钓鱼网站深度配置1

一、apache主配置文件解析

1. 基础配置

apache

```
ServerRoot "/etc/httpd"                    # 安装根目录（默认路径，无需修改）
Listen 80                                    # 监听所有IPv4的80端口（未绑定具体IP，兼容所有接口）
Include conf.modules.d/*.conf                # 动态加载模块配置（推荐做法，便于管理）
User apache                                  # 运行Apache的用户（默认已创建）
Group apache                                 # 运行Apache的组（默认已创建）
ServerAdmin root@localhost                   # 管理员邮箱（紧急联系用）
```

- **重点**：`Listen 80` 表示Apache监听所有网络接口的80端口，若需绑定特定IP请改为 `Listen 192.168.1.100:80`。

---

2. 全局安全策略

apache

```
<Directory />                                # 根目录匹配（优先级最高）
    AllowOverride none                       # 禁用所有.htaccess文件（提升安全性）
    Require all denied                       # 拒绝访问根目录下的任何文件（防止目录遍历攻击）
</Directory>
```

- **安全意义**：
  通过禁止根目录的访问，避免攻击者直接访问服务器文件系统。
  典型场景：若网站内容仅在`/var/www/html`下，此配置可有效隔离风险。

---

3. 网站根目录配置

apache

```
DocumentRoot "/var/www/html"                 # 网站静态文件根目录（默认路径）
<Directory "/var/www">                       # 匹配父目录（包含html子目录）
    AllowOverride None                       # 禁用.htaccess（推荐统一管理）
    Require all granted                      # 允许所有人访问该目录下的内容
</Directory>
<Directory "/var/www/html">                  # 精确匹配html目录
    Options Indexes FollowSymLinks           # 允许目录索引和符号链接跟随
    AllowOverride None                       # 禁用.htaccess
    Require all granted                      # 允许所有人访问
</Directory>
```

- 关键逻辑：

- 外层`<Directory "/var/www">`的作用范围更大，内层`<Directory "/var/www/html">`会覆盖部分配置（如`Options`）。
- `Indexes`允许自动列出目录内容，若需禁用可改为`Options -Indexes`。

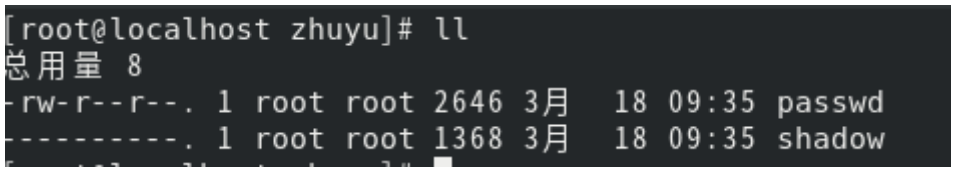
实验1：理解目录索引

在默认网页存放目录建立一个共享文件夹共享 系统文件。能实现下载。

关闭共享功能 重启http服务验证 是否无法进行共享下载

```
[root@localhost conf]# cd /var/www/html
[root@localhost html]# mkdir zhuyu
[root@localhost html]# cp /etc/passwd /etc/shadow zhuyu
[root@localhost html]# cd zhuyu
[root@localhost zhuyu]# ls
passwd  shadow
[root@localhost zhuyu]#
```

实验2：理解apache的权限




```
[root@localhost zhuyu]# chmod o+r shadow
```

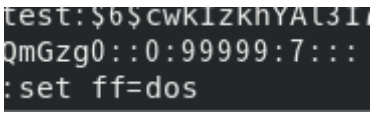
实验3：理解windows和linux的换行符

- windows换行符：`\r\n`
- linux换行符：`\n`
- 转换方法

  ```
  [root@localhost zhuyu]# unix2dos passwd
  unix2dos: 正在转换文件 passwd 为DOS格式...
  ```

- 转换方法2

  ```
  [root@localhost zhuyu]# vim shadow
  [root@localhost zhuyu]# chmod 644 shadow
  ```



