Alibaba Cloud Marketplace

Image Security Review Standard

Version: 2.0 (20170320)

Table of Contents

Chapter 1 System Component Security

1.1 Basic requirements

1) No public, usable security vulnerability for which a fix exists
2) No backdoors, bots, mining, or other malicious programs
3) Ensure that Server Guard has been installed and launches automatically at startup (there is no need to install Server Guard on special gateway-class and security-class image products or international site products)
4) In principle, it is not allowed to use released versions for which maintenance has been discontinued, such as Debian6, CentOS4, and Win2003
5) At the time of image creation, all official security updates must be installed. The solution is as follows:

1.2 Suggested operations

1.2.1 Install security updates

1) Windows: Enable *Windows Update* to check for updates periodically, and ensure the latest updates are installed
2) Debian: This includes Debian, Ubuntu, and other Linux releases. When the correct APT image source address has been properly configured, use the *apt update && apt upgrade* command for updates
3) Red Hat: This includes RHEL, CentOS, AliOS (Alibaba Cloud Linux), and OpenSUSE etc. Please use the *yum update* command to automatically perform updates
4) Other releases include BSD derivative versions. For these, please use the corresponding commands to perform updates

1.2.2 Check Server Guard Status

1) Windows: Task Manager => Processes => AliYunDunUpdate.exe and AliYunDun.exe
2) Linux: ps –ef |grep AliYunDun => AliYunDunUpdate and AliYunDun

1.3 Important component list

Ensure there are no usable vulnerabilities in the components listed below. For update methods, see 1.2.1 Install security updates

1) Boot and kernel layers: grub, kernel, initramfs, sysvinit, systemd, efistub, etc.
2) Operation dependency: libc6, glibc, libssl(openssl), libgnutls, OpenJDK, SunJDK, libtomcat, libxml, libgd, libpng, zlib, libpython, libnet, libkrb, libcup, libfuse, libdbus, etc.
3) Common user state programs: openssh, sshfs, shell (bash, zsh, csh, dash…), ftp, wget, curl, tar, gzip, sudo, su, ppp, rsync, fcitx, exim, apt, dpkg, rpm, yum, dnf, etc.

Chapter 2 Third-party Component Security

2.1 Basic requirements

1) No public, usable security vulnerability for which a fix exists
2) It is not allowed to use software versions or series for which maintenance has been discontinued, such as PHP 5.2, 5.3, and 5.4, MySQL 5.1, and Tomcat versions under 6.0 (in special circumstances when it is necessary to use such versions or series, please explain via email)
3) When creating images, please use the latest stable versions of third-party components
4) Please download software through official channels. Do not use certain search engines or download sites, to avoid any backdoors from being implanted

2.2 Suggested operations

2.2.1 Web containers

1) PHP: Current stable versions with maintenance support:
   - 5.5.x
   - 5.6.x
   - 7.0.x

   Official PHP site: http://php.net/

2) MySQL: Current stable versions with maintenance support:
   - 5.5.x
   - 5.6.x
   - 5.7.x

   Official MySQL site: http://dev.mysql.com/downloads/mysql/

3) Apache: Current stable versions with maintenance support:
   - 2.2.x
   - 2.4.x

   Official Apache HTTP Server site: https://httpd.apache.org/

4) Nginx: Current stable versions with maintenance support:
   - 1.10.x
   - 1.11.x

   Official Nginx download site: http://nginx.org/en/download.html

5) Tomcat: Current stable versions with maintenance support:
   - 9.0.x
   - 8.5.x
   - 7.0.x
   - 6.0.x

   Tomcat download URL: https://tomcat.apache.org/whichversion.html

6) Nodejs: Current stable versions with maintenance support:
   - V4 (maintenance to be discontinued on: 04/01/2018)
   - V6 (maintenance to be discontinued on: 04/18/2019)
   - V0.10 (maintenance discontinued on: 10/31/2016)
   - V0.12 (maintenance discontinued on: 12/31/2016)

