**Web安全与漏洞攻防**

环境搭建：

安装好数据库mysql建立好数据表

Npm install -g jspm

Npm install –save-dev

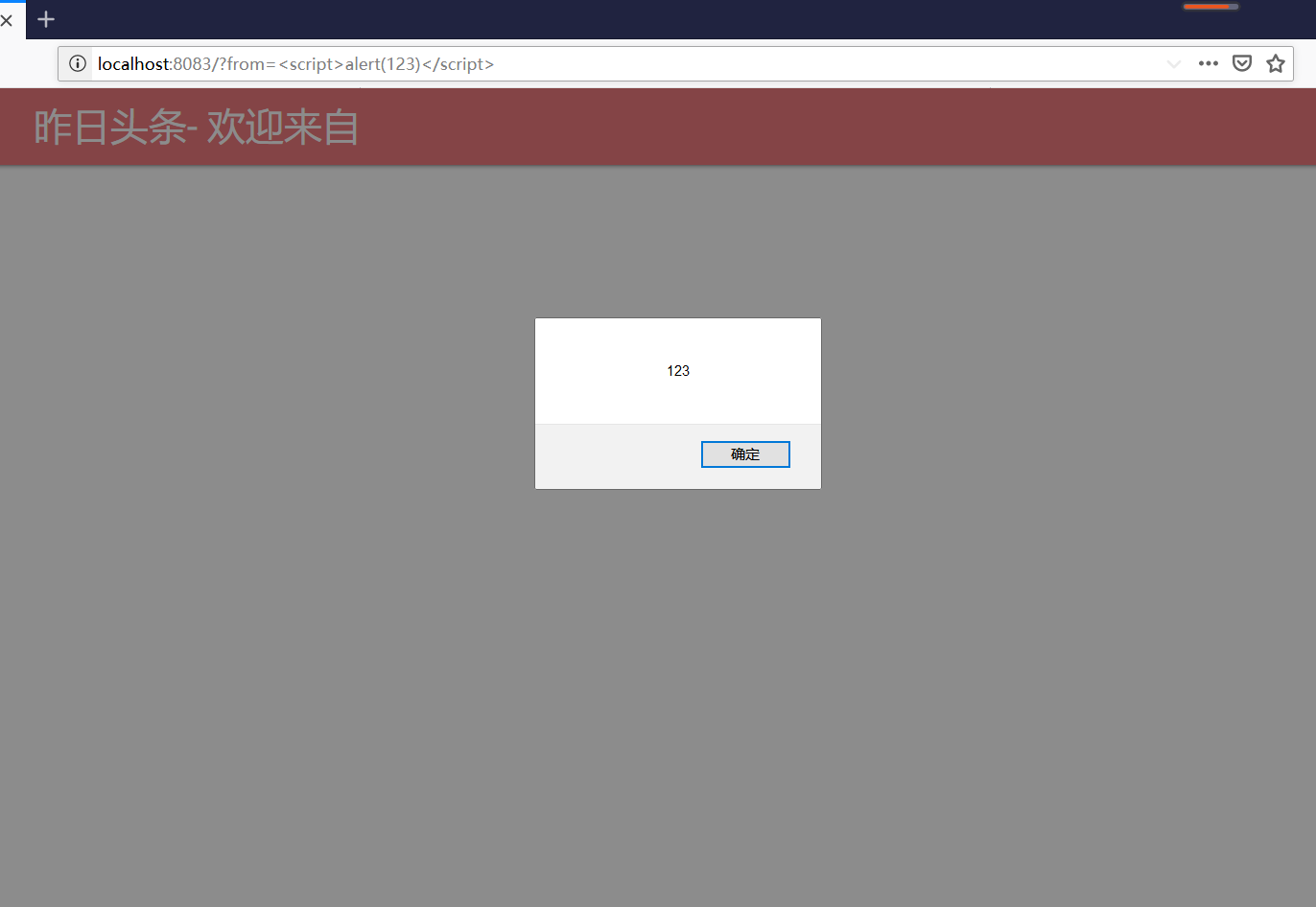
Npm start

跨站脚本xss攻击：

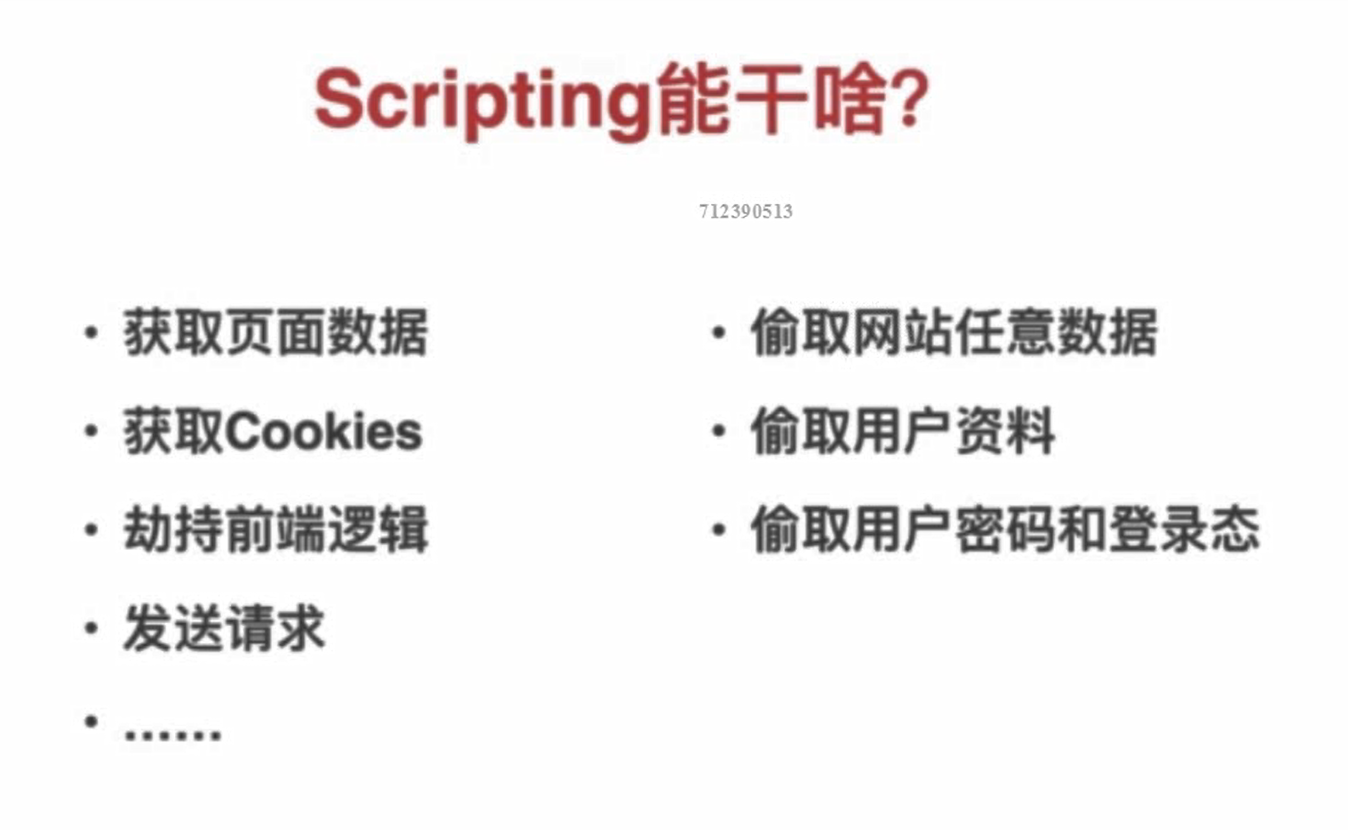
Cross Site Scripting xss

网站运行了来自别的网站的脚本

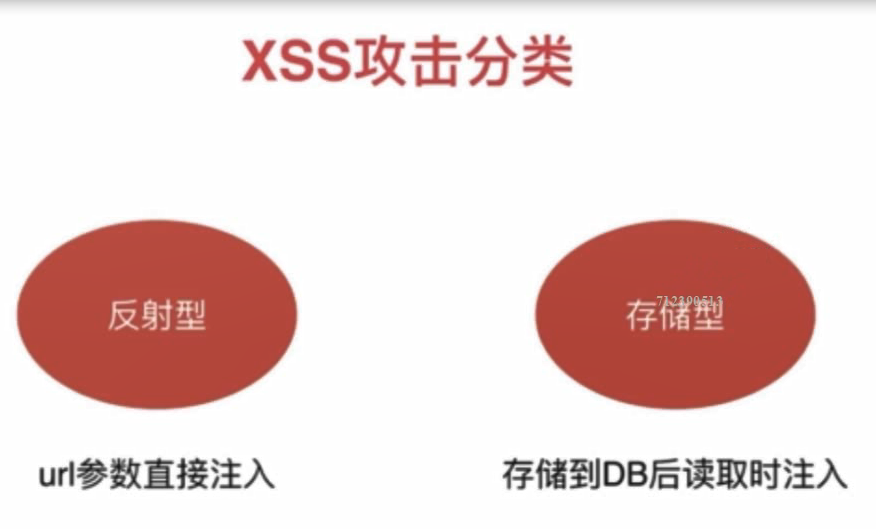
Chrome浏览器会自动过滤掉url带有脚本参数



弹个框能上天啊



能够读取cookie截取代码



<https://dwz.cn/>

使用短网址伪装











