

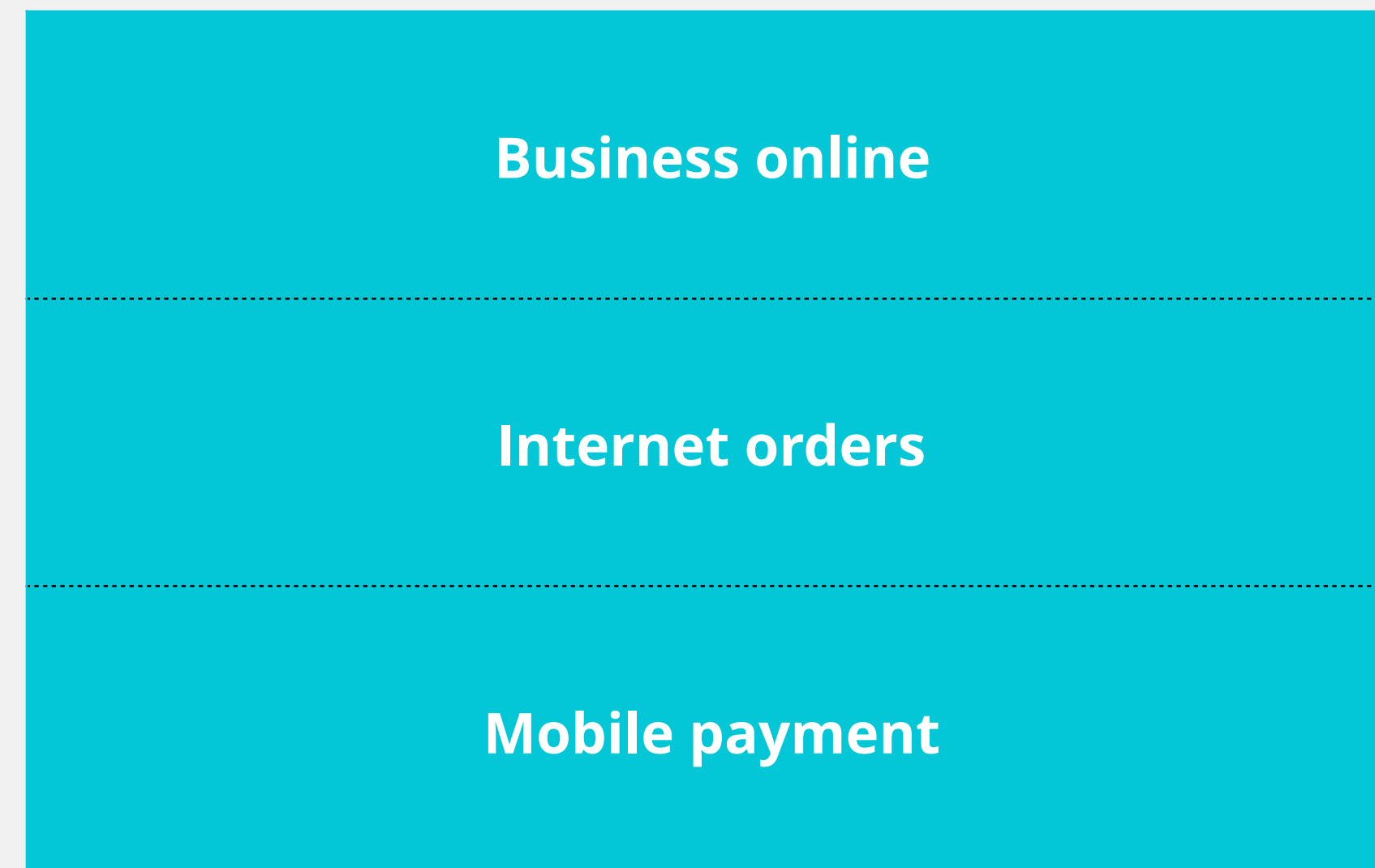
ThoughtWorks®

QA MEET BUILD SECURITY IN DNA



CHANGING

Industry and life are changing

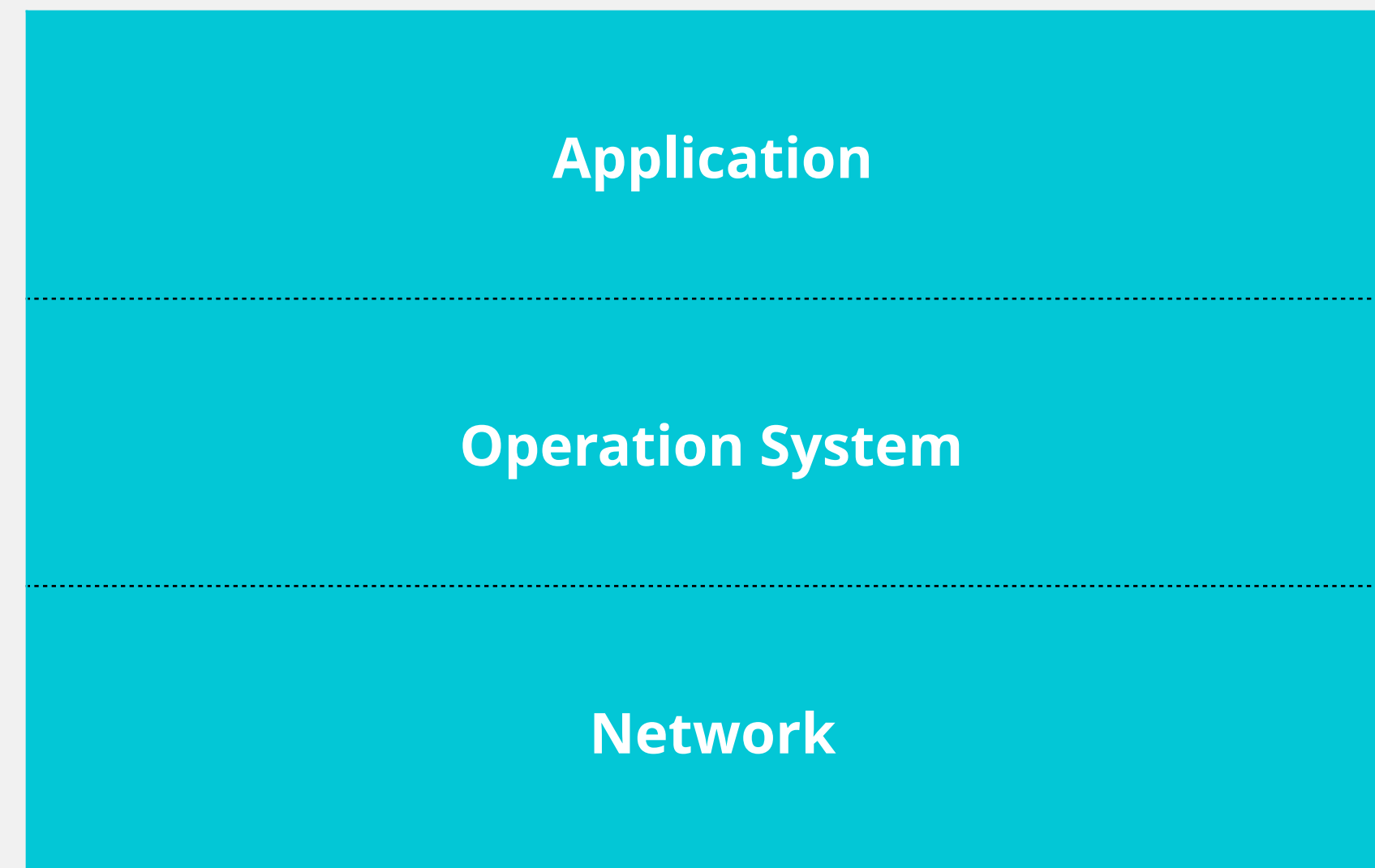


~ 62.2%

~ 216.4%

World Quality Report 2015/16

Threat is changing



~ 80%

World Quality Report 2015/16

BSI OVERVIEW

安全人员培养

注入安全意识和基因，帮助企业培养各个安全角色和安全团队



既有角色



既有流程



BSI 流程注入



注入安全的行为和基因，帮助建立全生命周期的安全研发流程



BSI PROCESS INJECTION

01. Project Plan

Security Training

Based on OWASP TOP 10, common web security issues, solution and precaution will be introduced with live demos to make every trainee fully understand the security risks.

