1 웹 서버 취약점

1 웹 서버 취약점

- 윈도우 서버 2008 R2(x86) 평가판 다운로드
  - http://care.dlservice.microsoft.com/dl/download/4/1/D/41DEA7E0-B30D-4012-A1E3-F24DC03BA1BB/7601.17514.101119-1850_x64fre_server_eval_enus_GRMSXEVAL_EN_DVD.iso

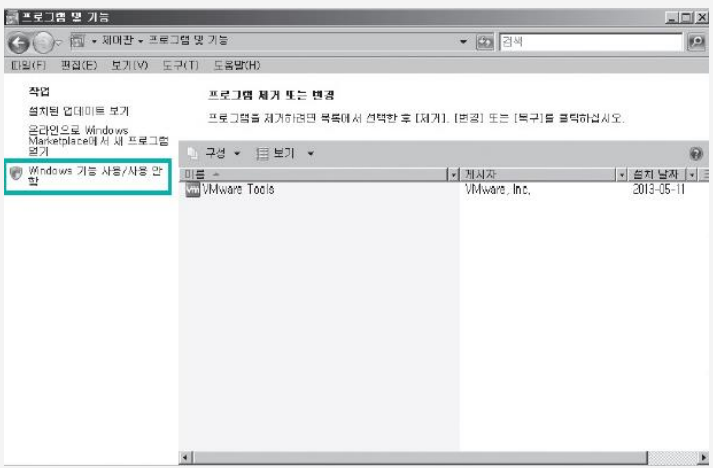
1 웹 서버 취약점

- 한글 언어팩을 사용하려면 아래 파일을 내려 받은 후 설치
  - http://download.microsoft.com/download/4/B/9/4B9533BB-4296-4DA6-9667D1F36A868ED0/Windows6.1-KB2483139-x64-ko-KR.exe
  - 평가판은 60일 동안 무료로 사용할 수 있고 세 번 연장할 수 있기 때문에 최대 180일 동안 추가 비용 없이 쓸 수 있음

2 IIS 웹서버 설치하기

1 서버 관리자 열기

- [시작]-[제어판]-[프로그램 및 기능]의 왼쪽 상단에 있는 [Windows 기능 사용/사용 안 함] 클릭



[프로그램 및 기능 화면]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 IIS 웹서버 설치하기

2 역할 추가 선택

- [서버 관리자] 대화상자가 나타나면 '역할 요약' 항목에서 [역할 추가] 클릭

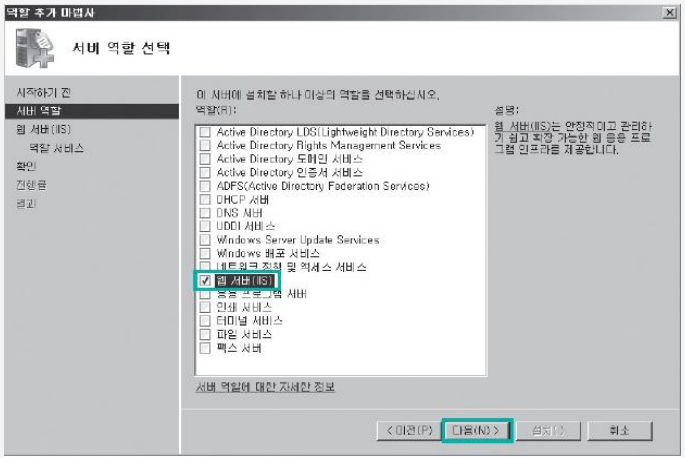
[서버 관리자에서 역할 추가]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 IIS 웹서버 설치하기