---

4. 日志

apache

```
ErrorLog "logs/error_log"                  # 错误日志路径（默认路径）
LogLevel warn                               # 日志级别（建议生产环境设为error）
```

实验3：查看错误日志和访问日志

---

5. CGI脚本支持

apache

```
<IfModule alias_module>                  # 若启用alias模块
    ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"  # 将/cgi-bin/映射到实际目录
</IfModule>
<Directory "/var/www/cgi-bin">           # CGI脚本执行目录
    AllowOverride None                     # 禁用.htaccess
    Options None                            # 禁用目录索引等选项
    Require all granted                    # 允许执行脚本
</Directory>
```

- **注意**：
  若未使用CGI服务，建议删除相关配置以减少攻击面。
  若需执行CGI脚本，需确保目录权限正确且脚本有可执行权限（`chmod +x script.cgi`）。

---

6. MIME类型与字符集

apache

```
AddDefaultCharset UTF-8                  # 默认字符集（推荐配置，避免乱码）
```

- **兼容性**：
  确保HTML文件保存为UTF-8编码，否则可能导致显示异常。

---

7. 性能优化项

apache

```
EnableSendfile on                        # 启用sendfile传输静态文件（提升性能）
```

- **原理**：
  直接通过内核传输文件，减少Apache进程的IO开销，适用于高并发场景。

---

8. 模块加载说明

apache

```
# 动态加载常用模块（根据需求启用/禁用）
<IfModule dir_module>       # 目录索引模块（默认需要）
    DirectoryIndex index.html
</IfModule>
<IfModule log_config_module> # 日志模块（默认需要）
    # 日志格式配置（已优化）
</IfModule>
<IfModule alias_module>     # 别名模块（用于CGI）
    ScriptAlias /cgi-bin/...
</IfModule>
<IfModule mime_module>      # MIME类型模块（默认需要）
    # 文件类型映射配置
</IfModule>
```

