目录

01 系统加固

- Windows操作系统加固
- Linux操作系统加固

02 中间件加固

- IIS加固
- Apache加固
- Nginx加固

03 数据库加固

- Mysql加固
- Mongodb加固

Apache 安全加固

目录

01 Apache 基础

02 Apache 服务器安全加固

Apache 基础

安装httpd

后台进程：httpd

脚本：/etc/rc.d/init.d/httpd

默认使用端口：80(http)，443(https)

所需RPM包：httpd

配置路径：/etc/httpd/*

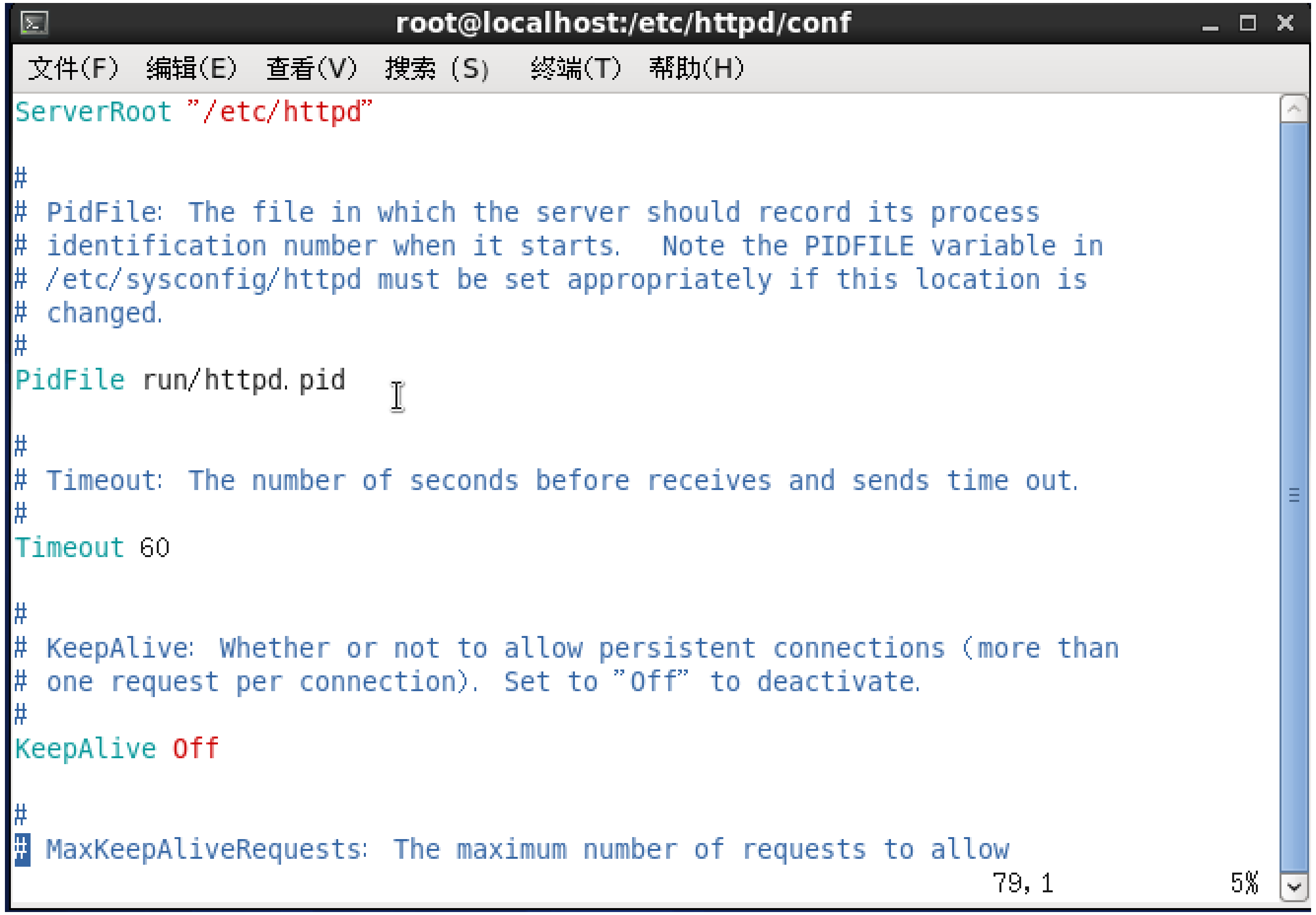
默认网站存放路径：/var/www/*

优点：免费，稳定，速度快

安装：yum install httpd*

httpd.conf

配置文件是Apache的核心！！！
/etc/httpd/conf/httpd.conf



root@localhost:/etc/httpd/conf
文件(F) 编辑(E) 查看(V) 搜索 (S) 终端(T) 帮助(H)

```
ServerRoot "/etc/httpd"

#
# PidFile: The file in which the server should record its process
# identification number when it starts.  