3 웹 서버(IIS) 체크

- [역할 추가 마법사]에서 [서버 역할]을 선택하고 '웹 서버(IIS)'에 체크 표시한 후 <다음> 클릭



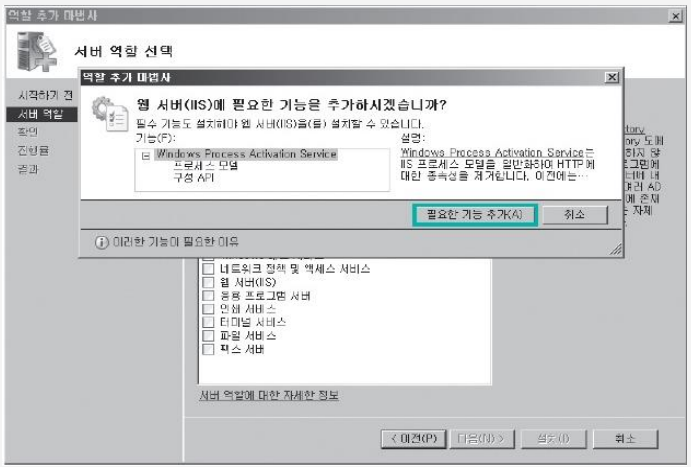
[서버 역할 선택]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 IIS 웹서버 설치하기

4 필요한 기능 추가

- 〈필요한 기능 추가〉 버튼 클릭



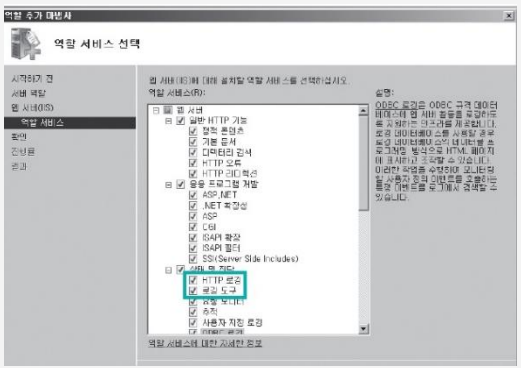
[필요한 기능 추가 화면]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

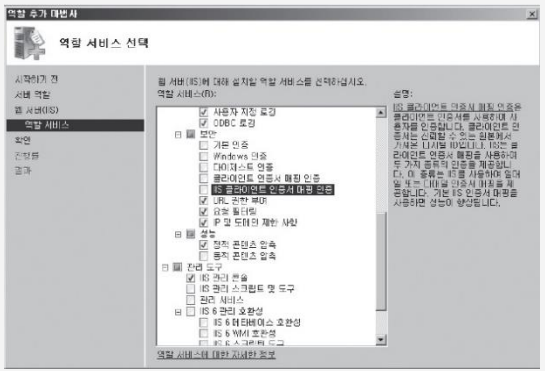
2 IIS 웹서버 설치하기

5 역할 서비스 선택

- 웹 서버 역할에 필요한 역할 서비스 선택



[역할 서비스 선택 1]



[역할 서비스 선택 2]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 IIS 웹서버 설치하기

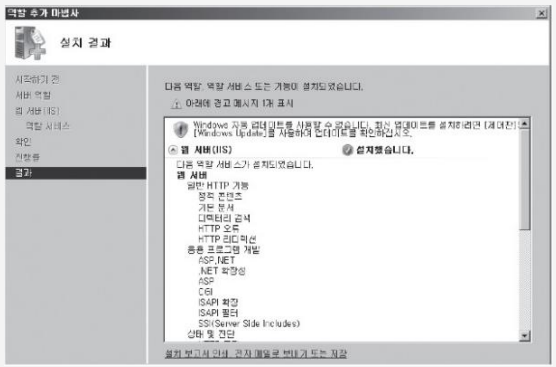
6 선택한 옵션 확인

- 수정이 필요하면 〈이전〉 클릭 후 옵션 변경,
  변동 사항이 없다면 〈설치〉 클릭

2 IIS 웹서버 설치하기

7 설치 결과 확인

- [서버 관리자] 대화상자의 '역할' 항목에 웹 서버(IIS)가 설치된 것 확인



[IIS 웹 서버 설치 결과]

