ThoughtWorks®

微服务场景下的安全测试

杨乐涵

自我介绍

杨乐涵，

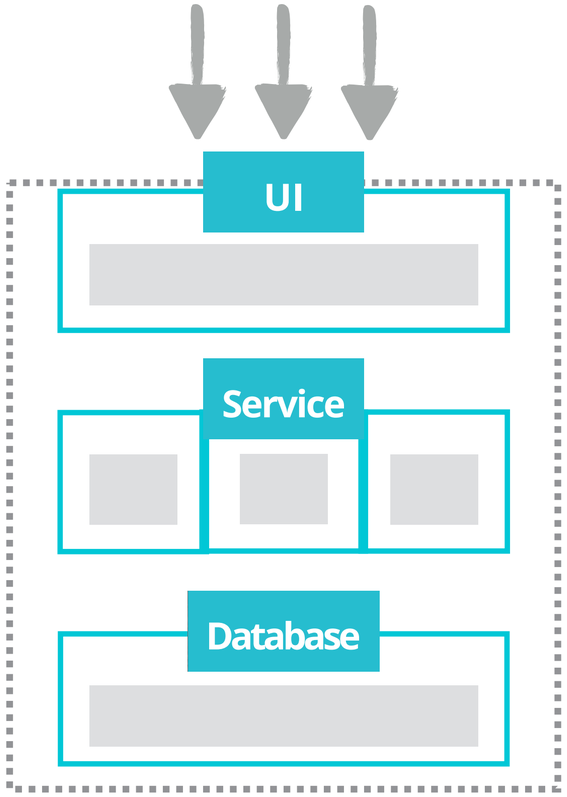
*ThoughtWorks*软件开发工程师/咨询师，主要从事敏捷团队中的开发工作。

