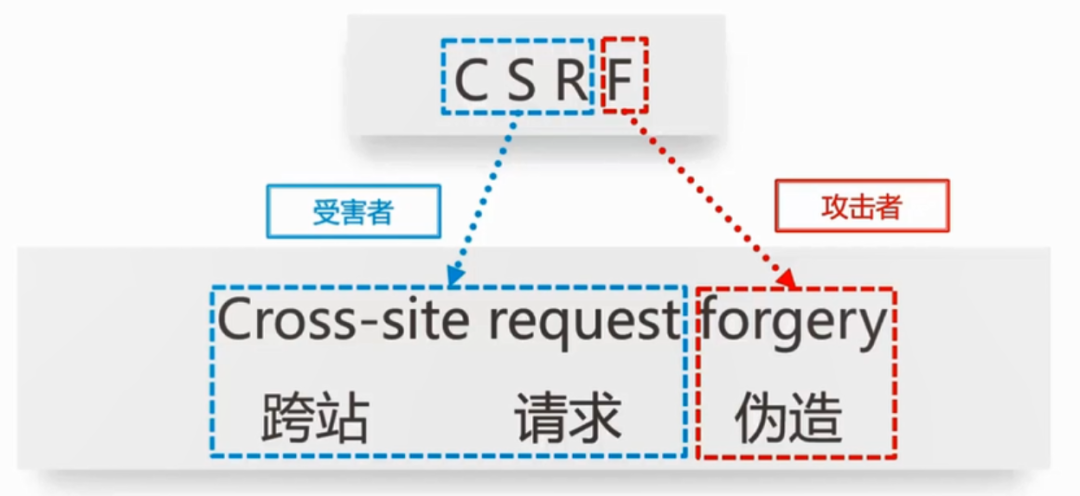
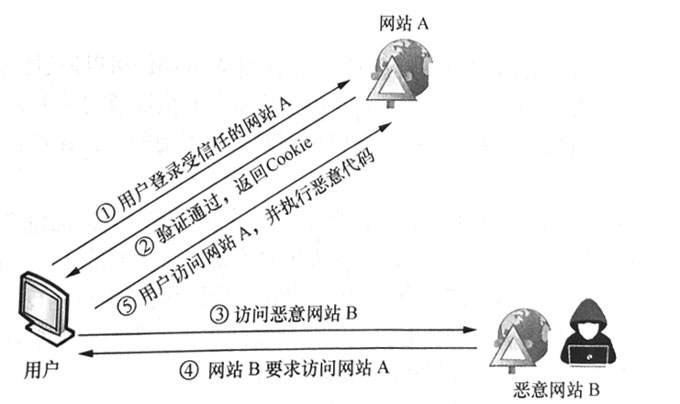
Web攻防-CSRF跨站请求伪造&Referer同源&Token校验&复用删除置空&联动上传或XSS

