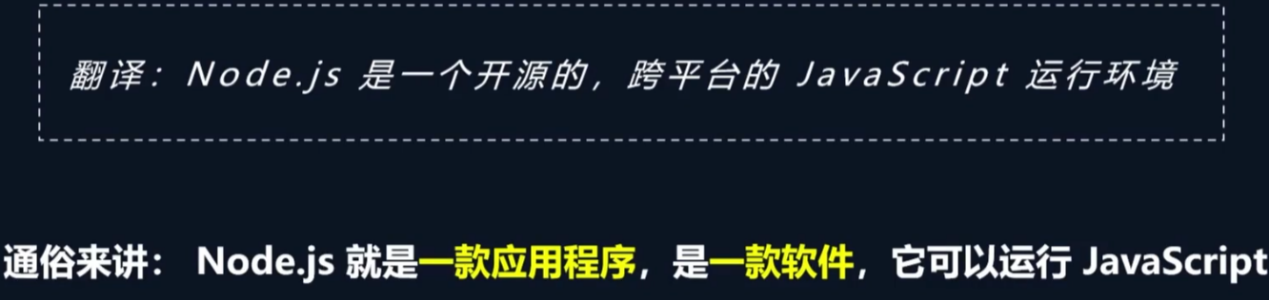
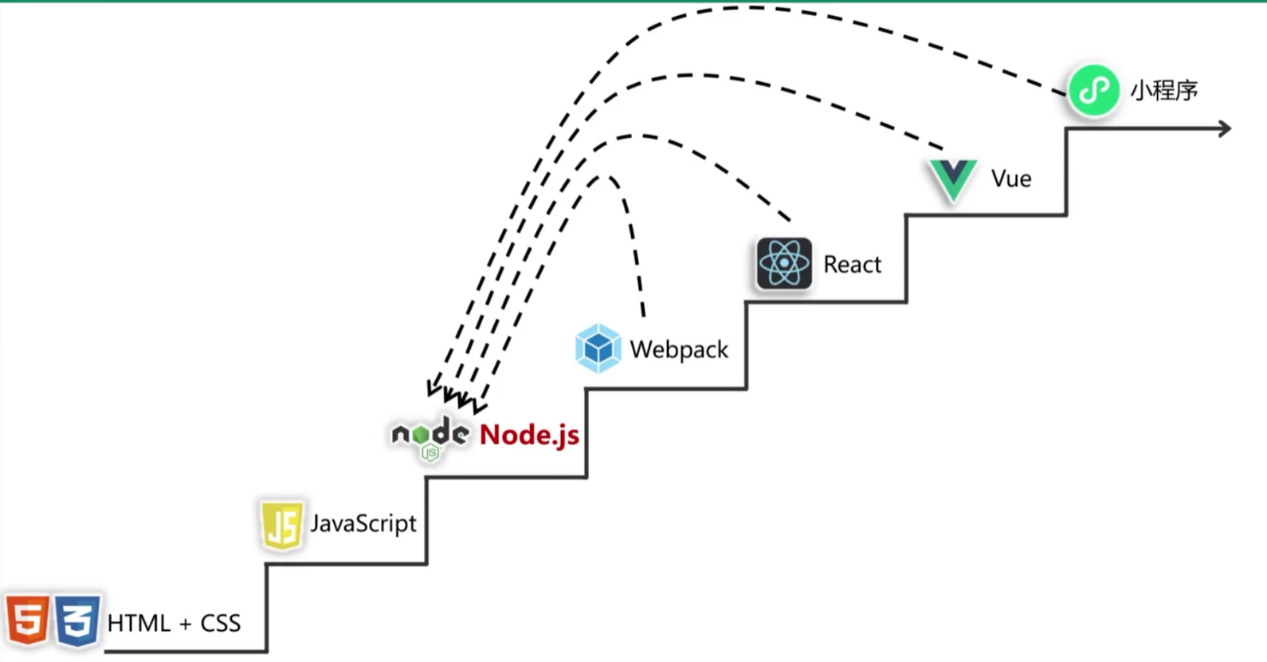
Web开发-JS应用&NodeJS&原型链污染&文件系统&Express模块&数据库通讯&审计