曾在专业安全服务公司从事信息安全工程师职位。关注信息安全领域，擅长*web*应用安全测试。

目录

- 单体应用和微服务应用
- 开发团队需要承担一定的安全质量保证职责
- 避免常规的安全问题
- 避免由于微服务的出现而凸显的安全问题
- 最佳实践

传统单体应用

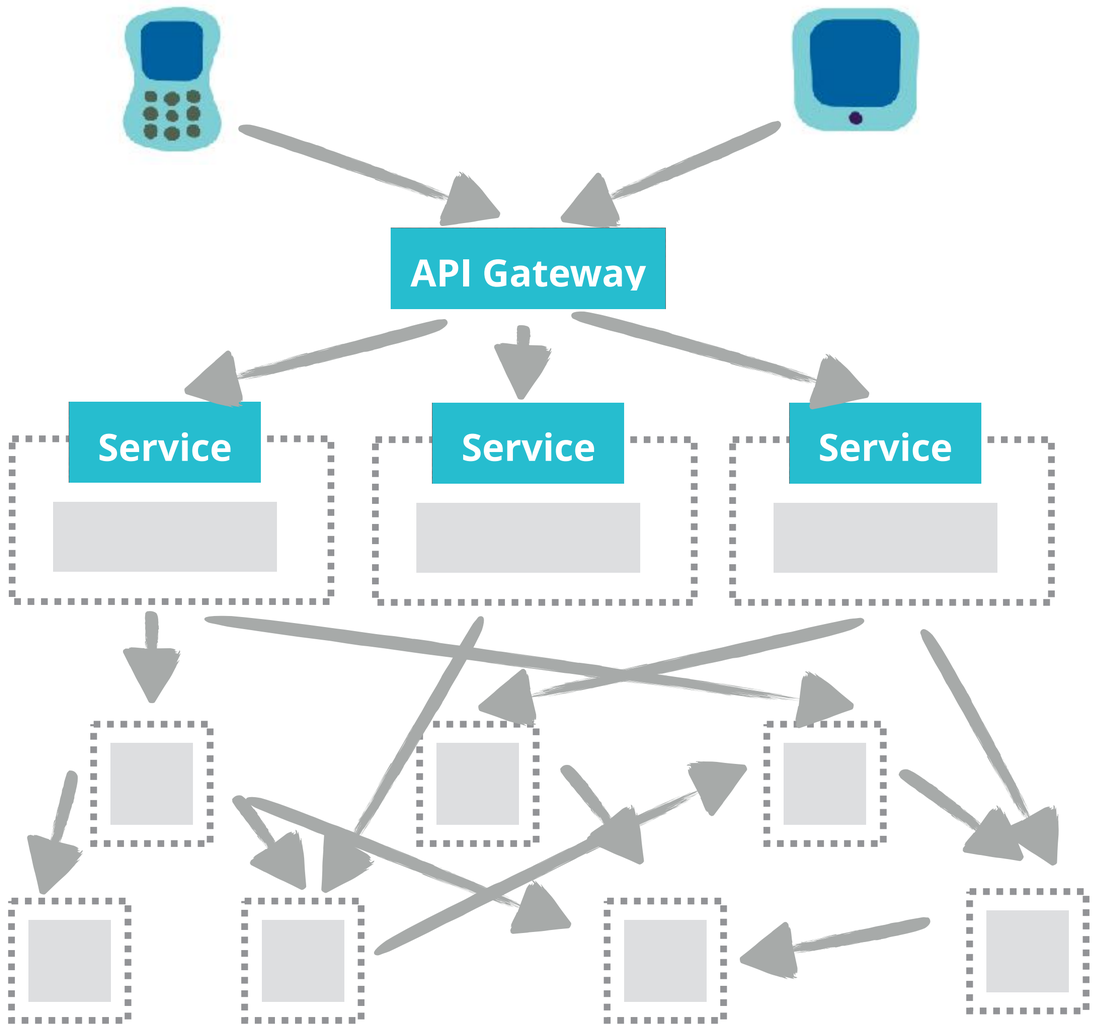


单体应用会随着业务的扩展逐渐变得臃肿和庞大

代码难以维护和修改，同一段代码可能被多个不同的地方使用

对应用程序做任何细微的修改都需要对整个应用程序重新测试和部署

微服务应用

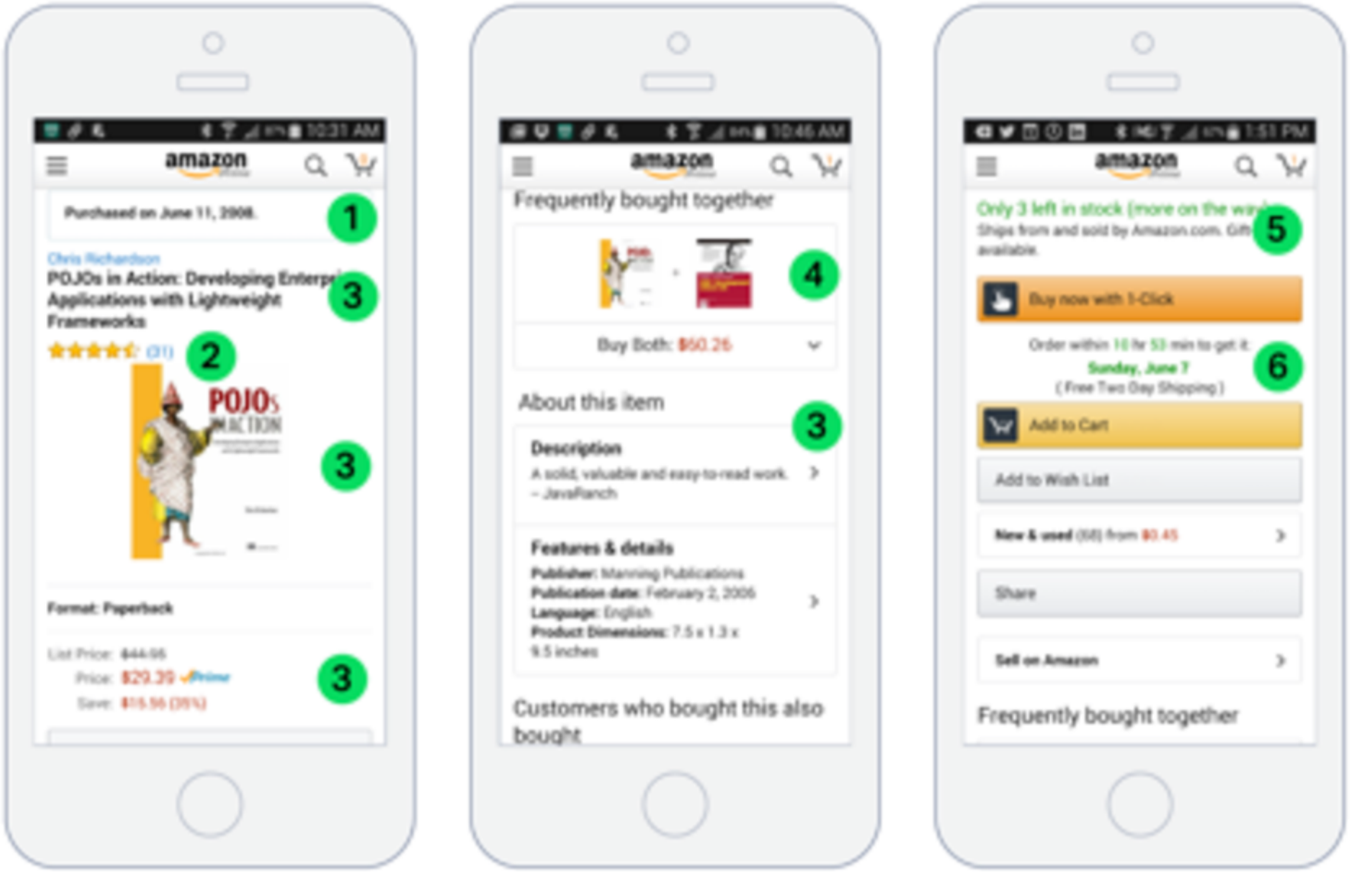


服务职责单一，解耦，容易维护

独立发布，快速迭代

增加重用，服务间可组合