Note the PIDFILE variable in
# /etc/sysconfig/httpd must be set appropriately if this location is
# changed.
#
PidFile run/httpd.pid

#
# Timeout: The number of seconds before receives and sends time out.
#
Timeout 60

#
# KeepAlive: Whether or not to allow persistent connections (more than
# one request per connection). Set to "Off" to deactivate.
#
KeepAlive Off

#
# MaxKeepAliveRequests: The maximum number of requests to allow
                                                   79,1          5%
```

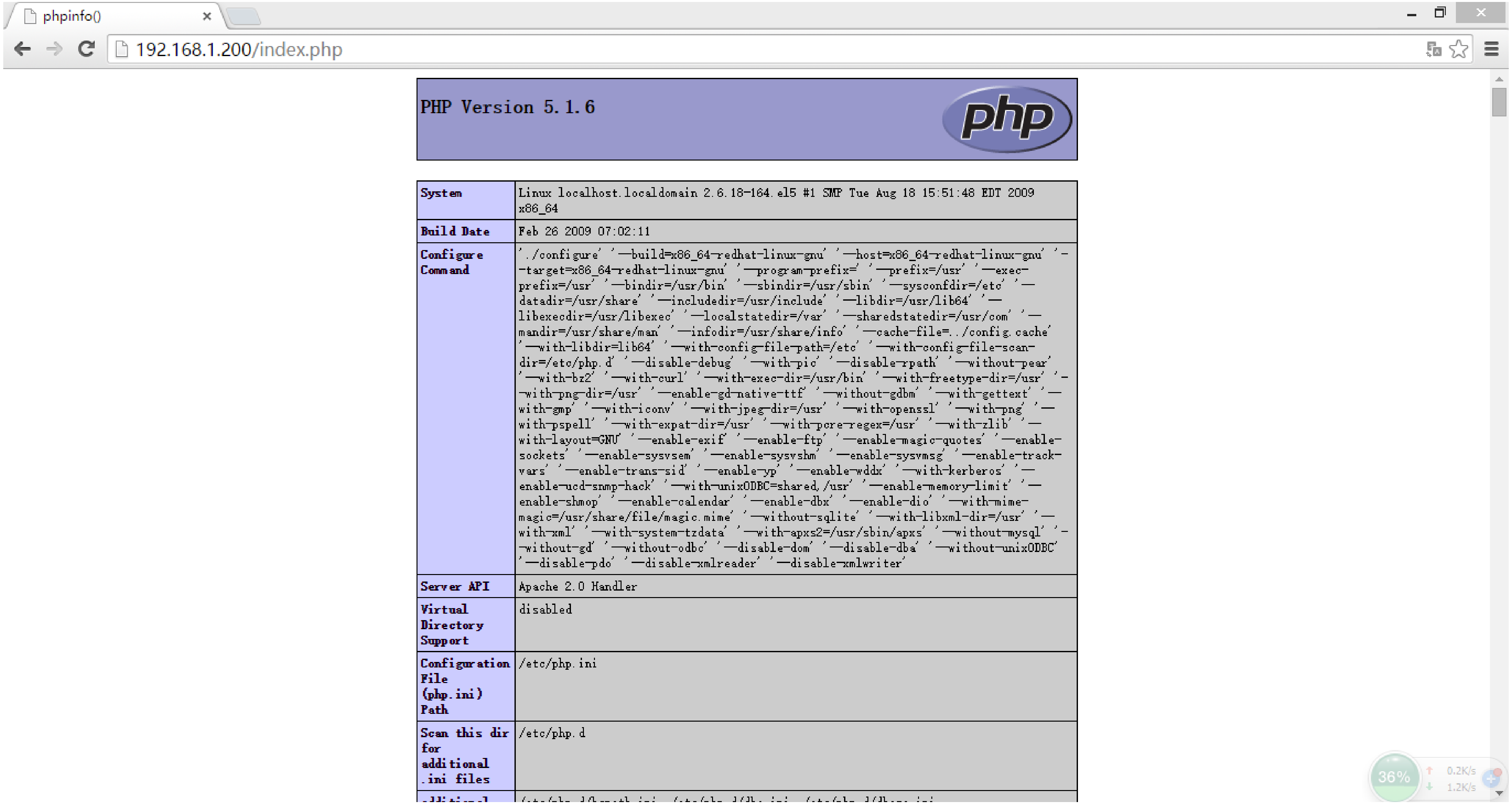
安装php

```
[root@localhost ~]# yum -y install php*
[root@localhost ~]# service httpd restart
停止 httpd：[失败]
启动 httpd：[确定]
```