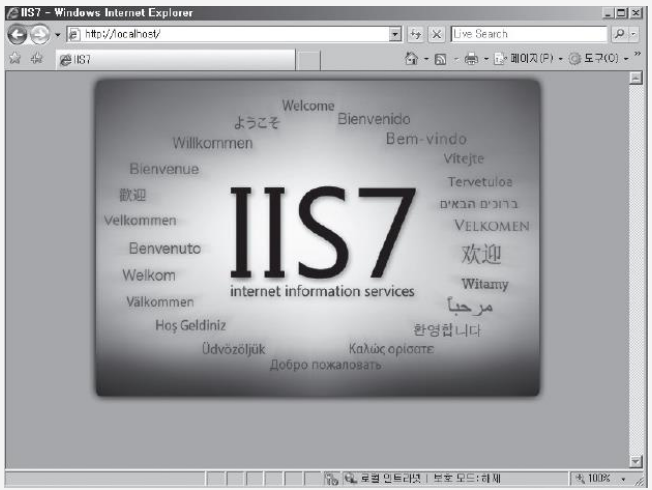
[IIS 웹 서버 설치 확인]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 IIS 웹서버 설치하기

8 설치 결과 확인

- 웹 브라우저에서 IIS 웹 서버 설치 확인



[웹 브라우저에서
IIS 웹 서버 설치 확인]

※ 출처 : 인터넷 해킹과 보안,
김경곤, 한빛아카데미, 2017

3 IIS

- 마이크로소프트 인터넷 정보 서비스(Internet Information Services, IIS)는 마이크로소프트 윈도우를 사용하는 서버들을 위한 인터넷 기반 서비스들의 모임임. 이전 이름은 인터넷 정보 서버(Internet Information Server)임

- 서버는 현재 FTP, SMTP, NNTP, HTTP/HTTPS를 포함하고 있음(FTP, SMTP, HTTP)

3 IIS

- 2017년 10월 기준으로 실질적으로 작동하는 웹 사이트(Active site)들에서 쓰이는 웹 서버 소프트웨어 순위는 아파치(44.89%), 엔진엑스 (20.65%), 구글 웹 서버(7.86%), 마이크로소프트 IIS(7.32%)순임, 이 조사에서 생성은 되어있으나 정상적으로 작동하지 않는 웹 사이트들은 배제되었으며 특히 MS의 인터넷 정보 서비스(IIS)를 설치한 웹 사이트들의 상당수가 비활성 사이트임,

  그런 사이트들도 포함하면 MS IIS가 1위

4 IIS 역사

- IIS는 처음에 윈도우 NT 3.51용 인터넷 기반 서비스의 부가적인 기능으로 공개됨. IIS 2.0은 윈도우 NT 4.0 운영 체제에 대한 지원을 추가하기에 이르렀으며, IIS 3.0은 액티브 서버 페이지의 동적인 스크립트 환경을 도입(ASP)

- IIS 4.0은 고퍼 프로토콜에 대한 지원을 끊고, 별도의 옵션 팩 CD-ROM으로 윈도우 NT에 번들로 추가

4 IIS 역사

- 마지막에 나온 IIS 버전은 윈도우 8.1을 위한 8.5, 윈도우 8을 위한 8.0, 윈도우 7을 위한 7.5, 윈도우 비스타를 위한 7.0, 윈도우 서버 2003을 위한 6.0, 윈도우 XP 프로페셔널을 위한 IIS 5.1임

- 윈도우 XP는 10개의 동시 접속과 단일 웹사이트만 지원하는 제한된 버전의 IIS 5.1을 포함하고 있음

  IIS 6.0은 IPv6에 대한 지원을 하였음(IPv4 vs. IPv6), FastCGI 모듈도 IIS 5.1과 IIS7에서 사용할 수 있음

4 IIS 역사

- 윈도우 비스타는 IIS 7.0을 기본으로 설치하지 않지만 설치된 구성 요소를 선택하는 목록에서 설치할 수 있게 되어 있음

  비스타에서 IIS 7.0는 허용 접속 수를 제한하지 않지만 활성화되는 동시 요청 기반의 성능을 제한(무한은 아님)

5 IIS 7.0

- IIS 7.0은 윈도우 비스타에 들어있음
  또한 윈도우 서버 2008에도 끼어 들어가 있음

  IIS 7.0은 모듈러(Modular)한 소프트웨어 아키텍처를 특징으로 함, 모든 서비스를 한 번에 가동시키는 모놀리딕 서버 대신, IIS 7.0는 코어 웹 서버 엔진 한 개를 갖추고 있음, 사람들은 특정한 기능을 제공하는 모듈을 이 엔진에 추가할 수 있음,

