Ch3 API Testing

Test Code Interactions (3)

Instructor: Haiying SUN

E-mail: hysun@sei.ecnu.edu.cn

Office: ECNU Science Build B1104

Available Time: Wednesday 8:00 -12:00 a.m.

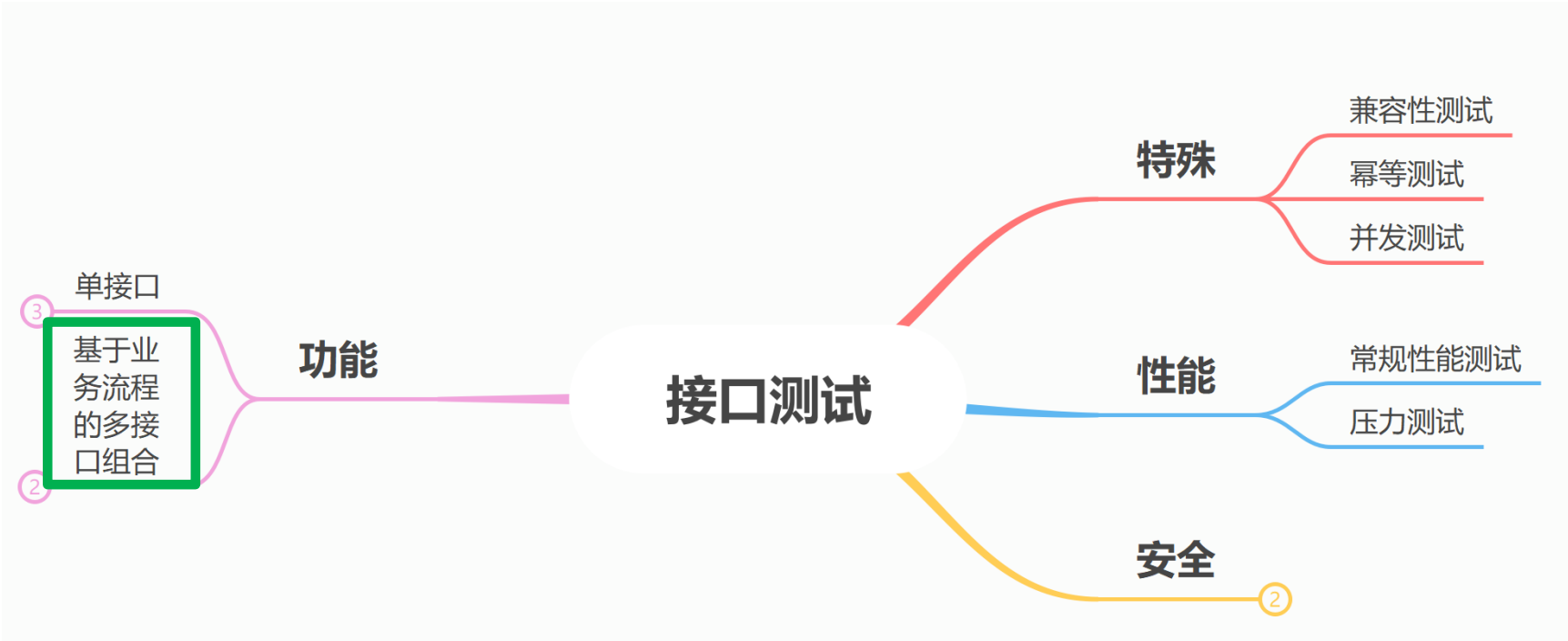
Overview

- Introduction to API Testing
- Common Integrated Defects
- API Tests Design
- API Tests Implementation
  - Postman & Rest Assured
- API Test Generation

Overview

- Introduction to API Testing
- Common Intergraded Defects
- API Tests Design
- API Tests Implementation
  - Postman & Rest Assured
- API Test Generation

