应用安全配置

Apache与Mysql安全配置

安全中心 杨勇 coolcyang

应用安全配置

- Apache

- Mysql

Apache安全配置

- 安全补丁更新
- 敏感信息保护
- 最小化安全原则
- 访问控制
- 防DOS配置
- 日志维护和保护

Apache安全配置

- 版本&安全补丁更新
  - security.oa.com
  - www.apache.org安全公告
  - http://httpd.apache.org/security_report.html
- 下载发行版校验

Apache安全配置

- 安全补丁更新
- 敏感信息保护
- 最小化安全原则
- 访问控制
- 防DOS配置
- 日志维护和保护

Apache安全配置

- 问题
  - Apache有哪些敏感信息？
  - 泄露这些敏感信息会有哪些危害？
  - 您如何屏蔽这些信息？

Apache安全配置

- 敏感信息保护
  - 屏蔽banner
    - ServerTokens Prod
    - ServerSignature Off
  - 屏幕默认目录
    - /var/www/icons 下文件
    - /var/www/htdocs下默认文件
    - /var/www/manual下默认文件
    - /var/www/cgi-bin下默认文件
  - 屏蔽枚举帐户
    - **UserDir public_html**
    - 注释掉该行
    - **#UserDir public_html**

Apache安全配置

- 敏感信息保护
  - 去掉索引功能Options –Indexes
  - 例子
    - Apache虚拟主机的配置应该在httpd.conf里第一个虚拟主机前面加上这段设置，当用户用IP访问时候默认跳转到部门主页中。
    - <VirtualHost XXX.XXX.XXX.XXX>
    - ServerName serverdomin.qq.com
    - DocumentRoot /usr/local/apache/htdocs
    - <Directory "/usr/local/apache/htdocs">
    - Options -Indexes -Includes
    - Order deny,allow
    - Deny from all
    - </Directory>
    - </VirtualHost>

Apache安全配置

- 安全补丁更新
- 敏感信息保护
- 最小化安全原则
- 访问控制
- 防DOS配置
- 日志维护和保护

Apache安全配置

- 最小化安全原则--模块
  - 编译
    - 例子
      - $ **./configure **
      - > **--prefix=/usr/local/apache **
      - > **--enable-module=rewrite **
      - > **--enable-module=so **
      - > **--disable-module=imap **
      - > **--disable-module=userdir**
  - 检查
    - 静态编译
    - DSO编译方式

Apache安全配置

- 安全补丁更新
- 敏感信息保护
- 最小化安全原则
- 访问控制
- 防DOS配置
- 日志维护和保护

Apache安全配置

- 访问控制
  - Web根目录设置
    - DocumentRoot /应为 web首页目录
  - 启动帐户
    - 启动Apache的帐号应为nobody
      - **User nobody**
      - **Group nogroup**

Apache安全配置

- 访问控制
  - 设置合理的属主
    - cp httpd /usr/local/apache/bin
    - chown 0 /usr/local/apache/bin/httpd
    - chgrp 0 /usr/local/apache/bin/httpd
    - chmod 511 /usr/local/apache/bin/httpd
  - 设置合理的权限
    - # chown -R root:root /usr/local/apache
    - # find /usr/local/apache -type d | xargs chmod 755
    - # find /usr/local/apache -type f | xargs chmod 644
    - # chmod -R go-w /usr/local/apache

Apache安全配置

- 安全补丁更新
- 敏感信息保护
- 最小化安全原则
- 访问控制
- 防DOS配置
- 日志维护和保护

Apache安全配置

- AntiDOS配置-配置连接参数
  - HARD_SERVER_LIMIT
  - MinSpareServers 与MaxSpareServers
  - MaxClient s
  - **Keep-Alive**
  - **StartServers**
  - **TimeOut**
  - MaxKeepAliveRequests
  - **KeepAliveTimeout**