   Nodejs download URL: https://nodejs.org/en/download/

7) Jetty: Current stable versions with maintenance support:

- 9.2.x
- 9.3.x
- 7.6.x (EOL, only a small number of security updates)
- 8.1.x (EOL, only a small number of security updates)

Jetty download URL: http://www.eclipse.org/jetty/download.html

8) ProFTPD: Current stable versions with maintenance support:
   - 1.3.5x
   - 1.3.6x

   Download URL: http://www.proftpd.org/

2.2.2 Web applications

1) Web applications are not allowed to have any known high-risk vulnerabilities, such as uploading of files at-will, SQL injection, command execution, or remote inclusion vulnerabilities
2) Open-source applications, such as CMS, BBS, and blogs, must be updated to the latest secure version
3) Ensure preinstalled web application plugins are updated to the latest safe version
4) The web application background forces users to modify their passwords upon their first logins

Chapter 3 System Security Configuration

3.1 Basic requirements

1) Reasonably configure system security updates (this can be accomplished by using the default ECS setting for image source configuration)
2) Do not use weak passwords. Use random strings as the default passwords for various programs
3) System passwords must meet certain length and complexity requirements (default ECS configuration shall suffice)
4) Do not allow non-essential SUID privilege programs
5) Reasonably configure key system directory permissions, such as /etc, /bin, and ~/.ssh
6) Except for the /tmp directory, the 777 permission shall not be allowed for other directories
7) Ensure the default daily log service, such as dmesg, syslog, wtmp, btmp, or sudo, runs properly

8) Set reasonable firewall policies that shield unsecure ports (such as redis 6379 and mongodb27017) and only open necessary ports. We suggest using iptables to shield all ports by default and then open individual ports as needed, such as HTTP 80, SSH 22, RDP 3389, and HTTPS 443

3.2 Suggested operations

3.2.1 Common Linux image source configurations

The configurations listed here can be used for custom images:

- **Debian 8**
  Use root permission to edit the file /etc/apt/sources.list and add the following content:

```
deb http://mirrors.aliyun.com/debian jessie main contrib non-free
deb http://mirrors.aliyun.com/debian jessie-proposed-updates main contrib non-free
deb http://mirrors.aliyun.com/debian jessie-updates main contrib non-free
deb http://mirrors.aliyun.com/debian-security/ jessie/updates main non-free contrib
```

- **Debian 7**
  Use root permission to edit the file /etc/apt/sources.list and add the following content:

```
deb http://mirrors.aliyun.com/debian wheezy main contrib non-free
deb http://mirrors.aliyun.com/debian wheezy-proposed-updates main contrib non-free
deb http://mirrors.aliyun.com/debian wheezy-updates main contrib non-free
deb http://mirrors.aliyun.com/debian-security/ wheezy/updates main non-free contrib
```

- **CentOS: First, backup the original configuration:**

```
mv /etc/yum.repos.d/CentOS-Base.repo /etc/yum.repos.d/CentOS-Base.repo.backup
```

CentOS 5

```
wget -O /etc/yum.repos.d/CentOS-Base.repo http://mirrors.aliyun.com/repo/Centos-5.repo
```

CentOS 6

```
wget -O /etc/yum.repos.d/CentOS-Base.repo http://mirrors.aliyun.com/repo/Centos-6.repo
```

CentOS 7

```
wget -O /etc/yum.repos.d/CentOS-Base.repo http://mirrors.aliyun.com/repo/Centos-7.repo
```

- **Ubuntu 14.04**
  Use root permission to edit the file /etc/apt/sources.list and add the following content

```
deb http://mirrors.aliyun.com/ubuntu/ trusty main restricted universe multiverse
deb http://mirrors.aliyun.com/ubuntu/ trusty-security main restricted universe multiverse
deb http://mirrors.aliyun.com/ubuntu/ trusty-updates main restricted universe multiverse
deb http://mirrors.aliyun.com/ubuntu/ trusty-proposed main restricted universe multiverse
deb http://mirrors.aliyun.com/ubuntu/ trusty-backports main restricted universe multiverse
```