Design API Test Cases



APIs Call Sequences Testing

- Scenarios
  - 前端一个操作触发后端一系列API调用
  - API之间存在耦合关系
  1. API A的某些响应输出是API B的请求输入： A;B
  2. API A在内部调用了API B (B可能是自己也可能是第三方提供)
  - 服务器拒绝在执行A;B之后执行API C
- Test Strategy
  - 使用请求序列模拟API调用序列

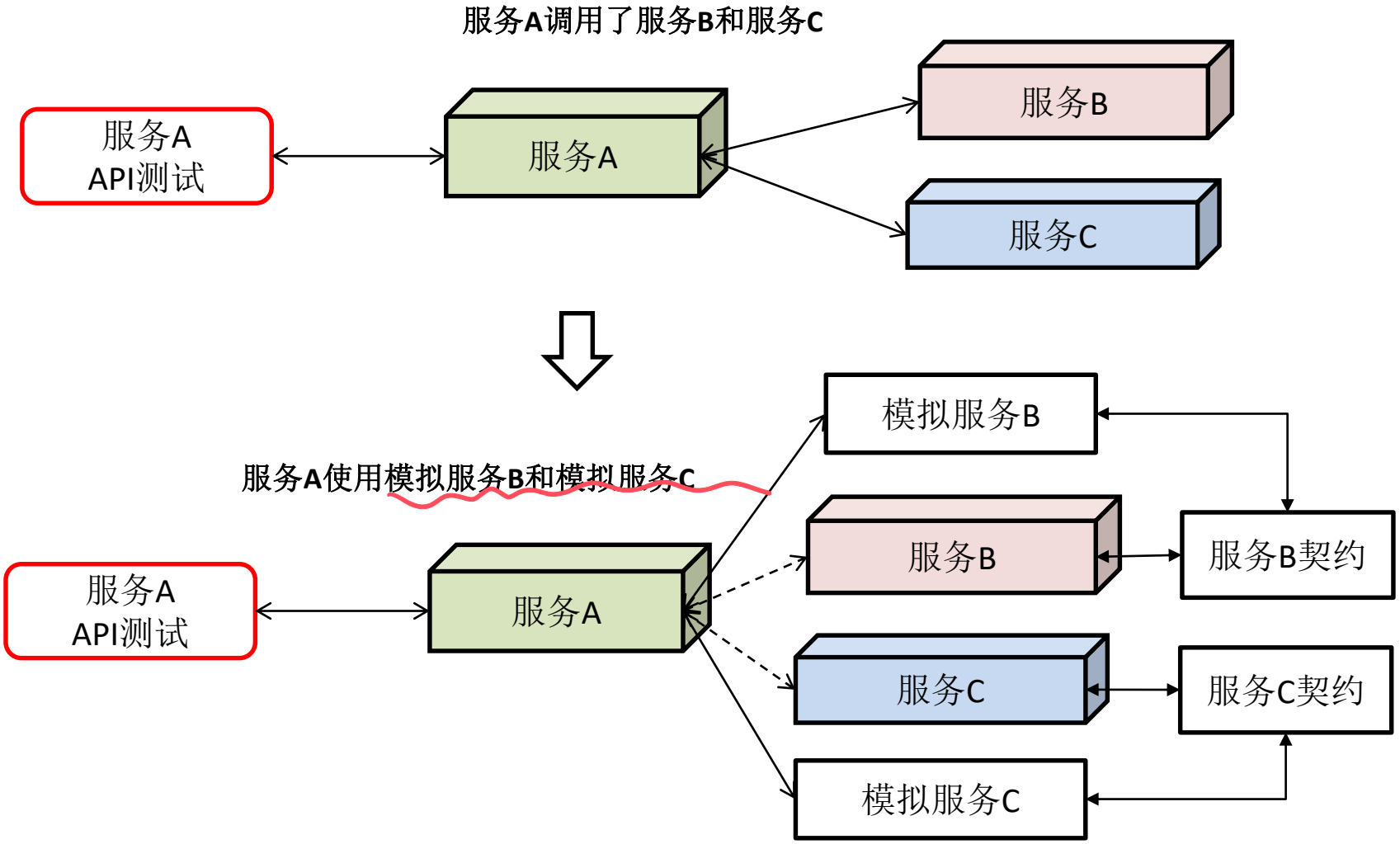
APIs Call Sequences Testing

- Problem

1. 获取API调用序列：抓包分析，用户行为日志
2. API之间的解耦：

- API A的某些响应输出是API B的请求输入
  - ✓接口脚本代码化提取有关联的输入/输出
- API之间（服务与服务）存在调用关系
  - ✓Mock Server，即使用模拟服务替代被依赖的真实服务

