

ThoughtWorks®

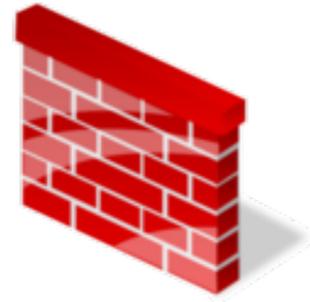
ThoughtWorks® | IT大咖说  
知识分享平台

*Build Security In*

---

# 内建安全的软件开发

---



WAF



安全监控



渗透测试



规范文档



安全培训

# 一个漏洞引发的反思

如有雷同，说明你也踩过同样的坑...

## 发现异常

订单总价和实际商品不符合

## 调查结果

某个影响价格计算的参数  
在等待订单支付期间可被强行修改



## □ 为何防火墙没有拦截或者报警

该漏洞和业务强相关，防火墙无法提供有力支持

## □ 为何渗透测试没有报告这个问题？

该漏洞和业务强相关，躲过了渗透测试的检查

# 反思

## #1 太晚才做渗透测试 报告的安全问题来不及全部修复



耗时长



数量多



时间紧

## #2 产品功能在持续迭代改进 然后渗透测试却没办法每次发布都做



## #3 安全活动流于形式

- 威胁建模，拖了很久才做
- 有安全编码规范，但是过于冗长，没人愿意用
- 理论上团队对应用进行安全自查，但是落地

## #4 排查第三方组件安全漏洞工作量大

```
dependencies {  
    compile 'org.springframework.boot:spring-boot-starter-web'  
    compile 'org.springframework.boot:spring-boot-starter-data-jpa'  
    compile 'org.postgresql:postgresql:9.4.1212'  
    compile 'org.apache.poi:poi:3.15'  
    compile 'org.apache.poi:poi-ooxml:3.15'  
    compile 'io.springfox:springfox-swagger2:2.6.1'  
    compile 'io.springfox:springfox-swagger-ui:2.6.1'  
    compile 'commons-io:commons-io:2.4'  
    compile 'org.apache.commons:commons-lang3:3.5'  
    compile 'com.yunpian.sdk:yunpian-java-sdk:1.2.2'  
    compile 'org.springframework.boot:spring-boot-starter-security:1.3.0.RC1'  
    compile 'io.jsonwebtoken:jjwt:0.7.0'  
    compile 'org.json:json:20160810'  
    compile 'org.quartz-scheduler:quartz:2.2.3'  
    compile 'org.springframework:spring-context-support:4.1.6.RELEASE'  
  
    testCompile 'org.springframework.boot:spring-boot-starter-test'  
    testCompile 'com.h2database:h2'  
    testCompile 'org.springframework.security:spring-security-test'  
    testCompile 'org.powermock:powermock-module-junit4:1.6.5'  
    testCompile 'org.powermock:powermock-api-mockito:1.6.5'  
}
```

```
dependencies  
-----  
Root project  
-----  
archives - Configuration for archive artifacts.  
No dependencies  
-----  
checkstyle - The Checkstyle libraries to be used for this project.  
├── com.puppycrawl.tools:checkstyle:7.6  
│   ├── antlr:antlr:2.7.7  
│   ├── org.antlr:antlr4-runtime:4.6  
│   ├── commons-beanutils:commons-beanutils:1.9.3  
│   └── commons-collections:commons-collections:3.2.2  
└── commons-cli:commons-cli:1.3.1  
    └── com.google.guava:guava:19.0  
-----  
compile - Dependencies for source set 'main'.  
├── org.springframework.boot:spring-boot-starter-web -> 1.5.1.RELEASE  
│   ├── org.springframework.boot:spring-boot-starter:1.5.1.RELEASE  
│   │   ├── org.springframework.boot:spring-boot:1.5.1.RELEASE  
│   │   ├── org.springframework:spring-core:4.3.6.RELEASE  
│   │   └── commons-logging:commons-logging:1.2  
│   └── org.springframework:spring-context:4.3.6.RELEASE  
│       ├── org.springframework:spring-aop:4.3.6.RELEASE  
│       ├── org.springframework:spring-beans:4.3.6.RELEASE  
│       ├── org.springframework:spring-core:4.3.6.RELEASE (*)  
│       ├── org.springframework:spring-core:4.3.6.RELEASE (*)  
│       ├── org.springframework:spring-beans:4.3.6.RELEASE (*)  
│       ├── org.springframework:spring-core:4.3.6.RELEASE (*)  
│       └── org.springframework:spring-expression:4.3.6.RELEASE  
│           └── org.springframework:spring-core:4.3.6.RELEASE (*)  
├── org.springframework.boot:spring-boot-autoconfigure:1.5.1.RELEASE  
│   └── org.springframework.boot:spring-boot:1.5.1.RELEASE (*)  
├── org.springframework.boot:spring-boot-starter-logging:1.5.1.RELEASE  
│   ├── ch.qos.logback:logback-classic:1.1.9  
│   ├── ch.qos.logback:logback-core:1.1.9  
│   └── org.slf4j:slf4j-api:1.7.22  
│       ├── org.slf4j:slf4j-api:1.7.22  
│       ├── org.slf4j:slf4j-api:1.7.22  
│       ├── org.slf4j:slf4j-api:1.7.22  
│       └── org.slf4j:log4j-over-slf4j:1.7.22  
│           └── org.slf4j:slf4j-api:1.7.22  
├── org.springframework:spring-core:4.3.6.RELEASE (*)  
├── org.yaml:snakeyaml:1.17  
├── org.springframework.boot:spring-boot-starter-tomcat:1.5.1.RELEASE  
│   ├── org.apache.tomcat.embed:tomcat-embed-core:8.5.11  
│   ├── org.apache.tomcat.embed:tomcat-embed-el:8.5.11  
│   ├── org.apache.tomcat.embed:tomcat-embed-websocket:8.5.11  
│   └── org.apache.tomcat.embed:tomcat-embed-core:8.5.11  
├── org.hibernate:hibernate-validator:5.3.4.Final  
│   ├── javax.validation:validation-api:1.1.0.Final  
│   ├── org.jboss.logging:jboss-logging:3.3.0.Final  
│   └── com.fasterxml:classmate:1.3.1 -> 1.3.3  
├── com.fasterxml.jackson.core:jackson-databind:2.8.6  
│   ├── com.fasterxml.jackson.core:jackson-annotations:2.8.0  
│   └── com.fasterxml.jackson.core:jackson-core:2.8.6  
└── com.fasterxml.jackson.core:jackson-core:2.8.6
```