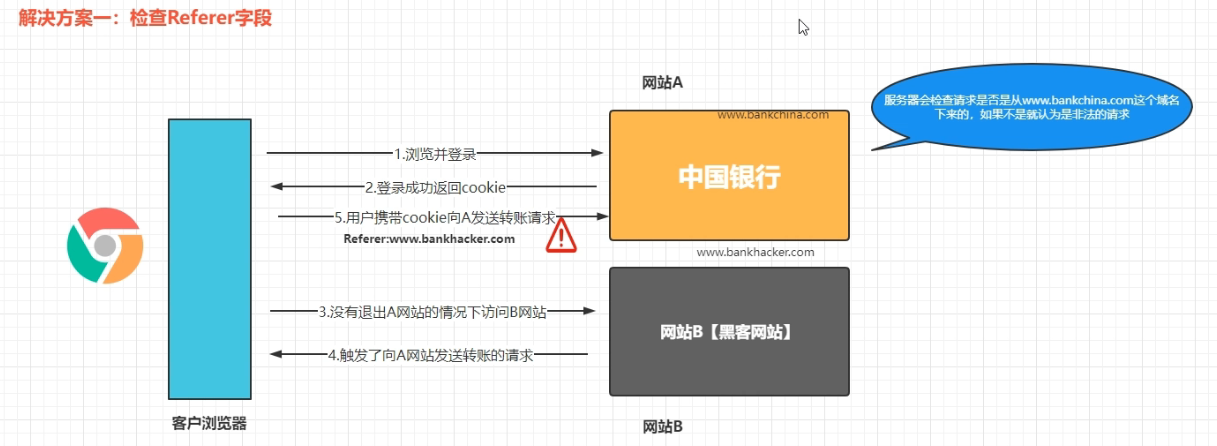


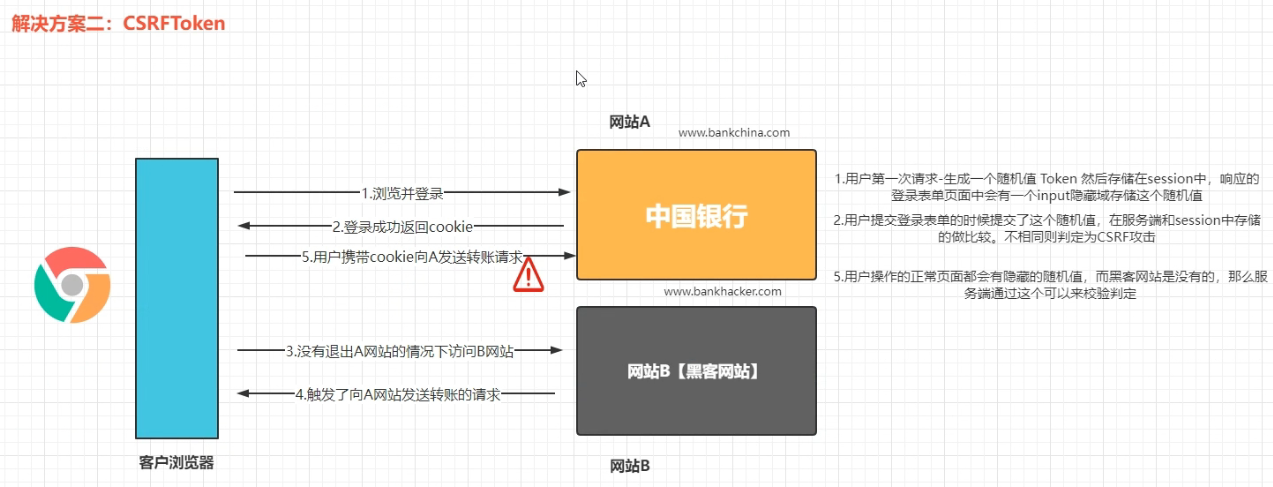
#知识点：  
1、Web攻防-SQL注入-产生原理&应用因素  
2、Web攻防-SQL注入-各类数据库类型利用  
----------------------------------------------  
1、Web攻防-SQL注入-参数类型\*参数格式  
2、Web攻防-SQL注入-XML&JSON&BASE64等  
3、Web攻防-SQL注入-数字字符搜索等符号绕过  
----------------------------------------------  
1、Web攻防-SQL注入-操作方法&增删改查  
2、Web攻防-SQL注入-HTTP头&UA&Cookie  
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  
----------------------------------------------  
1、Web攻防-XSS跨站-文件类型-html&pdf&swf&svg  
2、Web攻防-XSS跨站-功能逻辑-postMessage&localStorage  
----------------------------------------------  
1、Web攻防-XSS跨站-浏览器&转换-UXSS&MXSS  
2、Web攻防-XSS跨站-框架和库-VUE&React&Electron&JQuery  
----------------------------------------------  
1、Web攻防-XSS跨站-手工代码&框架工具&在线平台  
2、Web攻防-XSS跨站-Cookie盗取&数据提交&网络钓鱼  
----------------------------------------------  
1、Web攻防-XSS跨站-安全防护&CSP&Httponly&WAF等  
2、Web攻防-XSS跨站-工具项目&XSStrike&Chypass\_pro  
----------------------------------------------  
1、Web攻防-CSRF-原理&检测&利用&防御  
2、Web攻防-CSRF-防御-Referer策略隐患  
3、Web攻防-CSRF-防御-Token校验策略隐患  
   
#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-CSRF利用-原理&构造
* WEB攻防-CSRF防御-同源&Token

CSRF 功能点:  
删除帐户  
更改电子邮件  
如果不需要旧密码，请更改密码  
如果您的目标支持角色，请添加新管理员  
更改正常信息，名字，姓氏等......  
类似复选框的接收通知  
更改个人资料图片/删除它  
   
CSRF 绕过:  
删除令牌并发送带有空白参数的请求  
删除token参数  
将请求从 POST 更改为 GET  
更改正文编码  
将 token 替换为随机值  
删除裁判或在 CSRf 文件中使用此行|`  
<meta name="referrer" content="no-referrer">  
使用另一个用户令牌  
更改令牌中的一个字符，内容长度绕过  
   
#案例-CSRF利用-无防护  
检测：黑盒手工利用测试，白盒看代码检验（有无token，来源检验等）  
生成：BurpSuite->Engagement tools->Generate CSRF Poc  
利用：将文件防止自己的站点下，诱使受害者访问（或配合XSS触发访问）  
   
#案例-CSRF利用-同源策略防护  
绕过1：规则匹配绕过问题（代码逻辑不严谨）  
功能逻辑：<meta name="referrer" content="no-referrer">  
匹配机制：[http://xx.xx.xx.xx/http://xx.xx.xx.xx](http://xx.xx.xx.xx/http:/xx.xx.xx.xx)  
绕过2：配合文件上传绕过（严谨使用同源绕过）  
绕过3：配合存储XSS绕过（严谨使用同源绕过）  
   
#案例-CSRF利用-Token校验防护  
绕过1：将Token参数值复用（代码逻辑不严谨）  
绕过2：将Token参数删除（代码逻辑不严谨）  
绕过3：将Token参数值置空（代码逻辑不严谨）  
   
#复盘  
SRC-CVE的CSRF报告

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