  이러한 아키텍처 덕분에, 필요한 기능만 "활성화" (Enable)시킬 수 있게 되었으며, 커스텀(Custom) 모듈을 사용해 기능들을 추가할 수 있게 됨(모놀리딕 vs. 모듈러)

5 IIS 7.0

- 마이크로소프트는 IIS 7.0와 함께
  몇 가지 모듈들을 끼워 IIS 7.0을 유통시키고 있음

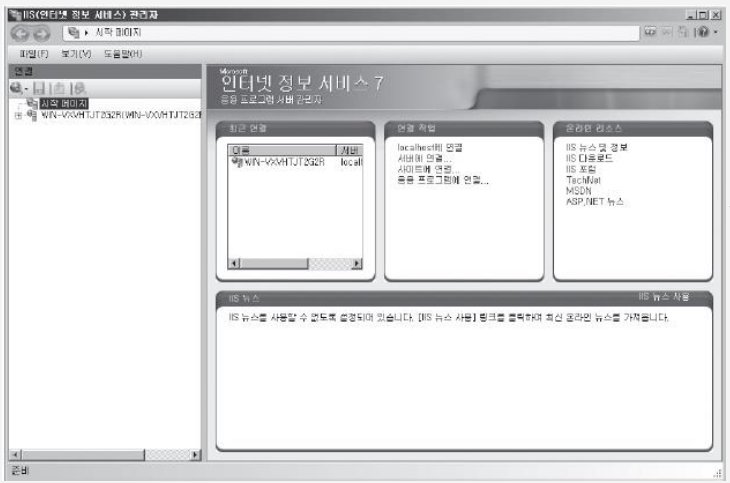
5 IIS 7.0

- 또한 마이크로소프트는 여러 다른 모듈도 온라인으로 받아갈 수 있게 해 놓았음, 마이크로소프트는 다음 모듈들을 서버와 함께 끼워 팔 예정
  - HTTP 모듈들
  - 보안 모듈들
  - 콘텐트 모듈들
  - 데이터 압축 모듈들
  - 캐싱 모듈들
  - 로깅 및 다이어그노스틱스 모듈들

2 웹 서버 보안 설정

1 IIS 웹 서버 보안 설정

- [시작]-[제어판]-[관리도구]-[IIS(인터넷 정보 관리자)]를 선택하면 웹 서버의 설정을 수정할 수 있는 관리자 화면이 나타남



[IIS(인터넷 정보 서비스) 관리자 화면]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

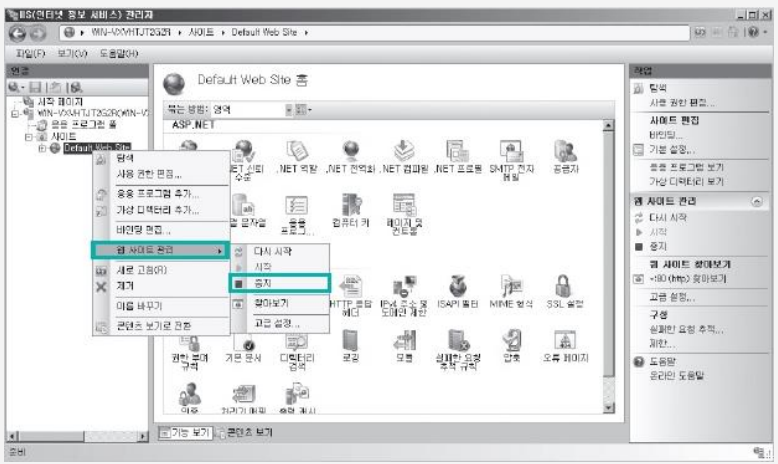
2 기본 웹사이트 중지하고 새로운 웹사이트 추가하기

- IIS 관리자에서 웹 사이트 추가
  - 새로운 웹 사이트를 만들기 전
    C:₩ 디렉터리에 website 폴더 생성
  - [IIS(인터넷 정보 서비스) 관리자] 화면 왼쪽의
    [Default Web Site]에서 마우스 오른쪽 버튼을
    클릭 후 [웹 사이트 관리]-[중지]를 눌러 중지