新建测试文件：

```
[root@localhost ~]# cd /var/www/html/
[root@localhost html]# ls
[root@localhost html]# cat index.php
<?php
phpinfo();
?>
```

解析PHP



PHP Version 5.1.6

System	Linux localhost.localdomain 2.6.18-164.el5 #1 SMP Tue Aug 18 15:51:48 EDT 2009 x86_64
Build Date	Feb 26 2009 07:02:11
Configure Command	’./configure’ ’—build=x86_64-redhat-linux-gnu’ ’—host=x86_64-redhat-linux-gnu’ ’--target=x86_64-redhat-linux-gnu’ ’—program-prefix=’ ’—prefix=/usr’ ’—exec-prefix=/usr’ ’—bindir=/usr/bin’ ’—sbindir=/usr/sbin’ ’—sysconfdir=/etc’ ’—datadir=/usr/share’ ’—includedir=/usr/include’ ’—libdir=/usr/lib64’ ’—libexecdir=/usr/libexec’ ’—localstatedir=/var’ ’—sharedstatedir=/usr/com’ ’—mandir=/usr/share/man’ ’—infodir=/usr/share/info’ ’—cache-file=../config.cache’ ’—with-libdir=lib64’ ’—with-config-file-path=/etc’ ’—with-config-file-scan-dir=/etc/php.d’ ’—disable-debug’ ’—with-pic’ ’—disable-rpath’ ’—without-pear’ ’—with-bz2’ ’—with-curl’ ’—with-exec-dir=/usr/bin’ ’—with-freetype-dir=/usr’ ’--with-png-dir=/usr’ ’—enable-gd-native-ttf’ ’—without-gdbm’ ’—with-gettext’ ’—with-gmp’ ’—with-iconv’ ’—with-jpeg-dir=/usr’ ’—with-openssl’ ’—with-png’ ’—with-pspell’ ’—with-expat-dir=/usr’ ’—with-pcre-regex=/usr’ ’—with-zlib’ ’—with-layout=GNU’ ’—enable-exif’ ’—enable-ftp’ ’—enable-magic-quotes’ ’—enable-sockets’ ’—enable-sysvsem’ ’—enable-sysvshm’ ’—enable-sysvmsg’ ’—enable-track-vars’ ’—enable-trans-sid’ ’—enable-yp’ ’—enable-wddx’ ’—with-kerberos’ ’—enable-ucd-snmp-hack’ ’—with-unixODBC=shared,/usr’ ’—enable-memory-limit’ ’—enable-shmop’ ’—enable-calendar’ ’—enable-dbx’ ’—enable-dio’ ’—with-mime-magic=/usr/share/file/magic.mime’ ’—without-sqlite’ ’—with-libxml-dir=/usr’ ’—with-xml’ ’—with-system-tzdata’ ’—with-apxs2=/usr/sbin/apxs’ ’—without-mysql’ ’--without-gd’ ’—without-odbc’ ’—disable-dom’ ’—disable-dba’ ’—without-unixODBC’ ’—disable-pdo’ ’—disable-xmlreader’ ’—disable-xmlwriter’
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d