Apache安全配置

调整参数	建议参数
HARD_SERVER_LIMIT	设置Apache同时连接的最大进程数。
MinSpareServers	最小空闲子进程数。
MaxSpareServers	最大空闲子进程数。
MaxClient	同时处理的最大用户连接数。
Keep-Alive	关闭HTTP/1.0和HTTP/1.1的长连接特性。 当有静态页面时，开启，但应调小 KeepAliveTimeOut
StartServers	启动Apache服务后的启动的进程数。
TimeOut	客户端和服务端连接超时时间。
MaxKeepAliveRequests	一个连接发起的请求数
KeepAliveTimeout	服务在关闭连接前，等待下一次请求的时间。

Apache安全配置

调整参数	建议参数
HARD_SERVER_LIMIT	8193
MinSpareServers	100
MaxSpareServers	200
MaxClient	400
Keep-Alive	off
StartServers	300
TimeOut	60
MaxKeepAliveReques	根据实际负载调整
KeepAliveTimeout	2

Apache安全配置

- 安全补丁更新
- 敏感信息保护
- 最小化安全原则
- 访问控制
- 防DOS配置
- 日志维护和保护

Apache安全配置

- 日志维护和保护
  - 设置权限
  - 日志格式
    - 存放位置（独立分区）
    - Common Log Format (CLF)

127.0.0.1 - username [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326

    - 组合记录格式(Combined Log Format ）

127.0.0.1 - username [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326 "http://www.example.com/start.html" "Mozilla/4.08 [en] (Win98; I ;Nav)"

Apache安全配置

- 日志维护和保护
  - 日志回滚
    - 回卷日志
      - mv access_log access_log.old
        mv error_log error_log.old
        apachectl graceful
        sleep 600
        gzip access_log.old error_log.old
    - 管道&rotatelogs回卷日志
    - CustomLog "|/usr/local/apache/bin/rotatelogs /var/log/access_log 86400" common

MySQL安全配置

- 安全补丁更新
- 敏感信息
- 帐户及数据库角色
  - 默认帐户安全问题
  - 网络连接
  - Msql授权表
  - 如何进行加固
- 危险函数
- Mysql启动运行安全

MySQL安全配置

- 经常关注安全更新
  - Security.oa.com
  - Mysql官方网站
- 不轻易更换（eg：Mysql3->Mysql4）
  - Union带来的漏洞

MySQL安全配置

- 安全补丁更新
- 敏感信息
- 帐户及数据库角色
  - 默认帐户安全问题
  - 网络连接
  - Msql授权表
  - 如何进行加固
- 危险函数
- Mysql启动运行安全

MySQL安全配置

- 泄露密码
  - bash_history
  - .mysql_history
- 两个shell命令vs一个好习惯
  - Shell>rm .bash_history
  - Shell>rm .mysql_history
  - Shell>ln –s /dev/null .bash_history
  - Shell>ln –s /dev/null .mysql_history

MySQL安全配置

- 安全补丁更新
- 敏感信息
- 帐户及数据库角色
  - 默认帐户安全问题
  - 网络连接
  - Msql授权表
- 危险函数
- Mysql启动运行安全

MySQL安全配置

- Root空口令
- 匿名用户

```
mysql> select * from user where not (host="localhost" and user="root")
    -> ;
+-----------+------+----------+-------------+-------------+-------------+-------------+-------------
-------------+--------------+-----------+-------------+--------------+-----------+------------+
| Host      | User | Password | Select_priv | Insert_priv | Update_priv | Delete_priv | Create_priv |
Shutdown_priv | Process_priv | File_priv | Grant_priv | References_priv | Index_priv | Alter_priv |
+-----------+------+----------+-------------+-------------+-------------+-------------+-------------
-------------+--------------+-----------+-------------+--------------+-----------+------------+
| localhost |      |          | N           | N           | N           | N           | N
N            | N            | N         | N           | N               | N         | N          |
+-----------+------+----------+-------------+-------------+-------------+-------------+-------------
-------------+--------------+-----------+-------------+--------------+-----------+------------+
1 row in set (0.00 sec)

mysql>
```

MySQL安全配置

- 帐户和口令安全
  - 给mysql的root用户设置口令
    - mysql> use mysql;
      mysql> update user set password=password('test')
      where user='root';
      mysql> flush privileges;
  - 删除匿名用户
    - Mysql>delete from user where user=''