Tips: The training content covers over 90% of the application security threats.



This training will raise trainee security awareness and basic security understanding as well as a preparation for the development stage of BSI practice.



- *A1 Injection*
- *A2 Broken Authentication and Session Management*
- *A3 Cross-Site Scripting*
- *A4 Broken Access Control*
- *A5 Security Misconfiguration*
- *A6 Sensitive Data Exposure*
- *A7 Insufficient Attack Protection - NEW*
- *A8 Cross-Site Request Forgery*
- *A9 Using Components with Known Vulnerabilities*
- *A10 Underprotected APIs - NEW*

02. Requirement Analysis

Threat Modelling

Using attack tree, DREAD and STRIDE model to identify, quantify, and address the security risks associated with an application.

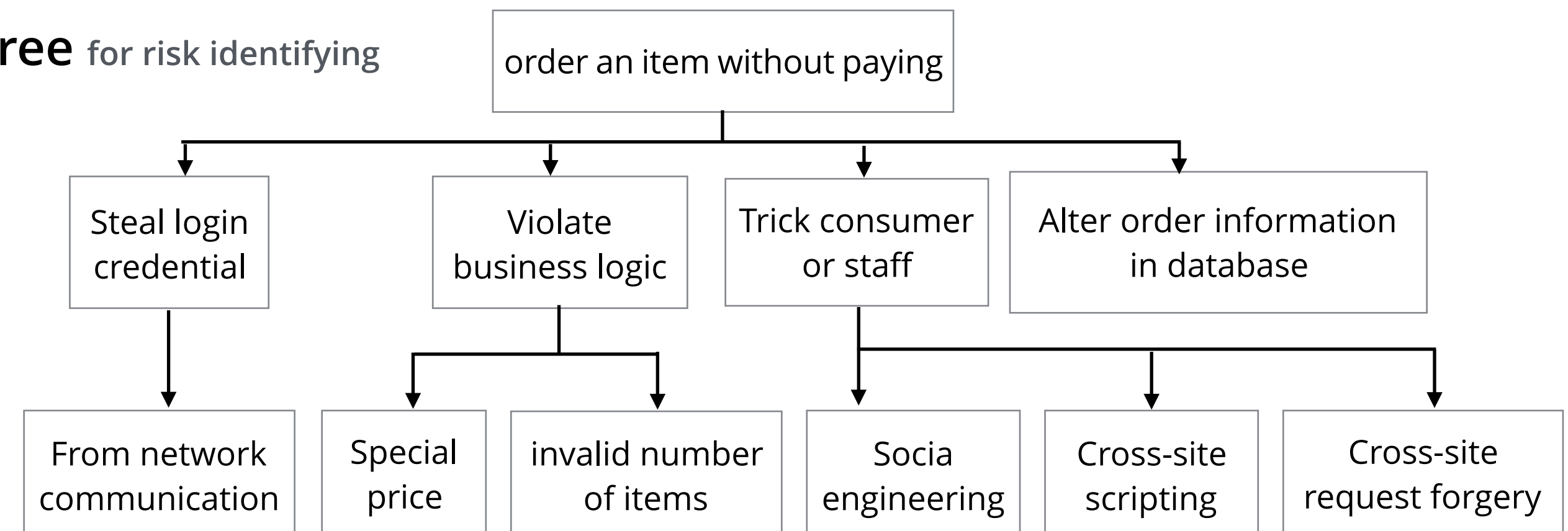
DREAD for risk quantifying

Risk	Questions	Risk Rating
Damage potential	How great is the damage if the vulnerability is exploited?	High: 12-15 Medium: 8-11 Low: 0-7 When a given threat is assessed using DREAD, each category is assigned a value between 1,2 and 3. The sum of all categories for a given exploit can be used to set the risk rating.
Reproducibility	How easy is it to reproduce the attack?	
Exploitability	How easy is it to launch an attack?	
Affected users	How many users are affected?	
Discoverability	How easy is it to find the vulnerability?	