微服务应用



1 订单历史

2 商品评价

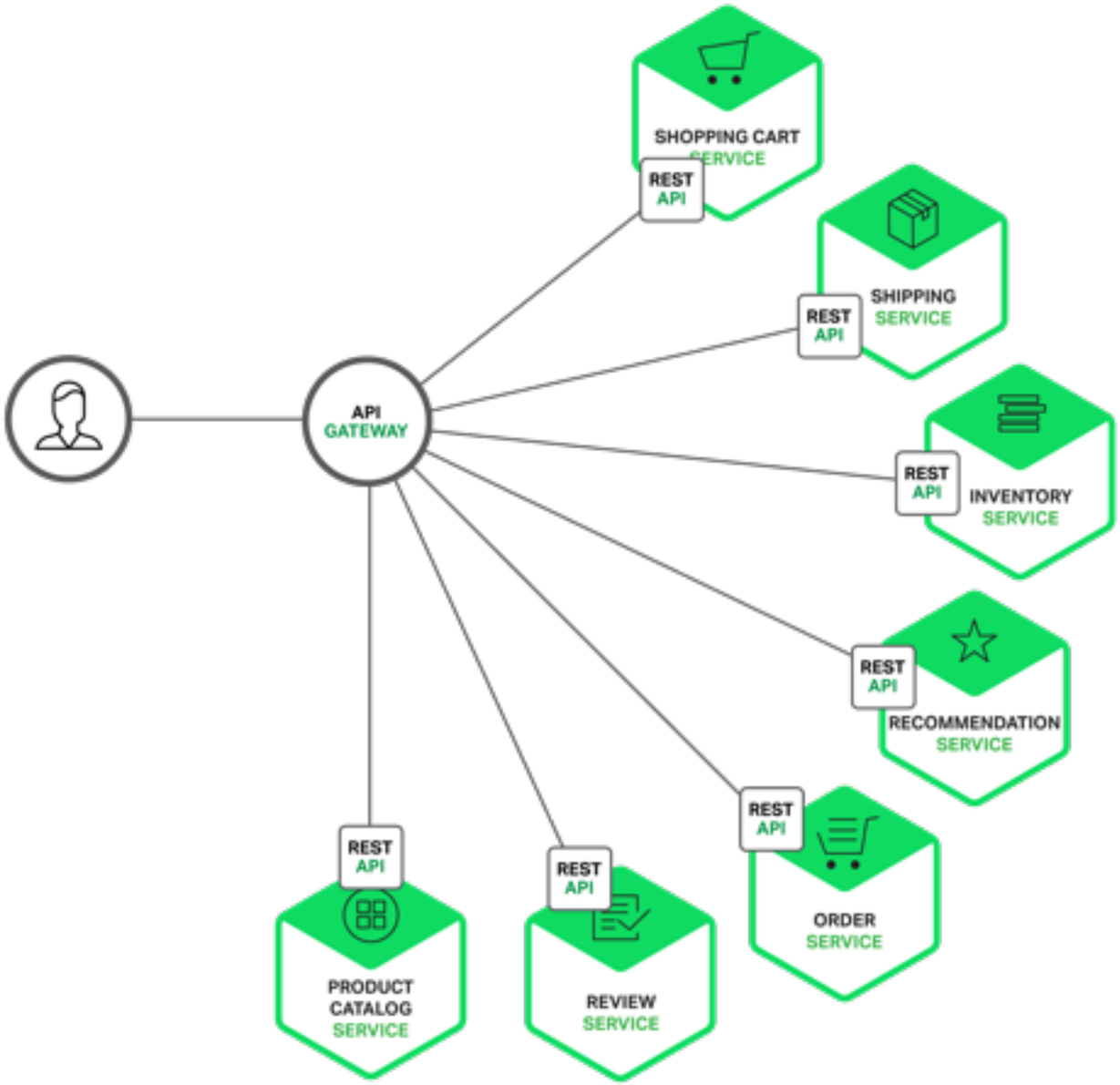
3 商品信息

4 商品推荐

5 货存信息

6 货运信息

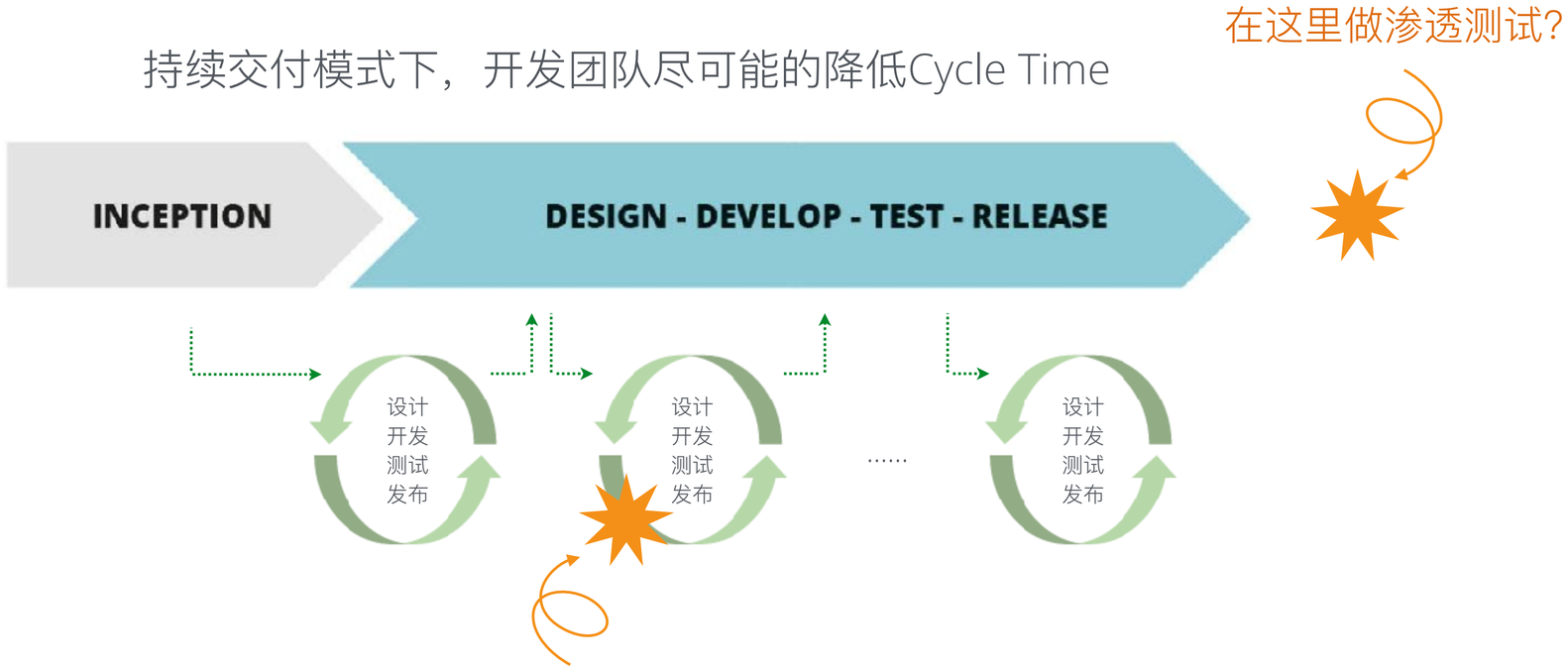
微服务应用


SHOPPING CART
SERVICE
REST
API
SHIPPING
SERVICE
REST
API
API
GATEWAY
INVENTORY
SERVICE
REST
API
RECOMMENDATION
SERVICE
REST
API
ORDER
SERVICE
REST
API
REST
API
PRODUCT
CATALOG
SERVICE
REVIEW
SERVICE

