Company Name, Inc. Project name

보안대책-WEB
보안가이드라인

openmaru

2017-04-19

오픈나루

Table of Contents

1. 개요

1.1 목적

본 문서는 'KISA 의 취약점 분석 · 평가 모델, CSI 의 IPAK 등 국내/외 위험분석 모델'에 의거한 점검 항목 및 보안 대책을 다루고 있으며, 정보 시스템 담당자의 취약점 이해 및 취약점 조치를 위한 보안 가이드를 제시하고자 한다.

주의사항
본 보안가이드 라인에서 제시하는 취약점 조치 방안은 일반적인 기술적 해결방안을 명시하고 있으며, 해당 OS·장비별 특성 등을 모두 반영하지 못한 실정입니다.

따라서,
취약점 조치 전 OS 벤더사, 담당운영자, APP 담당자 등과 사전 협의 후 조치하시기 바랍니다.

1.2 WEB 점검 항목

본 가이드 라인은 총 28 개 취약점 점검항목을 기준으로 하여 Apache WEB 응용 프로그램에 대한 조치 방안을 제시하고 있다.

진단항목	Apache
WB-01. 데몬 관리	●
WB-02. 디렉토리 쓰기 권한 관리	●
WB-03. 소스/설정파일 권한 관리	●
WB-04. 디렉토리 검색 기능 제거	●
WB-05. 로깅 디렉토리/파일 권한 관리	●
WB-06. 에러 메시지 관리	●
WB-07. 응답 메시지 관리	●
WB-08. HTTP Method 제한	●
WB-09. 스크립트 실행 제거	N/A
WB-10. 상위 패스 기능 제거	●
WB-11. 불필요한 FTP 서비스 제거	N/A

WB-12. 불필요한 SMTP 서비스 제거	N/A
WB-13. 불필요한 NNIP 서비스 제거	N/A
WB-14. CGI 스크립트 실행 제한	●
WB-15. 링크 사용금지	●
WB-16. 파일 업로드 및 다운로드 제한	●
WB-17. Exec 명령어 쉘 호출진단	N/A
WB-18. WebDAV 비활성화	N/A
WB-19. Manual/Sample 디렉토리 삭제	●
WB-20. 숨겨진 디렉토리/파일 삭제	N/A
WB-21. ISAPI DLL 보한 취약점 삭제	N/A
WB-22. DB 연결	N/A
WB-23. 가상 디렉토리 삭제	N/A
WB-24. 데이터 파일 ACL 적용	N/A
WB-25. CGI 및 Scripts 디렉토리 사용권한 설정	N/A
WB-26. 웹 서비스 영역의 분리	●
WB-27. Open SSL 취약 버전 점검	●
WB-28. 최신 패치 적용	●

2. WEB 보안 가이드 라인

2.1 설정

WB-01. 데몬 관리

▶ 개요

- **취약점 설명**
  Unix 시스템의 경우, Web 서버 데몬이 root 권한으로 운영될 경우 Web Application 의 취약점이나 Buffer Overflow 시 공격자에게 root 권한을 획득할 수 있으므로 서버 데몬이 root 권한으로 운영되지 않도록 관리해야 함
- **위험도 : 상**
- **점검기준**
  - 양호 : 구동 데몬의 계정이 root 권한이 아닐 경우
  - 취약 : 구동 데몬의 계정이 root 권한일 경우

- **영향도**
  - 80 포트를 사용할 경우 root 로 기동 하지만 실제 프로세스는 로그인 불가능한 계정으로 보이게 설정한다면 서비스 영향 없음
  - 1024 이상의 포트는 전용 계정을 생성해서 기동한다면 서비스 영향 없음
- **비고**
  - 취약점 조치 시 WEB 운영자 담당자와 협의하여 영향도 검토 후 **<u>중기 적용 필요</u>**

▶ **대상 S/W**

APACHE
●

▶ **조치 방안**

- **APACHE**

■ **확인방법**

- Apache 데몬을 root 로 기동할 경우, 실제 프로세스는 root 가 아닌 다른 계정으로 보이는지 확인

■ **조치방법**

- 데몬 User / Group 변경
- 로그인 불가능하도록 설정 : /bin/false

예) nobody 계정이 로그인 하지 못하도록 설정

```
# vi /etc/passwd
  Nobody:x:65534:1001:nobody:/nonexistent:/bin/false
```

WB-02. 디렉토리 쓰기 권한 관리

▶ **개요**

- **취약점 설명**
  일반 사용자가 웹서버 홈 디렉토리에 임의의 파일을 생성, 삭제, 변경할 수 있으면, 홈페이지의 변조, 파일의 삭제 등의 피해가 발생할 수도 있음
- **위험도 : 하**
- **점검기준**

