渗透测试工程师技术实战课

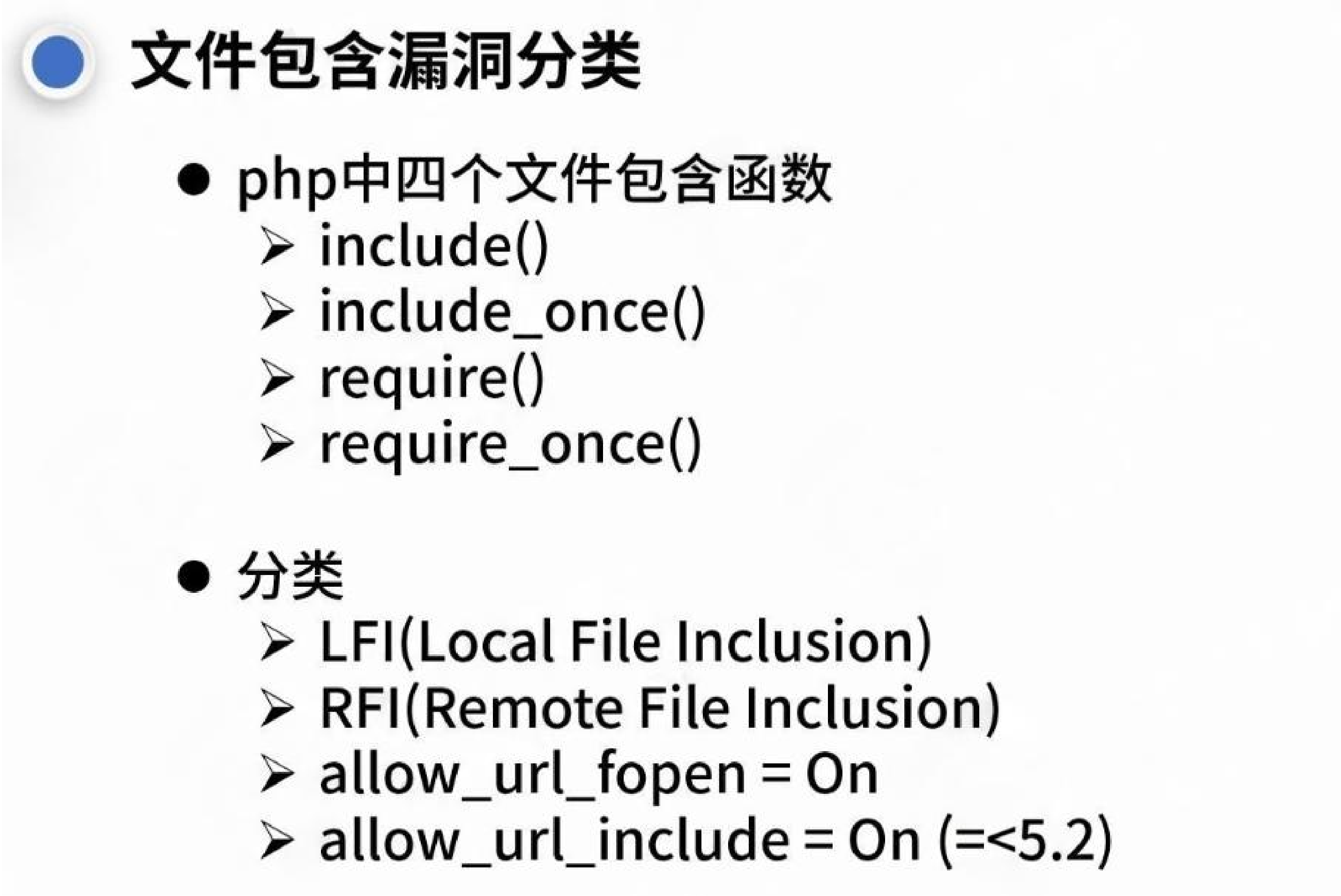
文件包含漏洞

教学目标

- ★ 文件包含漏洞基础
- ★ 文件包含姿势
- ★ 绕过技巧
- ★ 防御方案

文件包含漏洞基础

文件包含操作,在大多数Web语言中都会提供的功能,但PHP对于包含文件所提供的功能太强大,太灵活,所以包含漏洞经常出现在PHP语言中,这也就导致了出现了一个错误现状,很多初学者认为包含漏洞只出现PHP语言之中,殊不知在其他语言中可能出现包含漏洞。这也应了一句老话功能越强大,漏洞就越多。