STRIDE for threat identifying

Threat	Description
Spoofing	Forge as another user
Tampering	Malicious modification of data
Repudiation	Denial of the truth of something
Information disclosure	Disclose of information to individuals who aren't supposed to have it
Denial of service	Deny access to valid users
Elevation privilege	Unprivileged user gains privileged access

Attack tree for risk identifying



Example: E-commerce order payment attack tree model

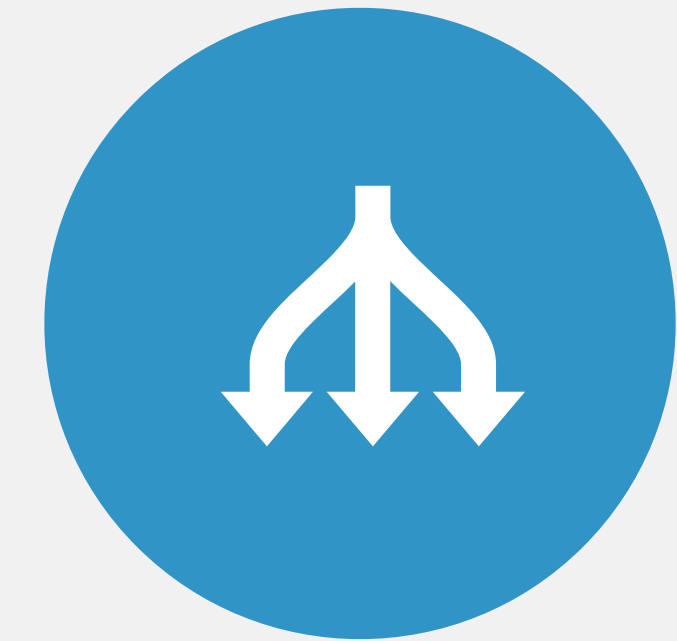
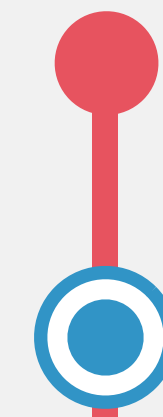
03. Architecture Design

- Identify security risks in IT infrastructure when it carries the software.

Although security is fully considered in software development phase, security risks may be introduced in IT topology design and implementation.



Step 2: IT Infrastructure Topology Review



Step 1: Software Architecture Review

- Identify security risks in software architecture

Layered structure or front-end and back-end separating are mostly adopted when software architecture to be designed as scalable and high performance, this step is to check whether all security risks have been fully considered in software architecture design.

