

DI (상)	디렉토리 인덱싱
취약점 개요	
점검목적	■ 디렉터리 인덱싱 취약점을 제거하여 특정 디렉터리 내 불필요한 파일 정보의 노출을 차단
보안위협	■ 해당 취약점이 존재할 경우 브라우저를 통해 특정 디렉터리 내 파일 리스트를 노출하여 응용시스템의 구조를 외부에 허용할 수 있고, 민감한 정보가 포함된 설정 파일 등이 노출될 경우 보안상 심각한 위험을 초래할 수 있음
참고	※ 디렉터리 인덱싱 취약점: 특정 디렉터리에 초기 페이지 (index.html, home.html, default.asp 등)의 파일이 존재하지 않을 때 자동으로 디렉터리 리스트를 출력하는 취약점
조치방법	웹 서버 설정을 변경하여 디렉터리 파일 리스트가 노출되지 않도록 설정
보안설정 방법	

* 웹 서버 환경설정에서 디렉터리 인덱싱 기능 제거

※ 웹 서버 별 상세 설정

■ Apache

httpd.conf 파일 내 DocumentRoot 항목의 Options에서 Indexes 제거
Indexes가 해당 디렉터리의 파일 목록을 보여주는 지시자임

설정 전

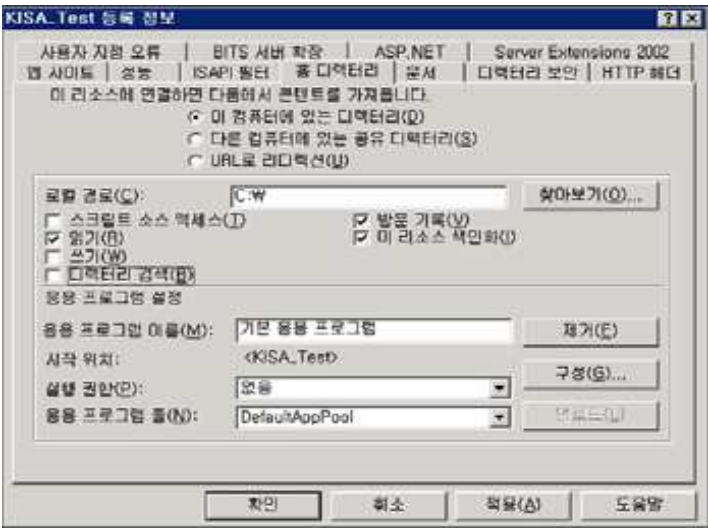
```
<Directory "/var/www/html">
Options Indexes
</Directory>
```

설정 후

```
<Directory "/var/www/html">
Options
</Directory>
```

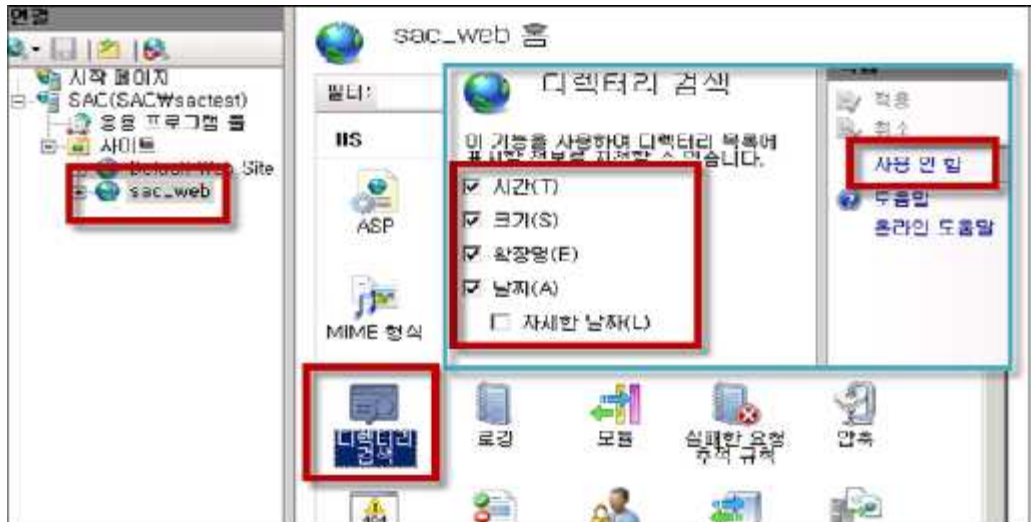
■ IIS 7.0

설정 > 제어판 > 관리도구 > "인터넷 서비스 관리자" 선택 후 해당 웹 사이트에서 우클릭 후
등록 정보 > [홈 디렉터리] 탭 > [디렉터리 검색] 체크 해제



■ IIS 7.5/8.0/8.5/10.0

IIS(인터넷 정보 서비스) 관리자 > [해당 웹 사이트] > [IIS] > [디렉터리 검색] 선택
우측의 [사용 안 함] 버튼을 눌러 비활성화



■ WebtoB 설정

Step 1) \${WEBTOBDIR}/config/http.m 파일 Options 항목에서 index 옵션 삭제 또는, -index
옵션으로 설정 (default: -index)

Step 2) \${WEBTOBDIR}/config/http.m에서 확인

```
# ${WEBTOBDIR}/config/http.m
*NODE
GuideSample  WEBTOBDIR="/home/user/webtob",
              SHMKEY = 54000,
              DOCROOT="/home/user/webtob/docs",
              PORT = "8080",
              HTH = 1,
              LOGGING = "log1",
              ERRORLOG = "log2",
              Options = "-index"
```