以渗透测试为依托的传统安全控制措施遭遇挑战

传统安全控制措施

持续交付模式下，开发团队尽可能的降低Cycle Time



开发团队需要承担一定的安全质量保证职责

敏感信息泄露

XSS

使用有漏洞的第三方依赖

注入

订单金额任意修改

信息重放

未进行登录凭证验证

任意文件下载

验证码回传

权限控制不严

任意文件上传

最初没有明确的安全需求；

创建有逻辑错误的概念设计；

使用糟糕的编码规范，从而带来了技术漏洞；

软件部署不当；

在维护或者更新过程中引入缺陷。

开发团队可以杜绝大部分的安全问题

避免常规的安全问题

- 注入
- 失效的身份验证和Session管理
- 跨站脚本攻击
- 失效的权限控制
- 不安全的配置
- 敏感信息泄露
- 不充足的攻击检测与预防
- 跨站请求伪造攻击
- 使用带有缺陷的第三方组件
- 未受保护的API

*OWASP*是一个开源的、非盈利的全球性安全组织，致力于应用软件的安全研究。

避免微服务下特有的安全问题

- 未对用户登录凭证检查
- 缺少资源从属关系检查
- 缺少API速率限制
- 敏感信息泄露

#1 未对用户登录凭证进行校验

- 详情：

  users\100**orders**\280010 敏感接口可以被任意调用

- 如何防范?

  对敏感数据存在的接口和页面做cookie，ssid，token或者其它验证

#2 缺少资源从属关系检查

- 详情：

users\100

users\100**orders**\280010 ◄----- 可能缺少从属关系检查

users\100**orders**\280010**comments**\5674 ◄----- 极有可能缺少从属关系检查

- 如何防范

检查资源间的从属关系

#3 缺少API速率限制

详请：

```
POST \captcha

{“mobile”: “13900001111”}
```

```
POST \user\login

{“user”: “13900001111”, “password”=“abc”}
```

```
GET \reports?range=all
```

如何防范?

添加API速率限制

#4 数据泄露

详情：

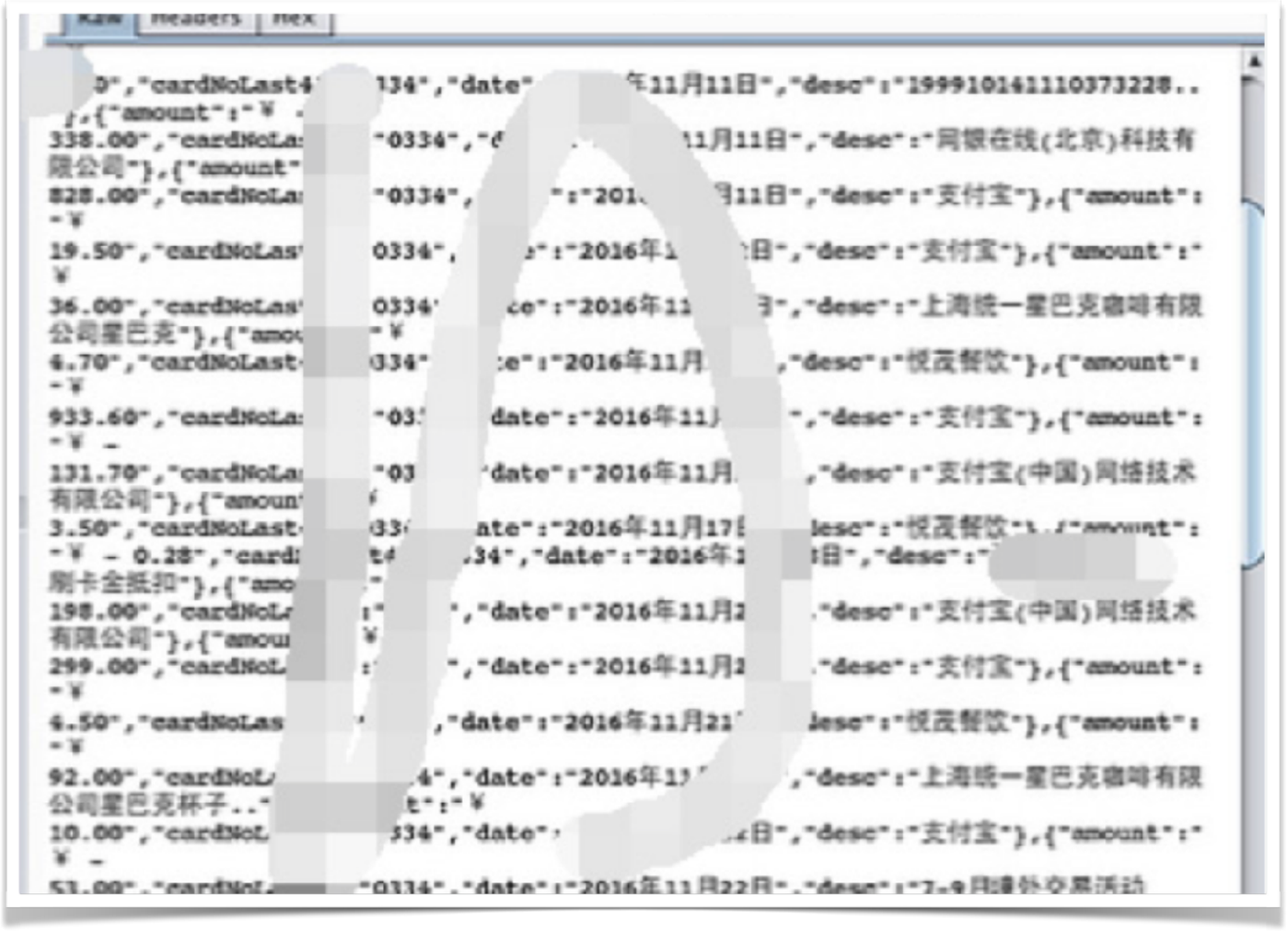
GET \orders\280010

```
{
   "id": 280010,
   "orderItems": [...],
   "user": {
      "id": 100,
      "password": “91B4E3E45B2465A4823BB5C03FF81B65"
   },
 ...
}
```

如何防范?