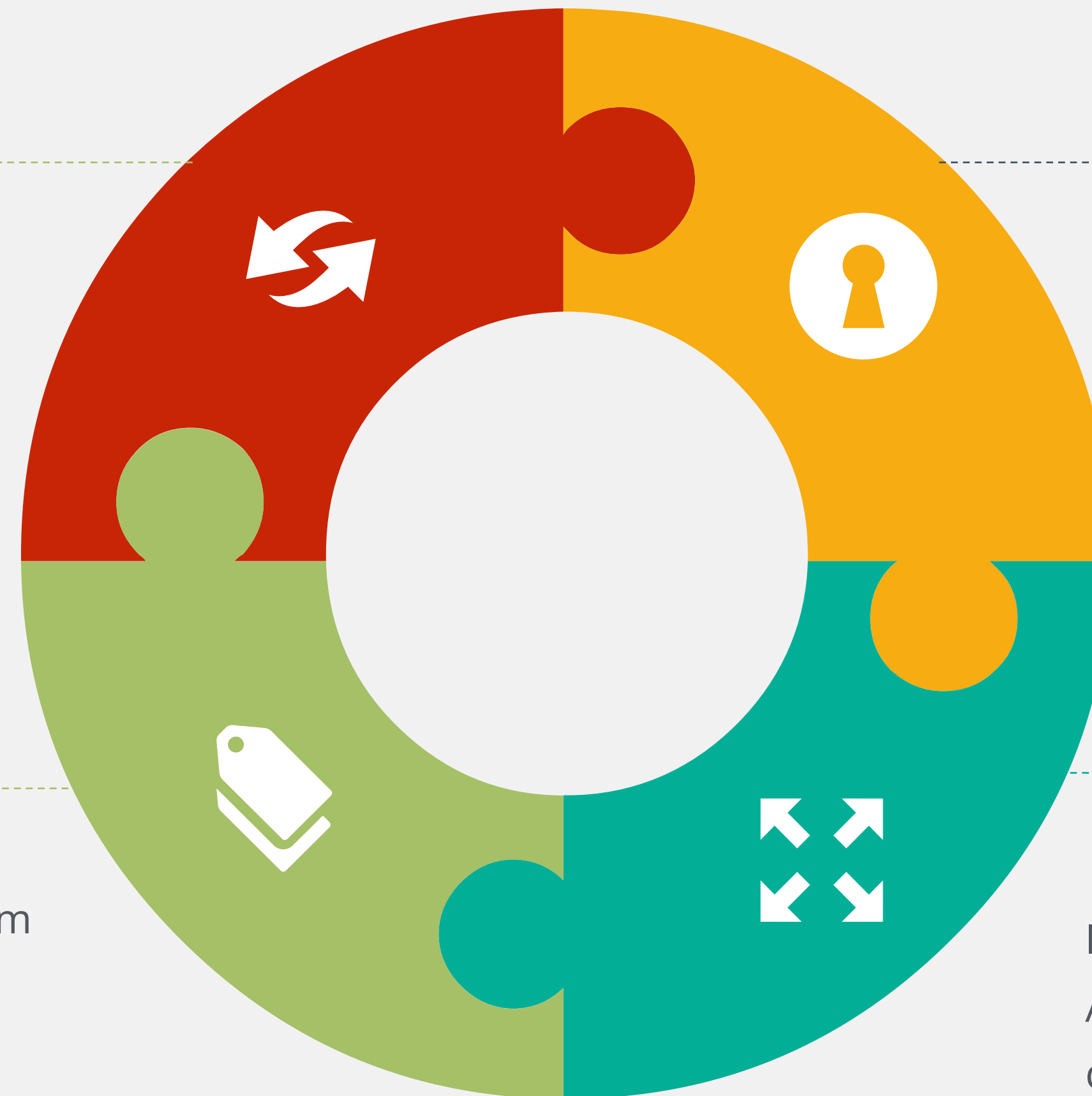
04. Development

Manual security review for source code

Based on secure programming principles, to perform manual security review and improve secure programming awareness.

Automatic dependencies scan

By using the dependency-check tool, to help R&D team to effectively find out the 3rd frameworks or libraries with the high risk security issues.



Automatic source code scan

Apply automatic source code static scan via tools (Fortify, Findbugs, Clockwork), some security issues introduced by inappropriate coding can be quickly identified then fixed.

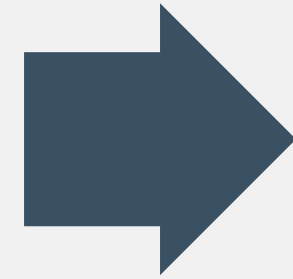
Development tool verification

In order to avoid the similar security issue caused by Apple's vulnerable developer tool XcodeGhost, the development tools used by the team should be verified to be secure.

05. Testing and Release

STEP 1

- 自动化安全扫描



STEP 2

- 手动安全测试



STEP 3

- 自动化安全测试用例

05. 实践 - 静态代码安全扫描

SonarQube

localhost:9000/issues/search#resolved=false|sort=UPDATE_DATE|asc=false

Dashboards Projects Measures Issues Rules Quality Profiles Quality Gates Settings Administrator Search

Issues New Search

Project: All Severity: All Status: All Assignee: All Resolution: Unresolved + More Criteria Search

Ordered by Update Date Found: 149

src/main/java/testcode/xmldecoder/XmlDecodeUtil.j...

src/main/java/testcode/sql/JPoSql.java

src/main/java/testcode/xpath/XmlUtils.java

src/main/java/testcode/xxe/DocumentBuilderVulnera...

src/main/java/testcode/xxe/DocumentBuilderSafePr...

src/main/java/testcode/xxe/DocumentBuilderSafePr...

src/main/java/testcode/xxe/DocumentBuilderSafePr...