Apache 服务器安全加固

以特定用户运行httpd服务

以特定用户运行服务,不要使用系统管理员账号启动APACHE，以免受到越权使用造成非法攻击。

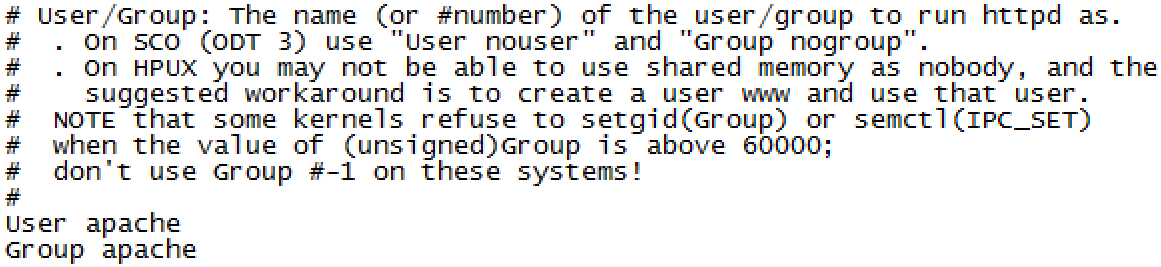
# vim /etc/httpd/conf/httpd.conf

修改：

User apache

Group apache

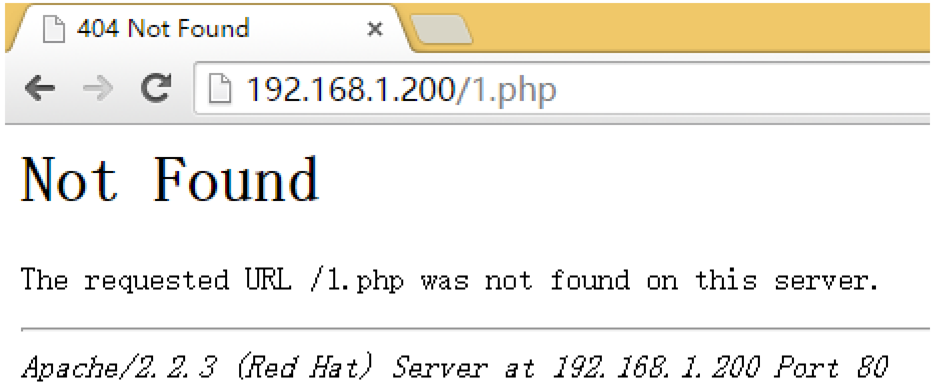
重启httpd服务修改生效



```
# User/Group: The name (or #number) of the user/group to run httpd as.
#  . On SCO (ODT 3) use "User nouser" and "Group nogroup".
#  . On HPUX you may not be able to use shared memory as nobody, and the
#    suggested workaround is to create a user www and use that user.
#  NOTE that some kernels refuse to setgid(Group) or semctl(IPC_SET)
#  when the value of (unsigned)Group is above 60000;
#  don't use Group #-1 on these systems!
#
User apache
Group apache
```

隐藏Apache banner信息

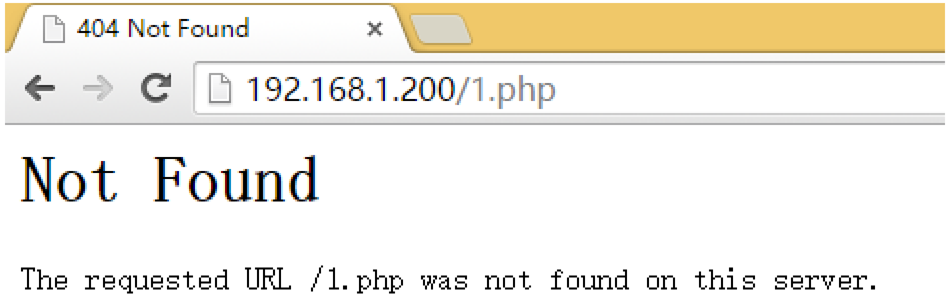
vim /etc/httpd/conf/httpd.conf
ServerTokens OS　　　　修改为：ServerTokens Prod
//在出现错误页的时候不显示服务器操作系统的名称
ServerSignature On　　　修改为：ServerSignature Off
//不回显apache版本信息



Not Found

The requested URL /1.php was not found on this server.