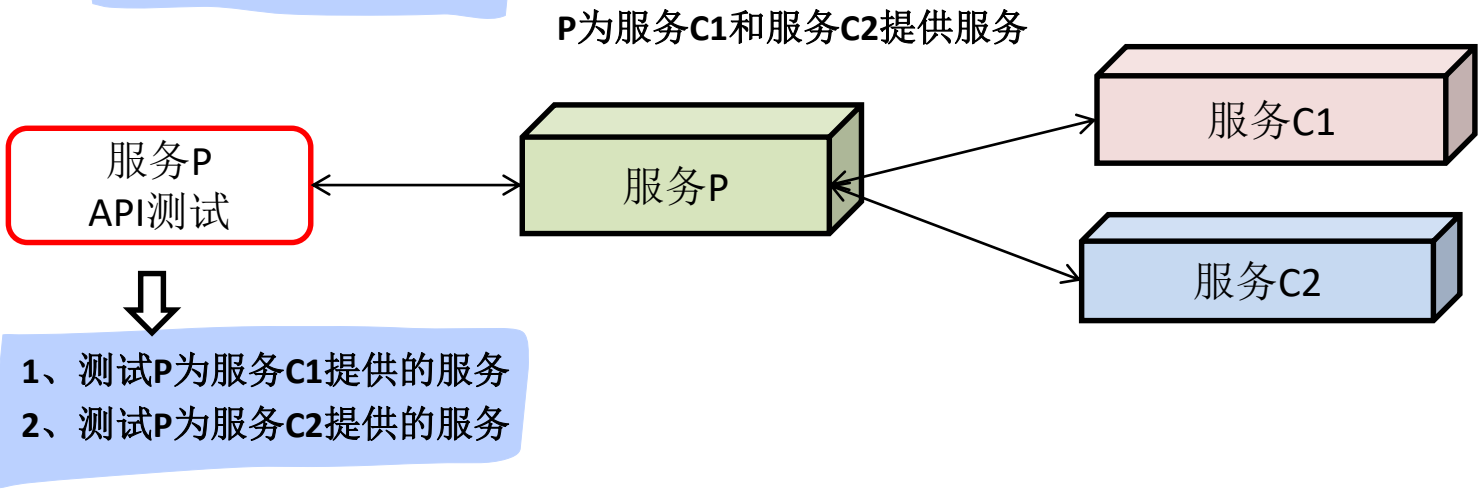
APIs Call Sequences Testing



APIs Call Sequences Testing

- 基于消费者契约的API测试
  - 测试用例过于庞大，资源有限
  - 策略：不都测，用什么测什么
  - 核心：收集对外提供的服务（契约）

1. 前置代理收集
2. 解析API网关获得

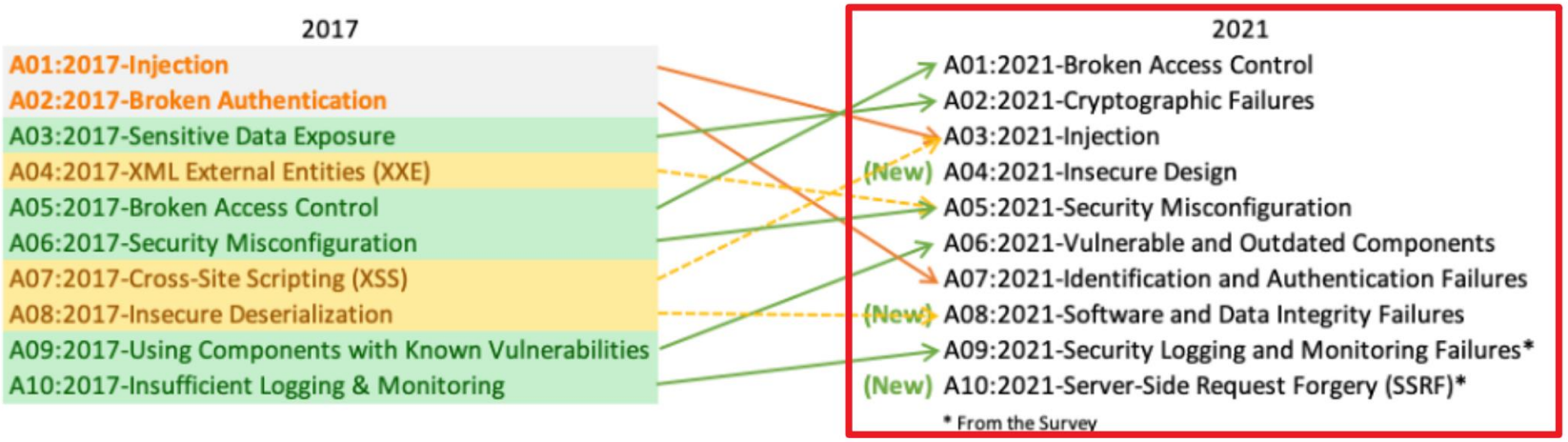


API Compatible Testing

- 向后兼容：新API版本应该兼容旧API版本，需满足
  1. 调用参数不变
  2. 不能删减/修改返回的响应中的字段
     - 删减字段
     - 修改字段名称
     - 字段值发生了非预期的变化
- 通过比较新旧API结构的差异进行测试
  - 参数个数、名称、类型
  - 响应字段的变化情况：测试断言并不检测每个响应字段，因此，针对不同版本API，需要提供一种方法，当响应中的所有字段发生变化时给出提示

API Security

- [Web Application Security] protect your users, devices, and wider network against internet-based cyberattacks that can lead to breaches and data loss of a public-facing websites.



OWASP[1] Top10 2021 [2]