- **Ubuntu 16.04**
  Use root permission to edit the file /etc/apt/sources.list and add the following content

```
deb http://mirrors.aliyun.com/ubuntu/ xenial main restricted universe multiverse
deb http://mirrors.aliyun.com/ubuntu/ xenial-security main restricted universe multiverse
deb http://mirrors.aliyun.com/ubuntu/ xenial-updates main restricted universe multiverse
deb http://mirrors.aliyun.com/ubuntu/ xenial-proposed main restricted universe multiverse
deb http://mirrors.aliyun.com/ubuntu/ xenial-backports main restricted universe multiverse
```

3.2.2 Linux password policy configuration

To be able to use pam_quality, you must add the following parameter in the /etc/pam.d/passwd file's password configuration:

```
password    required    pam_pwquality.so retry=3
```

The required password length must be at least 8 characters long and the password must contain all four types of characters. Add the following parameters to /etc/security/pwquality.conf:

```
minlen=8
minclass=4
```

- **Set password strength check**
  Check if the password has consecutive or repeated characters by adding the following in /etc/security/pwquality.conf:

```
maxsequence=3
maxrepeat=3
```

- **Set the user password expiration time to 90 days**

```
chage -M 90 <username>
#To disable the password expiration function, users usually set the -M option value to 99999 (equivalent to somewhat more than 273 years)
```

- **To force a password to expire immediately, use the following command:**

```
chage -d 0 username
# This command sets the password's last modification date to 1/1/1970. This means that, whatever the password expiration policy says, the password will immediately expire. The first time the user logs in, he will be immediately prompted to set a new password.
```

- **Failed login attempt limit**

  To lock any non-root user and unlock him after 10 minutes, enter the following command line in the /etc/pam.d/system-auth file's and /etc/pam.d/password-auth file's auth section:

```
auth        required      pam_faillock.so preauth silent audit deny=3 unlock_time=600
auth        sufficient    pam_unix.so nullok try_first_pass
auth        [default=die] pam_faillock.so authfail audit deny=3 unlock_time=600
```

- **View the failed attempt counter for each user**

```
faillock
```

- **Unlock a user's account**

```
faillock --user <username> --reset
```

3.2.3 SSH Server configuration

- **Root only allows public key login**

```
# vi /etc/ssh/sshd_config
PermitRootLogin without-password
```

- **Only use SSH Protocol 2:**

```
# vi /etc/ssh/sshd_config
```

```
Protocol 2
```

- **Do not support idle sessions and configure the Idle Log Out Timeout interval:**

```
# vi /etc/ssh/sshd_config
ClientAliveInterval 600          # (Set to 600 seconds = 10 minutes)
ClientAliveCountMax 0
```

- **Disable users' .rhosts files:**

```
# vi /etc/ssh/sshd_config
IgnoreRhosts yes
```

- **Configure the firewall to only accept SSH connections from known network segments:**

```
Update /etc/sysconfig/iptables (Redhat specific file) to accept connection only
from 192.168.100.0/24 and 209.64.100.5/27, enter:

-A RH-FW-1-INPUT -s 192.168.100.0/24 -m state --state NEW -p tcp --dport 22 -j ACCEPT
-A RH-FW-1-INPUT -s 209.64.100.5/27 -m state --state NEW -p tcp --dport 22 -j ACCEPT
```

- **Restrict the available interfaces for SSH listening and binding:**

```
# vi /etc/ssh/sshd_config
ListenAddress 192.168.100.17
ListenAddress 209.64.100.15
```

- **Use Chroot SSHD to restrict SFTP users to their own main directories:**

```
# vi /etc/ssh/sshd_config
ChrootDirectory /data01/home/%u
X11Forwarding no
AllowTcpForwarding no
```

- **Disable empty passwords:**

```
# vi /etc/ssh/sshd_config
PermitEmptyPasswords no
```