Vulnerable Web Application

22 Lines of code 0 Debt 1 Issues

```
6 import javax.xml.parsers.DocumentBuilder;
7 import javax.xml.parsers.DocumentBuilderFactory;
8 import javax.xml.parsers.ParserConfigurationException;
9 import java.io.ByteArrayInputStream;
10 import java.io.IOException;
11 import java.io.InputStream;
12
13 public class DocumentBuilderVulnerable {
14
15     public static void receiveXMLStream(InputStream in) throws ParserConfigurationException, IOException, Sa
16
17         DocumentBuilder db = DocumentBuilderFactory.newInstance().newDocumentBuilder();
18         Document doc = db.parse(in);
```

The usage of /DocumentBuilder.parse(...) is v...

The usage of /DocumentBuilder.parse(...) is v...

The usage of /DocumentBuilder.parse(...) is v...

The usage of /DocumentBuilder.parse(...) is v...

The usage of /DocumentBuilder.parse(...) is v...

The usage of /DocumentBuilder.parse(...) is v...

The usage of /DocumentBuilder.parse(...) is v...

The usage of /DocumentBuilder.parse(...) is v...

The usage of /DocumentBuilder.parse(...) is v...

The usage of /DocumentBuilder.parse(...) is vulnerable to XML External Entity attacks

Comment Open Confirm Resolve False Positive Assign [to me] Plan Change Severity

Rule Changelog

Security - XML Parsing Vulnerable to XXE (DocumentBuilder)

Attack

XML External Entity (XXE) attacks can occur when an XML parser supports XML entities while processing XML received from an untrusted s

Risk 1: Expose local file content (XXE: XML eXternal Entity)

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
  <!ENTITY xxe SYSTEM "file:///etc/passwd" > ]>
<foo>&xxe;</foo>
```

SonarQube™ technology is powered by SonarSource SA
Version 4.5.2 - LGPL v3 - Community - Documentation - Get Support - Plugins - Web Service API

05. 实践 - CI/CD 中集成安全扫描工具

配置

>>

运行

>>

获取报告

```
1  apply plugin: "java"
2  apply plugin: "idea"
3
4  apply plugin: "security-zap"
5
6  buildscript {
7      repositories {
8          mavenCentral()
9      }
10     dependencies {
11         classpath(
12             'com.thoughtworks.tools:security-zap:1.0.5'
13         )
14     }
15 }
```

```
→ customer-api git:(master) X gradle zapStart build -Dzap.proxy=localhost:7070 zapReport
:zapStop
stopping zap
Warning: failed to stop ZAP due to connection refused or ZAP already stopped.
:zapStart
Starting ZAP [apikey: 2Lz77g9YVi]
waiting ZAP
waiting ZAP
waiting ZAP
ZAP started
exclusion rules are removed
urls match following regex will be excluded:
.*\/css\/.*
.*\/js\/.*
.*\/fonts\/.*
.*\.css
.*\.js
```

2. Security Alerts Summary

Number of alerts in total: 541

Alerts by severity	Amount
High	2
Medium	5
Low	360
Informational	174

3. Security Alerts By Classification

Classification	Amount
Cross Site Scripting (Reflected)	1
SQL Injection	1
Session ID in URL rewrite	4

05. 实践 - 第三方依赖安全检查