Apache/2.2.3 (Red Hat) Server at 192.168.1.200 Port 80

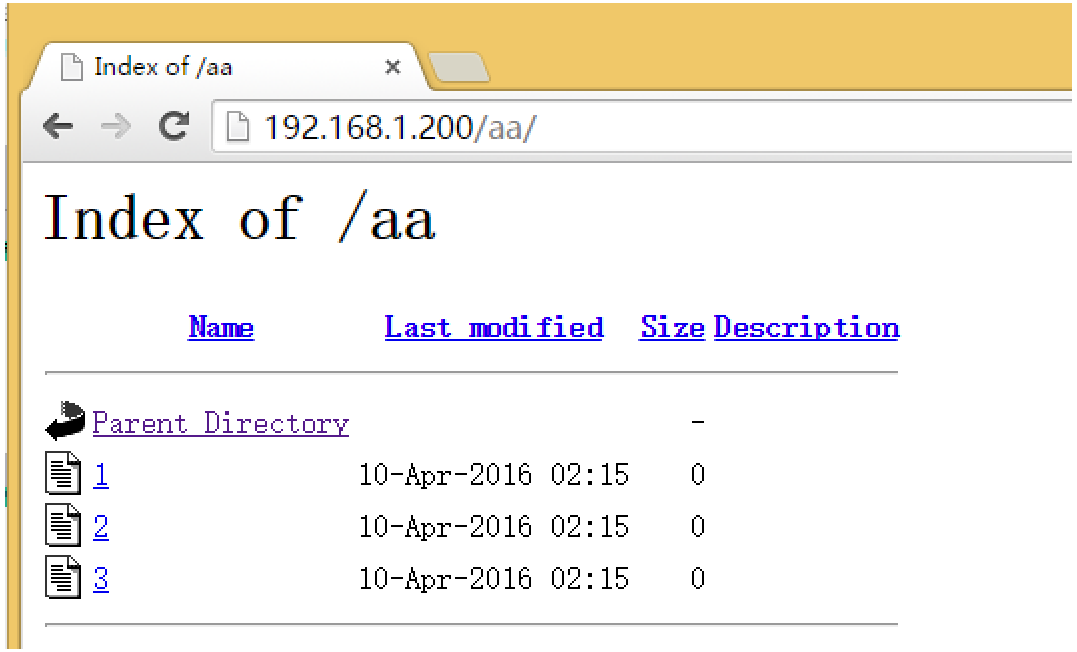


Not Found

The requested URL /1.php was not found on this server.

禁止目录浏览

Options Indexes FollowSymLinks
修改为：
# vim /etc/httpd/conf/httpd.conf
Options FollowSymLinks

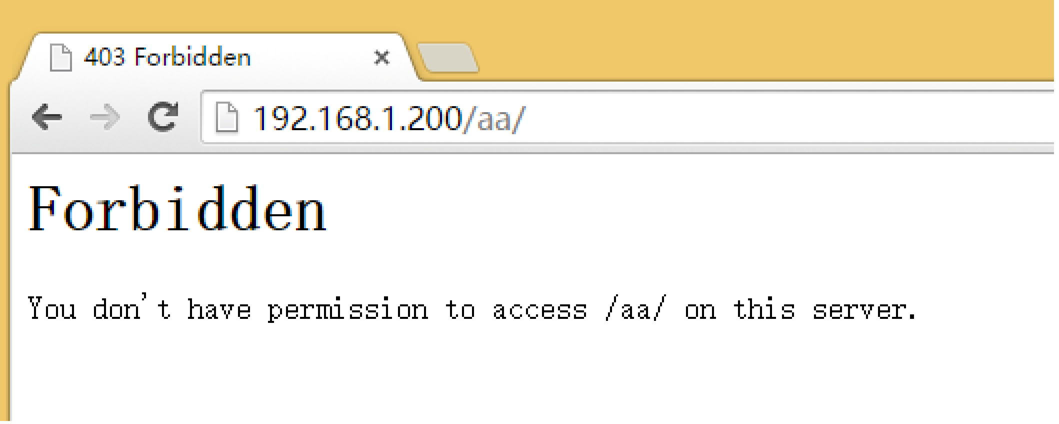


Index of /aa

192.168.1.200/aa/

Index of /aa

```
        Name           Last modified      Size Description
-----------------------------------------------------------
Parent Directory                             -
1                   10-Apr-2016 02:15    0
2                   10-Apr-2016 02:15    0
3                   10-Apr-2016 02:15    0
-----------------------------------------------------------
```



403 Forbidden

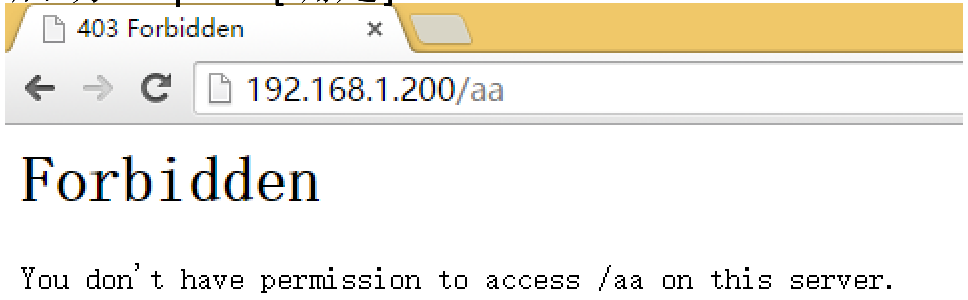
192.168.1.200/aa/

Forbidden

You don't have permission to access /aa/ on this server.

