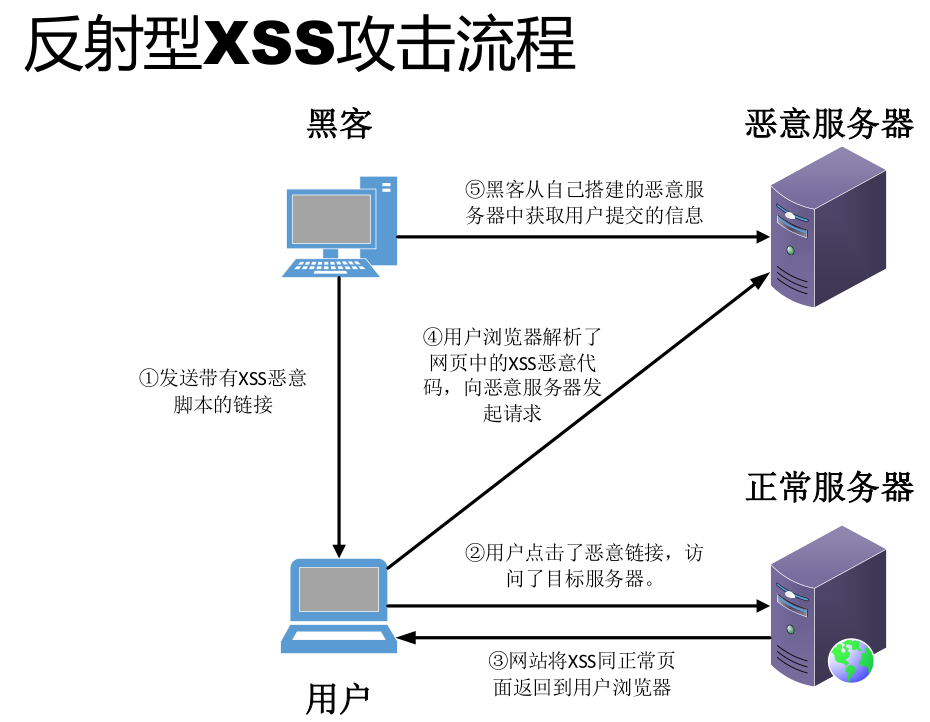
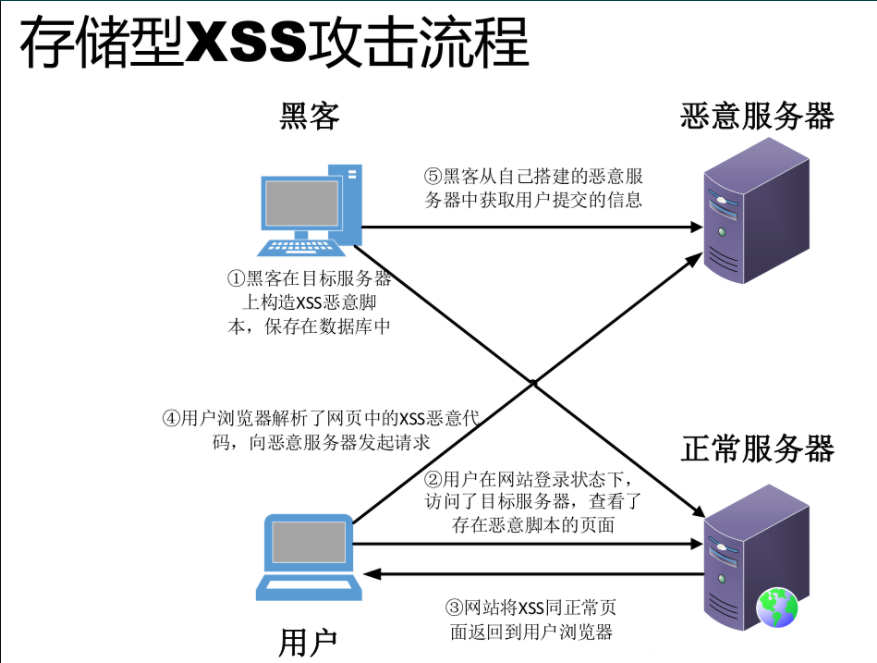
Web攻防-XSS跨站&反射型&存储型&DOM型&接受输出&JS执行&标签操作&SRC复盘