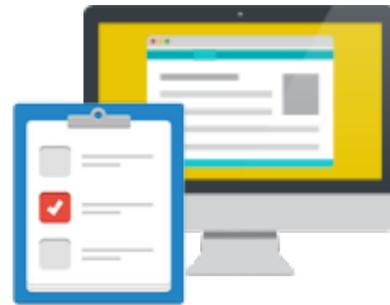
## #4 排查第三方组件安全漏洞工作量大

```
dependencies {  
    compile 'org.springframework.boot:spring-boot-starter-web'  
    compile 'org.springframework.boot:spring-boot-starter-data-jpa'  
    compile 'org.postgresql:postgresql:9.4.1212'  
    compile 'org.apache.poi:poi:3.15'  
    compile 'org.apache.poi:poi-ooxml:3.15'  
    compile 'io.springfox:springfox-swagger2:2.6.1'  
    compile 'io.springfox:springfox-swagger-ui:2.6.1'  
    compile 'commons-io:commons-io:2.4'  
    compile 'org.apache.commons:commons-lang3:3.5'  
    compile 'com.yunpian.sdk:yunpian-java-sdk:1.2.2'  
    compile 'org.springframework.boot:spring-boot-starter-security:1.3.0.RC1'  
    compile 'io.jsonwebtoken:jjwt:0.7.0'  
    compile 'org.json:json:20160810'  
    compile 'org.quartz-scheduler:quartz:2.2.3'  
    compile 'org.springframework:spring-context-support:4.1.6.RELEASE'  
  
    testCompile 'org.springframework.boot:spring-boot-starter-test'  
    testCompile 'com.h2database:h2'  
    testCompile 'org.springframework.security:spring-security-test'  
    testCompile 'org.powermock:powermock-module-junit4:1.6.5'  
    testCompile 'org.powermock:powermock-api-mockito:1.6.5'  
}
```

```
dependencies  
-----  
Root project  
-----  
archives - Configuration for archive artifacts.  
No dependencies  
-----  
checkstyle - The Checkstyle libraries to be used for this project.  
├── com.puppycrawl.tools:checkstyle:7.6  
│   ├── antirantlr:2.7.7  
│   ├── org.antlr:antlr4-runtime:4.6  
│   ├── commons-beanutils:commons-beanutils:1.9.3  
│   │   └── commons-collections:commons-collections:3.2.2  
│   ├── commons-cli:commons-cli:1.3.1  
│   └── com.google.guava:guava:19.0  
-----  
compile - Dependencies for source set 'main'.  
├── org.springframework.boot:spring-boot-starter-web -> 1.5.1.RELEASE  
│   ├── org.springframework.boot:spring-boot-starter:1.5.1.RELEASE  
│   │   ├── org.springframework:spring-core:4.3.6.RELEASE  
│   │   │   └── commons-logging:commons-logging:1.2  
│   │   └── org.springframework:spring-context:4.3.6.RELEASE  
│   ├── org.springframework:spring-aop:4.3.6.RELEASE  
│   ├── org.springframework:spring-beans:4.3.6.RELEASE  
│   └── org.springframework:spring-core:4.3.6.RELEASE (*)  
├── org.springframework.boot:spring-boot-starter-data-jpa -> 1.5.1.RELEASE  
│   ├── org.springframework.boot:spring-boot-starter:1.5.1.RELEASE  
│   │   ├── org.springframework:spring-core:4.3.6.RELEASE  
│   │   │   └── commons-logging:commons-logging:1.2  
│   │   └── org.springframework:spring-context:4.3.6.RELEASE  
│   ├── org.springframework.boot:spring-boot-starter-data-jpa:1.5.1.RELEASE  
│   │   ├── org.springframework:spring-orm:4.3.6.RELEASE  