2 기본 웹사이트 중지하고 새로운 웹사이트 추가하기

IIS 관리자에서 웹 사이트 추가

[Default Web Site 중지 화면]



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

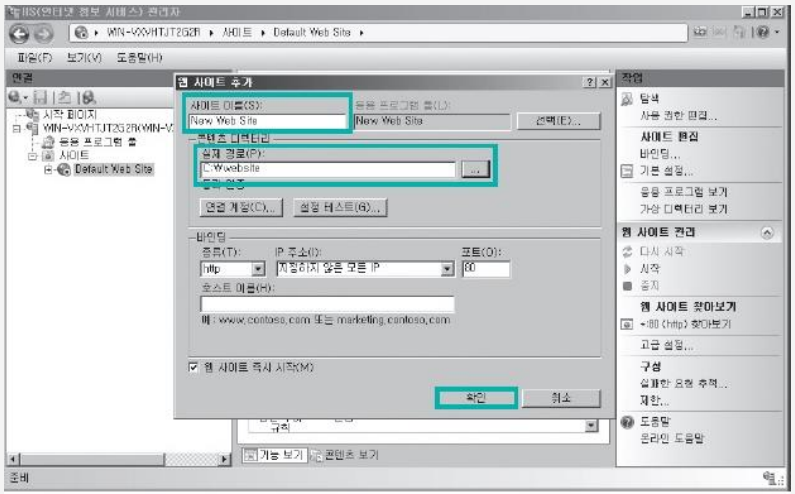
2 기본 웹사이트 중지하고 새로운 웹사이트 추가하기

- IIS 관리자에서 웹 사이트 추가
  - 새로운 웹 사이트를 만들기 위해 화면 왼쪽의 [사이트] 아이콘에서 마우스 오른쪽 버튼을 눌러 [웹 사이트 추가] 클릭
  - [웹 사이트 추가]가 나타나면 사이트 이름에 'New Web Site'를 입력하고, 실제 경로에는 C:₩websites를 찾아서 선택 후 <확인> 클릭

2 기본 웹사이트 중지하고 새로운 웹사이트 추가하기

IIS 관리자에서 웹 사이트 추가

[IIS 관리자에서 웹 사이트 추가]



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

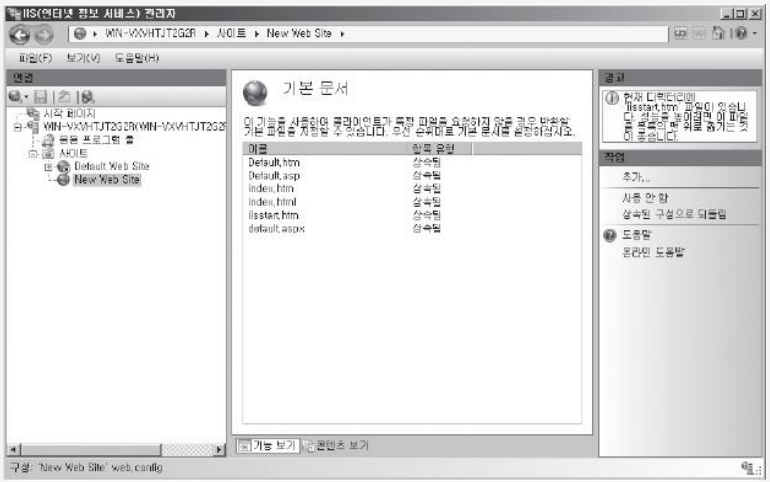
3 사용하지 않는 기본 문서 제거하기

1. 기본 문서의 순서 확인
   - 가장 위에 있는 파일을 웹 사이트에서 가장 먼저 불러옴
   - 웹 사이트를 방문했을 때 Default.htm 파일이 있으면 그 파일을 가장 먼저 읽고, 없으면 순서대로 Default.asp, index.htm, index.html, iisstart.htm, default.aspx를 읽음(백업 파일이 있으면 안됨)