在返回的JSON数据中删除不必要的信息

EXAMPLE 1



某银行存在越权漏洞，知晓用户卡号，即可查询任意卡号，任意月份的**消费详单**，包括**消费金额**，每笔**消费时间**、**消费时商户名称**等十分敏感的信息。

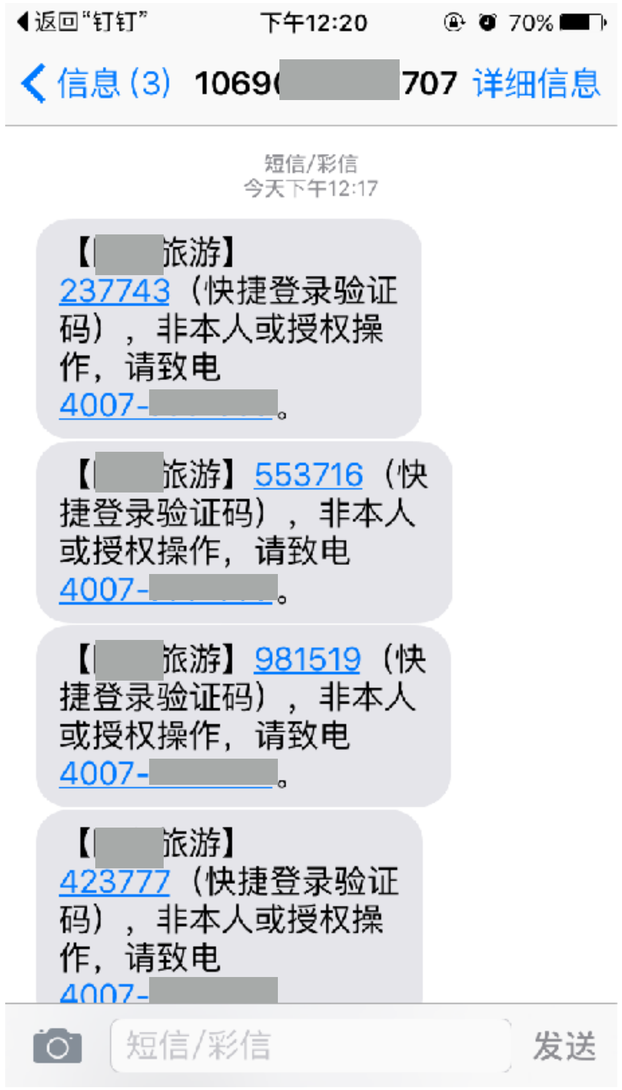
后经测试该接口无任何认证防御措施，可以通过遍历卡号的后几位，从而获取大量用户的敏感信息

EXAMPLE 2


```
{
  - list: [
      - {
            cargoName: "货物",
            orderNo: "NO10
            transNo: null,
            userId: "353
            shipperMobile: "181
            consigneeName: "陈
            orderStatus: "VOID",
            evaluate: null,
            senddate: 1491
            shipperName: "陈
            shipperProvince: "江苏省",
            shipperCity: "南京市",
            shipperArea: null,
            shipperAddress: "麒麟
            consigneeMobile: "183
            consigneeProvince: "江苏省",
            consigneeCity: "盐城市",
            consigneeArea: null,
            consigneeAddress: "富
            cargoVolume: 1,
            cargoWeight: 1,
            cargoPiece: 0,
            remarks: null,
            productTypeName: "定日达",
            orderId: null,
            orderOrigin: null,
            shipDept: null,
            einoEscoSecondCode: null,
            einoEscoSecondName: null,
            errcode: null,
            errmsg: null
        },
```


