



KISA□□ □□□ 2024 □□□□ □□ □□□ □□

- [1. □ □□□ □□□ □□](#)
- [2. □□□□ □□ □□](#)
- [3. □□ □□ □□](#)
- [4. □□ □□□ □ □□□□ □□](#)
- [5. □□□□ □□□ □□](#)
- [6. □ □□□□ □□ □□](#)
- [7. □□ □□ □□ □□](#)
- [□□ . □□□□ □□ □□](#)

1.

항목설명

Apache 설치 시 httpdocs 디렉터리를 Document로 사용하면 공격에 이용될 수 있는 시스템 관련 정보가 노출될 수 있으므로 default DocumentRoot 경로를 변경하여 사용해야 한다.

진단
기준



양호

default Document를 사용하고 있지 않은 경우



취약

default Document를 사용하고 있는 경우

 

Apache      .

/var/www/html

   Apache    ,  
     .

   DocumentRoot   ,    
DocumentRoot      .



         . ( **FM**  ..)

C     , apache    **D,E,F**   

 

apache    cat   grep  DocumentRoot  

Ubuntu / Debian   /etc/apache2/  

CentOS / RHEL / Fedora   /etc/httpd/   .

我们 Ubuntu 系统 安装 .

```
root@ochid:/etc/apache2/sites-available# ls
000-default.conf  default-ssl.conf
root@ochid:/etc/apache2/sites-available# cat 000-default.conf |grep DocumentRoot
    DocumentRoot /var/www/html
root@ochid:/etc/apache2/sites-available# _
```

/etc/apache2/sites-available/000-default.conf 文件 配置 文件 配置 config 文件 ,

我们 conf 文件 使用 a2ensite 命令 来 安装 文件 .

我们 安装 文件

我们 安装 文件 DocumentRoot 文件 配置 (/var/www/html) 文件 文件

我们 安装 文件 DocumentRoot 文件 配置 文件 文件

我们

2.

항목설명

Apache 웹 서버 설치 시 기본으로 생성되는 매뉴얼 파일은 비인가자에게 시스템 정보 및 웹 서버 정보를 제공할 수 있으므로 제거해야 한다.

진단 기준

양호

매뉴얼 파일 및 디렉터리가 제거되어 있는 경우

취약

매뉴얼 파일 및 디렉터리가 제거되어 있지 않은 경우

, .

,

test , .

□□ □□ □□

□□□□ □□□□ □ □□□ □□□ □□ □□□ □□

□□□□ □□□□ □□□ □□ □□□ □□ □□ □□□ , □□□□ □□□ □□□□ □□ □□□
□□□□ □□ □□ □ □□□

□□

3.

항목설명

심볼릭 링크가 활성화되어 있으면 기존의 웹 문서 이외의 파일 시스템 접근이 가능하기 때문에 편의성을 제공하는 반면 보안적으로 취약하므로 심볼릭 링크 사용을 금지해야 한다.

진단 기준



양호

심볼릭 링크, aliases 사용이 제한되어 있는 경우



취약

심볼릭 링크, aliases 사용이 제한되어 있지 않은 경우

 

        .

    **DocumentRoot**         

      , **/etc/passwd**        .



      

<https://www.ochidstudy.com/books/apache/page/9c838>

 

  **/etc/apache2/apache2.conf**  **FollowSymLinks**  **grep**  

```
root@ochid:/var/www/html# cat /etc/apache2/apache2.conf | grep FollowSymLinks
Options -FollowSymLinks
Options +Indexes -FollowSymLinks
# Options Indexes FollowSymLinks
root@ochid:/var/www/html#
```

□ □ □

FollowSymLinks □ □ □ - □ □ □ □ □

(□ **Indexes** □ □ □ □ □ + □ , □ **Follow** □ □ □ □ □ □ □
□ □ □ □ □ + □ - □ □ □ □)

□ □ □ # □ □ □ □ □ □ □ □ □ □ □ □

FollowSymLink □ - □ □ □ □ □ □ □ □ □

□ □

4.

항목설명

파일 업로드, 다운로드 시에 불필요한 파일 또는 대용량의 파일로 인해 서비스가 불능 상태에 빠질 수 있다. 따라서 가능한 파일 업로드, 다운로드 용량을 제한해야 한다.

진단
기준

 **양호**
파일 업로드 및 다운로드 용량을 제한하고 있는 경우

 **취약**
파일 업로드 및 다운로드 용량을 제한하고 있지 않은 경우

 

 /      ,      /          .



      .        

 **30**   ,          .

 **500**     .

 

apache2.conf  LimitRequestBody  grep 

```
cat /etc/apache2/apache2.conf | grep LimitRequestBody
```

```
root@ochid:/var/www/html# cat /etc/apache2/apache2.conf | grep LimitRequestBody
root@ochid:/var/www/html#
```

□□ □□ □□

□□□ □□ □ □□□ □□□□ □□□□ □□□□ □□

□□ □□ □□□□ □□□ □□ □□

□□□□ □□ □□ □□ □□□ □□□□ □□ □□□□ □□

□□

5.

디렉터리 리스팅 제거

항목설명

디렉터리 검색 기능이 활성화되어 있는 경우 외부에서 디렉터리 내 모든 파일에 접근이 가능하여 WEB 서버 구조를 파악하여 공격을 시도할 수 있으며 백업 파일이나 소스 파일 등 공개되면 안 되는 중요 파일이 노출될 수 있다.