│   │   ├── org.springframework:spring-tx:4.3.6.RELEASE  
│   │   └── org.springframework:spring-core:4.3.6.RELEASE (*)  
├── org.postgresql:postgresql:9.4.1212  
├── org.apache.poi:poi:3.15  
├── org.apache.poi:poi-ooxml:3.15  
├── io.springfox:springfox-swagger2:2.6.1  
├── io.springfox:springfox-swagger-ui:2.6.1  
├── commons-io:commons-io:2.4  
├── org.apache.commons:commons-lang3:3.5  
├── com.yunpian.sdk:yunpian-java-sdk:1.2.2  
├── org.springframework.boot:spring-boot-starter-security:1.3.0.RC1  
├── io.jsonwebtoken:jjwt:0.7.0  
├── org.json:json:20160810  
├── org.quartz-scheduler:quartz:2.2.3  
└── org.springframework:spring-context-support:4.1.6.RELEASE (*)  
-----  
testCompile - Dependencies for source set 'test'.  
├── org.springframework.boot:spring-boot-starter-test -> 1.5.1.RELEASE  
│   ├── org.springframework.boot:spring-boot-starter:1.5.1.RELEASE  
│   │   ├── org.springframework:spring-core:4.3.6.RELEASE  
│   │   │   └── commons-logging:commons-logging:1.2  
│   │   └── org.springframework:spring-context:4.3.6.RELEASE  
│   ├── org.springframework.boot:spring-boot-starter-test:1.5.1.RELEASE  
│   │   ├── org.springframework:spring-core:4.3.6.RELEASE  
│   │   │   └── commons-logging:commons-logging:1.2  
│   │   ├── org.springframework:spring-test:4.3.6.RELEASE  
│   │   ├── org.springframework:spring-core:4.3.6.RELEASE (*)  
│   │   ├── org.springframework:spring-context:4.3.6.RELEASE  
│   │   ├── org.springframework:spring-aop:4.3.6.RELEASE  
│   │   ├── org.springframework:spring-beans:4.3.6.RELEASE  
│   │   ├── org.springframework:spring-core:4.3.6.RELEASE (*)  
│   │   ├── org.springframework:spring-context-support:4.1.6.RELEASE (*)  
│   │   ├── org.springframework:spring-orm:4.3.6.RELEASE  
│   │   ├── org.springframework:spring-tx:4.3.6.RELEASE  
│   │   └── org.springframework:spring-core:4.3.6.RELEASE (*)  
├── com.h2database:h2:1.4.197  
├── org.springframework.security:spring-security-test -> 4.2.0.RELEASE  
│   ├── org.springframework:spring-core:4.3.6.RELEASE  
│   │   └── commons-logging:commons-logging:1.2  
│   ├── org.springframework:spring-context:4.3.6.RELEASE  
│   ├── org.springframework:spring-aop:4.3.6.RELEASE  
│   ├── org.springframework:spring-beans:4.3.6.RELEASE  
│   ├── org.springframework:spring-core:4.3.6.RELEASE (*)  
│   ├── org.springframework:spring-context-support:4.1.6.RELEASE (*)  
│   ├── org.springframework:spring-orm:4.3.6.RELEASE  
│   ├── org.springframework:spring-tx:4.3.6.RELEASE  
│   └── org.springframework:spring-core:4.3.6.RELEASE (*)  
├── org.powermock:powermock-module-junit4:1.6.5  
├── org.powermock:powermock-api-mockito:1.6.5  
└── org.springframework:spring-core:4.3.6.RELEASE (*)  
-----
```