- 양호 : 웹 서버 홈 디렉토리에 일반사용자의 쓰기 권한이 없을 경우
- 취약 : 웹 서버 홈 디렉토리에 일반사용자의 쓰기 권한이 있을 경우

- **영향도**
  - 실행 계정만 해당 디렉토리에 접근 가능하다면 서비스에 영향 없음
- **비고**
  - 취약점 조치 시 WEB 운영자 담당자와 협의하여 영향도 검토 후 **중기 적용 필요**

▶ **대상 S/W**

APACHE
●

▶ **조치 방안**

- **APACHE**

■ **확인방법**

- /[Apache_home]/conf/httpd.conf 에서 관리서버 / 웹 소스 디렉토리 확인

```
#
ServerRoot "/sw/report1/jboss-ews/jbcs-httpd24-2.4/httpd"
```

관리 서버 위치

```
DocumentRoot "/apps/jboss-ews/htdocs/daps"
```

웹 소스 위치

■ **조치방법**

- 관리 서버 홈 디렉토리

< Unix 환경 >

전용 Web Server 계정 소유, 755(rwxr-xr-x) 이하 권한

- 웹 소스 디렉토리

<Unix 환경 >

전용 Web Server 계정 소유, 755(rwxr-xr-x) 권한

※ 파일 업로드 폴더 쓰기 권한 부여

WB-03. 소스 및 설정파일 권한 관리

▶ 개요

- **취약점 설명**
  일반 사용자가 웹 사이트 소스 및 설정 파일을 삭제, 변경할 수 있으면 홈페이지 변조, 작업 실수로 인한 파일 삭제, 백도어 삽입 등의 피해가 발생할 수 있음
  이로 인해 시스템이 오작동하여 사용 불능 상태에 빠질 우려가 있음
- **위험도 : 중**
- **점검기준**
  - 양호 : 소스 파일 권한이 644(rw-r—r--) 및 설정 파일 권한이 600(rw-------)으로 설정되어 있을 경우
  - 취약 : 소스 파일 권한이 644(rw-r—r--) 및 설정 파일 권한이 600(rw-------)으로 설정되어 있지 않을 경우

  영향도
  - 소스 및 설정 파일은 실행 계정만 접근 가능하다면 서비스에 영향 없음
- **비고**
  - 취약점 조치 시 WEB 운영자 담당자와 협의하여 영향도 검토 후 **<u>중기 적용 필요</u>**

▶ 대상 S/W

APACHE
●

▶ 조치 방안

- **APACHE**

  ■ **확인방법**
  - 소스 코드 파일 경로
    /[Apache_home]/[웹 소스 디렉토리]/*
    웹 소스 디렉토리는 [1,2 디렉토리 쓰기 권한 관리]에서 확인
  - 설정 파일 경로
    /[Apache_home]/conf/* (Apache 1.x 버전 ~ 2.1.x 버전)
    /[Apache_home]/docs/conf/* (Apache2.2.x 버전)

    주 설정 파일은 httpd.conf 이지만 모든 설정 파일에 대한 권한 설정이 필요
    /[Apache_home]/conf/ 폴더 이하 모든 파일

httpd.conf , httpd-std.conf , highperformance.conf , higherperformance-std.conf , magic,mime.typem ssl-std.conf, ssl.conf 등

■ **조치방법**

- 소스 파일 권한 점검

< Unix 환경 >

전용 Web Server 계정 소유이고, 644(rw-r—r--) 이하 권한

- 설정 파일 권한 점검

<Unix 환경 >

전용 Web Server 계정 소유, 600(rw------) 권한

※ Apache 2.2.x 버전에서는 설정 파일이 /[Apache-home]/docs/conf 및 /[Apache_home]/docs/conf/extra 이므로 extra 이하의 파일도 동일한 권한 설정 권고함

WB-04. 디렉토리 검색 기능 제거

▶ **개요**

- **취약점 설명**
  디렉토리 검색 기능이 활성화 되어 있으면 해당 디렉토리에 존재하는 모든 파일 리스트를 보여주어 Web 서버 구조 노출 및 주요 설정 파일의 내용이 유출될 가능성이 있음
- **위험도 : 상**
- **점검기준**
  - 양호 : 디렉토리 검색 기능이 제거 되어 있는 경우
  - 취약 : 디렉토리 검색 기능이 제거 되어 있지 않은 경우

  영향도
  - 일반적인 경우 서비스에 영향 없음
- **비고**
  - 취약점 조치 시 WEB 운영자 담당자와 협의하여 영향도 검토 후 **단기 적용 필요**

▶ **대상 S/W**

APACHE

●

▶ 조치 방안

- **APACHE**

■ **확인방법**

- httpd.conf 파일에서 설정된 모든 디렉토리에 Indexes 옵션이 삭제되어 있거나, IncludesNoExec 옵션 또는 –Indexes 옵션이면 양호