- **Use the following configuration to increase the level of detail for SSH logging:**

```
# vi /etc/ssh/sshd_config
LogLevel DEBUG
```

- **Delete rlogin and rsh binary programs and replace them with an SSH symlink:**

```
# find /usr -name rsh
/usr/bin/rsh
# rm -f /usr/bin/rsh
# ln -s /usr/bin/ssh /usr/bin/rsh
```

3.2.4 Linux firewall configuration

- **Syn-flood protection:**

```
iptables -A FORWARD -p tcp --syn -m limit --limit 1/s -j ACCEPT
```

- **Port scan defense:**

```
iptables -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit 1/s -j ACCEPT
```

- **ICMP packet speed limit:**

```
iptables -A FORWARD -p icmp --icmp-type echo-request -m limit --limit 1/s -j ACCEPT
```

- **Do not return ping packets**

```
# vim /etc/sysctl.conf
# Add: net.ipv4.icmp_echo_ignore_all = 1
# sysctl –p
```

- **Check for open ports**

```
# View all open TCP ports
netstat –nlp | grep tcp

View all open UDP ports
netstat –nlp |grep udp
```

3.2.5 View Linux special permission files

- **Find all "s"-bit programs in the system**
  Remove nonessential "s" bits or simply delete unnecessary ones

```
find / -type f ( -perm -04000 -o -perm -02000 ) -exec ls -lg {}
```

- **Ownerless files in the system:**

```
find / -nouser -o -nogroup
```

- **Files and directories for which all users have write permission:**

```
find / -type f ( -perm -2 -o -perm -20 ) -exec ls -lg {}
find / -type d ( -perm -2 -o -perm -20 ) -exec ls -ldg {}
```

3.2.6 Windows system reinforcement

- **System event audit policy configuration**

```
“Open” --> ”Run” --> secpol.msc ->Security Settings->Local Policies->Audit Policies
Suggested settings:
Audit policy modification: Successful
Audit login event: Successful, failed
Audit object access: Successful
Audit process tracking: Successful, failed
Audit directory service access: Successful, failed
Audit system event: Successful, failed
Audit account login event: Successful, failed
Audit account management: Successful, failed
```

- **Increase log file size limit**
  This avoids incomplete logs due to small log file capacity

```
“Open” --> ”Run” --> eventvwr.msc ->“windows log”->View the “Application”, “Security”, and “System” attributes
Suggested setting: Log size limit: 20480 KB
```

- **Check Everyone permissions**

Right-click on the system driver (disk)->“Properties”->“Security” and check if the system driver's root directory is set to "Everyone" permission. Delete "Everyone" permissions or cancel the "Everyone" write permission

- **Strengthen passwords and lock policies**

“Open” --> ”Run” --> secpol.msc (local security policies) ->Security Settings

1. Account Policies->Password Policy

Passwords must comply with complexity requirements: Enabled

Minimum password length: 8 characters

Minimum password use time: 0 days

Maximum password use time: 90 days

Mandatory password history: 1 remembered password

Use reversible encryption to store password: Disabled

2. Account Settings->Account Lock Policy

Account lock time: 30 minutes

Account lock threshold: 5 unsuccessful logins

Reset account lock counter: 30 minutes

3. Local Policies->Security Options

Interactive login: Do not show last username: Enabled

- **Remove unused system accounts to reduce risk**

“Open” --> ”Run” --> compmgmt.msc (computer management)->Local Users and Groups, check if there are unused accounts, system accounts belong to the correct groups, and guest accounts are locked

Use the “net user username /del” command to delete accounts

Use the “net user username /active:no” command to lock accounts

3.2.7 Windows network reinforcement

- Users who do not require IPv6 may choose to disable it

Control Panel-> Network and Sharing Center->Change Adaptor Settings->Local Connections->Properties->Internet Protocol Version 6 (TCP/IPv6), uncheck the option in the selection box to disable IPv6