Step 3) 확인 후 설정파일 컴파일 및 재구동

wscfl -i http.m (http.m 파일 컴파일)

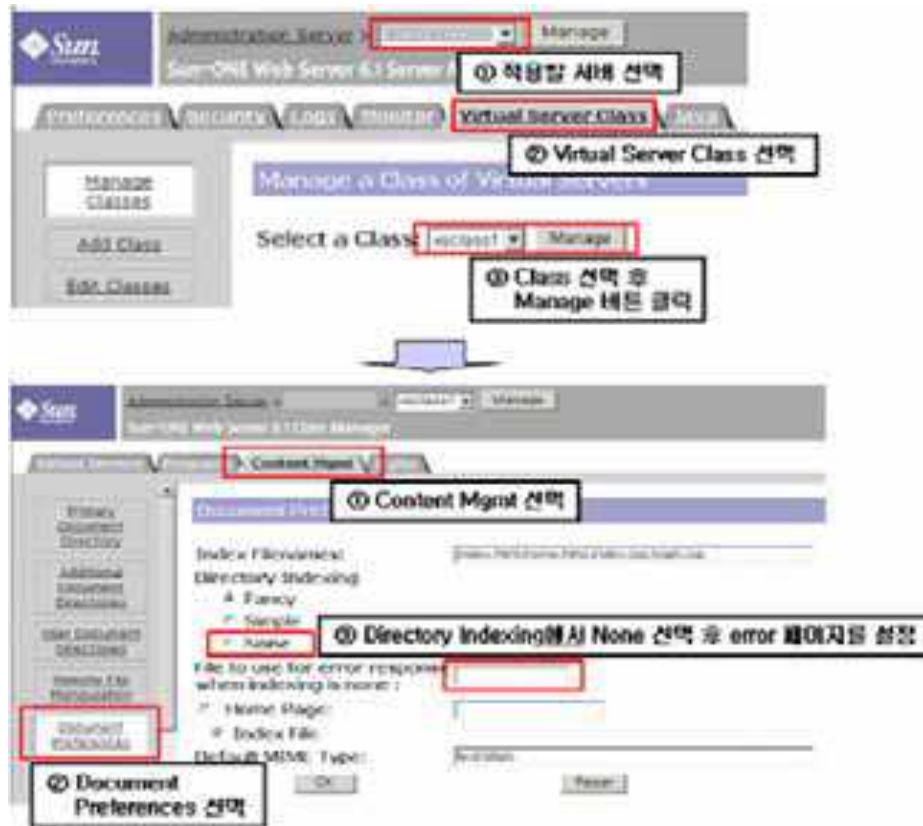
wsdown

wsboot (재구동)

■ iPlanet

Step 1) 관리자 콘솔에서 설정 (※ 1번 또는, 2번 방법 중 선택 적용)

관리자 콘솔 > Server Name > Virtual Server Class > Class Manage > Content Mgmt > Document Preferences > Directory Indexing 항목 "None" 설정



Step 2) 설정 파일에서 설정

/[iPlanet Dir]/https-[Server_name]/config/obj.c

```
<Object name="default">
AuthTrans fn="match-browser" browser="*MSIE*" ssl-unclean-shutdown="true"
NameTrans fn="ntrans-j2ee" name="j2ee"
NameTrans fn="ptx2dir" from="/mc-icons" dir="C:/Sun/WebServer6.1/mc-icons" name="es-internal"
NameTrans fn="document-root" root="$docroot"
PathCheck fn="nt-uri-clean"
PathCheck fn="check-acl" acl="default"
PathCheck fn="find-pathinfo"
PathCheck fn="find-index" index-names="index.html,home.html,index.jsp"
ObjectType fn="type-by-extension"
ObjectType fn="force-type" type="text/plain"
Service method="(GET|HEAD)" type="magnus-internal/imagemap" fn="imagemap"
Service method="(GET|HEAD)" type="magnus-internal/directory" fn="send-error"
path="C:/Sun/WebServer6.1/docs/error/error1.html"
Service method="(GET|HEAD)" type="magnus-internal/trace" fn="trace"
Service method="TRACE" fn="trace"
Error fn="error-j2ee"
Error fn="send-error" reason="Unauthorized" path="C:/Sun/WebServer6.1/docs/error/error1.html"
Error fn="send-error" reason="Forbidden" path="C:/Sun/WebServer6.1/docs/error/error1.html"
Error fn="send-error" reason="Not Found" path="C:/Sun/WebServer6.1/docs/error/error1.html"
Error fn="send-error" reason="Server Error" path="C:/Sun/WebServer6.1/docs/error/error1.html"
AddLog fn="flex-log" name="access"
</Object>
```

문구 없거나, send-error로 설정되어 있지 않을 경우 취막 error page path가 설정되어 있어야 함.

■ %3f.jsp 취약점 제거

웹 서버를 Apache로 사용한다면 아래와 같이 설정하여 %3f.jsp 문자를 필터링해야 하며, Resin이나 Tomcat을 사용한다면 최신 버전으로 업그레이드함

```
<LocationMatch "/(%3f|w?)w.jsp">  
AllowOverride None  
Deny from all  
</LocationMatch>
```

Resin 2.1.x 버전은 최신 버전으로 업그레이드하거나 아래와 같이 설정할 수 있음

Step 1) Resin 환경설정 파일 (resin.conf)에서 가상 디렉터리 설정 부분인 "web-app id"를 찾음

Step 2) 아래 내용 추가

```
<directory-servlet>none</directory-servlet>
```

※ 주의할 점: 모든 가상 디렉터리에 적용 필요