限制IP访问

```
<Directory "/var/www/html/aa/">
    Options Indexes MultiViews FollowSymLinks
    AllowOverride AuthConfig
    AuthType Basic
    AuthName "testuser's paasword"
    AuthUserFile /usr/local/etc/passwd.httpd
    Require user testuser
    Order allow,deny
    Allow from 172.16.1.0
</Directory>
[root@localhost html]# service httpd restart
停止 httpd：[确定]
启动 httpd：[确定]
```

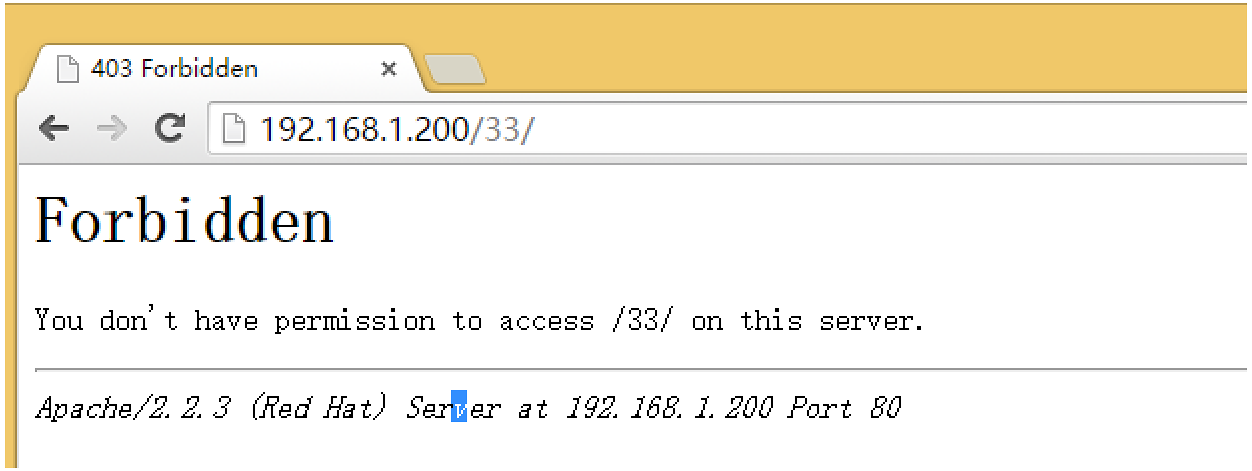


Forbidden

You don't have permission to access /aa on this server.

限制禁止访问的文件夹，例如后台目录

```
<Directory "/var/www/html/33">
        Deny from all
</Directory>
```



Forbidden

You don't have permission to access /33/ on this server.

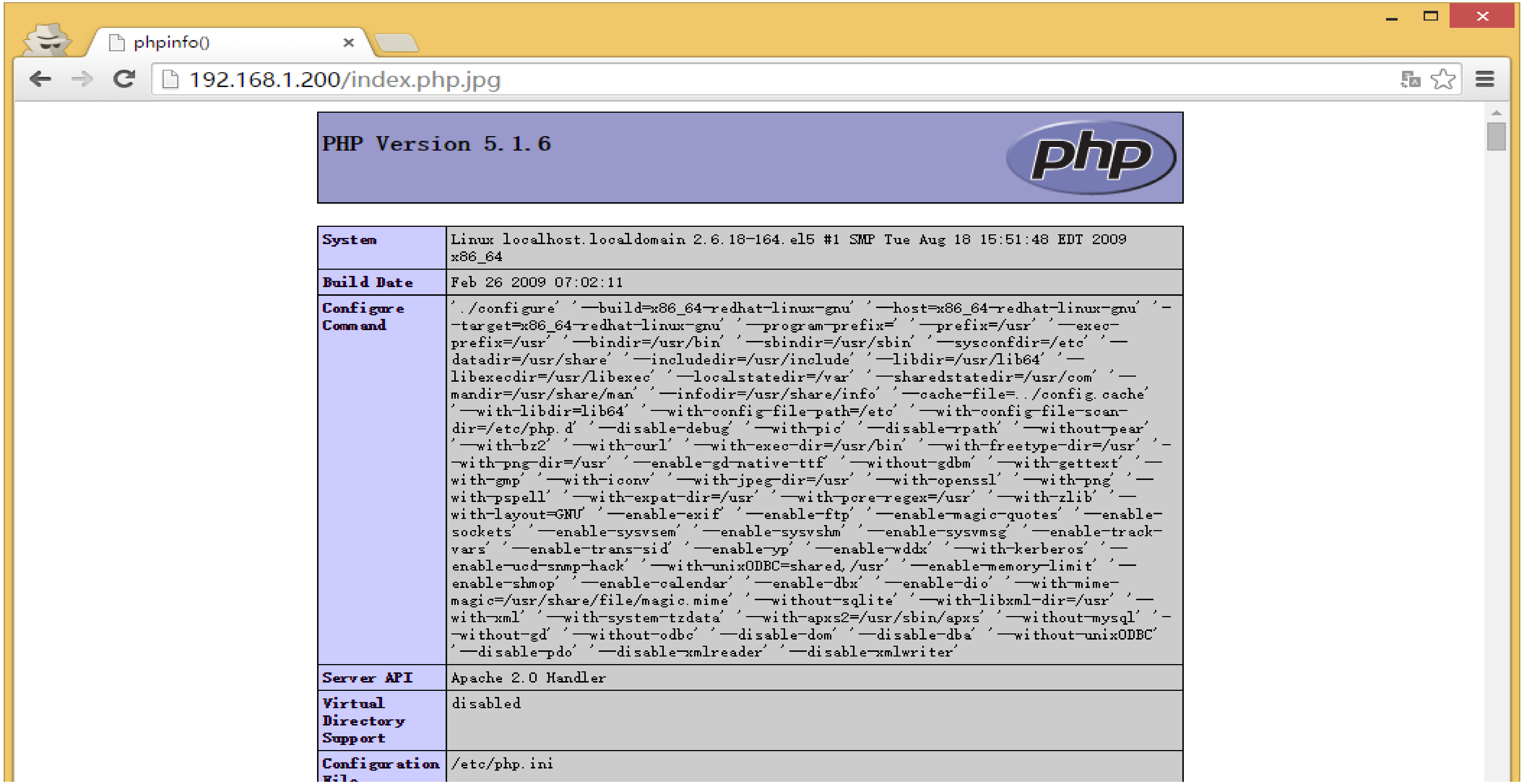
Apache/2.2.3 (Red Hat) Server at 192.168.1.200 Port 80