/[Apache_home]/conf/httpd.conf 에서 확인

```
<Directory "/sw/report1/jboss-ews/jbcs-httpd24-2.4/httpd/www/error">
    AllowOverride None
    Options -FollowSymLinks -Indexes +IncludesNoExec
    AddOutputFilter Includes html
    AddHandler type-map var
    Order allow,deny
    Allow from all
    LanguagePriority en es de fr
    ForceLanguagePriority Prefer Fallback
</Directory>
```

■ **조치방법**

- /[Apache_home]/conf/httpd.conf 파일에 설정된 모든 디렉토리 별로 Options 항목에서 Indexes 를 제거하거나, "IncludesNoExec" 옵션 또는 -Indexes 옵션으로 설정

예) Options –FollowSymLinks 또는 Options –Indexes –FollowSymLinks 또는 Options IncludesNoExec -FollowSymLinks

WB-05. 로깅 디렉토리 및 권한 관리

▶ 개요

- **취약점 설명**
  로그 파일에는 공격자에게 유용한 정보가 들어있을 수 있으므로 권한 관리가 필요함
  일반 사용자에 의한 정보 유출이 불가능하도록 권한 설정 필요함
- **위험도 : 상**
- **점검기준**
  - 양호 : 로깅 디렉토리 및 파일 권한이 설정되어 있는 경우
  - 취약 : 로깅 디렉토리 및 파일 권한이 설정되어 있지 않은 경우
- **영향도**

- 타 계정에서 로그 디렉토리 및 로그 파일을 접근해야 하는지 확인 후 적용 필요

- **비고**
  - 취약점 조치 시 WEB 운영자 담당자와 협의하여 영향도 검토 후 **단기 적용 필요**

▶ **대상 S/W**

APACHE
●

▶ **조치 방안**

- **APACHE**

■ **확인 /조치 방법**

- 로그 디렉토리 및 파일 권한 강화

일반 사용자에 의한 정보 유출이 불가능 하도록 권한 설정을 강화

<Unix 환경 >

디렉토리

전용 Web Server 계정 소유이고, 740(drwxr-----) 이하 권한

로그파일

전용 Web Server 계정 소유이고, 640(rw-r-----) 이하 권한

※ logs 폴더의 권한 설정 시 하위의 폴더도 동일한 설정이 적용될 수 있도록 설정 바람

WB-06. 에러 메시지 관리

▶ **개요**

- **취약점 설명**
  웹 서버에서 제공하는 default 에러 메시지가 출력되도록 설정되어 있는 경우, 공격자가 대상 시스템의 정보를 획득하기 위해 고의적으로 다양한 에러를 유발하여 발생되는 에러 메시지를 통해 웹 프로그램의 구조 및 환경 설정을 추정할 수 있음
- **위험도 : 상**
- **점검기준**

- 양호 : 별도의 에러 메시지를 생성하여 관리 할 경우
- 취약 : 별도의 에러 메시지를 생성하여 관리를 하지 않을 경우

- **영향도**
  - 일반적인 경우 서비스에 영향 없음
- **비고**
  - 취약점 조치 시 WEB 운영자 담당자와 협의하여 영향도 검토 후 **<u>중기 적용 필요</u>**

▶ 대상 S/W

APACHE
●

▶ 조치 방안

- **APACHE**

■ 확인방법

- 사용자 브라우저로 에러 메시지 반환 여부

- httpd.conf 파일에서 에러 메시지 설정이 Default 나 주석 처리 된 것이 아니라, 시스템의 정보를 노출하지 않는 별도의 에러 메시지로 연결되어 있으면 양호
모든 에러코드에 대하여 별도의 페이지 설정(필수항목 : 400,401,403,404,500)

■ 조치방법

- httpd.conf 파일에서 모든 에러 코드에 대하여 별도의 에러 메시지 설정
/[apache_home]/conf/httpd.conf 파일에서 ErrorDocument [에러코드][사용자정의 에러 페이지] 형식으로 Error Handling 설정함
Ex) ErrorDocument 400 /errmsg/err-400.html

- 별도의 에러 페이지를 작성

- 에러 페이지 파일의 권한은 644(-rw-r—r--)이하로 설정

WB-07. 응답 메시지 관리

▶ 개요

- **취약점 설명**
  공격자가 대상 시스템의 정보를 획득하기 위해 고의적으로 웹 서버 헤더 정보를 유출할 수 있음
  HTTP Header 를 통해 웹 서버의 정보를 유추할 수 있음
- **위험도 : 하**
- **점검기준**
  - 양호 : 응답 메시지 헤더 정보를 숨겼을 경우
  - 취약 : 응답 메시지 헤더 정보를 노출했을 경우
- **영향도**
  - 일반적인 경우 서비스에 영향 없음
- **비고**
  - 취약점 조치 시 WEB 운영자 담당자와 협의하여 영향도 검토 후 **<u>중기 적용 필요</u>**