在某物流公司的移动端应用中，甚至都不需要身份验证，外部均可任意调用*APP*接口查询寄送物流信息，造成上千万物流订单敏感信息泄露。

EXAMPLE 3



发送短信接口未做任何限制，导致短信轰炸攻击

最佳实践

安全测试策略

#1 自动化安全扫描工具

acunetix

NIKTO

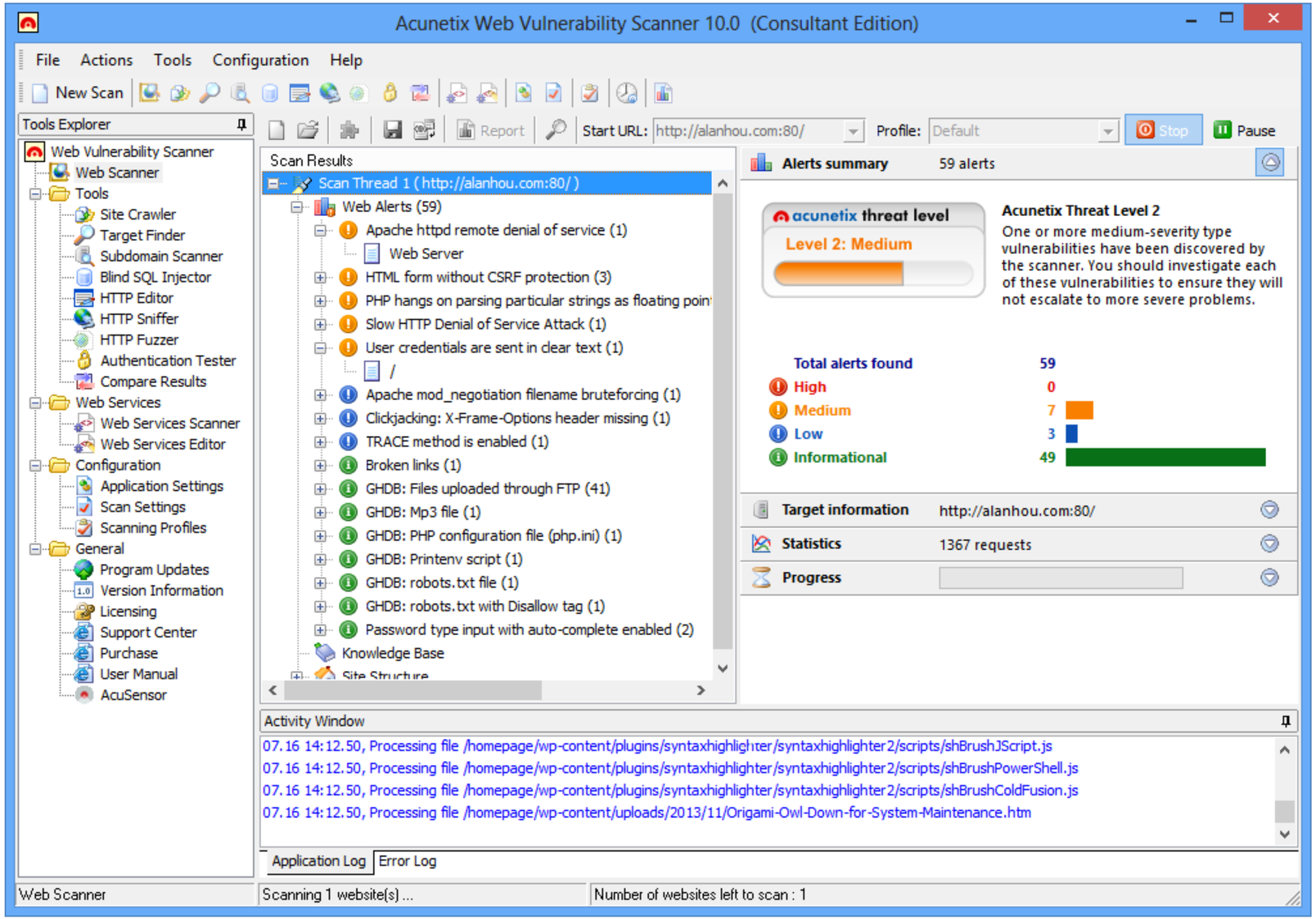
netsparker

N-Stalker®
THE WEB SECURITY SPECIALISTS

AppScan
IBM Security

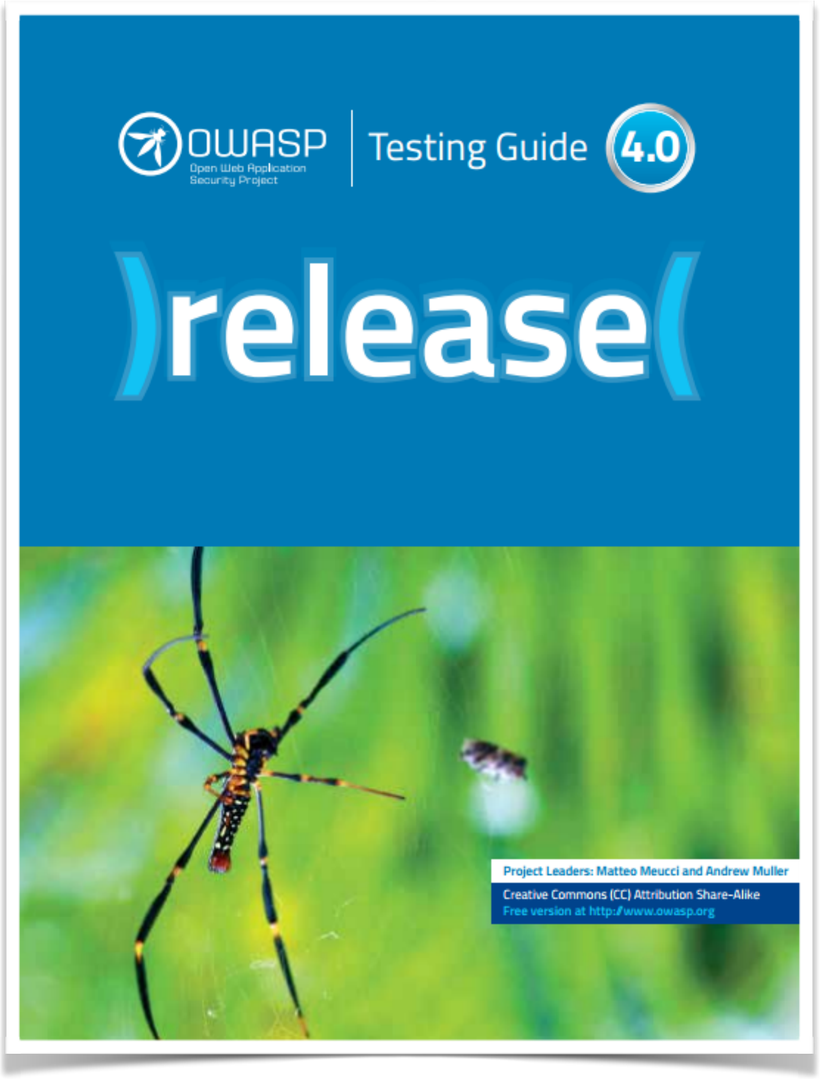
FORTIFY
An HP Company
www.FortifyMyApp.com