진단
기준

양호

디렉터리 검색 기능을 사용하지 않는 경우



취약

디렉터리 검색 기능을 사용하는 경우

(www.test.com/main.php ☐ ☐ www.test.com/upload/ ☐ ☐)

Index of /uploads

Name	Last modified	Size	Description
 Parent Directory		-	
 data.php	2026-02-19 01:48	0	
 passwd.php	2026-02-19 01:48	0	
 test.php	2026-02-19 01:48	0	

Apache/2.4.52 (Ubuntu) Server at 172.30.1.56 Port 80

이 디렉토리는 현재 비어 있습니다.

apache2 conf Indexes

cat /etc/apache2/apache2.conf | grep Indexes

```
root@ochid:/var/www/html/uploads# cat /etc/apache2/apache2.conf | grep Indexes
Options +Indexes -FollowSymLinks
# Options Indexes FollowSymLinks
root@ochid:/var/www/html/uploads#
```

□□ □□ □□

Indexes □ □ - □□ □□□□ , □□ □□□ □□ □□

Indexes □□ □□□□ □□□□ , □□□ □□ □□□□ □□ □□□□ □ □ □□□□ -
□□□ □□□□ □□

Indexes □ □ - □□ □□□□ □□□ + □□□ □□ □□

□□

6.

항목설명

Unix 시스템에서 apache 서버 데몬이 root 권한으로 운영되는 경우 Web Application 취약점 또는 버퍼 오버플로우로 인하여 root 권한을 획득할 수 있으므로 apache 서버 데몬이 root 권한으로 운영되지 않도록 별도 계정으로 실행해야 한다.

진단 기준



양호

데몬이 root 권한으로 구동되지 않는 경우



취약

데몬이 root 권한으로 구동되는 경우

 

apache   root         , 
  root    

   .

 **www-data**   .

 

   **apache2**    

```
ps -ef | grep apache2
```



      .

```

root@ochid:/var/www/html/uploads# ps -ef |grep apache2
root      2525      1  0 01:45 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  2526     2525  0 01:45 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  2527     2525  0 01:45 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  2528     2525  0 01:45 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  2529     2525  0 01:45 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  2530     2525  0 01:45 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  2533     2525  0 01:48 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  2541     2525  0 01:49 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  2542     2525  0 01:49 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  2543     2525  0 01:49 ?        00:00:00 /usr/sbin/apache2 -k start

```

1. 检查 apache2 是否安装

2. 检查 apache2 是否启动

3. 检查 apache2 是否运行

4. 检查 apache2 是否配置正确

5. 检查 apache2 是否运行

6. 检查 apache2 是否运行

7. 检查 apache2 是否运行

```

# Since there is no sane way to get the parsed apache2 config in scripts, some
# settings are defined via environment variables and then used in apache2ctl,
# /etc/init.d/apache2, /etc/logrotate.d/apache2, etc.
export APACHE_RUN_USER=www-data
export APACHE_RUN_GROUP=www-data

```

8. 检查 apache2 是否运行

9. 检查 apache2 是否运行

7.

항목설명

최신 보안 패치를 적용하지 않으면 해당 버전의 취약점으로 인해 침해사고가 발생할 수 있으므로 주기적으로 공식 릴리즈 사이트를 방문하여 보안 패치를 적용해야 한다.

진단
기준



양호

최신 보안 패치를 적용한 경우



취약

최신 보안 패치를 적용하지 않은 경우

 

       .

EOS           .

 

     

```
apache2 -v
```

EOS   **apache2**  **EOS**  

<https://endoflife.date/>

Apache HTTP Server

APACHE

SERVER-APP

WEB-SERVER

Last updated on 09 December 2025



[Apache HTTP Server](#) is a collaborative software development effort aimed at creating a robust, commercial-grade, feature-rich and freely available source code implementation of an HTTP (Web) server.

Release	Released	Security Support	Latest
2.4	14 years ago (21 Feb 2012)	Yes	2.4.66 (04 Dec 2025)
2.2	20 years ago (01 Dec 2005)	Ended 8 years ago (11 Jul 2017)	2.2.34 (11 Jul 2017)
2.0	23 years ago (05 Apr 2002)	Ended 12 years ago (10 Jul 2013)	2.0.65 (09 Jul 2013)
1.3	27 years ago (01 Jun 1998)	Ended 16 years ago (03 Feb 2010)	1.3.42 (02 Feb 2010)

📄 📄 📄

```
root@ochid:/etc/apache2# apache2 -v
Server version: Apache/2.4.52 (Ubuntu)
Server built: 2025-12-09T15:50:28
root@ochid:/etc/apache2#
```

apache📄 📄 📄 (Security Support)📄 📄 📄 📄

2.4📄 52📄 📄 📄 📄 .📄 2.4, 2.2📄 📄 📄 📄 📄 📄 📄 📄

📄

www.localhost

www

www.localhost, www.localhost Not Found

← → ↻ ⚠ 주의 요함 172.30.1.56/test

Not Found

The requested URL was not found on this server.

Apache/2.4.52 (Ubuntu) Server at 172.30.1.56 Port 80

www.localhost Apache

www

www.localhost ;
www.localhost ..?

www

apache2/conf-available security.conf

```
root@ochid:/etc/apache2/conf-available# pwd
/etc/apache2/conf-available
root@ochid:/etc/apache2/conf-available# ls -la security.conf
-rw-r--r-- 1 root root 2174 Feb 19 02:33 security.conf
root@ochid:/etc/apache2/conf-available#
```

ServerToken OS ()

ServerToken Prod ()

ServerSignature On ()

ServerSignature Off ()

100% 100%

Not Found

The requested URL was not found on this server.

100% 100% 100% 100% , 401, 403, 404 100% 100% 100% 100%
 100% 100% 100% 100%
 100% 100% 100% 100% 100% 100% .