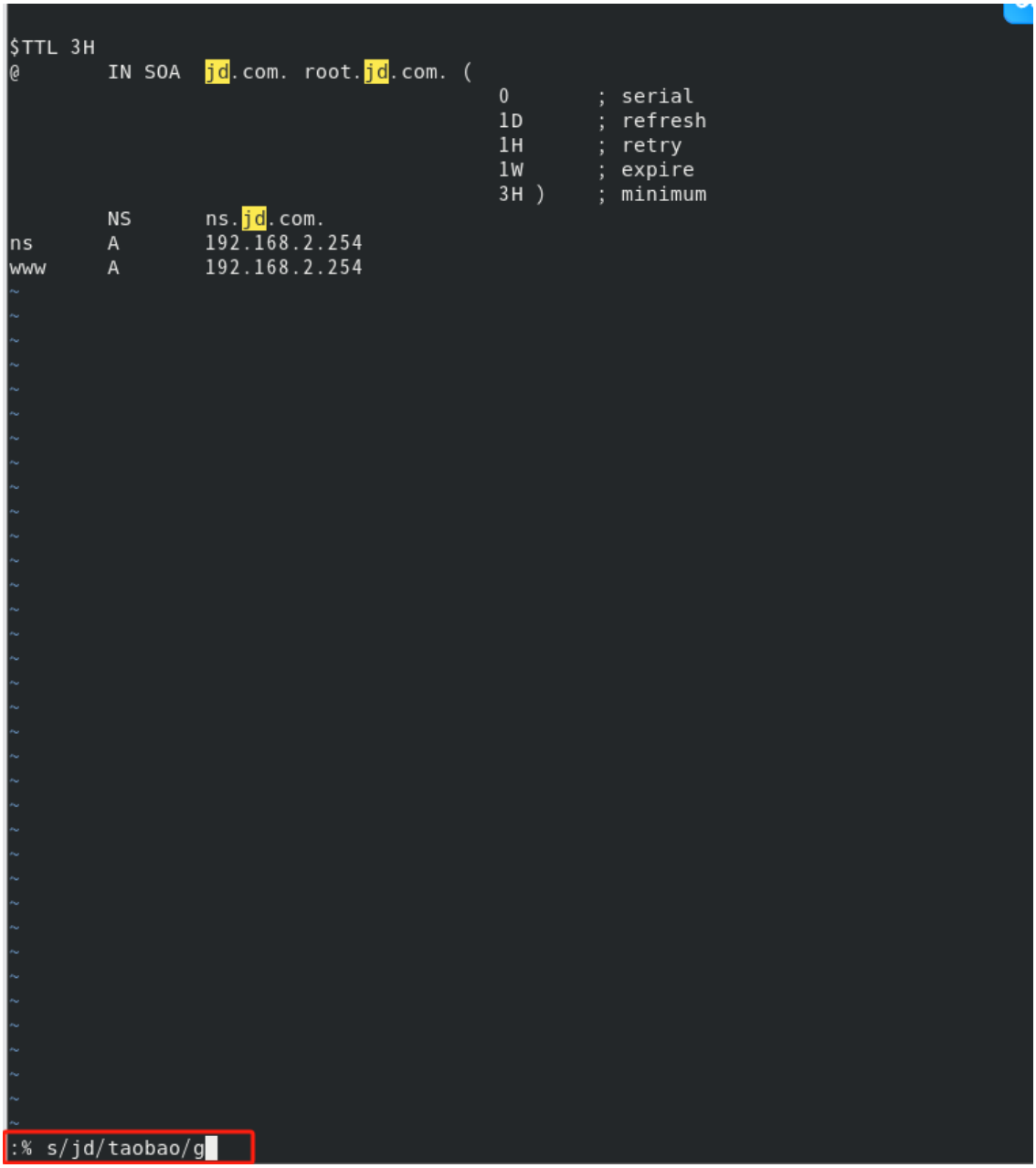
二、apache的虚拟主机配置

1.配置taobao的DNS配置

- 修改dns主配置文件`/etc/named.conf`

- 创建taoabao的解析文件

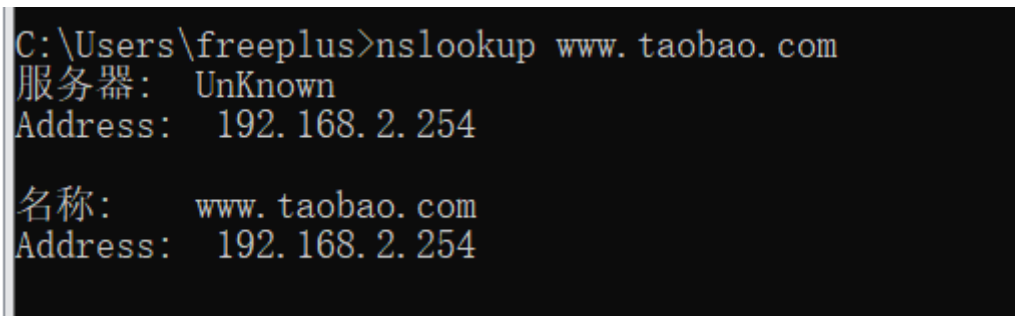
```
[root@localhost zhuyu]# cd /var/named
[root@localhost named]# touch taobao.com.zone
```



- 重启DNS服务

```
[root@localhost named]# systemctl restart named
```

- 通过win10进行验证，能解析，但不能访问



2.apache的虚拟主机配置

```
[root@localhost named]# cd /var/www/html
[root@localhost html]# ls
index.html  zhuyu
[root@localhost html]# mkdir jd
[root@localhost html]# mkdir taobao
[root@localhost html]# mv index.html jd
[root@localhost html]# cd taobao
[root@localhost taobao]# cp ../jd/index.html  .
[root@localhost taobao]# ls
index.html
```