- **Network access control**

“Open” --> ”Run” --> secpol.msc ->Security Settings->Local Policies->Security Options
Network access: Do not allow anonymous enumeration for SAM accounts: Enabled
Network access: Do not allow anonymous enumeration for SAM accounts and sharing: Enabled
Network access: Apply Everyone permissions to anonymous users: Disabled
Account: A local account with blank password can only be used to log onto the console: Enabled

- **Disable default sharing**

“Open” --> ”Run” --> cmd.exe->net share, check sharing
“Open” --> ”Run” -->->regedit->
Find HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters,
create AutoShareServer (REG_DWORD), key value: 0

- **Users that do not require RPC can choose to disable the 135 port**

1. “Open”—>“Run”, enter “dcomcnfg”, click "OK", and open the component service.
2. In the pop-up "Component Service" dialog box, select the “Computers” option.
3. To the right of the “Computers” option, right-click "My Computer", and select "Properties".
4. In the default properties tab of the pop-up "My Computer Properties" dialog box, deselect “Enable distributed COM on this computer”.
5. Select the "Default Protocol" tab, select "Connection-oriented TCP/IP", and click "Delete".
6. Click "OK" to complete setting. After the computer is restarted, the 135 port will be disabled.

- **Disable Netbios-related services (ports 137, 138, 139, etc.)**

1. Control Panel-> Network and Sharing Center->Change Adaptor Settings->Local Connections->Properties->Internet Protocol Version 4->Properties->Advanced->WINS->Disable NetBIOS on TCP/IP
2. Disable printer sharing service (disable port 139)

Chapter 4 Web Container Security Configuration

4.1 Basic requirements

1) Web containers must run with lower privileges

2) Disable some high-risk functions
3) Disable HTTP directory indexing
4) Disable Tomcat and other auxiliary container management functions
5) Do not use weak passwords. Use a random string as the default password
6) Set reasonable directory permissions to prevent unauthorized cross-directory access, such as for the .git/.svn directory
7) Set reasonable error message output, to prevent leaks of sensitive information

4.2 Suggested operations

4.2.1 PHP security configuration

- **Security Mode: Modify php.ini file**

```
safe_mode = on
safe_mode_gid = off
```

- **Disable dangerous functions:**

```
disable_functions=exec,passthru,popen,proc_open,shell_exec,system,phpinfo,assert
# Except in special cases
```

- **Other configurations:**

```
# Disable error message prompts
display_errors = off
display_startup_errors = off
# Disable global variables
register_globals = off
# Do not permit dl calling
enable_dl = off
# Disable remote files
allow_url_fopen = off
allow_url_include = off
# Enable http only
session.cookie_httponly = 1
cookie domain
# Enable https secure
```

```
session.cookie_secure = 1
# Suitable PHP redirects
cgi.force_redirect = 0
# SQL security mode
sql.safe_mode = on
```

4.2.2 Jboss security configuration standard

Disable directory browsing

Modify the web.xml file under deploy\jbossdomain\deploy\jbossweb-tomcat55.sar\conf\ to the following:

```
<init-param>
<param-name>listings</param-name>
<param-value>false</param-value>
</init-param>
```

Set the "param-value" from the default value 'true' to 'false'

Delete dangerous services

- Delete /web-console console for Jboss (web-console has a remote code execution vulnerability):
- Delete root.war in the jboss/server/default/deploy/jbossweb-tomcat55.sar directory
- Delete jboss/server/default/deploy/management/console-mgr.sar/web-console.war
- Delete Jboss' /jmx-console console (jmx-console has a remote code execution vulnerability)
- Delete jboss/server/default/deploy/jmx-console.war and jmx-console.war files in other directories
- Delete jboss/server/default/deploy/jbossws.sar/jbossws-context.war and jbossws-context.war files in other directories
- Delete http-invoker for Jboss (http-invoker has a remote code execution

vulnerability)

