渗透测试工程师技术实战课

第3课 XSS简介、常见的攻击流程

跨站脚本检测和常见的攻击利用手段

- 攻击WEB客户端
- 客户端脚本语言
  - 弹窗警告、广告
  - Javascript
  - 在浏览器中执行
- XSS(cross-site scripting)
  - 通过WEB站点漏洞，向客户端交付恶意脚本代码，实现对客户端的攻击目的
  - 注入客户端脚本代码
  - 盗取cookie
  - 重定向
- VBScript,ActiveX,or Flash

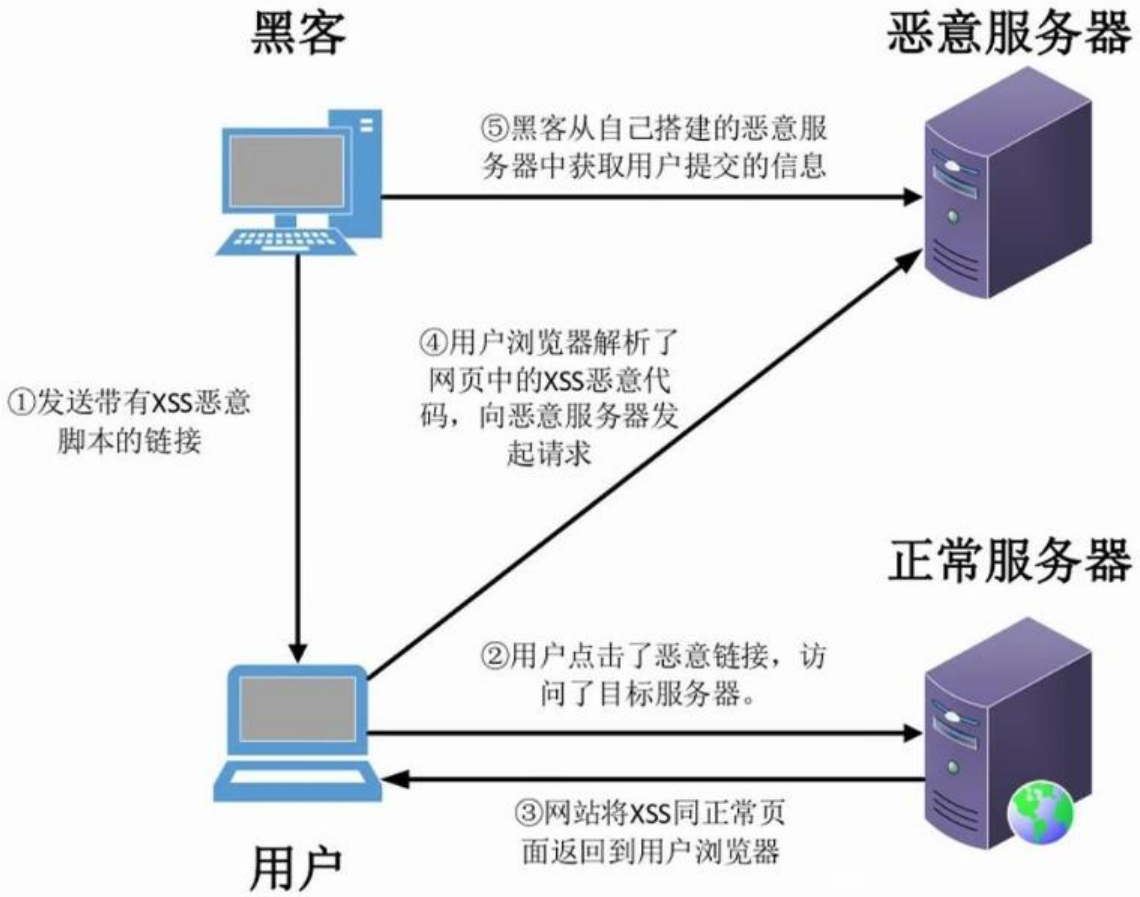
XSS

- JavaScript
  - 与Java语言无关
  - 命令完全出于市场原因
  - 使用最广的客户端脚本语言
- 使用场景
  - 直接嵌入html:<script>aler('XSS');</script>
  - 元素标签事件: <body onload=alert('XSS')>
  - 图片标签: <img src="javascript:alert('XSS');">
  - 其他标签: <iframe>,<dir>,and<link>
  - DOM对象，篡改页面内容

XSS

- 攻击参与方
  - 攻击者
  - 被攻击者
  - 漏洞站点
  - 第三方站点（攻击目标、攻击参与站）
- 漏洞形成的根源
  - 服务器对用户提交数据过滤不严
  - 提交给服务器的脚本被直接返回给其他客户端执行
  - 脚本在客户端执行恶意操作

反射型XSS攻击流程


黑客
恶意服务器
⑤黑客从自己搭建的恶意服务器中获取用户提交的信息
④用户浏览器解析了网页中的XSS恶意代码，向恶意服务器发起请求
①发送带有XSS恶意脚本的链接
正常服务器
②用户点击了恶意链接，访问了目标服务器。
③网站将XSS同正常页面返回到用户浏览器
用户

谢谢观赏