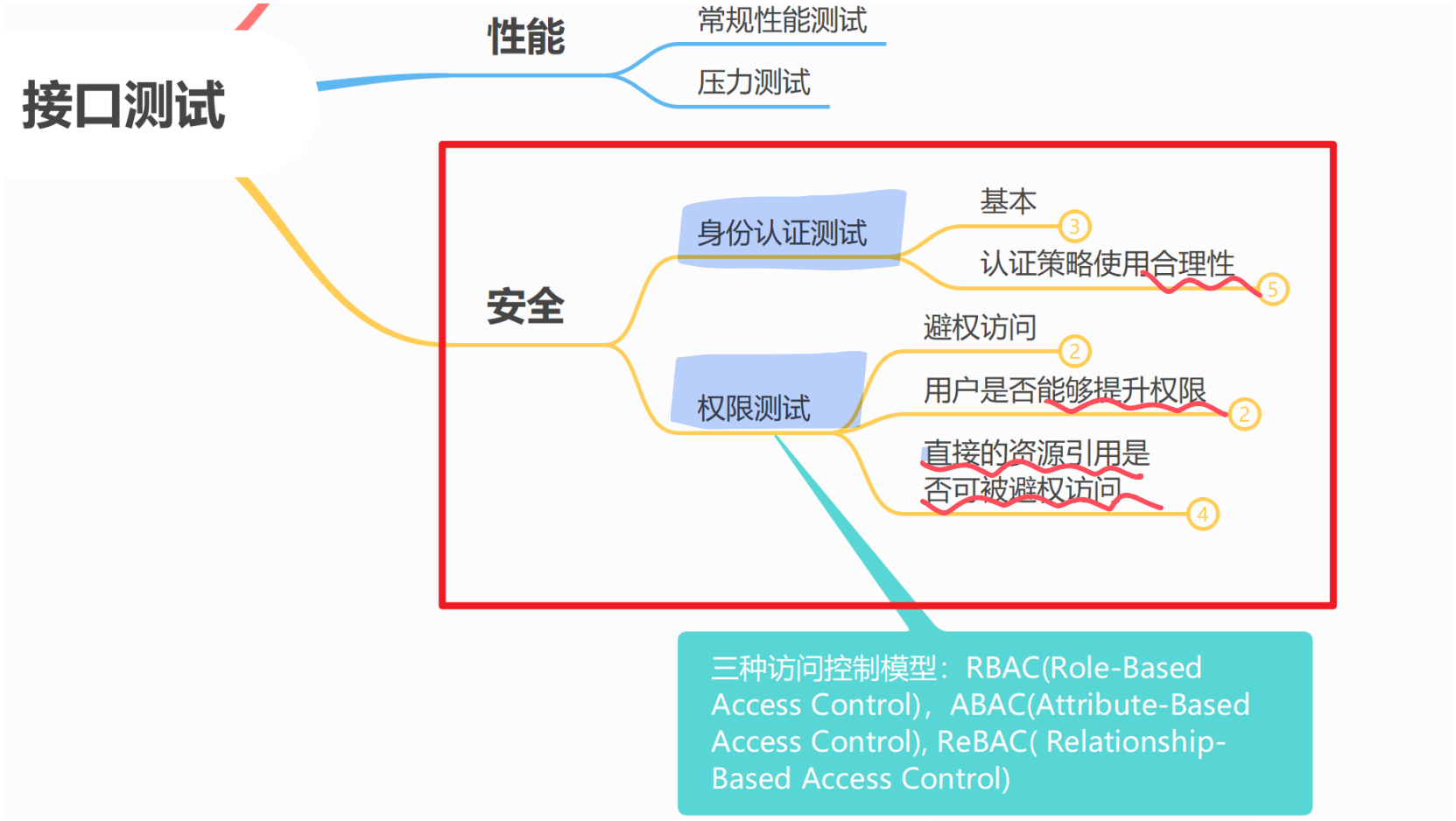
[1] Open Web Application Security Project
[2] https://owasp.org/Top10/

