Web攻防-任意文件下载&文件读取&文件删除&索引泄露&目录遍历&路径穿越&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  
----------------------------------------------  
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  
----------------------------------------------  
1、WEB攻防-SSRF利用绕过-伪协议&IP及域名  
2、WEB攻防-SSRF挖掘思路-功能逻辑&SRC复盘  
----------------------------------------------  
1、WEB攻防-SSRF插件结合-SRC复盘与实战  
----------------------------------------------  
1、WEB攻防-文件上传-前端&黑白名单&MIME&文件头等  
2、WEB攻防-文件上传-执行权限&解码还原&云存储&分站等  
----------------------------------------------  
1、WEB攻防-文件上传-思维导图形成  
2、WEB攻防-文件上传-JS提取&特定漏洞&第三方编辑器  
----------------------------------------------  
1、WEB攻防-文件包含-LFI&RFI利用思路  
2、WEB攻防-文件上传-伪协议玩法&无文件  
3、WEB攻防-文件上传-黑白盒案例&SRC复盘  
----------------------------------------------  
1、WEB攻防-文件下载&读取&删除-功能点&URL  
2、WEB攻防-目录遍历&泄露\*穿越-功能点&URL  
   
#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-文件上传-安全验证&层面逻辑
* WEB攻防-文件上传-执行权限&解码还原
* WEB攻防-文件上传-分站存储&OSS存储
* WEB攻防-文件上传-JS提取&源码类&编辑器
* WEB攻防-文件包含-LFI&RFI&伪协议&无文件
* WEB攻防-文件包含-PHP&JAVA&SRC复盘
* WEB攻防-文件下载&读取&删除-URL参数&功能点
* WEB攻防-目录索引&遍历&穿越-URL参数&功能点

#文件安全-读取下载&删除-黑白盒  
1、下载=读取  
常规下载URL：http://www.xiaodi8.com/upload/123.pdf  
可能存在安全URL：http://www.xiaodi8.com/xx.xx?file=123.pdf  
利用：常规下载敏感文件（数据库配置，中间件配置，系统密匙等文件信息）  
2、文件删除（常出现后台中）  
可能存在安全问题：前台或后台有删除功能应用  
利用：常规删除重装锁定配合程序重装或高危操作  
   
#目录安全-遍历&穿越-黑白盒  
1、目录索引  
目录权限控制不当，通过遍历获取到有价值的信息文件去利用  
2、目录穿越（路径遍历常出现后台中）  
目录权限控制不当，通过控制查看目录路径穿越到其他目录或判断获取价值文件再利用  
   
#黑盒分析：  
1、功能点  
文件上传，文件下载，文件删除，文件管理器等地方  
2、URL特征  
文件名：  
download，down，readfile，read，del，dir，path，src，Lang等  
参数名：  
file、path、data、filepath、readfile、data、url、realpath等  
#白盒分析：  
上传类，删除类，下载类，目录操作函数，读取查看方法或函数等  
   
#复盘  
https://mp.weixin.qq.com/s/Kiec7FhvpAmPf7zTWvJa3g  
https://mp.weixin.qq.com/s/QqXxpTwXSjCNN622fSsZAQ  
https://mp.weixin.qq.com/s/A2FvZMuPpHiewGrL5UDlHw  
https://mp.weixin.qq.com/s/w2PH7EI6Z2R9diV\_tBA1Zw

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