```
1  dependencies
2
3  -----
4  Root project
5  -----
6
7  archives - Configuration for archive artifacts.
8  No dependencies
9
10 checkstyle - The Checkstyle libraries to be used for this project.
11 \--- com.puppycrawl.tools:checkstyle:7.6
12      \--- antlr:antlr:2.7.7
13      \--- org.antlr:antlr4-runtime:4.6
14      \--- commons-beanutils:commons-beanutils:1.9.3
15           \--- commons-collections:commons-collections:3.2.2
16      \--- commons-cli:commons-cli:1.5.1
17      \--- com.google.guava:guava:19.0
18
19 compile - Dependencies for source set 'main'.
20 \--- org.springframework.boot:spring-boot-starter-web:1.5.1.RELEASE
21      \--- org.springframework.boot:spring-boot-starter:1.5.1.RELEASE
22           \--- org.springframework.boot:spring-boot:1.5.1.RELEASE
23           \--- org.springframework:spring-core:4.3.6.RELEASE
24           \--- commons-logging:commons-logging:1.2
25           \--- org.springframework:spring-context:4.3.6.RELEASE
26           \--- org.springframework:spring-aop:4.3.6.RELEASE
27           \--- org.springframework:spring-beans:4.3.6.RELEASE
28           \--- org.springframework:spring-core:4.3.6.RELEASE (*)
29           \--- org.springframework:spring-core:4.3.6.RELEASE (*)
30           \--- org.springframework:spring-beans:4.3.6.RELEASE (*)
31           \--- org.springframework:spring-core:4.3.6.RELEASE (*)
32           \--- org.springframework:spring-expression:4.3.6.RELEASE
33           \--- org.springframework:spring-core:4.3.6.RELEASE (*)
34           \--- org.springframework.boot:spring-boot-starter-actuator:1.5.1.RELEASE
35           \--- org.springframework.boot:spring-boot:1.5.1.RELEASE (*)
36           \--- org.springframework.boot:spring-boot-starter-logging:1.5.1.RELEASE
37           \--- ch.qos.logback:logback-classic:1.1.9
38           \--- org.slf4j:slf4j-api:1.7.22
39           \--- org.slf4j:jcl-over-slf4j:1.7.22
40           \--- org.slf4j:slf4j-api:1.7.22
41           \--- org.slf4j:jul-to-slf4j:1.7.22
42           \--- org.slf4j:slf4j-api:1.7.22
43           \--- org.slf4j:log4j-over-slf4j:1.7.22
44           \--- org.slf4j:slf4j-api:1.7.22
45           \--- org.springframework:spring-core:4.3.6.RELEASE (*)
46           \--- org.yaml:snakeyaml:1.17
47           \--- org.springframework.boot:spring-boot-starter-tomcat:1.5.1.RELEASE
48           \--- org.apache.tomcat.embed:tomcat-embed-core:8.5.11