▶ 대상 S/W

APACHE
●

▶ 조치 방안

- **APACHE**

■ 확인방법

- httpd.conf 파일에서 ServerTokens 설정 확인

/[apache_home]/conf/httpd.conf 파일에서 ServerTokens 설정이 Prod 로 설정되어 있는지 확인

```
#
# The directives in this section affect the overall operation of Apache,
# such as the number of concurrent requests it can handle or where it
# can find its configuration files.
#

#
# Don't give away too much information about all the subcomponents
# we are running.  Comment out this line if you don't mind remote sites
# finding out what major optional modules you are running
ServerTokens Prod
```

■ 조치방법

- httpd.conf 파일에서 ServerTokens 를 설정하여 헤더에 의해 전송되는 정보를 제한할 수 있음
  ServerTokens 의 설정 값이 "Min /OS / Full" 일 경우 "Prod" 설정 권고
  Ex) ServerTokens Prod
※ 일반적으로 ServerTokens 은 httpd.conf 에 명시되어 있지 않는 경우가 많은데, 이럴 경우에는 기본값인 ServerTokens Full 이 적용되어 모든 정보가 서버의 응답 헤더에 포함되어 클라이언트에게 전송 되므로 꼭 설정을 해주어야 함

WB-08. HTTP Method 제한

▶ 개요

- **취약점 설명**
  OPTIONS, GET, POST 이외의 다른 HTTPD Method 를 지원하는 경우, 악의적인 공격자가 임의의 파일을 삭제하거나 업로드 하여 서버의 정상 운영에 지장을 줄 수 있음
- **위험도 : 중**
- **점검기준**
  - 양호 : OPTIONS, GET, POST 이외의 다른 HTTP Method 가 설정되어 있지 않은 경우
  - 취약 : OPTIONS, GET, POST 이외의 다른 HTTP Method 가 설정되어 있는 경우
- **영향도**
  - 운영상 지원되어야 하는 Method 가 있다면 확인 후 적용 필요
- **비고**
  - 취약점 조치 시 WEB 운영자 담당자와 협의하여 영향도 검토 후 **중기 적용 필요**

▶ 대상 S/W

APACHE
●

▶ 조치 방안

- **APACHE**

■ 확인방법
- OPTIONS 메서드를 이용한 점검 수행하여 불필요한 메서드가 설정되어 있는지 확인

telnet [웹사이트 URL 또는 IP][사용포트 – 일반적으로는 80](엔터)
telnet> OPTIONS * HTTP/1.0(엔터 2 번)

- httpd.conf 파일 /[apache_home]/conf/httpd.conf 에서 확인

■ 조치방법

- HTTP Method 를 일부 항목으로 제한

Apache 웹 서버는 GET, POST, PUT, DELETE, CONNECT, OPTIONS, PATCH, PROPFIND, PROPPATCH, MKCOL, COPY, MOVE, LOCK, UNLOCK 등의 다양한 Method 를 지원함
이 Method 들은 WebDAV 나 telnet 을 이용해 해당 Method 를 요청하는 경우 서버에 임의의 파일을 생성하거나, 삭제 할 수 있음

- httpd.conf 파일에서 사용 가능한 Method 를 아래와 같이 조치 권고

```
<Directory    /home>
      AllowOverride FileInfo AutoConfig Limit
      Options MultiViews Indexes   SymLinksIfOwnerMatch IncludesNoExec
      <Limit OPTIONS PROPFIND>
        Order allow,deny
        Allow from all
      </Limit>
      <LimitExcept GET POST>
         Order deny,allow
         Deny from all
       </LimitExcept>
</Directory>
```

※ 위와 같이 설정하면 정상적으로 Apache 웹 서버에 로그인 권한을 가진 사용자 외의 사용자는 제한된 Method 인 PUT DELETE COPY MOVE PATCH MKCOL Method 를 사용할 수 없음

WB-10. 상위 패스 기능 제거

▶ 개요

- **취약점 설명**
  상위패스로 이동하는 것이 가능할 때 하위 경로에 접속하여 상위로 이동함으로써 해킹을 당할 위험이 있으며 , Unicode 버그 및 서비스 거부 공격에 이용당하기 쉬우므로 되도록 "../" 와 같은 상위 경로를 사용하지 못하도록 설정하는 것이 바람직함
  "../"는 Unicode 버그, 서비스 거부와 같은 공격에 쉽게 이용되므로 허용하지 않는 것을 권장함

- **위험도 : 중**
- **점검기준**
  - 양호 : 상위 디렉토리에 이동제한을 설정한 경우
    Apache : AllowOverride 지시자에 AutoConfig 옵션이 설정 되어 있을 경우
    IIS : "상위 경로 사용" 옵션이 체크 등 되어 있지 않을 경우
  - 취약 : 상위 디렉토리에 이동제한을 설정하고 있지 않을 경우
  ※ 조치시 마스터 속성과 모든 사이트에 적용을 해야함
- **영향도**
  - 어플리케이션에서 "../"와 같이 상대경로를 사용하도록 Coding 되어 있을 경우 영향 있음
- **비고**
  - 취약점 조치 시 WEB 운영자 담당자와 협의하여 영향도 검토 후 **단기 적용 필요**