- Delete the jboss/server/default/deploy/http-invoker.sar directory

Restrict dangerous services

- Set Jboss' Bootstrap JNP and RMI naming services to only allow local access (they have remote code execution vulnerabilities)
- Modify the content of the jboss-service.xml file in server/default/conf and the jboss-service.xml files in other directories
- Modify Bootstrap JNP (Port 1099) and RMI naming service (1098) to only allow local access

The content should be changed to the following:

```
<mbean code="org.jboss.naming.NamingService"
name="jboss:service=Naming"
xmbean-dd="resource:xmdesc/NamingService-xmbean.xml">
<attribute name="CallByValue">false</attribute>
<attribute name="Port">1099</attribute>
<attribute name="BindAddress">127.0.0.1</attribute>
<attribute name="RmiPort">1098</attribute>
<attribute name="RmiBindAddress">127.0.0.1</attribute>
<depends optional-attribute-name="LookupPool"
  proxy-type="attribute">jboss.system:service=ThreadPool</depends>
<depends optional-attribute-name="Naming"
proxy-type="attribute">jboss:service=NamingBeanImpl</depends>
</mbean>
```

Here, the default value of "BindAddress", "${jboss.bind.address}", is changed to "127.0.0.1"; and the default value of "RmiBindAddress", "${jboss.bind.address}", is changed to "127.0.0.1"

- Set the Jboss' RMI/JRMP invoker service to only allow local access (it has a remote code execution vulnerability)
- Modify the content of the jboss-service.xml file in server/default/conf and the jboss-service.xml files in other directories
- Modify RMI/JRMP invoker (4444) to only allow local access

The content should be changed to the following:

```
<mbean code="org.jboss.invocation.jrmp.server.JRMPInvoker"
name="jboss:service=invoker,type=jrmp">
<attribute name="RMIObjectPort">4444</attribute>
<attribute name="ServerAddress">127.0.0.1</attribute>
<depends>jboss:service=TransactionManager</depends>
</mbean>
```

Here, the default value of "RMIObjectPort", "${jboss.bind.address}", is changed to "127.0.0.1"

4.2.3 Jetty security configuration standard

Disable directory browsing

Modify etc/webdefault.xml

```
<init-param>
<param-name>dirAllowed</param-name>
<param-value>false</param-value>
</init-param>
```

Set the "param-value" from the default value 'true' to 'false'

Exception Page Processing

Modify etc/webdefault.xml. By default, this file does not have this, and the following must be added

```
<error-page>
<error-code>500</error-code>
<location>/</location>
</error-page>
<error-page>
<error-code>501</error-code>
<location>/</location>
</error-page>
<error-page>
<error-code>502</error-code>
```

```
<location>/</location>
</error-page>
<error-page>
<error-code>503</error-code>
<location>/</location>
</error-page>
<error-page>
<error-code>404</error-code>
<location>/</location>
</error-page>
```

Restrict file parsing types

Modify etc/webdefault.xml, only retaining the content for jsp parsing:

```
<servlet-mapping>
<servlet-name>jsp</servlet-name>
<url-pattern>*.jsp</url-pattern>
<url-pattern>*.JSP</url-pattern>
</servlet-mapping>
```

Disable server version display

Change etc/jetty.xml from the default value 'true' to 'false':

```
<Set name="sendServerVersion">false</Set>
```

Disable CGI

- Delete the test.war file in the webapps/ directory
- Delete contexts/test.d. It is Ok to choose not to delete this file and the following one. The program will show an error upon startup, but this will not affect its actual use.
- Delete contexts/test.xml

File Access Control

```
#chmod 755 jetty/etc/*
```

4.2.4 Tomcat security configuration

- Delete Tomcat's admin console software: Delete the admin.xml file in {Tomcat installation directory}\webapps
- Delete Tomcat's Manager console software: Delete the manager.xml file in {Tomcat installation directory}\webapps

4.2.5 Apache configuration

- Ensure that only root users have permission to write to any directory containing scripts or CGI. To do this, you must run the following commands as a root user:

```
chown root <directory_name>
chmod 755 <directory_name>
```