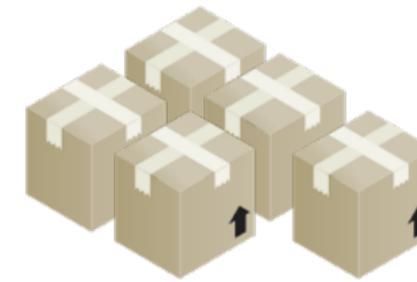
其实一共有100个依赖

## #4 相似的困境



软件测试

- 很晚才测试
- 测试执行速度慢
- 集中式的、一次性测试
- 专人负责测试



系统集成

- 很晚才集成
- 集成过程缓慢
- 一次性集成
- 专人负责集成

---

# 三大安全挑战

---

- 一次性的安全检查无法匹配持续性的交付
- 缺乏自动化、自助化的安全服务
- 部门墙阻碍开发和安全团队高效协作

# 挑战1: 一次性的安全检查无法匹配持续性的交付

## 传统安全控制设施



持续交付模式下，开发团队尽可能的降低 Cycle Time



# 挑战1: 一次性的安全检查无法匹配持续性的交付

## 传统安全控制设施



持续交付模式下，开发团队尽可能的降低 Cycle Time

在这里做渗透测试?



在这里做渗透测试?

## 核心原则

不再依赖一次性的安全检查  
而是将安全实践融入持续交付流程  
通过持续性的搜集安全质量反馈，及时对应用做出调整



## 威胁建模

### *Threat Modeling*



Threat modeling is an approach for analysing the security of an application. It is a structured approach that enables you to identify, quantify, and address the security risks associated with an application.



## 威胁建模产出物：安全故事卡

The image shows a screenshot of a Security Story Card from a threat modeling tool. The card title is "[Security] Prevent the signed in session from being used by unauthorized users" with ID #473. It includes sections for "Story Phrase", "Assumptions", and "Acceptance Criteria". Three green speech bubble annotations are overlaid on the card:

- 攻击场景** (Attack Scenario): Points to the "Story Phrase" section, which describes a hacker stealing session tokens to access unauthorized data.
- 对应技术方案** (Corresponding Technical Solution): Points to the "Assumptions" section, which lists conditions like using the same IP address and browser.
- 验收标准** (Acceptance Criteria): Points to the "Acceptance Criteria" section, which lists requirements for denying access when IP or browser changes.

**[Security] Prevent the signed in session from being used by unauthorized users #473**  
(v23 - Latest version, last modified 9 months ago)  
Security + |  
✓ Checklist +  
Description  
**Story Phrase**  
As a hacker  
I can steal the the session tokens of signed in user somehow, then from my own network environment I can access data and functions of [redacted] which I'm not authorized  
Below is one of the technical solutions can be adopted as a **mitigation**, This is also the **mitigation** for the flaw that we are unable to immediately invalidate the session tokens on server side when remote client signs out  
.....  
Bind the remote client specific information(ip address and User-Agent of browser) to session tokens(cook [redacted] m to access [redacted] unless the hacker  
(1) uses the same IP address and  
(2) uses the same browser and  
(3) the tokens doesn't expire.  
**Assumptions**  
It is acceptable that after signing into [redacted] and before session expires if remote [redacted] such as disconnect and reconnect to network so ip is changed by DHCP) the re-sign in is required to go on with the operations in [redacted]  
**Acceptance Criteria**  
**AC01**  
(1) If remote client's ip address is changed for existing valid session [redacted] should deny the access request to protected resource till re-sign in.  
(2) If remote client's browser is changed for existing valid session(obviously it is abnormal behavior,90% hacker attack) [redacted] should deny the access request to protected resource till re-sign in

## 威胁建模产出物：威胁清单及应对方法

### □ 数据传输过程存在泄漏风险

- 应对办法：SSL / 敏感数据加密后传输

### □ 产品有多种用户角色，可能出现鉴权漏洞

- 应对办法：严格的权限校验 / 默认只给最小权限 / 异常访问报警 / 专门针对角色和权限的自动化测试 ...