3 사용하지 않는 기본 문서 제거하기

1 기본 문서의 순서 확인

[IIS 관리자의 기본 문서 화면]



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 사용하지 않는 기본 문서 제거하기

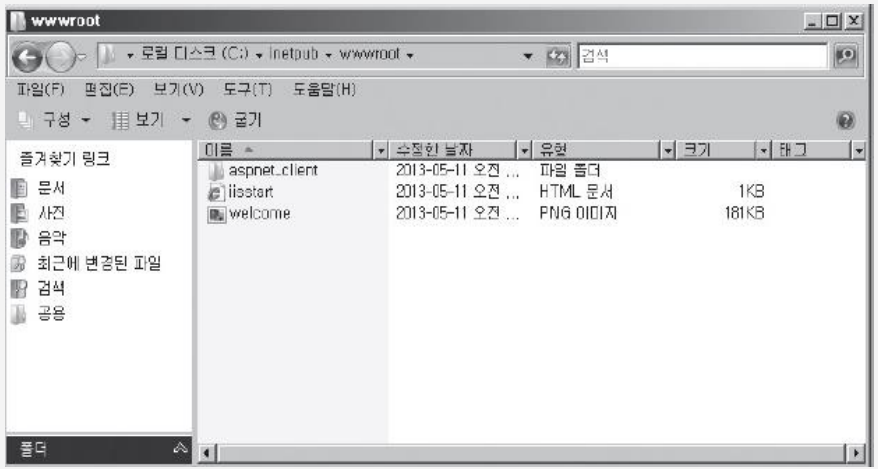
2 새로운 웹 사이트 디렉터리로 이동

- IIS7을 설치하고 Default Web Site가 운영되고 있는 경우에는 iisstart.htm 파일이 기본으로 설치
- 처음에 새로운 웹 사이트를 만들면 이 디렉터리는 비어 있음

3 사용하지 않는 기본 문서 제거하기

2 새로운 웹 사이트 디렉터리로 이동

[Default Web Site 디렉터리에 생성된 iisstart.htm 파일]



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 사용하지 않는 기본 문서 제거하기

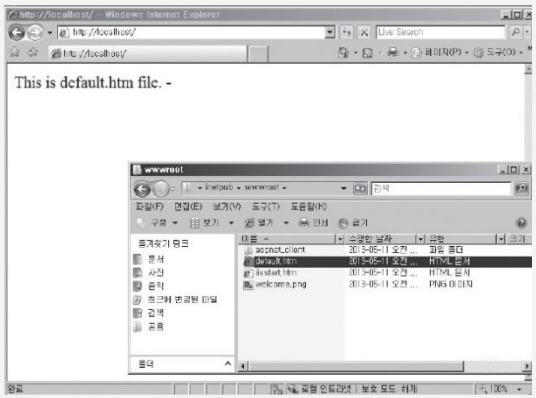
3 default.htm 파일 생성

- 해당 디렉터리에 노트패드와 같은 프로그램으로 default.htm 파일을 생성하고 아무 내용이나 입력(백업 파일 조심)

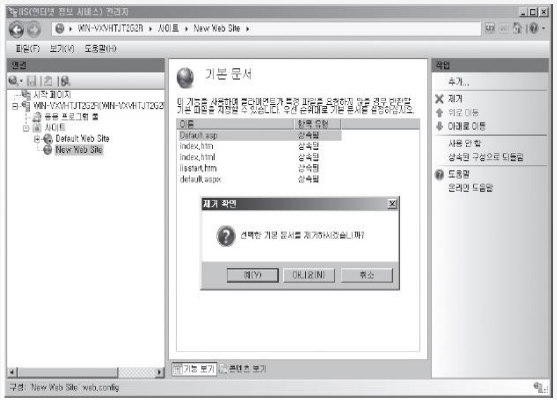
3 사용하지 않는 기본 문서 제거하기

4 웹 사이트에 접속해서 확인

- 기본 문서에서 사용하지 않는 파일은 모두 삭제



[default.htm 파일 브라우징]