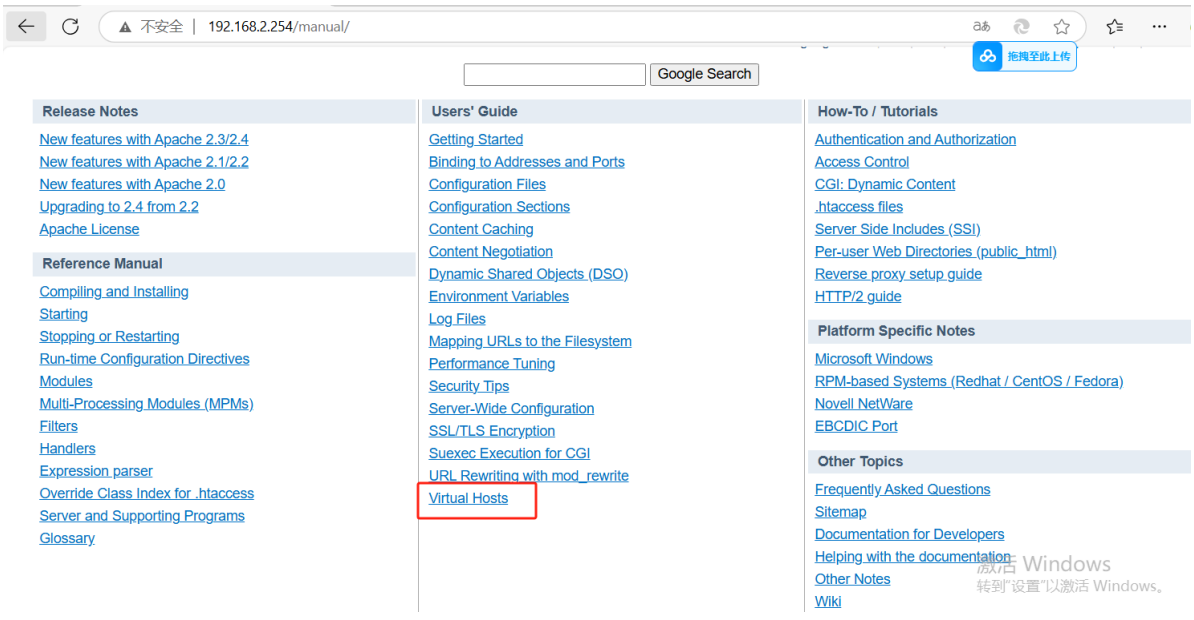
- apache的官方文档说明

```
[root@localhost taobao]# yum install httpd-manual   #官方手册
```

```
已安装：
  httpd-manual-2.4.37-43.module_el8.5.0+1022+b541f3b1.noarch

完毕！
```

```
[root@localhost taobao]# firefox /usr/share//httpd/manual/index.html &    #通过firefox后台打开
[1] 9451
```



points at the same IP address. Then you simply add the following to httpd.conf:

```
<VirtualHost *:80>
    # This first-listed virtual host is also the default for *:80
    ServerName www.example.com
    ServerAlias example.com
    DocumentRoot "/www/domain"
</VirtualHost>

<VirtualHost *:80>
    ServerName other.example.com
    DocumentRoot "/www/otherdomain"
</VirtualHost>
```

- 通过模板编辑`/etc/httpd/conf/httpd.conf`

```
354 #
355 # Load config files in the "/etc/httpd/conf.d" direct
356 IncludeOptional conf.d/*.conf
357 NameVirtualHost *:80
358 <VirtualHost *:80>
359         ServerName www.jd.com
360         DocumentRoot /var/www/html/jd
361 </VirtualHost>
362
363 <VirtualHost *:80>
364         ServerName www.taobao.com
365         DocumentRoot /var/www/html/taobao
366 </VirtualHost>
-- 插入 --
```