### □ 可能有XSS漏洞

- 应对办法：前端输出编码 / 使用AngularJS的时候避免使用原始数据输出

### □ .....

通过自动化测试用例，对应用的安全功能进行测试

API	期待的安全行为
/customers	<ol style="list-style-type: none"><li>1. 必须经过身份认证后才允许访问</li><li>2. 只允许具有 CustomerManager 角色的用户访问</li><li>3. 只应该返回该 CustomerManager 所管辖的区域的客户数据</li><li>4. ....</li></ol>

通过自动化测试用例，对应用的安全功能进行测试

API	期待的安全行为
/customers	<ol style="list-style-type: none"><li>1. 必须经过身份认证后才允许访问</li><li>2. 只允许具有 CustomerManager 角色的用户访问</li></ol>
/customers/{id}	区域的客户

```
17 @Test
18 public void should_not_return_all_the_customers() throws Exception {
19     String token = loginAsDefaultCustomer();
20
21     given().header("Authorization", token)
22         .when().get("/customers")
23         .then().body(empty())
24         .statusCode(SC_NOT_FOUND);
25 }
26
27 @Test
28 public void should_return_information_of_current_customer() throws Exception {
29     String tokenOfCustomer1 = loginAsCustomer(authData.customer1, authData.pwdOfCustomer1);
30     String customerId = given().header("Authorization", tokenOfCustomer1)
31         .when().get(format("/customers/%s", authData.customer1))
32         .then().statusCode(SC_OK).extract().path("customerId");
33     assertThat(customerId, is(authData.customer1));
34 }
35
36 @Test
37 public void should_not_return_information_of_other_customer() throws Exception {
38     String tokenOfCustomer1 = loginAsCustomer(authData.customer1, authData.pwdOfCustomer1);
39     given().header("Authorization", tokenOfCustomer1)
40         .when().get(format("/customers/%s", authData.customer2))
41         .then().statusCode(SC_UNAUTHORIZED).body("errorKey", is("authorize_failed"));
42 }
43 }
```

我们知道安全很重要，但是安全实践落地难

## 核心原则

- 凡是能自动化的，统统自动化
- 凡是必须人工参与的，统统进行自助化改造



## 以前

1. 通过新闻报道获知组件安全漏洞
2. 手动进行排查

大量人工成本  
&  
一次性的检查

```
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:1.3.1
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-autoconfigure: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 |             \--- ch.qos.logback:logback-core:1.1.9
39 |             \--- org.slf4j:slf4j-api:1.7.22
40 |             \--- org.slf4j:jcl-over-slf4j:1.7.22
41 |             \--- org.slf4j:slf4j-api:1.7.22
42 |             \--- org.slf4j:jul-to-slf4j:1.7.22
43 |             \--- org.slf4j:slf4j-api:1.7.22
44 |             \--- org.slf4j:log4j-over-slf4j:1.7.22
45 |             \--- org.slf4j:slf4j-api:1.7.22
46 |   \--- org.springframework:spring-core:4.3.6.RELEASE (*)
47 |   \--- org.yaml:snakeyaml:1.17
48 |   \--- org.springframework.boot:spring-boot-starter-tomcat:1.5.1.RELEASE
49 |        \--- org.apache.tomcat.embed:tomcat-embed-core:8.5.11
50 |        \--- org.apache.tomcat.embed:tomcat-embed-el:8.5.11
51 |        \--- org.apache.tomcat.embed:tomcat-embed-websocket:8.5.11
52 |             \--- org.apache.tomcat.embed:tomcat-embed-core:8.5.11
53 |   \--- org.hibernate:hibernate-validator:5.3.4.Final
54 |        \--- javax.validation:validation-api:1.1.0.Final
55 |        \--- org.jboss.logging:jboss-logging:3.3.0.Final
56 |        \--- com.fasterxml:classmate:1.3.1 -> 1.3.3
57 |   \--- com.fasterxml.jackson.core:jackson-databind:2.8.6
58 |        \--- com.fasterxml.jackson.core:jackson-annotations:2.8.0
59 |        \--- com.fasterxml.jackson.core:jackson-core:2.8.6
60 |   \--- org.springframework:spring-web:4.3.6.RELEASE
```

## 以前

1. 通过新闻报道获知组件安全漏洞
2. 手动进行排查

大量人工成本  
&  
一次性的检查

## 现在

全程自动化  
OWASP DependencyCheck  
Node Security Platform ...

