IL (상)	정보 누출
취약점 개요	
점검목적	■ 웹 서비스 시 불필요한 정보가 노출되는 것을 방지함으로써 2차 공격에 활용될 수 있는 정보 노출을 차단하기 위함
보안위협	■ 웹 사이트에 중요정보(개인정보, 계정정보, 금융정보 등)가 노출되거나 에러 발생 시 과도한 정보(애플리케이션 정보, DB 정보, 웹 서버 구성 정보, 개발 과정의 코멘트 등)가 노출될 경우 공격자들의 2차 공격을 위한 정보로 활용될 수 있음
참고	※ 소스코드 및 취약점 점검 필요
조치방법	웹 사이트에 노출되는 중요정보는 마스킹을 적용하여야 하며, 발생 가능한 에러에 대해 최소한의 정보 또는 사전에 준비된 메시지만 출력함
보안설정 방법	

* 사용자가 주민등록번호 뒷자리, 비밀번호 입력 시 별표 표시하는 등 마스킹 처리를 하여 주변 사람들에게 노출되지 않도록 함
* 개인정보의 조회, 출력 시 아래와 같은 원칙으로 일부 정보에 마스킹을 적용하여 표시

1) 성명 중 이름의 가운데 글자 (ex : 홍*동)
2) 생년월일 (ex : ****년 **월 **일
3) 전화번호 또는 휴대전화번호 (ex : 02-**-5678, 010-****-5678)**
4) 주소의 읍/면/동 (ex : 서울시 송파구 ***동)
5) IP v4 주소의 경우 17~24bit, IP v6 주소의 경우 113~128bit

* 웹페이지를 운영 서버에 이관 시 주석은 모두 제거하여 이관
* 중요정보(개인정보, 계정정보, 금융정보 등)를 HTML 소스에 포함하지 않도록 함
* 로그인 실패 시 반환되는 에러 메시지는 특정 ID의 가입 여부를 식별할 수 없게 구현 (예: '가입하지 않은 아이디이거나, 잘못된 비밀번호입니다.')
* 일반적으로 웹에서 발생하는 에러 메시지는 400, 500번대의 에러 코드를 반환하는데 이러한 에러 코드에 대해 별도의 에러 페이지로 Redirect 하거나 적절한 에러처리 루틴을 설정하여 처리되도록 함(전체적인 통합 에러 페이지를 작성한 후 모든 에러 코드에 대해 통합 에러 페이지로 Redirect 되도록 설정)

※ 웹 서버 별 상세 설정

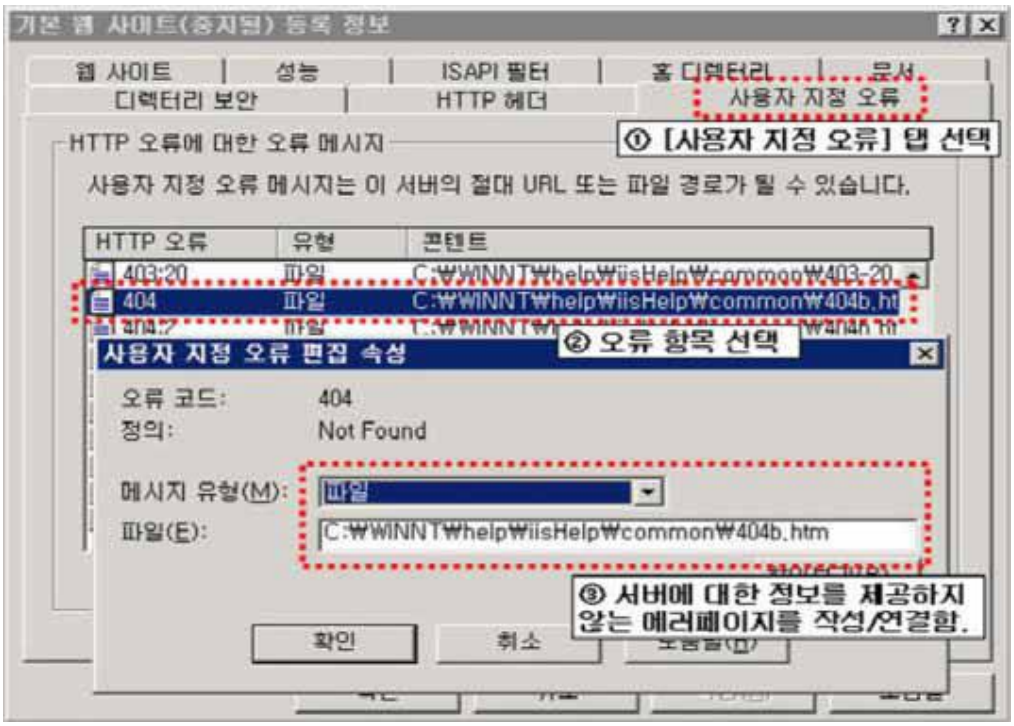
■ Apache

```
ErrorDocument 500 "Error Message"
ErrorDocument 404 "/your web root/error.html"
ErrorDocument 404 "/your web root/error.html"
ErrorDocument 402 http:/xxx.com/error.html
```

