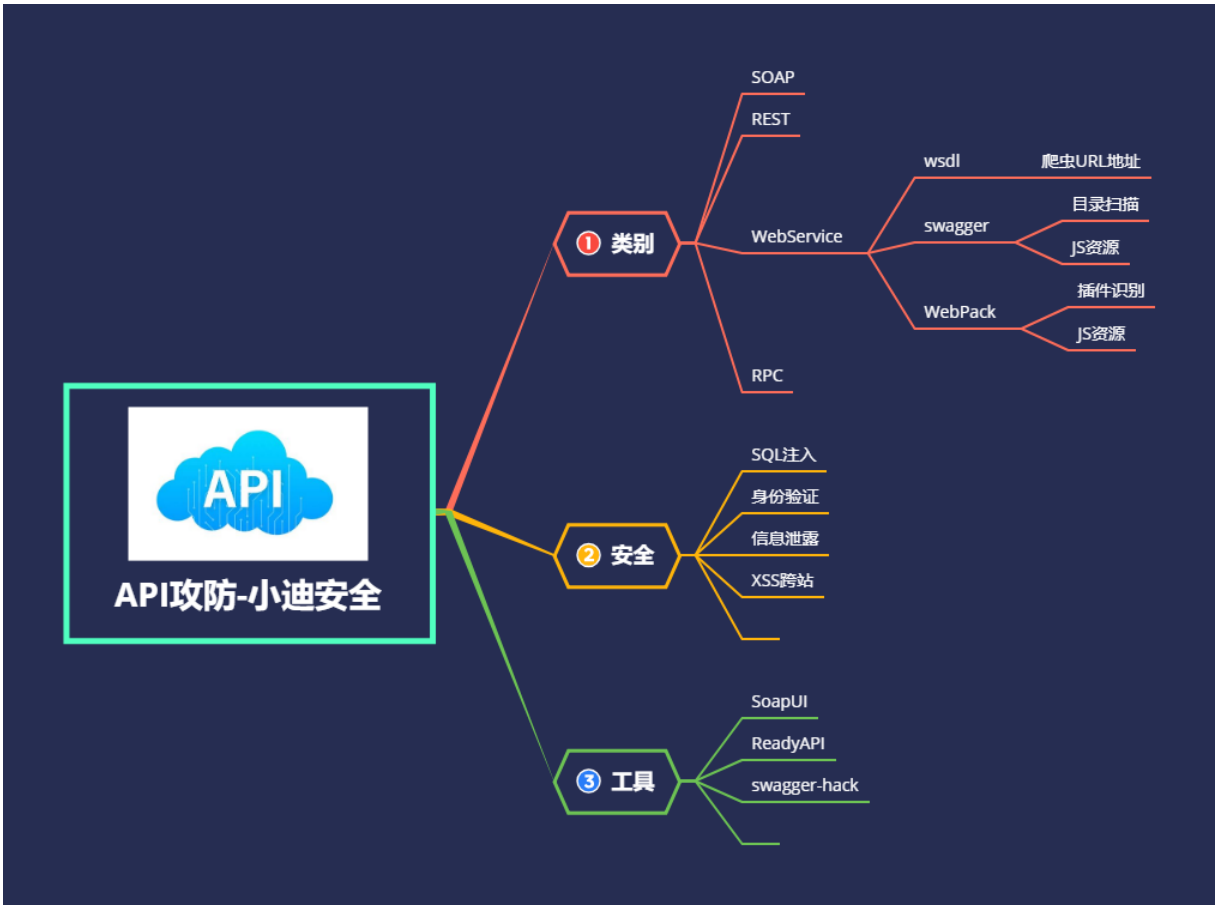
API 攻防-接口安全&阿里云 KEY&Postman&XXE&DVWS&鉴权&泄漏



#知识点：

1.HTTP 类接口-测评

2.RPC 类接口-测评

3.Web Service 类-测评

#内容点：

SOAP（Simple Object Access Protocol）简单对象访问协议是交换数据的一种协议规范，是一种轻量的、简单的、基于 XML（标准通用标记语言下的一个子集）的协议，它被设计成在 WEB 上交换结构化的和固化的信息。SOAP 不是 Web Service 的专有协议。

SOAP 使用 HTTP 来发送 XML 格式的数据，可以简单理解为：SOAP = HTTP +XML

REST（Representational State Transfer）即表述性状态传递，在三种主流的 Web 服务实现方案中，因为 REST 模式的 Web 服务与复杂的 SOAP 和 XML-RPC 对比来讲明显的更加简洁，越来越多的 Web 服务开始采用 REST 风格设计和实现。例如，Amazon.com 提供接近 REST 风格的 Web 服务进行图书查找；雅虎提供的 Web 服务也是 REST 风格的。

WSDL（Web Services Description Language）即网络服务描述语言，用于描述 Web 服务的公共接口。这是一个基于 XML 的关于如何与 Web 服务通讯和使用的服务描述；也就是描述与目录中列出的 Web 服务进行交互时需要绑定的协议和信息格式。通常采用抽象语言描述该服务支持的操作和信息，使用的时候再将实际的网络协议和信息格式绑定给该服务。

#接口数据包：

Method：请求方法

攻击方式：OPTIONS,PUT,MOVE,DELETE

效果：上传恶意文件，修改页面等

URL：唯一资源定位符

攻击方式：猜测，遍历，跳转

效果：未授权访问等

Params：请求参数

攻击方式：构造参数，修改参数，遍历，重发

效果：爆破，越权，未授权访问，突破业务逻辑等

Authorization：认证方式

攻击方式：身份伪造，身份篡改

效果：越权，未授权访问等

演示案例：

- 工具使用-Postman 自动化测试
- 安全问题-Dvws 泄漏&鉴权&XXE
- 安全问题-阿里 KEY 信息泄漏利用
- 应用方向-违法 APP 打包接口分析

#工具使用-Postman 自动化测试

https://www.postman.com/downloads/

#安全问题-Dvws 泄漏&鉴权&XXE

https://github.com/snoopysecurity/dvws-node

遍历数据 接口数据

鉴权安全 越权判定

越权：

观察注册后，返回数据包

修改注册时，数据包 admin=true

JWT：

XXE 安全

```
<?xml version="1.0"?>
<!DOCTYPE Mikasa [
<!ENTITY test SYSTEM  "file:///etc/passwd">
]>

<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:urn="urn:examples:usernameservice">
   <soapenv:Header/>
   <soapenv:Body>
      <urn:Username
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
>
         <username xsi:type="xsd:string">&test;</username>
      </urn:Username>
   </soapenv:Body>
</soapenv:Envelope>
```

#安全问题-阿里 KEY 信息泄漏利用

https://yun.cloudbility.com/

https://github.com/mrknow001/aliyun-accesskey-Tools

接口配置文件泄漏导致云资源主机受控

#应用方向-违法 APP 打包接口分析

完整的分析流程

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址