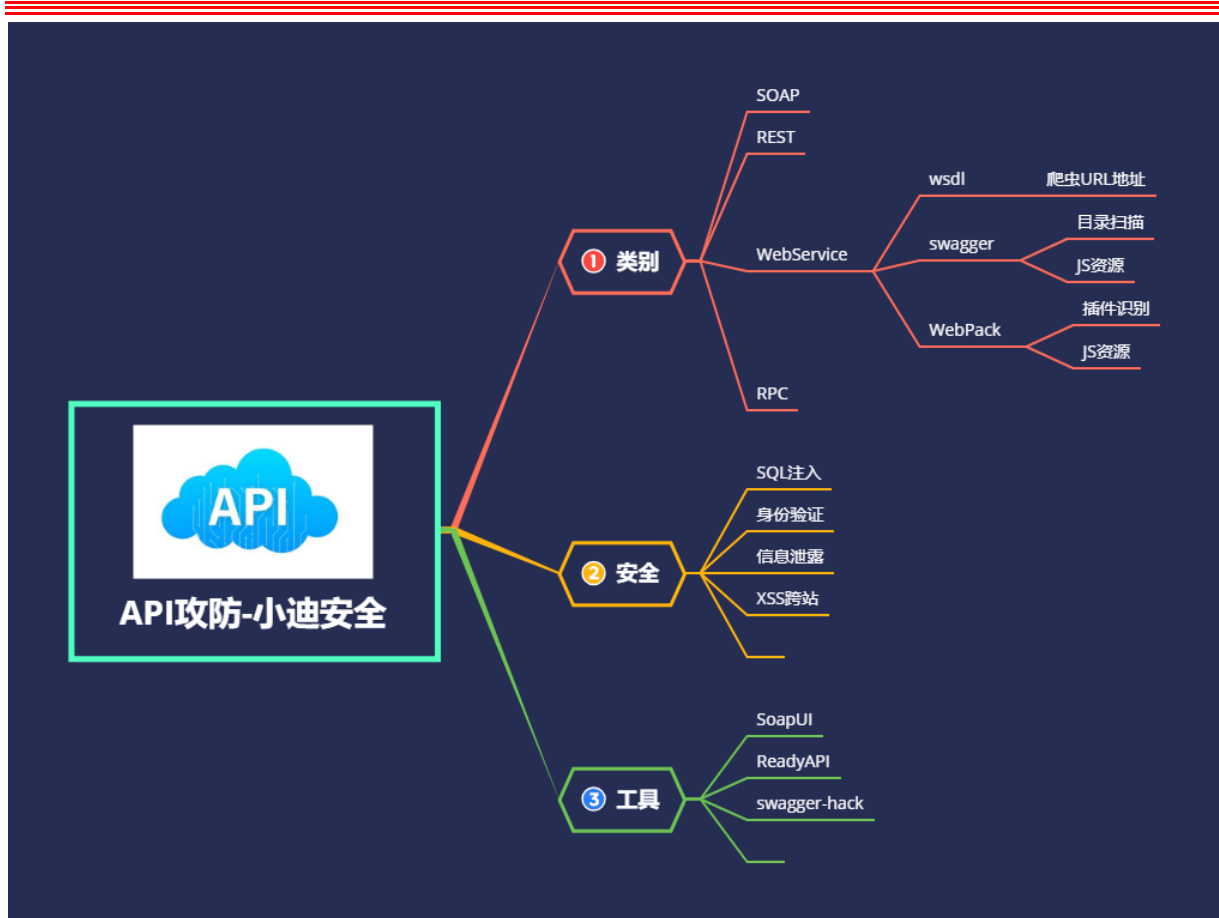


API 攻防-接口安全

&WebPack&REST&SOAP&WSDL&WebService



#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：

- WebService 类-Wsdl&ReadyAPI-SQL 注入
 - SOAP 类-Swagger&SoapUI&EXP-信息泄露
 - HTTP 类-Webpack&PackerFuzzer-信息泄露
-
-

#WebService 类-Wsdl&SoapUI

探针：?wsdl

利用：SoapUI&ReadyAPI

#SOAP 类-Swagger&SoapUI&EXP

探针：目录&JS 资源

利用：SoapUI&EXP

<https://github.com/lijiejie/swagger-exp>

<https://github.com/jayus0821/swagger-hack>

目录：

/swagger

/api/swagger

/swagger/ui

/api/swagger/ui

/swagger-ui.html

/api/swagger-ui.html

/user/swagger-ui.html

/libs/swaggerui

/api/swaggerui

/swagger-resources/configuration/ui

/swagger-resources/configuration/security

#HTTP 类-Webpack&PackerFuzzer

探针：插件&JS 资源

利用：PackerFuzzer

<https://github.com/rtcatc/Packer-Fuzzer>

涉及资源：

补充：[涉及录像课件资源软件包资料等下载地址](#)