- Other configuration instructions

```
FollowSymLinks
# This command is enabled by default. Therefore, be very careful when creating symbolic links to the webpage server document root directory. # For example, do not provide a symbolic link for “/”.

Indexes
# Although this command is enabled by default, it is not necessary. To prevent visitors from browsing the files on the server,
you must delete this command

UserDir
# Because this command can determine whether or not user accounts exist in the system, the UserDir command must be disabled by default
# To enable username directory browsing on the server, you must use the following command:
UserDir enabled
  UserDir disabled root
# These commands are used for all user directories except for /root/ and can activate the browsing function for these directories
# To add users to the disabled account list, enter the list of users separated by spaces in the UserDir
```

disabled command line

ServerTokens

The ServerTokens command controls server response header information. This information will be returned to clients.

You can use the following parameters to perform custom operations on the different information contained in headers:

ServerTokens Full (Sample output: Apache/2.0.41 (Unix) PHP/4.2.2 MyMod/1.2)

ServerTokens Prod or **ServerTokens ProductOnly** (Sample output: Apache)

ServerTokens Major (Sample output: Apache/2)

ServerTokens Minor (Sample output: Apache/2.0)

ServerTokens Min or **ServerTokens Minimal** (Sample output: Apache/2.0.41)

ServerTokens OS (Sample output: Apache/2.0.41 (Unix))

4.2.6 IIS configuration

- **Delete default IIS site**

Delete c:\Inetpub and other default site directories

- **IIS access permission configuration**

If IIS contains multiple websites, we suggest configuring a different anonymous access account for each site.

1. Create an account and add it to the Guests group

2. “Website Properties”--->“Directory Security”--->“ID Verification and Access Control”, select “Enable anonymous access” and use the account you just created to replace the default account

- Disable unnecessary web service extensions

Open the IIS manager and check for unnecessary web service extensions. If you find any, disable them

- Website directory permission configuration

Principles:

Execution permissions must not be allocated to directories with write permission

Write permissions must not be allocated to directories with execution permission

Website upload directories and database directories usually require write permissions, but should never be allocated execution permissions

Other directories generally should only be allocated read and logging permissions

- **Do not display detailed ASP error messages**

"IIS Manager"--->"Properties"--->"Main Directory"--->"Configuration"--->"Debugging", select the "Send following error messages to clients" option and customize the error messages returned when an error occurs

- **Modify default error page**

"IIS Manager"--->"Properties"--->"Custom Errors", use custom error pages to replace the default page

- Custom IIS Banner information

  Modify the default HTTP header information

"IIS Manager"--->"Properties"--->"HTTP Header", in "Custom HTTP Header", select the default HTTP header information and edit or remove it, or add new HTTP header information

4.2.7 Nginx configuration

- Disable autoindex

```
cat /etc/nginx/nginx.conf
# In the configuration file, disable autoindex, i.e. select autoindex off or do not configure autoindex
```

- **Disable server tokens**

```
cat /etc/nginx/nginx.conf
# Add this configuration line: server_tokens off
```

- **Set cache restrictions**

```
http{
    ... ...
```

```
server{
    ... ...
    client_body_buffer_size  16K;
    client_header_buffer_size  1k;
    client_max_body_size  1m;
    large_client_header_buffers  4  8k;
    ... ...
```

- **Set timeout to defend against some DDoS attacks**

```
http {
    ... ...
    client_body_timeout    10;
    client_header_timeout  30;
    keepalive_timeout     30  30;
    send_timeout           10;
```

4.2.8 vsFTPd configuration

- Change vsftpd login information
  Add the following in the /etc/vsftpd/vsftpd.conf file:

```
ftpd_banner=<insert_greeting_here>
```

- To allow anonymous users to upload files, we suggest generating a write-only directory in /var/ftp/pub/

```
mkdir /var/ftp/pub/upload
```

- Change permissions to prevent anonymous users from viewing the content in this directory:

```
chmod 730 /var/ftp/pub/upload
```