API Security

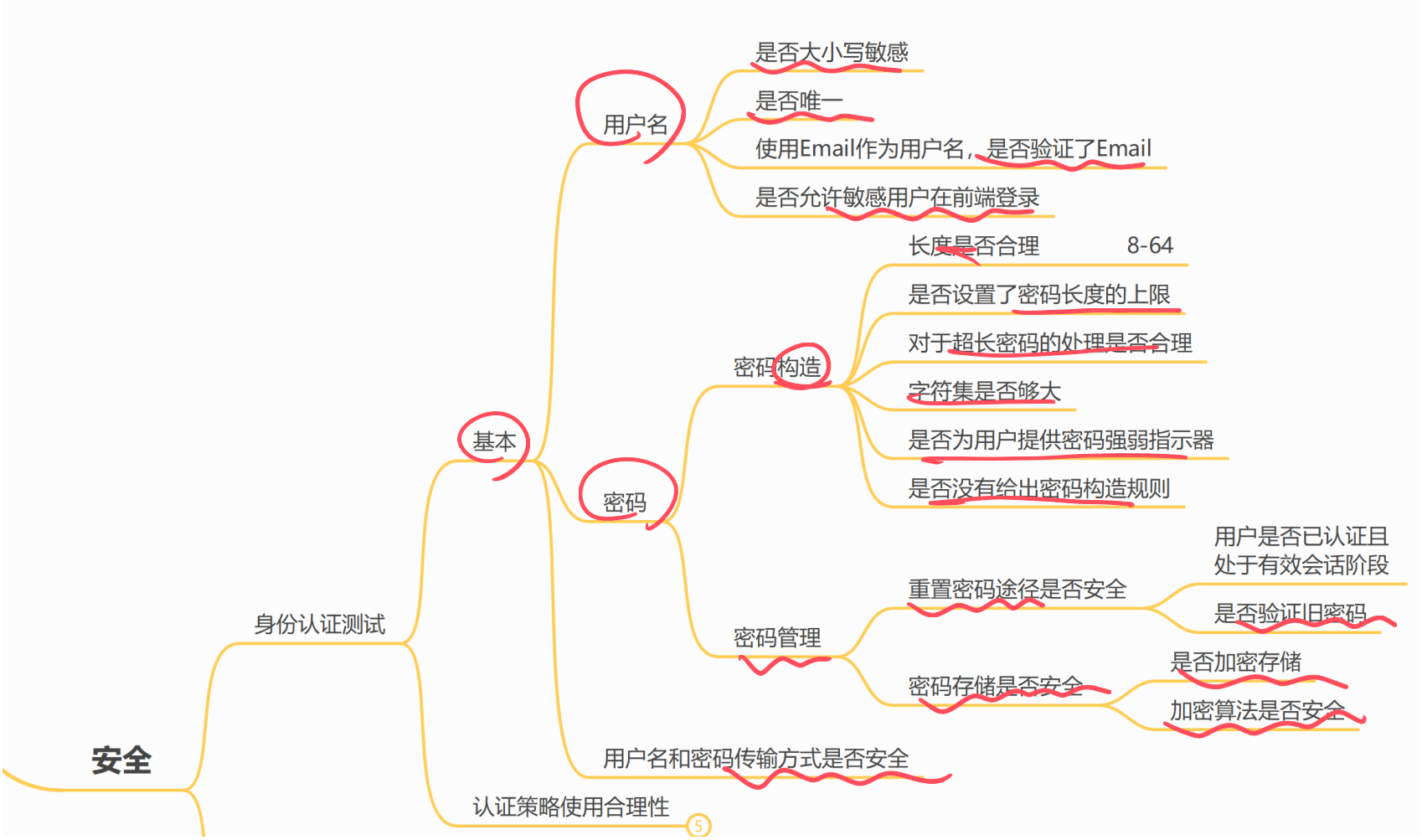
- Input Validation should not be used as the primary method of preventing attacks, but can significantly contribute to reducing their impact if implemented properly.
- Authentication（身份认证）
  - The process of verifying that an individual, entity or website is whom it claims to be[1]
- Authority（访问控制）
  - The process of verifying that a requested action or service is approved for a specific entity [2]

[1] https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html
[2] https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Testing_Automation_Cheat_Sheet.html