- 重启服务

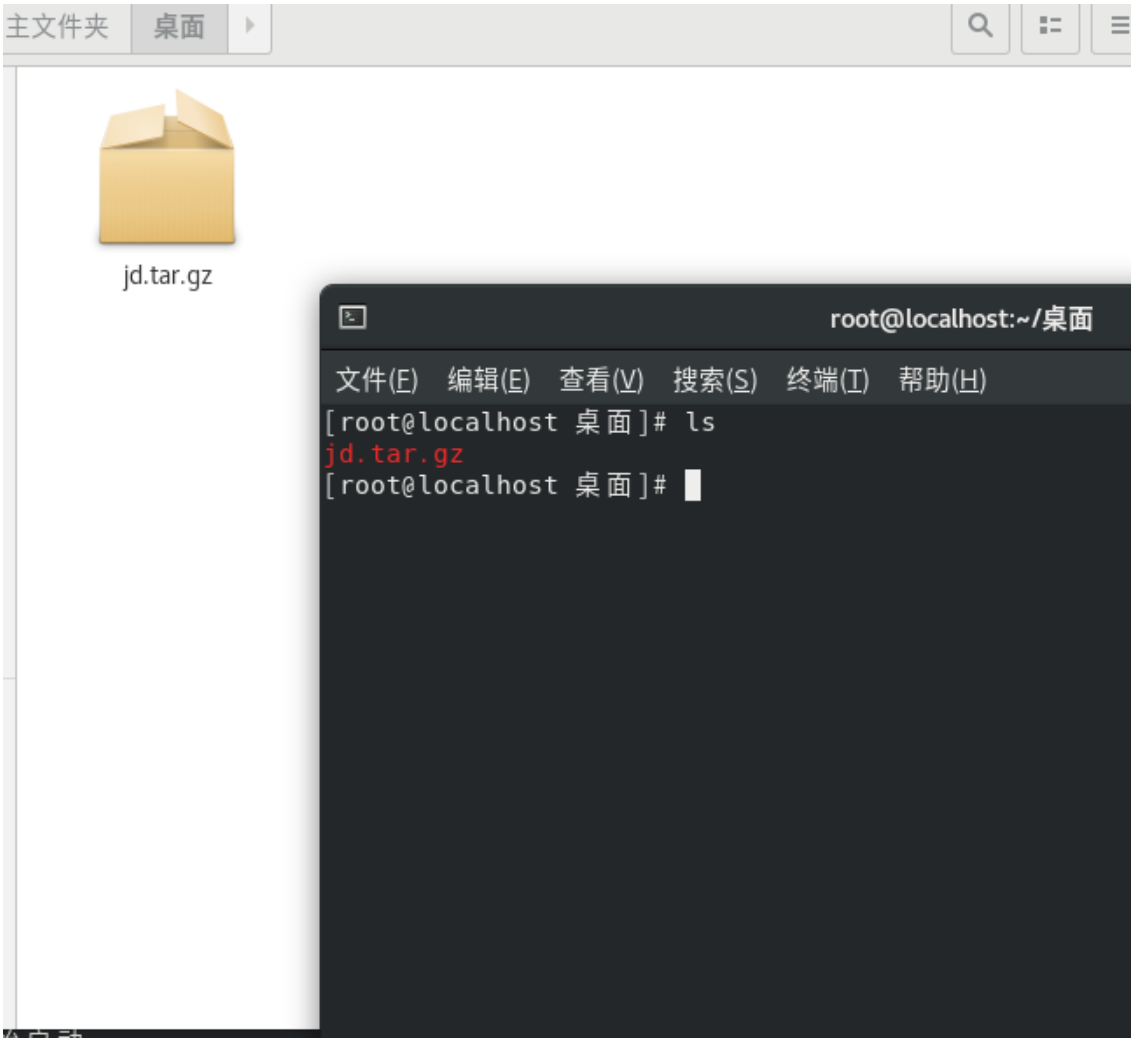
```
systemctl restart httpd.service
```

- 使用win10访问taobao

三、钓鱼页面的伪造

1.布置防jd页面源码

- 将源码复制到centos8中



- 解压

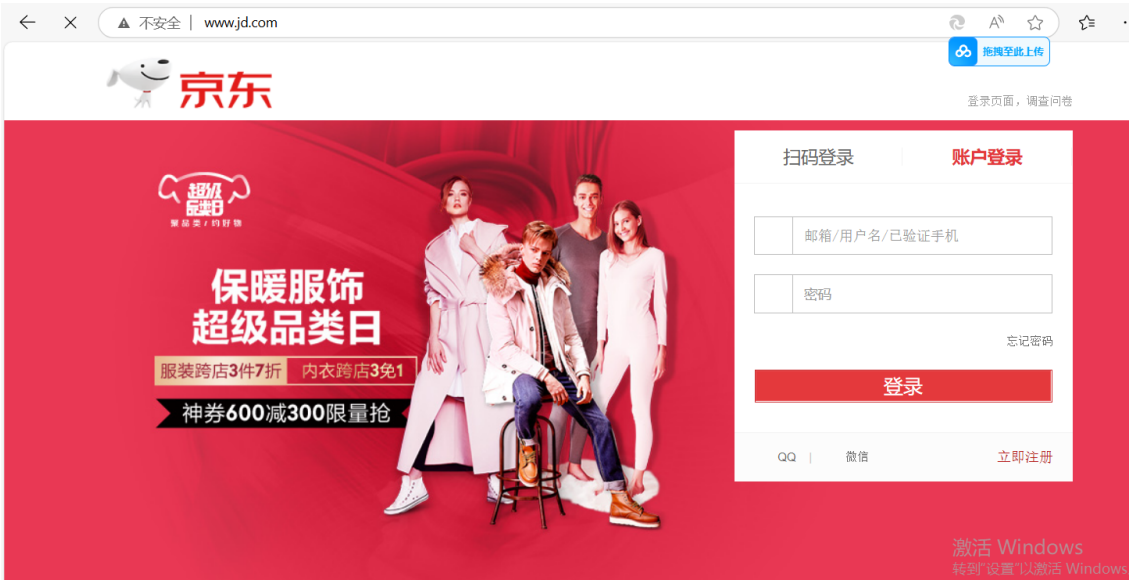
```
[root@localhost 桌面]# tar -zxf jd.tar.gz
[root@localhost 桌面]# ls
html  jd.tar.gz
[root@localhost 桌面]# cd html/
[root@localhost html]# ls
error.php  index.php  jd_files  jd.html
```

- 将解压后的文件复制到jd的根目录中

```
[root@localhost html]# rm -rf /var/www/html/jd/index.html
[root@localhost html]# mv * /var/www/html/jd
[root@localhost html]# cd /var/www/html/jd
[root@localhost jd]# ls
error.php  index.php  jd_files  jd.html
```

- 在win10中访问jd

```
[root@localhost jd]# mv jd.html index.html
[root@localhost jd]# systemctl restart httpd.service
```



四、安装数据库

1.安装并启动

```
[root@localhost yum.repos.d]# yum install mysql-server
[root@fishserver ~]# systemctl start mysqld
```

```
  验证     : mariadb-connector-c-config-3.1.11-2.el8_3.noarch                                                1/7
  验证     : mecab-0.996-1.module_el8.4.0+589+11e12751.9.x86_64                                              2/7
  验证     : mysql-8.0.26-1.module_el8.4.0+915+de215114.x86_64                                               3/7
  验证     : mysql-common-8.0.26-1.module_el8.4.0+915+de215114.x86_64                                        4/7
  验证     : mysql-errmsg-8.0.26-1.module_el8.4.0+915+de215114.x86_64                                        5/7
  验证     : mysql-server-8.0.26-1.module_el8.4.0+915+de215114.x86_64                                        6/7
  验证     : protobuf-lite-3.5.0-13.el8.x86_64                                                               7/7

已安装:
  mysql-server-8.0.26-1.module_el8.4.0+915+de215114.x86_64          mariadb-connector-c-config-3.1.11-
le_el8.4.0+589+11e12751.9.x86_64          mysql-8.0.26-1.module_el8.4.0+915+de215114.x86_64
  mysql-common-8.0.26-1.module_el8.4.0+915+de215114.x86_64          mysql-errmsg-8.0.26-1.module_el8.4
0-13.el8.x86_64

完毕！
```