防止APPACHE的解析漏洞

Apache对于文件名的解析是从后往前解析的，直到遇见一个它认识的文件类型为止。因此，如果web目录下存在以类似webshell.php.test这样格式命名的文件，Apache在解析时因为不认识.test这个文件类型，所以会一直往前解析，当解析到.php时，它认识了，因此会将它解析为PHP文件。

Apache的这种解析特性经常被用来绕过Web应用的文件上传检测。当Web应用的文件上传功能在检测上传文件的合法性时，如果仅通过检测上传文件的扩展名来判断文件是否合法，就可以利用Apache的这种文件名解析特征绕过Web应用的检测。

禁止httpd解析index.php.jgp文件



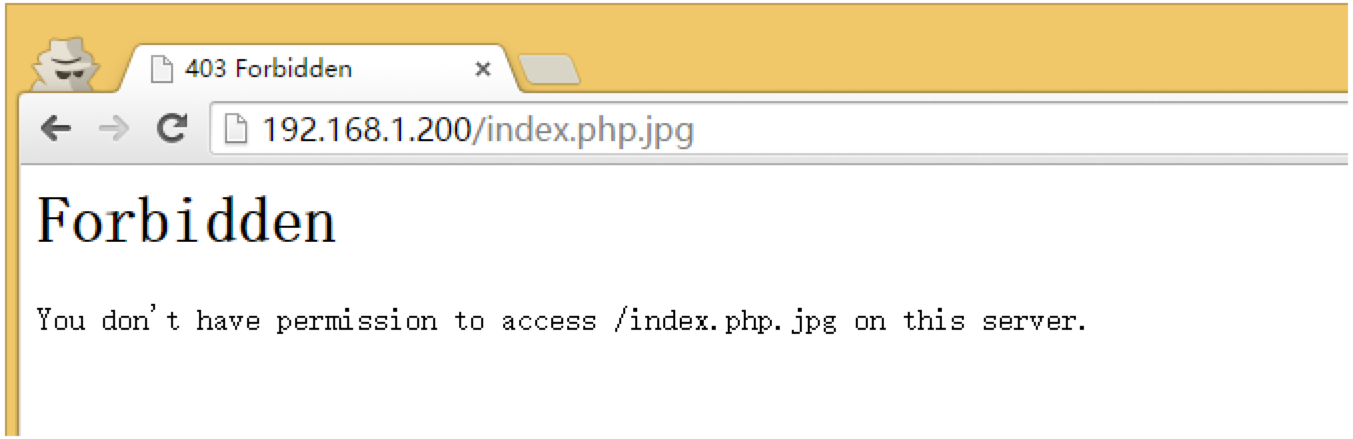
PHP Version 5.1.6

System	Linux localhost.localdomain 2.6.18-164.el5 #1 SMP Tue Aug 18 15:51:48 EDT 2009 x86_64
Build Date	Feb 26 2009 07:02:11
Configure Command	'./configure' '--build=x86_64-redhat-linux-gnu' '--host=x86_64-redhat-linux-gnu' '--target=x86_64-redhat-linux-gnu' '--program-prefix=' '--prefix=/usr' '--exec-prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin' '--sysconfdir=/etc' '--datadir=/usr/share' '--includedir=/usr/include' '--libdir=/usr/lib64' '--libexecdir=/usr/libexec' '--localstatedir=/var' '--sharedstatedir=/usr/com' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--cache-file=../config.cache' '--with-libdir=lib64' '--with-config-file-path=/etc' '--with-config-file-scan-dir=/etc/php.d' '--disable-debug' '--with-pic' '--disable-rpath' '--without-pear' '--with-bz2' '--with-curl' '--with-exec-dir=/usr/bin' '--with-freetype-dir=/usr' '--with-png-dir=/usr' '--enable-gd-native-ttf' '--without-gdbm' '--with-gettext' '--with-gmp' '--with-iconv' '--with-jpeg-dir=/usr' '--with-openssl' '--with-png' '--with-pspell' '--with-expat-dir=/usr' '--with-pcre-regex=/usr' '--with-zlib' '--with-layout=GNU' '--enable-exif' '--enable-ftp' '--enable-magic-quotes' '--enable-sockets' '--enable-sysvsem' '--enable-sysvshm' '--enable-sysvmsg' '--enable-track-vars' '--enable-trans-sid' '--enable-yp' '--enable-wddx' '--with-kerberos' '--enable-ucd-snmp-hack' '--with-unixODBC=shared,/usr' '--enable-memory-limit' '--enable-shmop' '--enable-calendar' '--enable-dbx' '--enable-dio' '--with-mime-magic=/usr/share/file/magic.mime' '--without-sqlite' '--with-libxml-dir=/usr' '--with-xml' '--with-system-tzdata' '--with-apxs2=/usr/sbin/apxs' '--without-mysql' '--without-gd' '--without-odbc' '--disable-dom' '--disable-dba' '--without-unixODBC' '--disable-pdo' '--disable-xmlreader' '--disable-xmlwriter'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File	/etc/php.ini