▶ 대상 S/W

APACHE
●

▶ 조치 방안

- **APACHE**

■ 확인방법

- vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일을 연 후
  # vi /[Apache_home]/conf/httpd.conf
- AllowOverride 지시자에 AutoConfig 옵션 설정 여부 확인

■ 조치방법

- vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일을 연 후
  #vi /[Apache_home]/conf/httpd.conf

- 설정된 모든 디렉터리의 AllowOverride 지시자에서 AutoConfig 옵션 설정

(수정 전) AllowOverride 지시자에 None 옵션이 설정되어 있음

```
<Directory    /home>
        AllowOverride None
        Allow from all
</Directory>
```

(수정 후) AllowOverride 지시자에 AutoConfig 옵션이 설정되어 있음

```
<Directory    "/usr/local/apache2/htdocs">
        AllowOverride AutoConfig
        Allow from all
</Directory>
```

- 사용자 인증을 설정할 디렉터리에 .htaccess 파일 생성(아래 내용 삽입)

```
AutoName "디렉터리 사용자 인증"
AutoType Basic
AutoUserFile /usr/local/apache/test/.auth
Require valid-user
```

지시자	설명
AutoName	인증 영역 (웹 브라우저의 인증 창에 표시되는 문구)
AutoType	인증 형태 (Basic 또는, Digest)
AutoUserFile	사용자 정보(아이디 및 패스워드) 저장 파일 위치
AutoGroupFile	그룹 파일의 위치 (옵션)
Require	접근을 허용할 사용자 또는, 그룹 정의

- 사용자 인증에 사용할 아이디 및 패스워드 생성

```
#htpasswd –c /usr/local/apache/test/.auto test
New password:
Re-type new password:
Adding password for user test
[root@localhost apache]#
```

- 변경된 설정 내용을 적용하기 위하여 Apache 데몬 재시작

WB-14. CGI 스크립트 실행 제한

▶ **개요**

- **취약점 설명**
  CGI 스크립트는 정해진 디렉토리에서만 실행 되도록 해야 함
  게시판이나 자료실과 같이 업로드 된 파일이 저장되는 디렉토리에 CGI 스크립트가 실행 가능하다면 악의적인 파일을 업로드하고 이를 실행하여 시스템의 중요 정보가 노출 될 수 있으며 침해사고의 통로를 이용 될 수 있음

- **위험도 : 중**
- **점검기준**
  - 양호 : ScriptAlias 에 지정된 디렉토리가 게시판이나 업로드 디렉토리가 아닌 경우

  - 취약 : ScriptAlias 에 지정된 디렉토리가 게시판이나 업로드 디렉토리인 경우
- **영향도**
  - 게시판이나 업로드 디렉토리 일 경우 조치시 검증이 필요함
- **비고**
  - 취약점 조치 시 WEB 운영자 담당자와 협의하여 영향도 검토 후 **증기 적용 필요**

▶ **대상 S/W**

APACHE
●

▶ **조치 방안**

- **APACHE**

  ■ **확인방법**

  - 환경 설정 파일의 ScriptAlias 지시자 또는 Options 지시자 확인

  ■ **조치방법**

- 특정 디렉터리에 있는 CGI 스크립트 파일만 실행되도록 설정하는 방법은 ScriptAlias 지시자를 설정하거나 Options 지시자에 ExecCGI 를 설정하는것이며, 파일이 업로드 되는 자료실이나 게시판 등에 스크립트가 실행 가능하도록 설정되어 있으면 이를 제거함

- ScriptAlias 지시자 설정
ScriptAlias 는 지정된 디렉터리에 저장된 모든 파일들을 CGI 스크립트로 간주하여 실행되도록 함
<httpd.conf>
ScriptAlias /cgi-bin/ "/export/home/httpd/cgi-bin/"

WB-15. 링크 사용금지

▶ 개요

- **취약점 설명**
일부 서버는 심볼릭 링크(Symbolic link)를 이용하여 기존의 웹 문서 이외의 파일시스템 접근이 가능하도록 하고 있음
이러한 방법은 편의성을 제공하는 반면, 일반 사용자들도 시스템 중요 파일에 접근할 수 있게 하는 보안 문제를 발생시킴
가령 시스템 자체의 root 디렉터리(/)에 링크를 걸게 되면 웹 서버 구동 사용자 권한으로 모든 파일 시스템의 파일에 접근할 수 있게 되어 "/etc/passwd" 파일과 같은 민감한 파일을 누구도 열람할 수 있게 됨
- **위험도 : 상**
- **점검기준**
- 양호 : 심볼릭 링크, aliases 사용을 제한한 경우