分分钟获得扫描结果  
&  
持续监控

## OWASP DependencyCheck Report



Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO warranties, implied or otherwise, with regard to the analysis. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

[How to read the report](#) | [Suppressing false positives](#) | [Getting Help: google group](#) | [github issues](#)

**Project: xxxxxxxx**

Scan Information ([show all](#)):

- dependency-check version: 1.4.5
- Report Generated On: May 9, 2017 at 11:35:22 +08:00
- Dependencies Scanned: 100 (100 unique)
- Vulnerable Dependencies: 9
- Vulnerabilities Found: 21
- Vulnerabilities Suppressed: 0
- ...

Display: [Showing Vulnerable Dependencies \(click to show all\)](#)

Dependency	CPE	GAV	Highest Severity	CVE Count	CPE Confidence	Evidence Count
<a href="#">logback-classic-1.1.9.jar</a>	cpe:/a:logback:logback:1.1.9	<a href="#">ch.qos.logback:logback-classic:1.1.9</a>	High	1	LOW	18
<a href="#">logback-core-1.1.9.jar</a>	cpe:/a:logback:logback:1.1.9	<a href="#">ch.qos.logback:logback-core:1.1.9</a>	High	1	LOW	18
<a href="#">jackson-annotations-2.8.0.jar</a>	cpe:/a:fasterxml:jackson:2.8.0	<a href="#">com.fasterxml.jackson.core:jackson-annotations:2.8.0</a>	Medium	1	LOW	25
<a href="#">jackson-core-2.8.6.jar</a>	cpe:/a:fasterxml:jackson:2.8.6	<a href="#">com.fasterxml.jackson.core:jackson-core:2.8.6</a>	Medium	1	LOW	25
<a href="#">jackson-databind-2.8.6.jar</a>	cpe:/a:fasterxml:jackson:2.8.6	<a href="#">com.fasterxml.jackson.core:jackson-databind:2.8.6</a>	Medium	1	LOW	25
<a href="#">jwt-0.7.0.jar</a>	cpe:/a:sonatype:nexus:0.7.0	<a href="#">io.jsonwebtoken:jwt:0.7.0</a>	High	1	LOW	18
<a href="#">tomcat-embed-core-8.5.11.jar</a>	cpe:/a:apache:tomcat:8.5.11	<a href="#">org.apache.tomcat.embed:tomcat-embed-core:8.5.11</a>	High	7	HIGHEST	16
<a href="#">tomcat-embed-websocket-8.5.11.jar</a>	cpe:/a:apache:tomcat:8.5.11	<a href="#">org.apache.tomcat.embed:tomcat-embed-websocket:8.5.11</a>	High	7	HIGHEST	18
<a href="#">spring-boot-starter-data-jpa-1.5.1.RELEASE.jar</a>	cpe:/a:pivotal_software:spring_data_jpa:1.5.1	<a href="#">org.springframework.boot:spring-boot-starter-data-jpa:1.5.1.RELEASE</a>	Medium	1	LOW	20



## Docker 容器安全最佳实践

### Host Configuration

- Keep Docker up to date
- Audit Docker files and directories - /var/lib/docker
- Audit Docker files and directories - /etc/docker
- Audit Docker files and directories - docker.service

.....

### Docker daemon configuration files

### Container Images and Build File

### Container Runtime

.....

```
docker run -it --net host --pid host --cap-add  
audit_control \  
-e DOCKER_CONTENT_TRUST=$DOCKER_CONTENT_TRUST \  
-v /var/lib:/var/lib \  
-v /var/run/docker.sock:/var/run/docker.sock \  
-v /usr/lib/systemd:/usr/lib/systemd \  
-v /etc:/etc --label docker_bench_security \  
docker/docker-bench-security
```