MySQL安全配置

- 老版本权限的问题
  - 版本3.21.xx:755
  - 版本3.22.xx:770
  - 版本3.23.xx:700(推荐)
- 推荐两个命令
  - Shell>chown –R mysql.mysql /usr/local/mysql/var
  - Shell>chown –R go-rwx /usr/local/mysql/var

MySQL安全配置

- 网络连接访问控制
  - 避免外部连接
    - 启动时Skip-networking
    - my.cnf bind-address=内网ip
  - 限定连接IP
    - mysql> grant select,insert,update,delete,create,drop privileges on test.* to test1@'192.168.1.0/255.255.255.0' identified by 'test';
  - NT主机默认允许远程连接

MySQL安全配置

- User表
  - mysql>desc user;
  - 版本3.22.11版本以前的授权机制不完善(建议升级)
  - GRAND&REVOK
  - 危险的权限
    - Shutdown
    - Process
    - file

MySQL安全配置

- User表

```
mysql> desc user;
+-----------------+-----------------+------+-----+---------+-------+
| Field           | Type            | Null | Key | Default | Extra |
+-----------------+-----------------+------+-----+---------+-------+
| Host            | char(60) binary |      | PRI |         |       |
| User            | char(16) binary |      | PRI |         |       |
| Password        | char(16) binary |      |     |         |       |
| Select_priv     | enum('N','Y')   |      |     | N       |       |
| Insert_priv     | enum('N','Y')   |      |     | N       |       |
| Update_priv     | enum('N','Y')   |      |     | N       |       |
| Delete_priv     | enum('N','Y')   |      |     | N       |       |
| Create_priv     | enum('N','Y')   |      |     | N       |       |
| Drop_priv       | enum('N','Y')   |      |     | N       |       |
| Reload_priv     | enum('N','Y')   |      |     | N       |       |
| Shutdown_priv   | enum('N','Y')   |      |     | N       |       |
| Process_priv    | enum('N','Y')   |      |     | N       |       |
| File_priv       | enum('N','Y')   |      |     | N       |       |
| Grant_priv      | enum('N','Y')   |      |     | N       |       |
| References_priv | enum('N','Y')   |      |     | N       |       |
| Index_priv      | enum('N','Y')   |      |     | N       |       |
| Alter_priv      | enum('N','Y')   |      |     | N       |       |
+-----------------+-----------------+------+-----+---------+-------+
17 rows in set (0.00 sec)

mysql>
```

MySQL安全配置

- Db表

```
mysql> desc db;
+-----------------+-----------------+------+-----+---------+-------+
| Field           | Type            | Null | Key | Default | Extra |
+-----------------+-----------------+------+-----+---------+-------+
| Host            | char(60) binary |      | PRI |         |       |
| Db              | char(64) binary |      | PRI |         |       |
| User            | char(16) binary |      | PRI |         |       |
| Select_priv     | enum('N','Y')   |      |     | N       |       |
| Insert_priv     | enum('N','Y')   |      |     | N       |       |
| Update_priv     | enum('N','Y')   |      |     | N       |       |
| Delete_priv     | enum('N','Y')   |      |     | N       |       |
| Create_priv     | enum('N','Y')   |      |     | N       |       |
| Drop_priv       | enum('N','Y')   |      |     | N       |       |
| Grant_priv      | enum('N','Y')   |      |     | N       |       |
| References_priv | enum('N','Y')   |      |     | N       |       |
| Index_priv      | enum('N','Y')   |      |     | N       |       |
| Alter_priv      | enum('N','Y')   |      |     | N       |       |
+-----------------+-----------------+------+-----+---------+-------+
13 rows in set (0.01 sec)

mysql>
```