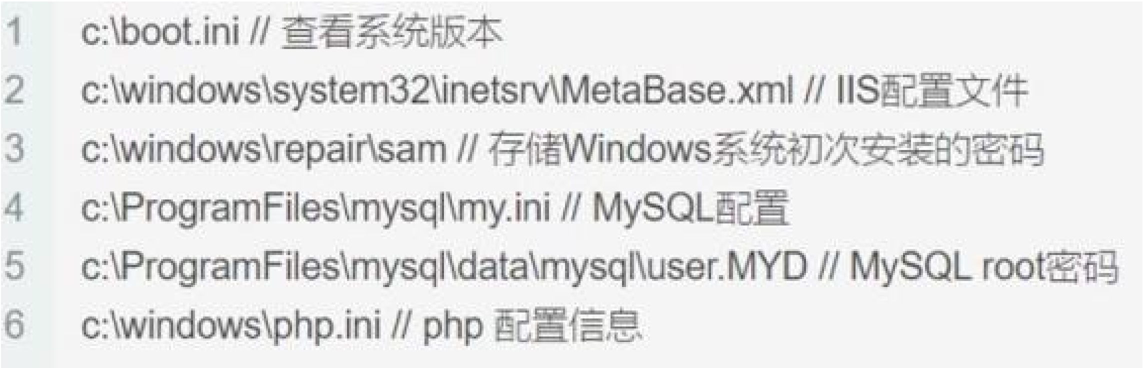


文件包含漏洞分类

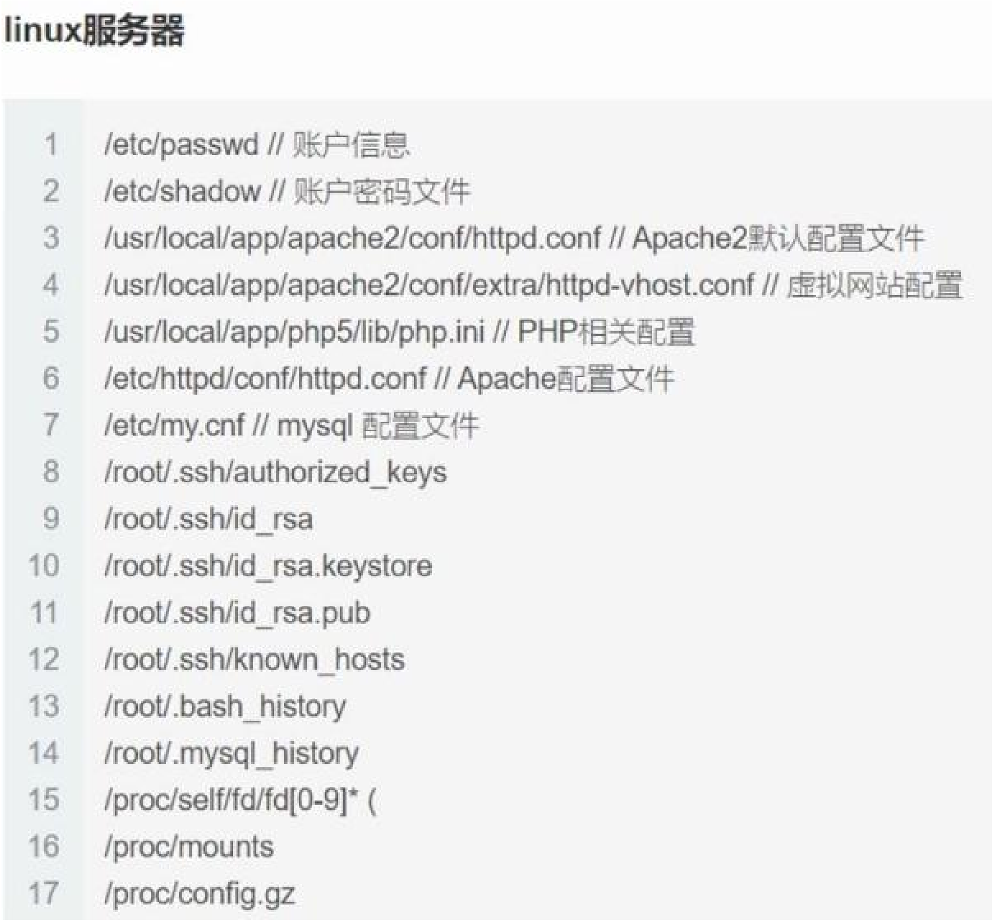
- php中四个文件包含函数
  - include()
  - include_once()
  - require()
  - require_once()