## Docker bench for security

```
docker run -i audit_control -e DOCKER -v /var/lib/docker -v /var/run/docker.sock -v /usr/lib/docker -v /etc:/etc:ro docker/docker
```

```
# -----  
# Docker Bench for Security v1.3.0  
#  
# Docker, Inc. (c) 2015-  
#  
# Checks for dozens of common best-practices around deploying Docker containers in production.  
# Inspired by the CIS Docker 1.13 Benchmark.  
# -----  
Initializing Thu Jan 26 08:58:33 UTC 2017  
[INFO] 1 - Host Configuration  
[WARN] 1.1 - Create a separate partition for containers  
[INFO] 1.2 - Harden the container host  
[PASS] 1.3 - Keep Docker up to date  
[INFO] * Using 1.13.0 which is current as of 2017-01-18  
[INFO] * Check with your operating system vendor for support and security maintenance for Docker  
[INFO] 1.4 - Only allow trusted users to control Docker daemon  
[INFO] * docker:x:998:ubuntu  
[WARN] 1.5 - Audit docker daemon - /usr/bin/docker  
[WARN] 1.6 - Audit Docker files and directories - /var/lib/docker  
[WARN] 1.7 - Audit Docker files and directories - /etc/docker  
[WARN] 1.8 - Audit Docker files and directories - docker.service  
[WARN] 1.9 - Audit Docker files and directories - docker.socket  
[WARN] 1.10 - Audit Docker files and directories - /etc/default/docker  
[INFO] 1.11 - Audit Docker files and directories - /etc/docker/daemon.json  
[INFO] * File not found  
[WARN] 1.12 - Audit Docker files and directories - /usr/bin/docker-containerd  
[WARN] 1.13 - Audit Docker files and directories - /usr/bin/docker-runc  
[INFO] 2 - Docker Daemon Configuration  
[WARN] 2.1 - Restrict network traffic between containers  
[WARN] 2.2 - Set the logging level  
[PASS] 2.3 - Allow Docker to make changes to iptables  
[PASS] 2.4 - Do not use insecure registries  
[WARN] 2.5 - Do not use the aufs storage driver  
[WARN] 2.6 - Configure TLS authentication for Docker daemon  
[WARN] * Docker daemon currently listening on TCP with TLS, but no verification  
[INFO] 2.7 - Set default ulimit as appropriate  
[INFO] * Default ulimit doesn't appear to be set  
[WARN] 2.8 - Enable user namespace support  
[PASS] 2.9 - Confirm default cgroup usage  
[PASS] 2.10 - Do not change base device size until needed  
[WARN] 2.11 - Use authorization plugin  
[WARN] 2.12 - Configure centralized and remote logging  
[WARN] 2.13 - Disable operations on legacy registry (v1)  
[WARN] 2.14 - Enable live restore  
[PASS] 2.15 - Do not enable swarm mode, if not needed  
[PASS] 2.16 - Control the number of manager nodes in a swarm (Swarm mode not enabled)  
[PASS] 2.17 - Bind swarm services to a specific host interface  
[WARN] 2.18 - Disable Userland Proxy  
[PASS] 2.19 - Encrypt data exchanged between containers on different nodes on the overlay network  
[PASS] 2.20 - Apply a daemon-wide custom seccomp profile, if needed  
[PASS] 2.21 - Avoid experimental features in production
```

-cap-add

NETENTRUST \

docker.sock \

and \

security \



```
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



**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