- 취약 : 심볼릭 링크, aliases 사용을 제한하지 않은 경우
- **영향도**
- 게시판이나 업로드 디렉토리 일 경우 조치시 검증이 필요함
- **비고**
- 일반적인 경우 서비스 영향 없으나 취약점 조치 시 어플리케이션 운영 담당자와 협의하여 영향도 검토 후 **단기 적용 필요**

▶ 대상 S/W

APACHE
●

▶ **조치 방안**

- **APACHE**

■ 확인방법

- vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일을 연 후
  # vi /[Apache_home]/conf/httpd.conf
- Options 지시자에 FollowSymLinks 옵션 확인

■ 조치방법

- vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일을 연 후
  #vi /[Apache_home]/conf/httpd.conf

- 설정된 모든 디렉터리의 Options 지시자에서 FollowSymLinks 옵션 제거
  (수정 전) Options 지시자에 FollowSymLinks 옵션이 설정되어 있음

```
<Directory />
Options Indexes FollowSymLinks
AllowOverride None
Order allow, deny
Allow from all
</Directory>
```

(수정 후) Options 지시자에 FollowSymLinks 옵션 제거 후 저장

```
<Directory />
Options Indexes
AllowOverride None
Order allow, deny
Allow from all
</Directory>
```

WB-16. 파일 업로드 및 다운로드 제한

▶ 개요

- **취약점 설명**
  불필요한 파일 업로드, 다운로드 시에 대량의 업로드, 다운로드로 인한 서비스 불능상태가 발생할 수 있음
  따라서 불필요한 업로드와 다운로드는 허용하지 않으며, 웹 서버에 의해 처리되지 못하게 하고, 자동이나 수동으로 파일의 보안성 검토를 수행함
- **위험도 : 상**
- **점검기준**
  - 양호 : 파일 업로드 및 다운로드를 제한한 경우

  - 취약 : 파일 업로드 및 다운로드를 제한하지 않은 경우
- **영향도**
  - 일반적인 경우 서비스 영향 없으나 취약점 조치 시 어플리케이션 운영 담당자와 협의하여 영향도 검토 후 **단기 적용 필요**

▶ 대상 S/W

APACHE
●

▶ 조치 방안

- **APACHE**

■ 조치방법

- vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일을 연 후
  #vi /[Apache_home]/conf/httpd.conf

- 설정된 모든 디렉터리의 LimitRequestBody 지시자에서 파일 사이즈 용량 제한 설정

```
<Directory />
LimitRequestBody 5000000(※ "/" 는 모든 파일 사이즈를 5M 로 제한하는 설정)
</Directory>
```

2.2 솔루션 취약점

WB-19. Manual/Sample 디렉토리 삭제

▶ **개요**

- **취약점 설명**
  Sample/Manual 디렉토리 자체에는 취약점이 없으나 불필요하므로 삭제 권고함
  불필요한 파일을 통해 공격 루트가 제공될 수 있음
- **위험도 : 하**
- **점검기준**
  - 양호 : Manual/Sample 가 존재하지 않을 경우
  - 취약 : Manual/Sample 가 존재하는 경우
- **영향도**
  - 일반적인 경우 서비스에 영향 없음
- **비고**
  - 취약점 조치 시 어플리케이션 운영자 담당자와 협의하여 영향도 검토 후 **단기적용 필요**

▶ **대상 S/W**

APACHE
●

▶ **조치 방안**

- **APACHE**

■ **확인 방법**

- 사용자 브라우저에서 접속 가능여부 확인(접속 불가능해야 함)
  http://[Domain]/manual

■ **조치 방법**

- Manual 디렉토리 삭제
  /[apache_home]/manual/

- /[apache_home]/conf/httpd.conf 에서 매뉴얼에 관한 부분 삭제(주석처리 권고함)

```
#AliasMatch ^/manual ( ? : / ( ? : de | en | es | fr | ja | ko |
 ru))?(/.*)?$ "/usr/local/httpd/manual$1"

#<Directory "/usr/local/httpd/manual">
#       Options Indexes
#       AllowOverride None
#       Order allow,deny
#       Allow from all
#
#      <Files *.html>
#       SetHandler type-map
#      </Files>
#
#      SetEnvIf Requst_URI ^/manual /(de | en | es | fr | ja | ko | ru ) / prefer –
#      langage=$1
#      RedirectMatch 301 ^/manual( ? : /(de | en | es | fr | ja | ko | ru ))
#      { 2, }( / .*) /manual /$1$2
#</Directory>
```

WB-26. 웹 서비스 영역의 분리

▶ 개요

- **취약점 설명**
  Apache 설치 시 htdocs 디렉터리를 DOcumentRoot 로 사용하고 있는데 htdocs 디렉터리는 공개되어서는 안 될(또는, 공개될 필요가 없는) Apache 문서뿐만 아니라 공격에 이용될 수 있는 시스템 관련 정보도 포함하고 있으므로 이를 변경하여야 함
  또한, 대량의 업로드와 다운로드 시 서비스 불능 상태가 발생할 수 있음
- **위험도 : 상**
- **점검기준**
  - 양호 : DocumentRoot 를 별도의 디렉터리로 지정한 경우
  - 취약 : DocumentRoot 를 기본 디렉터리로 지정한 경우
- **영향도**
  - 일반적인 경우 서비스에 영향 없으나 취약점 조치 시 어플리케이션 운영 담당자와 협의하여 영향도 검토 후 **단기적용 필요**