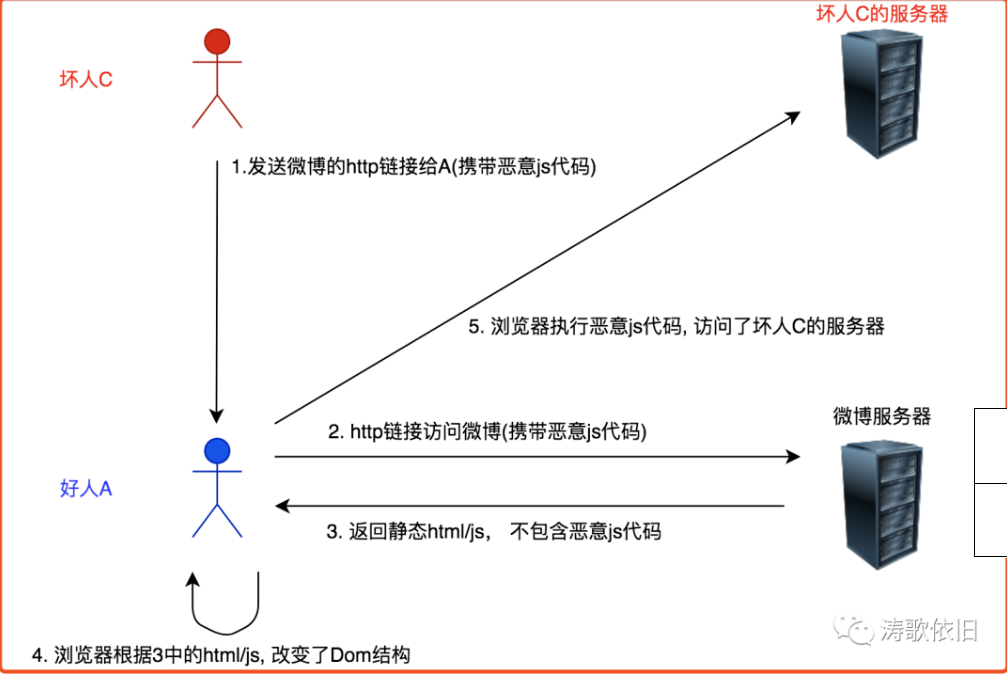


#知识点：  
1、Web攻防-SQL注入-产生原理&应用因素  
2、Web攻防-SQL注入-各类数据库类型利用  
----------------------------------------------  
1、Web攻防-SQL注入-参数类型\*参数格式  
2、Web攻防-SQL注入-XML&JSON&BASE64等  
3、Web攻防-SQL注入-数字字符搜索等符号绕过  
----------------------------------------------  
1、Web攻防-SQL注入-操作方法&增删改查  
2、Web攻防-SQL注入-HTTP头&UA&Cookie  
3、Web攻防-SQL注入-HTTP头&XFF&Referer  
----------------------------------------------  
1、Web攻防-SQL注入-操作方法&增删改查  
2、Web攻防-SQL注入-布尔&延时&报错&盲注  
----------------------------------------------  
1、Web攻防-SQL注入-高权限用户差异  
2、Web攻防-SQL注入-跨库&文件读写带外  
----------------------------------------------  
1、Web攻防-SQL注入-堆叠&二次注入  
2、Web攻防-SQL注入-SQLMAP进阶使用  
----------------------------------------------  
1、Web攻防-XSS跨站-原理&分类&利用点  
2、Web攻防-XSS跨站-反射&存储&DOM型  
   
#章节点：(待补充)  
OWTOP10，SQL注入，文件安全（上传,下载,读取,删除,包含等），目录遍历，  
CSRF，SSRF，CRLF，SSTI注入，XML&XXE安全，RCE执行（代码或命令等）  
反序列化，业务逻辑（验证码，接口枚举，支付购买，机制验证，越权，并发等）  
未授权访问，失效访问控制，弱口令安全，第三方组件安全，CORS，JSONP等









演示案例：

* WEB攻防-XSS跨站-原理&分类&利用点
* WEB攻防-XSS跨站-反射&存储&DOM型

#XSS跨站-输入输出-原理&分类&利用点  
漏洞原理：接受输入数据，输出显示数据后解析执行  
基础类型：反射(非持续)，存储(持续)，DOM-BASE  
拓展类型：jquery，mxss，uxss，pdfxss，flashxss，上传xss等  
常用标签：<https://www.freebuf.com/articles/web/340080.html>  
攻击利用：盲打，COOKIE盗取，凭据窃取，页面劫持，网络钓鱼，权限维持等  
安全修复：字符过滤，实例化编码，http\_only，CSP防护，WAF拦截等  
测试流程：看输出想输入在哪里，更改输入代码看执行（标签，过滤决定）  
   
#XSS跨站-分类测试-反射&存储&DOM型  
-数据交互的地方  
 get、post、headers  
 反馈与浏览  
 富文本编辑器  
 各类标签插入和自定义  
-数据输出的地方  
 用户资料  
 数据输出  
 评论，留言等  
 关键词、标签、说明  
 文件上传  
   
1、反射非持续型：（某案例测试）  
常见情况是攻击者通过构造一个恶意链接的形式，诱导用户传播和打开，由于链接内所携带的参数会回显于页面中或作为页面的处理数据源，最终造成XSS攻击。  
   
2、存储持续型：（某案例测试）  
存储型XSS是持久化的XSS攻击方式，将恶意代码存储于服务器端，当其他用户再次访问页面时触发，造成XSS攻击。  
   
3、DOM-Base型：（某案例测试）  
通过修改原始的客户端代码，受害者浏览器的DOM环境改变，导致有效载荷的执行。页面本身没有变化，但由于DOM环境被恶意修改，代码被包含进导致执行。  
   
4、SRC挖洞复盘  
上海交大xss漏洞  
私信xss  
微博两个反射xss  
腾讯相册bypass-xss  
某鹅邮箱xss

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