MySQL安全配置

- Host表

```
ysql> desc host;
+-----------------+-----------------+------+-----+---------+-------+
| Field           | Type            | Null | Key | Default | Extra |
+-----------------+-----------------+------+-----+---------+-------+
| Host            | char(60) binary |      | PRI |         |       |
| Db              | char(64) binary |      | PRI |         |       |
| Select_priv     | enum('N','Y')   |      |     | N       |       |
| Insert_priv     | enum('N','Y')   |      |     | N       |       |
| Update_priv     | enum('N','Y')   |      |     | N       |       |
| Delete_priv     | enum('N','Y')   |      |     | N       |       |
| Create_priv     | enum('N','Y')   |      |     | N       |       |
| Drop_priv       | enum('N','Y')   |      |     | N       |       |
| Grant_priv      | enum('N','Y')   |      |     | N       |       |
| References_priv | enum('N','Y')   |      |     | N       |       |
| Index_priv      | enum('N','Y')   |      |     | N       |       |
| Alter_priv      | enum('N','Y')   |      |     | N       |       |
+-----------------+-----------------+------+-----+---------+-------+
12 rows in set (0.00 sec)

ysql>
```

MySQL安全配置

- Table_prive表

```
mysql> desc tables_priv;
+-------------+-----------------------------------------------------------------------------------
-----+-------+
| Field       | Type
ault | Extra |
+-------------+-----------------------------------------------------------------------------------
-----+-------+
| Host        | char(60) binary
     |       |
| Db          | char(64) binary
     |       |
| User        | char(16) binary
     |       |
| Table_name  | char(60) binary
     |       |
| Grantor     | char(77)
     |       |
| Timestamp   | timestamp(14)
L    |       |
| Table_priv  | set('Select','Insert','Update','Delete','Create','Drop','Grant','References','Index',
     |       |
| Column_priv | set('Select','Insert','Update','References')
     |       |
+-------------+-----------------------------------------------------------------------------------
-----+-------+
8 rows in set (0.00 sec)

mysql>
```

MySQL安全配置

- Columns_priv表

```
mysql> desc columns_priv;
+-------------+---------------------------------------------------+------+-----+---------+-------+
| Field       | Type                                              | Null | Key | Default | Extra |
+-------------+---------------------------------------------------+------+-----+---------+-------+
| Host        | char(60) binary                                   |      | PRI |         |       |
| Db          | char(64) binary                                   |      | PRI |         |       |
| User        | char(16) binary                                   |      | PRI |         |       |
| Table_name  | char(64) binary                                   |      | PRI |         |       |
| Column_name | char(64) binary                                   |      | PRI |         |       |
| Timestamp   | timestamp(14)                                     | YES  |     | NULL    |       |
| Column_priv | set('Select','Insert','Update','References')      |      |     |         |       |
+-------------+---------------------------------------------------+------+-----+---------+-------+
7 rows in set (0.00 sec)

mysql>
```

MySQL安全配置

- 授权表运行机制
  - 服务器检查是否允许该用户连接
    - Host
    - user
  - 用户进行的是否是授权操作
    - 权限生效条件
    - *_priv

MySQL安全配置

- 思考题
  - 如何给数据库tencentdata设置如下权限
    - 用途：查询数据
    - 用户名：viewer
    - 密码：T3nc3t！965.A
    - Web CGI程序主机IP : 172.16.1.1

MySQL安全配置

- 安全补丁更新
- 敏感信息
- 帐户及数据库角色
  - 默认帐户安全问题
  - 网络连接
  - Msql授权表
- 危险函数
- Mysql启动运行安全

MySQL安全配置

- 危险的函数
  - LOAD DATA INFILE(只能读全局可读文件)
  - SELECT …INTO OUTFILE(不能覆盖文件)

MySQL安全配置

- 常见攻击
  - 拥有FILE权限
    - CREATE TABLE etc_passwd (pwd_entry TEXT);
    - LOAD DATA INFILE "/etc/passwd" into TABLE etc_passwd;
    - SELECT * FROM etc_passwd;