- 分类
  - LFI(Local File Inclusion)
  - RFI(Remote File Inclusion)
  - allow_url_fopen = On
  - allow_url_include = On (=<5.2)

•本地文件包含(LFI)

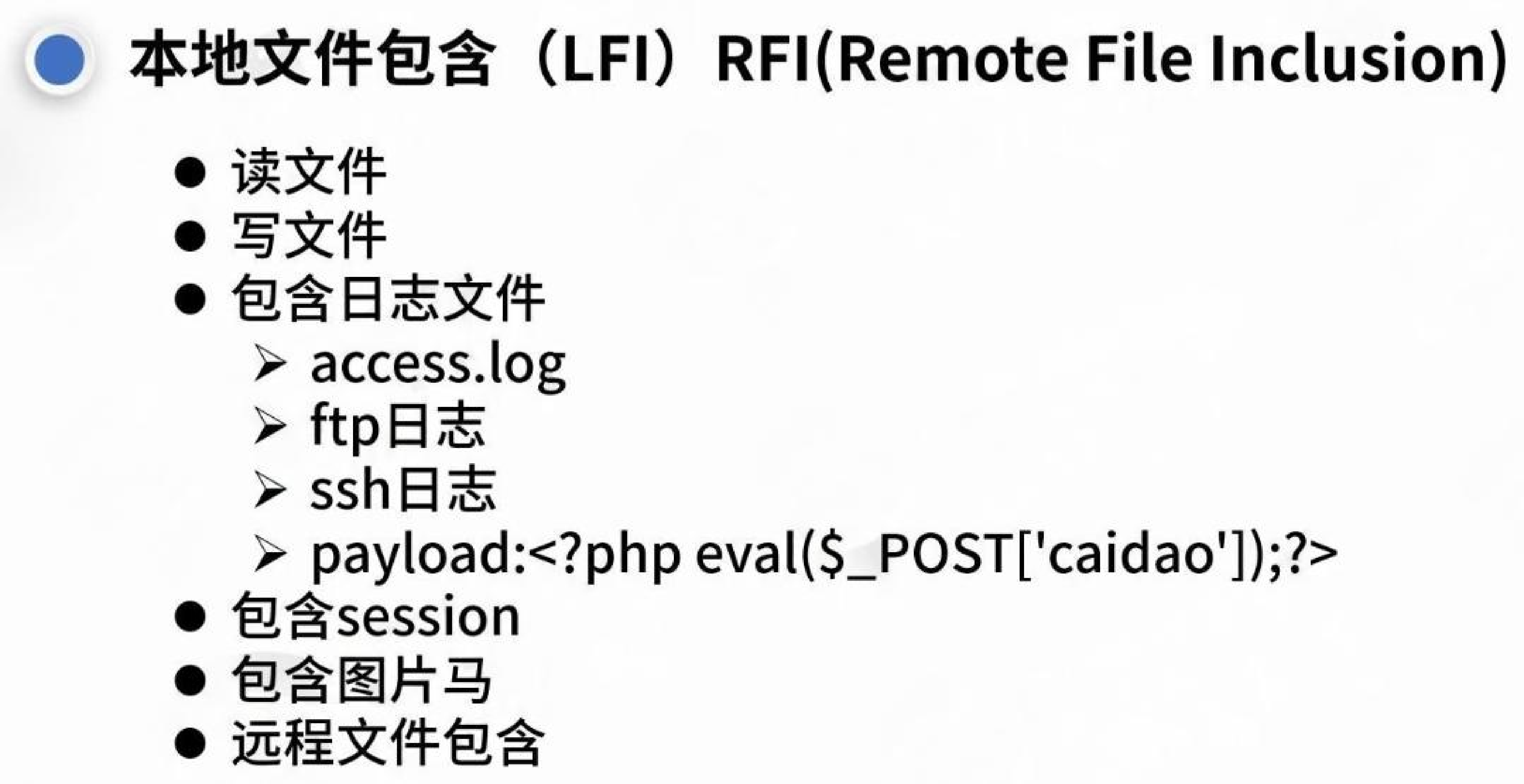


```
c:\boot.ini // 查看系统版本
c:\windows\system32\inetsrv\MetaBase.xml // IIS配置文件
c:\windows\repair\sam // 存储Windows系统初次安装的密码
c:\ProgramFiles\mysql\my.ini // MySQL配置
c:\ProgramFiles\mysql\data\mysql\user.MYD // MySQL root密码
c:\windows\php.ini // php 配置信息
```