▶ 대상 S/W

APACHE
●

▶ 조치 방안

- **APACHE**

■ **확인 / 조치 방법**

- DocumentRoot "/usr/local/apache/htdocs"-> DocumentRoot "별도 디렉터리" 로 변경

- vi 편집기를 이용하여 /[Apache_home]/conf/httpd.conf 파일을 연 후
  #vi /[Apache_home]/conf/httpd.conf
- DocumentRoot 설정 부분에 "/usr/local/apache/htdocs" 가 아닌 별도의 디렉터리로 변경
  DocumentRoot "디렉터리"

2.3 보안 패치

WB-27. Open SSL 취약 버전 점검

▶ 개요

- **취약점 설명**
  취약한 OpenSSL 버전을 사용하는 경우 서버와 클라이언트 사이에서 공격자가 암호화된 데이터를 복호화 할 수 있는 취약점, 임의코드 실행 취약점 등으로 인해 외부 공격에 노출 될 수 있음
- **위험도 : 상**
- **점검기준**
  - 양호 : 다음의 취약점이 존재하는 SSL 버전을 사용하지 않을 경우

취약점이 존재하는 버전	취약점을 보완한 버전
OpenSSL 0.9.8 대 버전	OpenSSL 0.9.8za
OpenSSL 1.0.0 대 버전	OpenSSL 1.0.0m
OpenSSL 1.0.1 대 버전	OpenSSL 1.0.1h

- 취약 : 취약점이 존재하는 SSL 버전을 사용하는 경우

- **영향도**
  - 버전 업데이트 시 어플리케이션에 영향이 있을 수 있으므로 , 취약점 조치 시 어플리케이션 운영 담당자와 협의하여 충분한 영향도 검토 후 **중기적용 필요**

▶ **대상 S/W**

APACHE
●

▶ **조치 방안**

- **APACHE**

■ **확인 방법**

- 운용 중인 OpenSSL 버전을 확인을 통해 취약점이 존재하는 버전인지 확인

```
# openssl  version –a
OpenSSL 1.0.1e-fips 11 Feb 2013
```

■ **조치 방법**

- 취약점을 보완한 OpenSSL 패키지를 다음의 사이트에서 다운받아 설치하여야 하나, OpenSSL 버전 변경으로 어플리케이션에 영향이 있을 수 있으므로, 어플리케이션 담당자와 협의하여 영향도 평가 후 적용해야 함

OpenSSL 패키지 다운 URL : www.openssl.org/source/

※ **OpenSSL 취약점**

CVE 코드	취약점 설명

	CVE-2014-0224	조작된 핸드셰이크 전송을 통한 중간자(MITM) 공격으로 전송 데이터를 복호화 하고 서버/클라이언트 간 전송 데이터의 조작이 가능한 취약점
	CVE-2014-0221	비정상적인 DTLS 핸드 쉐이크를 OpenSSL DTLS 클라이언트에 전송하여 서비스 거부 공격이 가능한 취약점
	CVE-2014-0195	비정상적인 DRLS 프래그먼크를 OpenSSL DTLS 클라이언트 또는 서버에 전송하여 임의코드 실행이 가능한 취약점
	CVE-2014-0198	do_ssl3_write 함수의 결함으로 인해 임의코드 실행이 가능한 취약점
	CVE-2014-3470	Anonuymous ECDH ciphersuites 가 활성화된 OpenSSL TLS 클라이언트에 서비스 거부 공격이 발생할 수 있는 취약점

WB-28. 최신 패치 적용

▶ 개요

- **취약점 설명**
  주기적으로 보안 패치를 적용하지 않으면 서버 침해가 발생할 수 있음
- **위험도 : 상**
- **점검기준**
  - 양호 : 최신 보안패치가 적용 되어 있을 경우
  - 취약 : 최신 보안패치가 적용 되어 있지 않을 경우
- **영향도**
  - 서비스 벤더를 통해 안정화된 버전을 문의하여 적용 할 필요 있음
- **비고**
  - 취약점 조치 시 WEB 운영자 담당자와 협의하여 영향도 검토 후 **단기 적용 필요**

▶ 대상 S/W

APACHE
●

▶ **조치 방안**

- **APACHE**

■ 확인 방법

- Apache 버전 확인

/[apache_home]/bin/httpd –v 로 확인

Apache 최신 Release 현황(최신 확인날짜 : 2014 년 6 월)

