPTS THAT SHOULD BE CONSIDERED DURING WEB APPLICATION DEVELOPMENT PHASE AND TESTED:

CONFIDENTIALITY.
Vital data should be accessible only to authorized users and information is secure from theft.

AUTHENTICATION
It helps establish the identity of the user.

AUTHORIZATION
Specific users should only get access to authorized functions.

INTEGRITY
The application and its data is not altered in course of time during transmission.

AVAILABILITY
Communication and information should be readily available, as required.

NON-REPUTATION
It helps prevent later denial of an action that happened.

WHAT TO DO TO ENSURE YOU ARE COMPLIANT WITH SIX SECURITY CONCEPTS?
READ OWASP APPLICATION SECURITY VERIFICATION STANDARD (HERE)
Contact: anna.pietras@pl.abb.com

Information Systems
Applications Performance Excellence
QA & Test

For the latest distributable version of this and other Quality Assurance & Test standards please visit this link to ABB Library.