MySQL安全配置

- 读取文件

```
mysql> LOAD DATA INFILE "/etc/passwd" into TABLE  shadow;
Query OK, 21 rows affected (0.00 sec)
Records: 21  Deleted: 0  Skipped: 0  Warnings: 0

mysql> select * from shadow;
+----------------------------------------------+
| shadow                                       |
+----------------------------------------------+
| root:x:0:0::/root:/bin/bash                  |
| bin:x:1:1:bin:/bin:                          |
| daemon:x:2:2:daemon:/sbin:                   |
| adm:x:3:4:adm:/var/log:                      |
| lp:x:4:7:lp:/var/spool/lpd:                  |
| sync:x:5:0:sync:/sbin:/bin/sync              |
| shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown |
| halt:x:7:0:halt:/sbin:/sbin/halt             |
| mail:x:8:12:mail:/:                          |
| news:x:9:13:news:/usr/lib/news:              |
| uucp:x:10:14:uucp:/var/spool/uucppublic:     |
| operator:x:11:0:operator:/root:/bin/bash     |
| games:x:12:100:games:/usr/games:             |
| ftp:x:14:50::/home/ftp:                      |
| smmsp:x:25:25:smmsp:/var/spool/clientmqueue: |
| mysql:x:27:27:MySQL:/var/lib/mysql:/bin/bash |
| rpc:x:32:32:RPC portmap user:/:/bin/false    |
```

MySQL安全配置

- 导出后门
  - mysql>create table a (cmd text);
  - mysql>insert into a values (“<?php");
  - mysql>insert into a values (“phpinfo");
  - mysql>insert into a values (“<php?>");
  - mysql>select * from a into outfile “/usr/local/apache/cgi-bin/cmd.php";

MySQL安全配置

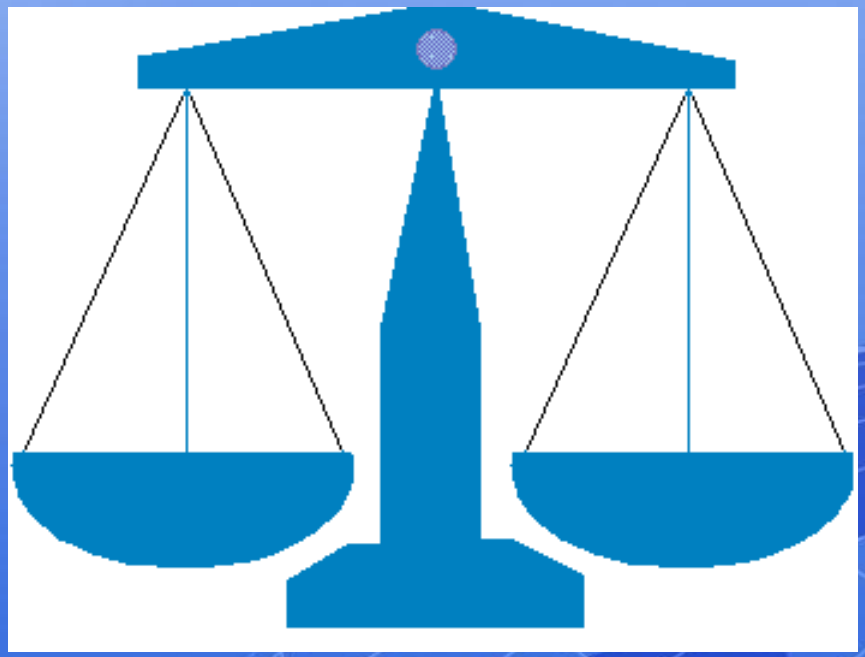
- 安全补丁更新
- 敏感信息
- 帐户及数据库角色
  - 默认帐户安全问题
  - 网络连接
  - Msql授权表
- 危险函数
- Mysql启动运行安全

MySQL安全配置

- 启动
  - 建议用非root权限启动（版本3.23.15）
  - 构建chroot环境
  - 启动MySQL服务器时加--skip-show-database
    使一般数据库用户不能浏览其它数据库

结　论

应用环境往往十分复杂多变，这种复杂多变造成诸多安全隐患，这些隐患随时都可能被黑客利用，完成一次成功的入侵。因此对于应用安全，我们需要更多关注应用层的安全配置和加固工作！



谢谢！