#1 自动化安全扫描工具


Acunetix Web Vulnerability Scanner 10.0 (Consultant Edition)
File Actions Tools Configuration Help
New Scan
Tools Explorer
Web Vulnerability Scanner
Web Scanner
Tools
Site Crawler
Target Finder
Subdomain Scanner
Blind SQL Injector
HTTP Editor
HTTP Sniffer
HTTP Fuzzer
Authentication Tester
Compare Results
Web Services
Web Services Scanner
Web Services Editor
Configuration
Application Settings
Scan Settings
Scanning Profiles
General
Program Updates
Version Information
Licensing
Support Center
Purchase
User Manual
AcuSensor
Report
Start URL: http://alanhou.com:80/
Profile: Default
Stop
Pause
Scan Results
Scan Thread 1 (http://alanhou.com:80/)
Web Alerts (59)
Apache httpd remote denial of service (1)
Web Server
HTML form without CSRF protection (3)
PHP hangs on parsing particular strings as floating poin
Slow HTTP Denial of Service Attack (1)
User credentials are sent in clear text (1)
/
Apache mod_negotiation filename bruteforcing (1)
Clickjacking: X-Frame-Options header missing (1)
TRACE method is enabled (1)
Broken links (1)
GHDB: Files uploaded through FTP (41)
GHDB: Mp3 file (1)
GHDB: PHP configuration file (php.ini) (1)
GHDB: Printenv script (1)
GHDB: robots.txt file (1)
GHDB: robots.txt with Disallow tag (1)
Password type input with auto-complete enabled (2)
Knowledge Base
Alerts summary 59 alerts
acunetix threat level
Level 2: Medium
Acunetix Threat Level 2
One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.
Total alerts found 59
High 0
Medium 7
Low 3
Informational 49
Target information http://alanhou.com:80/
Statistics 1367 requests
Progress
Activity Window
07.16 14:12.50, Processing file /homepage/wp-content/plugins/syntaxhighlighter/syntaxhighlighter2/scripts/shBrushJScript.js
07.16 14:12.50, Processing file /homepage/wp-content/plugins/syntaxhighlighter/syntaxhighlighter2/scripts/shBrushPowerShell.js
07.16 14:12.50, Processing file /homepage/wp-content/plugins/syntaxhighlighter/syntaxhighlighter2/scripts/shBrushColdFusion.js
07.16 14:12.50, Processing file /homepage/wp-content/uploads/2013/11/Origami-Owl-Down-for-System-Maintenance.htm
Application Log
Error Log
Web Scanner
Scanning 1 website(s) ...
Number of websites left to scan : 1

#2 OWASP TESTING GUIDE

- 信息搜集
- 配置以及部署管理测试
- 身份鉴别管理测试
- 认证测试
- 授权测试
- 会话管理测试
- 输入验证测试
- 错误处理测试
- 密码学测试
- 业务逻辑测试
- 客户端测试



例子 - 认证测试

- 加密信道证书传输
- 用户枚举测试
- 可猜解用户账户猜测(遍历)测试
- 暴力测试
- 认证架构绕过测试
- 记住密码和密码重置弱点测试
- ……

概要:

……

简单地跳过登录页面和直接调用一个理应在认证通过后才能访问的内部网页，就可以绕过认证计划。……

问题描述:

……

与认证模式有关的问题存在于软件开发周期中的各个阶段,如设计阶段,开发阶段,部署阶段……

黑盒测试实例: ……

灰盒测试实例: ……

参考: 工具……

手动测试辅助工具

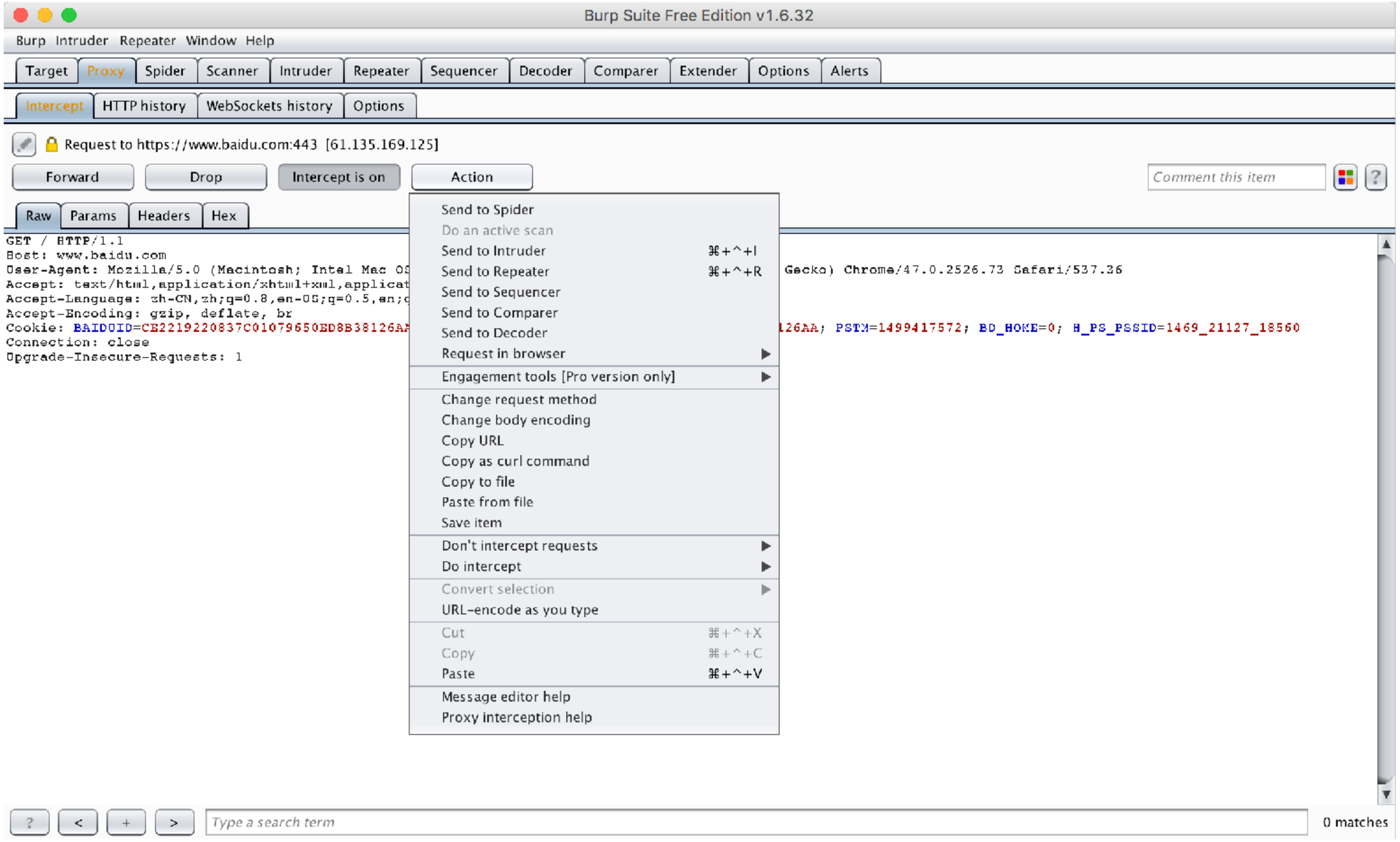

sqlmap
Automatic SQL injection and database takeover tool


OWASP ZAP


BURPSUITE
PROFESSIONAL


XENOTIX 5
XSS EXPLOIT FRAMEWORK
COPYRIGHT © OWASP XENOTIX| OPENSECURITY.IN

手动测试辅助工具


Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to https://www.baidu.com:443 [61.135.169.125]
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
GET / HTTP/1.1
Host: www.baidu.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS
Accept: text/html,application/xhtml+xml,applicat
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q
Accept-Encoding: gzip, deflate, br
Cookie: BAIDUID=CE2219220837C01079650ED8B38126AA
Connection: close
Upgrade-Insecure-Requests: 1
Gecko) Chrome/47.0.2526.73 Safari/537.36
126AA; PSTM=1499417572; BD_HOME=0; H_PS_PSSID=1469_21127_18560
Send to Spider
Do an active scan
Send to Intruder ⌘+^+I
Send to Repeater ⌘+^+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools [Pro version only]
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Convert selection
URL-encode as you type
Cut ⌘+^+X
Copy ⌘+^+C
Paste ⌘+^+V
Message editor help
Proxy interception help
? < + >
Type a search term
0 matches

威胁建模

使用威胁建模，使用STRIDE和DREAD模型来帮助我们识别和评估应用安全问题。

STRIDE模型

Spoofing (欺骗)
Tampering (篡改)
Repudiation (否认)
Information disclosure (信息泄露)
Denial of service (拒绝服务)
Elevation privilege (权限提升)

DREAD模型

Damage potential (潜在损害)
Reproducibility (可重现性)
Exploitability (可利用新)
Affected users (受影响的用户)
Discoverability (可发现性)

#4 编写自动化安全测试用例

安全需求:

消费清单 只能被其 **所有者** 看到

伪代码:

```
bob                = given_a_logged_in_user(“bob”);
bobs_expense  =
given_an_existing_expense_of_user(bob);
result             =
bob.request_expense_details(bobs_expense)
assert_that ( result, is ( APPROVED) );
```

```
bob                = given_a_logged_in_user(“bob”);
johns_expense  =
given_an_existing_expense_of_user(john);
result             =
bob.request_expense_details(johns_expense)
assert_that ( result, is ( REJECTED ) );
```

#5 持续监控安全质量

把安全测试加入到持续集成!

#6 第三方依赖安全扫描

Most used Java components with critical vulnerabilities

LIBRARY	VERSION	% OF JAVA APPLICATIONS
commons-collections-3.2.1.jar	3.2.1	25.0%
commons-fileupload-1.2.1.jar	1.2.1	10.4%
batik-css-1.7.jar	1.7	9.5%
batik-util-1.7.jar	1.7	9.4%
commons-fileupload-1.2.jar	1.2	9.3%
batik-ext-1.7.jar	1.7	9.2%
spring-web-3.1.1.RELEASE.jar	3.1.1.RELEASE	4.7%
spring-core-3.1.1.RELEASE.jar	3.1.1.RELEASE	4.7%
spring-beans-3.1.1.RELEASE.jar	3.1.1.RELEASE	4.6%
spring-context-3.1.1.RELEASE.jar	3.1.1.RELEASE	4.5%

#6 第三方依赖安全扫描

DEPENDENCY-CHECK

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 or its use. Any use of the tool and the reporting provided is at the user's risk. 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.

Project: Demo Insecure Project

Scan Information (show all):

- *dependency-check version*: 1.3.1
- *Report Generated On*: Nov 3, 2015 at 23:20:33 EST
- *Dependencies Scanned*: 14
- *Vulnerable Dependencies*: 3
- *Vulnerabilities Found*: 13
- *Vulnerabilities Suppressed*: 0
- ...

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	CPE	GAV	Highest Severity	CVE Count	CPE Confidence	Evidence Count
commons-fileupload-1.3.jar	cpe:/a:apache:commons_fileupload:1.3	commons-fileupload:commons-fileupload:1.3	Medium	1	HIGHEST	29
struts2-core-2.3.15.3.jar	cpe:/a:apache:struts:2.3.15.3	org.apache.struts:struts2-core:2.3.15.3	High	6	HIGHEST	25
xwork-core-2.3.15.3.jar	cpe:/a:apache:struts:2.3.15.3	org.apache.struts.xwork:xwork-core:2.3.15.3	High	6	HIGHEST	24

Dependencies

小贴士

#1 团队人员安全能力的培养

#2 用自动化来提高安全检测效率

#3 结合项目实际情况实施安全测试

#4 没有绝对的安全，只有相对的安全

Security is a life-long process, not a one shot accident.

THANK YOU

ThoughtWorks®