Xss防御方案

ctx.set('X-XSS-Protection', 1);

这是一种非常有限的手段，不能依赖这种手段进行防御

这种方式就不能防御

http://localhost:8083/?from=google%22;alert(123);%22



富文本chrome浏览器也不能防御xss攻击

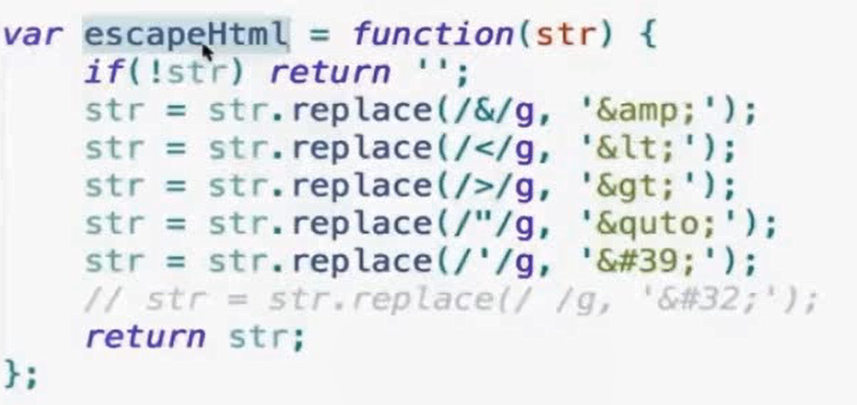
Html节点内容





Function escapeHtml(){

};



如何批量挖掘一个网站的xss漏洞对网站进行攻击？

跨站请求伪造攻击CSRF

前端cookies安全性

点击劫持

传输过程安全问题

Sql注入攻击

信息泄露和社会工程学

其他问题

目的

课程对象web前端工程师

Nodejs工程师