#知识点：  
1、安全开发-原生PHP-超级全局变量  
2、安全开发-原生PHP-代码审计案例  
---------------------------------------------  
0、安全开发-原生PHP-数据库通讯  
1、安全开发-原生PHP-身份验证技术  
2、安全开发-Cookie&Session&Token  
3、安全开发-原生PHP-代码审计案例  
---------------------------------------------  
1、安全开发-原生PHP-弱类型脆弱  
2、安全开发-原生PHP-函数&数据类型  
3、安全开发-原生PHP-代码审计案例  
---------------------------------------------  
1、安全开发-原生PHP-开发组件集合  
2、安全开发-原生PHP-模版引擎渲染  
3、安全开发-原生PHP-第三方编辑器  
---------------------------------------------  
1、安全开发-框架技术-ThinkPHP  
2、安全开发-框架安全-版本&写法  
3、安全开发-ThinkPHP-代码审计案例  
---------------------------------------------  
1、安全开发-原生PHP-文件安全操作  
2、安全开发-原生PHP-上传读取删除包含等  
3、安全开发-原生PHP-代码审计文件安全---------------------------------------------  
1、安全开发-原生PHP-RCE安全  
2、安全开发-原生PHP-代码执行&命令注入  
3、安全开发-原生PHP-代码审计案例  
---------------------------------------------  
1、安全开发-原生PHP-PHP.INI安全  
2、安全开发-原生PHP-全局文件&单函数  
3、安全开发-原生PHP-流量检测&AI算法  
---------------------------------------------  
1、安全开发-原生JS-语法模型概念  
2、安全开发-Ajax技术-JQuery&Axios  
3、安全开发-Ajax应用-文件上传&用户登录---------------------------------------------  
1、安全开发-原生JS-DOM树&BOM对象  
2、安全开发-原生JS-DOM安全&安全案例  
---------------------------------------------  
1、安全开发-原生JS-数据加密&代码混淆  
2、安全开发-原生JS-数据解密安全案例  
---------------------------------------------  
1、安全开发-NodeJS-开发环境&功能实现  
2、安全开发-NodeJS-安全漏洞&案例分析  
3、安全开发-NodeJS-特有漏洞&代码审计  
  
#章节点：(待补充)  
#具体点：(待补充)





演示案例：

* WEB开发-原生JS-语法模型概念
* WEB开发-Ajax技术-JQuery&Axios
* WEB开发-Ajax前端验证-上传&登录
* WEB开发-原生JS对象-DOM&BOM
* WEB开发-原生JS对象-DOM-XSS
* WEB开发-原生JS-数据加密&代码混淆
* WEB开发-NodeJS-安装&语法&模块&安全
* WEB开发-NodeJS-原型链污染&代码审计

#环境搭建-NodeJS-解析安装&库安装  
0、文档参考：  
https://www.runoob.com/nodejs/nodejs-tutorial.html  
1、Nodejs安装  
https://nodejs.org/en  
  
2、三方库安装  
express  
Express是一个简洁而灵活的node.js Web应用框架  
  
body-parser  
node.js中间件，用于处理 JSON, Raw, Text和URL编码的数据。  
  
cookie-parser  
这就是一个解析Cookie的工具。通过req.cookies可以取到传过来的cookie，并把它们转成对象。  
  
multer  
node.js中间件，用于处理 enctype="multipart/form-data"（设置表单的MIME编码）的表单数据。  
  
mysql  
Node.js来连接MySQL专用库，并对数据库进行操作。  
  
安装命令：  
npm i express  
npm i body-parser  
npm i cookie-parser  
npm i multer  
npm i mysql  
  
#功能实现-NodeJS-数据库&文件&执行  
1、Express开发   
2、实现用户登录   
3、加入数据库操作  
  
-文件操作  
1、Express开发  
2、实现目录读取  
3、加入传参接受  
  
-命令执行（RCE）  
1、eval  
2、exec & spawnSync  
  
#NodeJS安全  
1、SQL注入&文件操作  
2、RCE执行&原型链污染  
2、NodeJS黑盒无代码分析  
实战测试NodeJS安全：  
判断：参考前期的信息收集  
黑盒：通过对各种功能和参数进行payload测试  
白盒：通过对代码中写法安全进行审计分析  
-原型链污染  
如果攻击者控制并修改了一个对象的原型，(\_\_proto\_\_)  
那么将可以影响所有和这个对象来自同一个类、父祖类的对象。  
  
#案例应用  
1、CTF方向  
参考：https://f1veseven.github.io/2022/04/03/ctf-nodejs-zhi-yi-xie-xiao-zhi-shi/  
2、代码审计yapi：  
审计参考:https://mp.weixin.qq.com/s/mKOlTQclji-oEB5x\_bMEMg  
部署：https://hellosean1025.github.io/yapi/devops/index.html  
手工bug：  
https://github.com/YMFE/yapi/issues/2180  
Docker：https://github.com/MyHerux/code-note/blob/master/Program/%E5%B7%A5%E5%85%B7%E7%AF%87/Yapi/%E4%BD%BF%E7%94%A8DockerCompose%E6%9E%84%E5%BB%BA%E9%83%A8%E7%BD%B2Yapi.md  
3、代码审计：https://mp.weixin.qq.com/s/fe\_Kp7fOUiMXLWTY1KxSqg

涉及资源：[资源下载地址](https://docs.qq.com/doc/DQ3Z6RkNpaUtMcEFr)