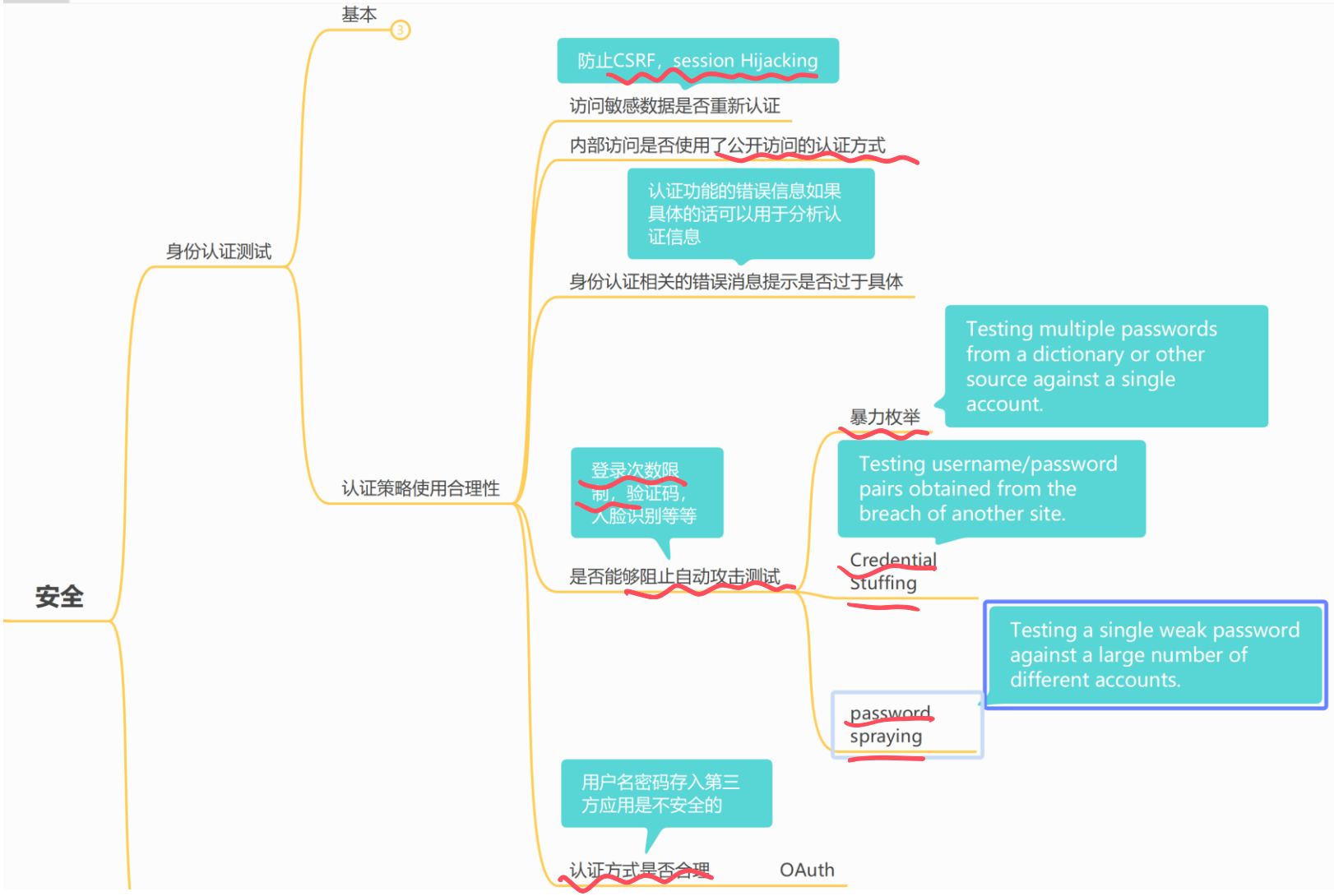
API Security Testing Requirements



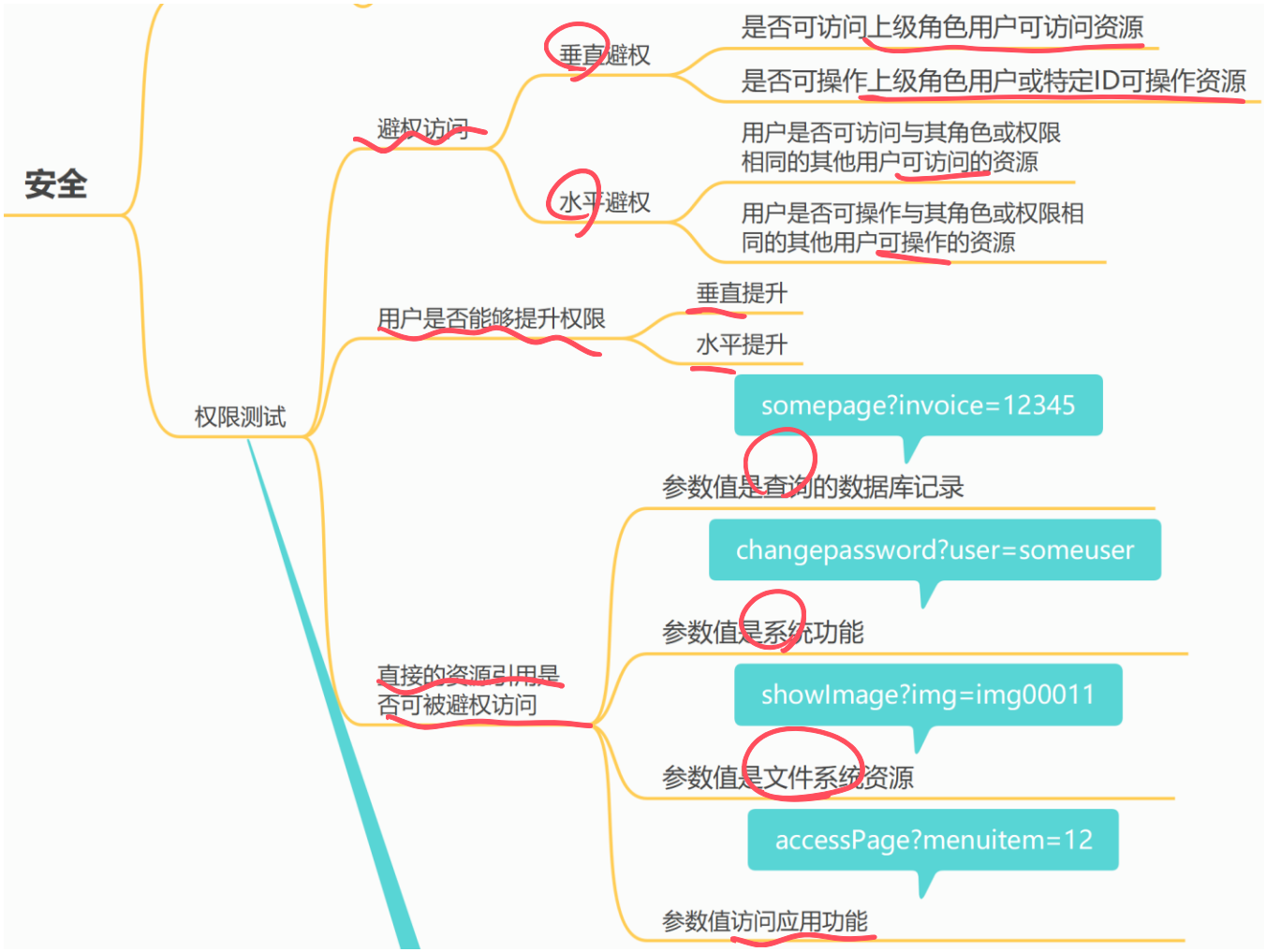
API Security Testing Requirements



API Security Testing Requirements



API Security Testing Requirements



Typical Security Attacks

- Injection Attack
  - SQL injection： A SQL injection attack consists of insertion or “injection” of a SQL query via the input data from the client to the application
  - OS Command injection： supplies operating system commands through a web interface in order to execute OS commands

```
String query = "SELECT \* FROM accounts WHERE custID='" + request.getParameter("id") + “’”;
http://example.com/app/accountView?id=' or '1'='1
```

SQL injection Example

```
http://sensitive/cgi-bin/userData.pl?doc=user1.txt
http://sensitive/cgi-bin/userData.pl?doc=/bin/ls|
```

OS Command injection

Typical Security Attacks

- Session Hijacking (会话劫持)
  - Cookie劫持
  1. 通过XSS(Cross Site Script)获取他人Cookie
  2. 获取电脑上保存的Cookie文件
- Replay Attack
  - 通过抓包方式得到客户端的请求数据及请求链接，重复地向服务器发送请求的行为
- Server Side Request Forgery（SSRF）
  - 利用外部可访问的Web Application存在的缺陷伪造请求，攻击外部无法访问（例如防火墙内）的内部服务

Summary

- Web API Interface should be testes form multiple dimensions, such as function, security, performance etc.
- API call sequence testing is becoming more and more important during the microservice era.
- How to deal with coherency is the kernel problem that faces API sequence testing
- APIs security testing aim to verify security strategies are working as expected

The End