linux服务器

```
/etc/passwd // 账户信息
/etc/shadow // 账户密码文件
/usr/local/app/apache2/conf/httpd.conf // Apache2默认配置文件
/usr/local/app/apache2/conf/extra/httpd-vhost.conf // 虚拟网站配置
/usr/local/app/php5/lib/php.ini // PHP相关配置
/etc/httpd/conf/httpd.conf // Apache配置文件
/etc/my.cnf // mysql 配置文件
/root/.ssh/authorized_keys
/root/.ssh/id_rsa
/root/.ssh/id_rsa.keystore
/root/.ssh/id_rsa.pub
/root/.ssh/known_hosts
/root/.bash_history
/root/.mysql_history
/proc/self/fd/fd[0-9]* (
/proc/mounts
/proc/config.gz
```



本地文件包含（LFI）RFI(Remote File Inclusion)

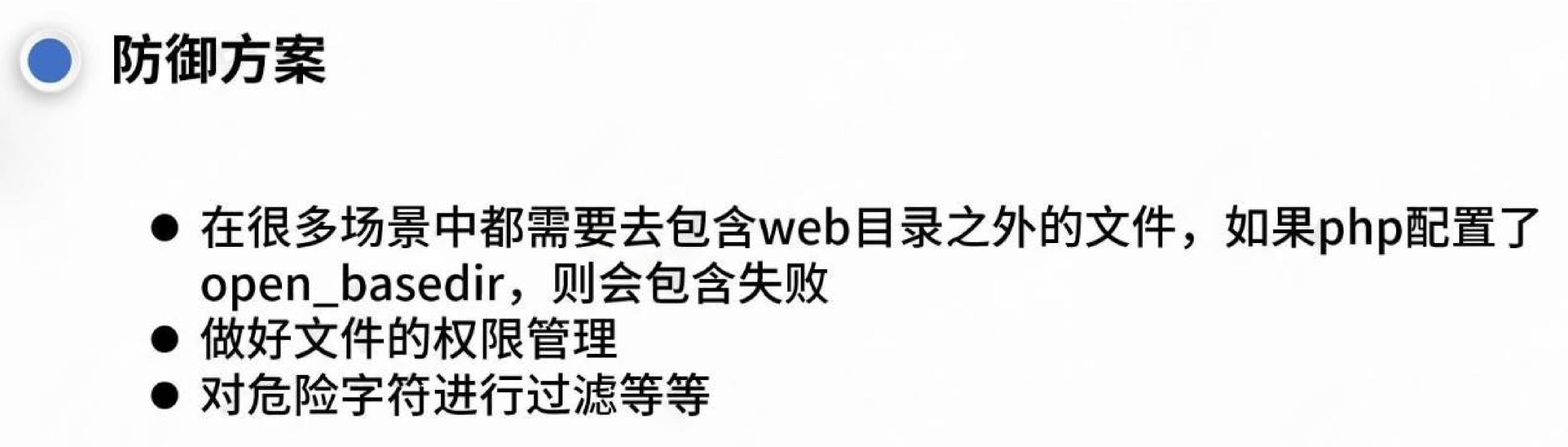
- 读文件
- 写文件
- 包含日志文件
  - ➢ access.log
  - ➢ ftp日志
  - ➢ ssh日志
  - ➢ payload:<?php eval($_POST['caidao']);?>
- 包含session
- 包含图片马
- 远程文件包含

本地文件包含（LFI）远程文件包含 (RFI)

- allow_url_include
- allow_url_fopen
- php版本
  - php://input
  - data:URI schema
  - php://filter
  - file://

绕过技巧

- 前缀
- 目录遍历
- 编码绕过
- %00 截断(php版本小于5.3)
- 长度截断
- 远程文件包含的绕过
- 特殊字符绕过



防御方案

- 在很多场景中都需要去包含web目录之外的文件，如果php配置了open_basedir，则会包含失败
- 做好文件的权限管理
- 对危险字符进行过滤等等

谢谢观赏