49           \--- org.apache.tomcat.embed:tomcat-embed-el:8.5.11
50           \--- org.apache.tomcat.embed:tomcat-embed-websocket:8.5.11
51           \--- org.apache.tomcat.embed:tomcat-embed-core:8.5.11
52           \--- org.hibernate:hibernate-validator:5.3.4.Final
53           \--- javax.validation:validation-api:1.1.0.Final
54           \--- org.jboss.logging:jboss-logging:3.3.0.Final
55           \--- com.fasterxml.classmate:3.3.1 -> 1.3.3
56           \--- com.fasterxml.jackson.core:jackson-databind:2.8.6
57           \--- com.fasterxml.jackson.core:jackson-annotations:2.8.0
58           \--- com.fasterxml.jackson.core:jackson-core:2.8.6
59           \--- org.springframework:spring-web:4.3.6.RELEASE
60
```

以前

通过媒体被动获取漏洞信息

人工审查

耗时长

&

不可持续

现在

全自动化的工具

迅速获取安全质量

&

持续监控

DEMO ONLINE

05. 实践 - 自动化安全测试用例

基于安全需求制定安全测试用例

Given an anonymous visitor
When I try to access report page without authentication
Then I was been redirected to login page

Given a user without report access permission
When I try to access report page with authentication
Then I was been redirected to error page

Given a system manager
When I try to access report page with authentication
Then I can access report page successfully

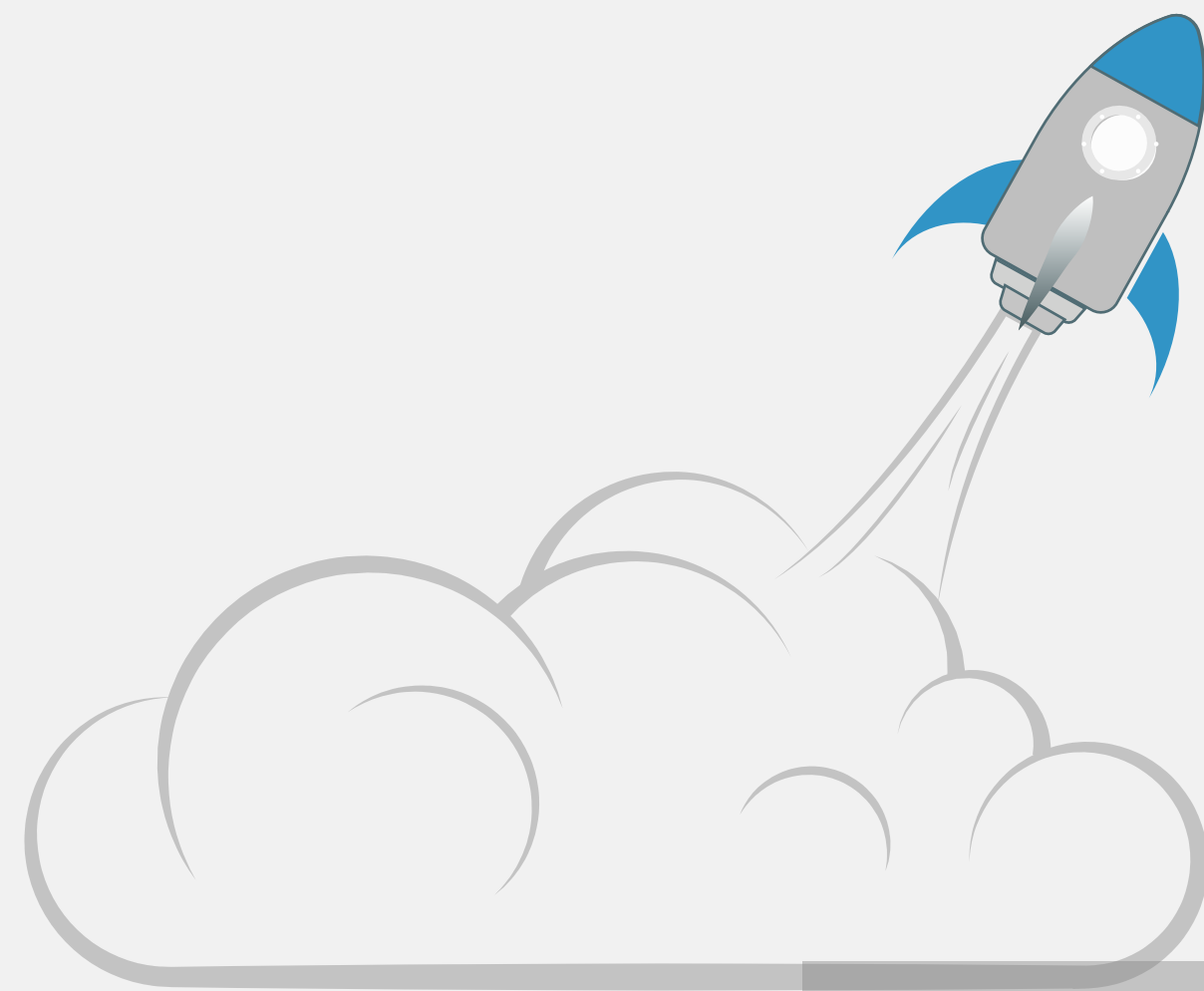
将安全测试用例通过普通的测试来实现

```
public void anonymousVisitorCanNotAccessReportPage() {  
    Page currentPage = accessReportPage();  
    assertThat(currentPage, is(LOGIN_PAGE));  
}
```

```
public void userWithoutProperPermissionCanNotAccessReportPage() {  
    loginAsMember();  
    Page currentPage = accessReportPage();  
    assertThat(currentPage, is(PERMISSION_REQUIRED_ERROR_PAGE));  
}
```

```
public void managerCanAccessReportPage() {  
    loginAsManager();  
    Page currentPage = accessReportPage();  
    assertThat(currentPage, is(REPORT_PAGE));  
}
```

06. Operation and Maintenance



Your system is secure currently, but it doesn't mean it is secure in the future, the reason is we just address all KNOWN issues. The unknown security issues will be raised as the time goes on, so regular security scan can help the team to find out and fix the new security issued in the system at a very early stage.



Regular Security Scan

Follow the industry security events, and take appropriate actions for the issues which have big impact on the system to reduce security risks.



Industry Security Event Monitoring

THANK YOU