```
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));  
}
```

为团队提供：自动化的工具 / 实用的检查清单



- Authentication verification
  - Verify all pages and resources by default require authentication except those specifically intended to be public
  - Verify all authentication controls are enforced on the server side.
  - Verify that account passwords are one way hashed with a salt
  - .....
- Session management
- Access control
- Malicious input handling
- Output encoding/escaping
- Cryptography as rest
- Error handling

.....

为团队提供：自动化的工具 / 实用的检查清单



OWASP ZAP



Burp Suite

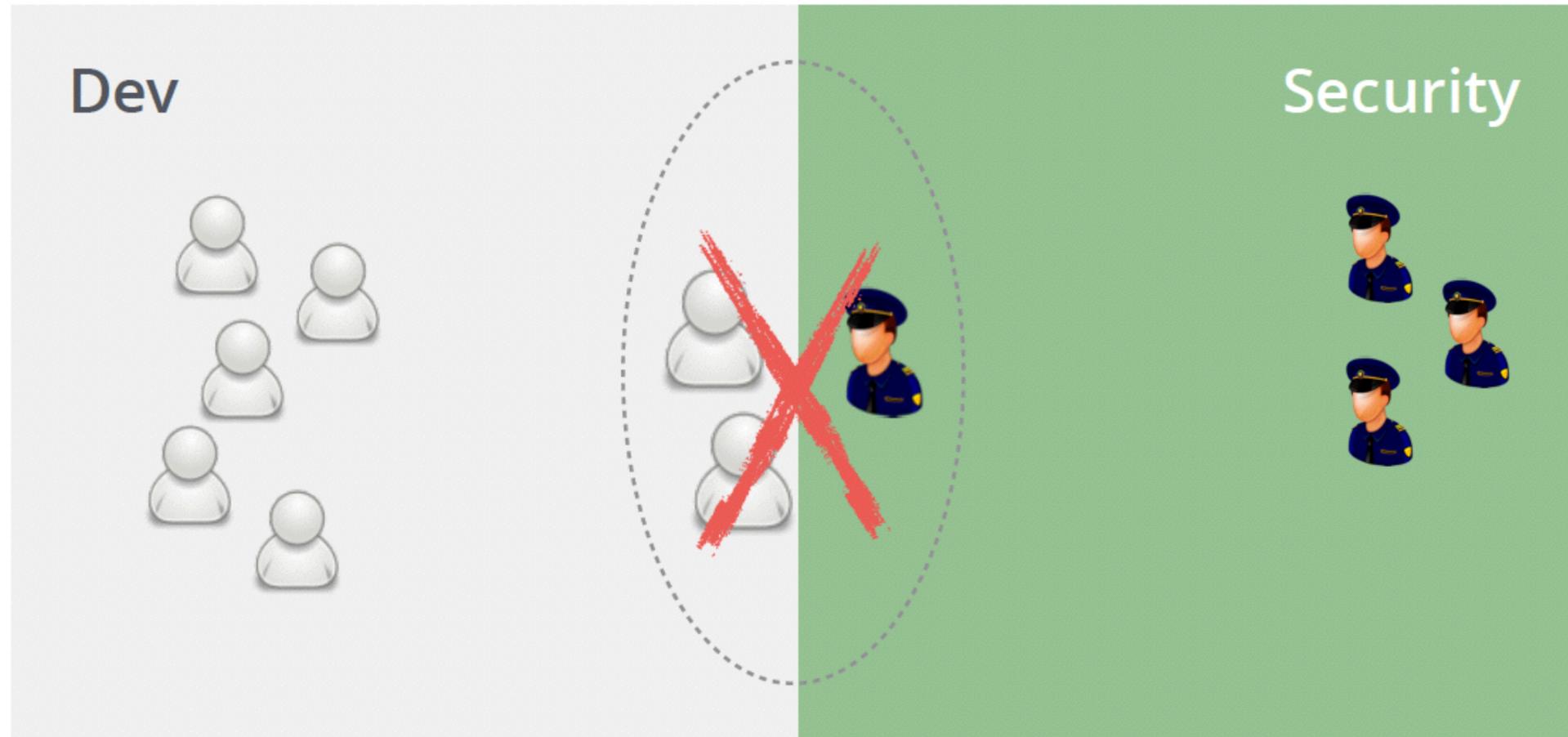


SQLMap

## 制定安全策略

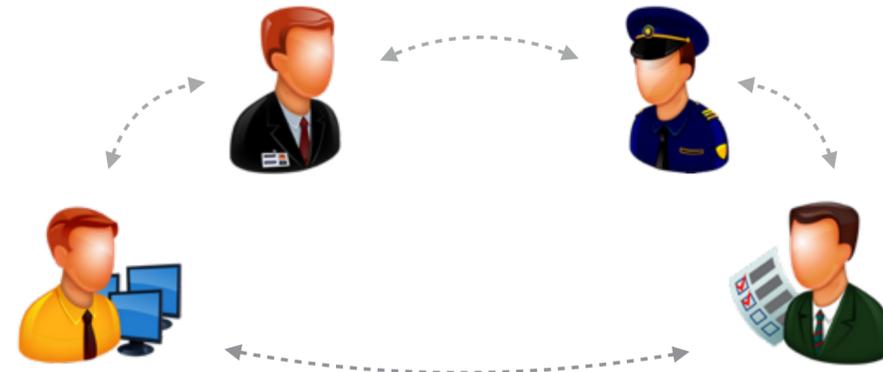


# 挑战3: 部门墙阻碍开发和安全团队的高效协作



## 核心原则

真正**高效的**沟通协作，而不是靠**强硬的**流程管控来保证应用安全质量



开发团队 & 安全团队





不是团队有了安全专家，一切问题都迎刃而解，  
关键在于**建立开发团队自己的安全能力**

## Build Security In

**主动发现安全漏洞** 胜于 被动等待漏洞报告

**前期安全威胁分析** 胜于 末期安全渗透测试

**持续安全扫描** 胜于 单次安全审查

**安全职责共担** 胜于 独立安全团队

## Q & A

---

谢谢

THANK YOU