Apache httpd 2.4.9, Apache httpd 2.2.27, Apache httpd 2.0.65

※ 참고 사이트 : http://www.apache.org

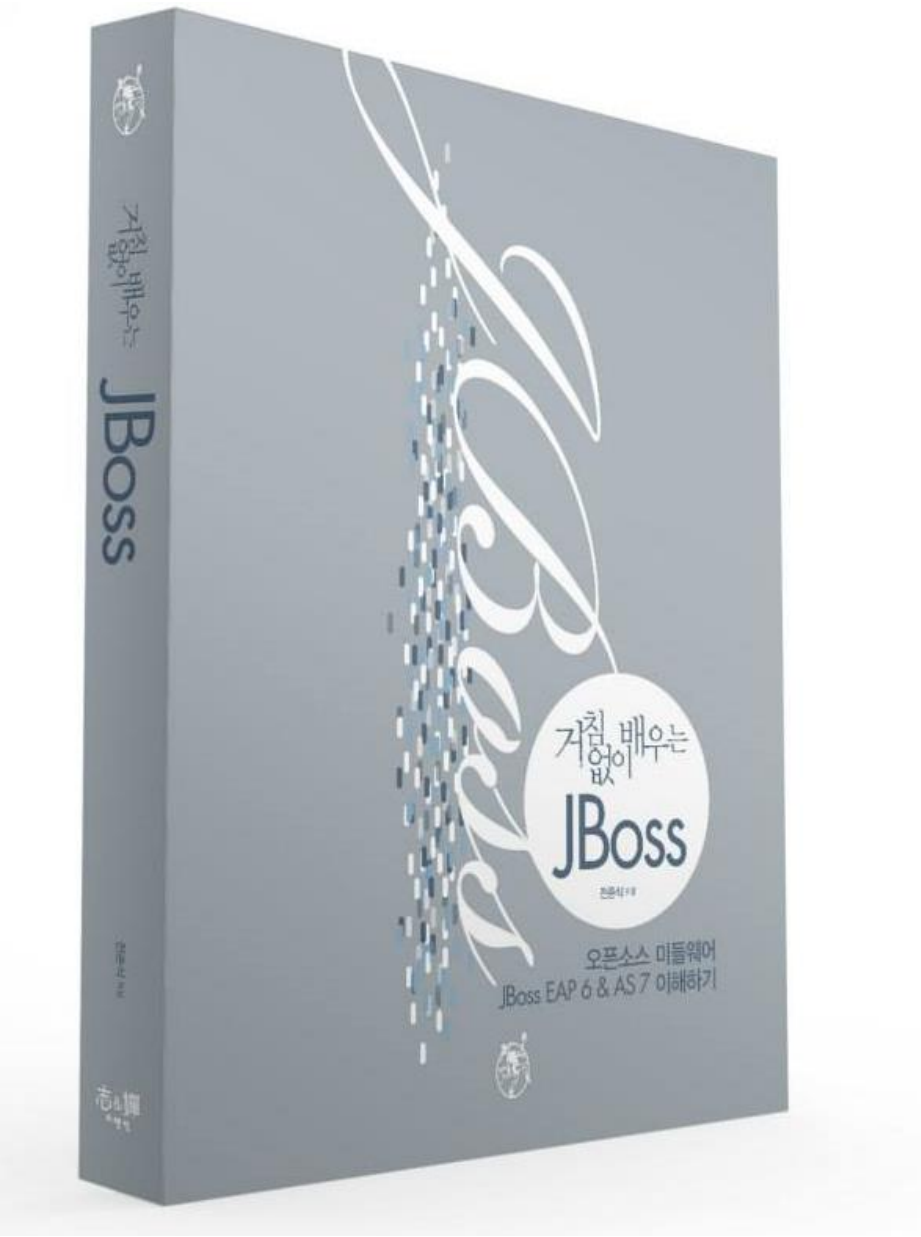
■ 조치 방법

- Apache 에 대한 최신의 버전과 패치를 확인 후 업그레이드 및 패치 수행 권고

※ **취약점 조치 시 WEB 운영자 담당자와 협의하여 영향도 검토 및 서비스 벤더를 통해 안정화된 버전을 문의하여 적용**

3. 도움이 필요하십니까?

만약 이 문서에 설명된 절차를 수행할 때 문제를 겪는다면, 오픈나루 고객 포털(http://support.opennaru.com)을 방문하십시오.



4. References

- **Red Hat Documentation**
  - http://docs.redhat.com/

- **Red Hat 고객지원 포탈**
  - http://access.redhat.com

- **오픈나루 고객지원 포탈**
  - http://support.opennaru.com

- **오픈나루 기술 Blog**
  - http://opennaru.tistory.com

- **오픈나루 Facebook Page**
  - https://www.facebook.com/opennaru

t : +82-2-469-5426 **f** : +82-2-469-7247

e : service@opennaru.com, sales@opennaru.com

h : http://www.opennaru.com