禁止httpd解析index.php.jgp文件

可以在httpd.conf配置文件中添加以下内容来阻止Apache解析这种文件。
修改后配置：

```
<FilesMatch \.php$>
   SetHandler application/x-httpd-php
</FilesMatch>
<FilesMatch "\.phps$">
   SetHandler application/x-httpd-php-source
</FilesMatch>
```



Forbidden

You don't have permission to access /index.php.jpg on this server.

错误页面重定向

在.htaccess 文件中加入如下内容即可：

```
ErrorDocument 400 /custom400.html
ErrorDocument 401 /custom401.html
ErrorDocument 403 /custom403.html
ErrorDocument 404 /custom404.html
ErrorDocument 405 /custom405.html
ErrorDocument 500 /custom500.html
```

Customxxx.html 为要设置的错误页面。

重新启动 Apache 服务生效

日志设置

编辑 httpd.conf 配置文件，设置日志记录文件、记录内容、记录 格式。其中，错误日志：

```
LogLevel notice                                    #日志的级别
ErrorLog  logs/error_log                           #日志的保存位置（错误日志）
```

访问日志：

```
LogFormat %h %l %u %t \”%r\” %>s %b “%{Accept}i\”%{Referer}i\” \”%{User-Agent}i\””
combined
CustomLog  logs/access_log combined （访问日志）
```

Apache httpd 将在这个文件中存放诊断信息和处理请求中出现的错误。 若要将错误日志送到 Syslog，则设置：ErrorLog syslog。

CustomLog 指令设置访问日志的文件名和位置。 访问日志中会记录服务器所处理的所有请求。

LogFormat 设置日志格式。 LogLevel 用于调整记录在错误日志中的信息的详细程度，建议设置为 notice

判定条件
查看 logs 目录中相关日志文件内容，记录完整。

拒绝服务防范

根据业务需要，合理设置 session 时间，防止拒绝服务攻击

vim httpd.conf 配置文件，

```
Timeout 10                  #客户端与服务器端建立连接前的时间间隔

KeepAlive On

KeepAliveTimeout 15 限制每个 session 的保持时间是 15 秒
```

注：此处为一建议值，具体的设定需要根据现实情况。

禁用CGI

如果服务器上不需要运行 CGI 程序，建议禁用 CGI

修改配置vim /etc/httpd/conf/httpd.conf，把 cgi-bin 目录的配置和模块都注释掉

```
#LoadModule cgi_module modules/mod_cgi.so
#ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"
#<Directory "/var/www/cgi-bin">
#    AllowOverride None
#    Options None
#    Order allow,deny
#    Allow from all
#</Directory>
```

防止SQL注入

SQL注入是非常危险的问题，小则网站后台被入侵，重则整个服务器沦陷，所以一定要小心。
php.ini中有一个设置：

magic_quotes_gpc = Off 改为 magic_quotes_gpc = On

关闭远程文件打开

allow_url_fopen = off

防止黑客远程远程包含漏洞

THANK YOU