4.2 应用安全配置

4.2.1 Apache+PHP+Mysql 安全配置

0x01 总体说明

Apache 与 Tomcat 有啥关系与区别

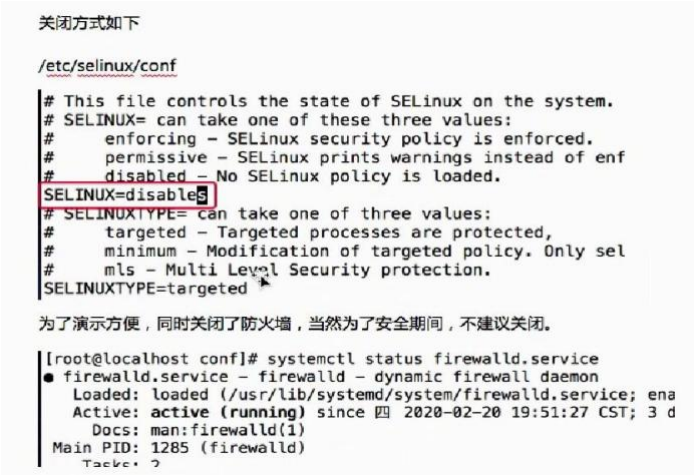
相同点：

都是 APACHE 组织开发；都能提供 HTTP 服务；都是开源和免费；

不同点：

Apache 是 Web 服务，Tomcat 是应用(java)服务器，它只是一个 serlet 容器，可以认为是 Apache 是扩展，但可以独立于 Apache 运行。

1)phpmvstudy



其它解读

https://www.jianshu.com/p/a8bab3f50c7b【简书，APACHE 服务器安全配置】

0x03php 安全与配置

0x01 禁用危险函数

打开 php.ini,查找 disable functions,按如下设置禁用一些函数

disable functions

=phpinfo,exec,passthru,shell_exec,system,proc_open,popen,curl_exec,curl_multi_exec,parse_ini_file,show_source,

dl evel,proc terminate,touch,escapeshellarg,escapeshellcmd 等

0x02 文件权限

不要给写的权限，禁止写入

find -type f-name *.php-exec chmod 444 {}\;

0x03 及时升级版本

0x04 禁用远程 URL 文件处理

allow_url_fopen =Off

0x05 限制 php 的读写操作

open_basedir =/var/www/htdocs/files

0x06Posing Limit

限制 PHP 的执行时间、内存使用量、post 和 upload 的数据是最好的策略　max_execution_time =30;Max script execution time

max_input_time =60 ;Max time spent parsing input

memory_limit =16M ;Max memory used by one script

upload_max_filesize =2M;Max upload file size

post_max_size =8M;Max post size

0x07 禁用错误消息和启用日志功能

在默认设置中，php 会向浏览器输出错误消息，在应用程序的开发过程中，这个默认设置是最合理的配置，然而，它也可以向用户泄漏一些安全信息，例如安装路径和用户名。在已经开发完成的网站中，最好禁用错误消息然后把错误消息输出到日志文件中。

display errors =Off

log errors =ON

0x08:隐藏 PHP 文件

expose_php =Off

0x09:限制公共用户对具有特定后缀名的文件的访问

由于安全的原因，很多具有特定后缀名的文件不能被公共用户所访问，比如 inc 后缀的文件，里面包含了一些敏感的信息，比如 mysql 连接信息，如果没有适当的配置，那么每个用户都能访问这个配置文件，为了加强网站的安全，你需要在..htaccess 文件进行如下的配置：

```
<filesmatch>
Order allow,deny
Deny from al
</filesmatch>
```

详见文档

《php 安全设置总结》

《PHP 安全加固规范》

0x04Mysql 安全与配置

详见文档《Mysql 安全配置规范》

yum repolist all |grep mysqll 查看安装的 mysql