위와 같이 특정 에러 코드에 대해 에러 메시지를 출력할 수도 있고 특정 웹 페이지로 Redirect 시킬 수 있으며, 이 설정은 httpd.conf 의 전역 설정에 추가하거나 원하는 가상 호스트의 <VirtualHost> </VirtualHost> 사이에 추가하면 됨

■ **IIS 5.0, 6.0**

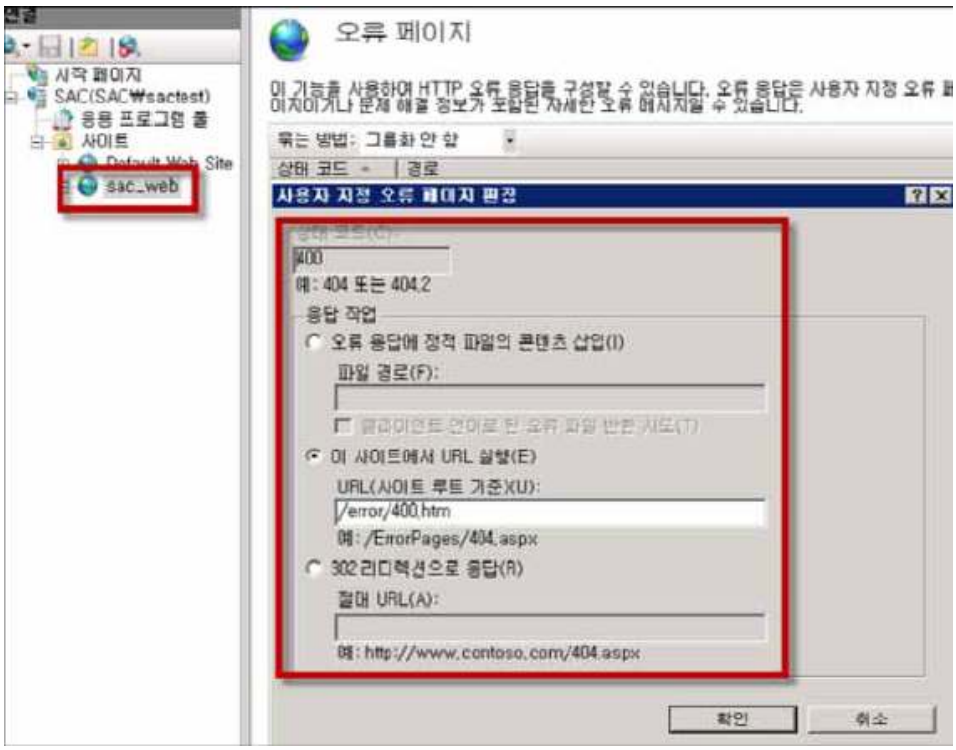
인터넷 정보 서비스(IIS) 관리 > 속성 > [사용자 지정 오류] 탭에서 400, 401, 403, 404, 500 등 웹 서비스 에러에 대해 별도 페이지 지정



■ **IIS 7.0, 7.5, 8.0, 8.5, 10.0 설정**

Step 1) 에러 메시지 설정

인터넷 정보 서비스(IIS) 관리자 > 해당 웹 사이트 > [오류 페이지]에서 400, 401, 403, 404, 500 등 웹 서비스 에러에 대해 별도 페이지 지정



Step 2) 오류 페이지 설정 편집
인터넷 정보 서비스(IIS) 관리자 > 해당 웹 사이트 > 오류 페이지 > [기능 설정 편집]에서
"서버 오류 발생 시 다음 반환" 항목을 "사용자 지정 오류 페이지"로 설정