[사용하지 않는 기본 문서 삭제]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

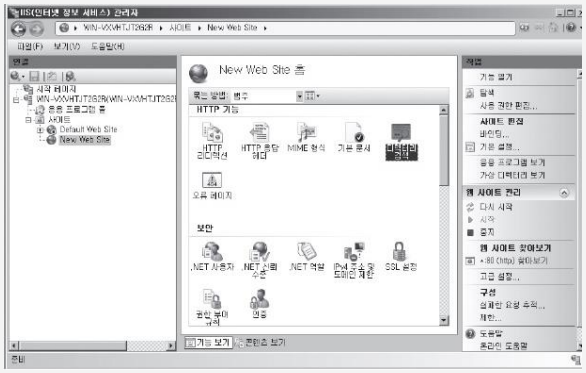
4 디렉터리 검색 기능 제한하기

- 디렉터리 검색 기능
  : 특정 디렉터리 내에 index.html과 같은
  기본 문서 파일이 없을 경우 웹 브라우저에서
  해당 디렉터리를 불러왔을 때 파일 목록이
  화면에 뜨는 기능(원치 않는 다운로드)

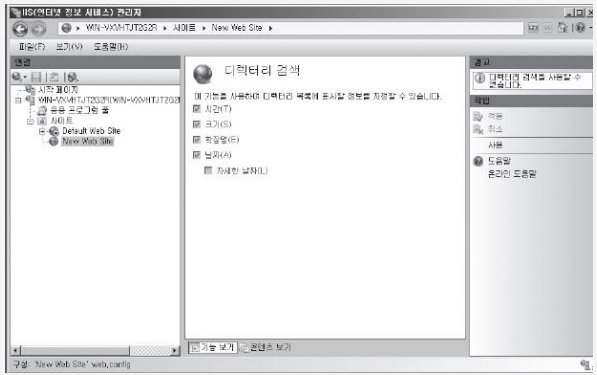
- 불필요할 뿐만 아니라 보안상 위험하기 때문에
  비활성화를 유지하는 것이 좋음

4 디렉터리 검색 기능 제한하기

- IIS7은 기본적으로 디렉터리 검색이 비활성화로 설정되어 있음



[IIS 관리자의 디렉터리 검색 선택]



[디렉터리 검색 비활성화 화면]

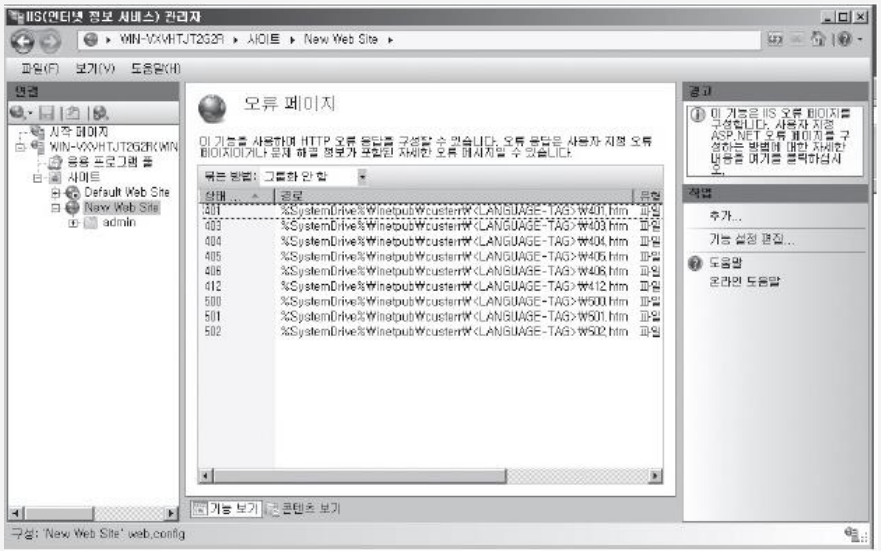
※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

5 맞춤형 오류페이지 생성하기

1. IIS에서 제공하는 오류 페이지 확인
   - IIS 관리자에서 오류 페이지를 더블 클릭하면 IIS에서 제공하는 오류 페이지를 볼 수 있음
   - 공격자가 주로 관심을 갖는 상태 코드는 400번대와 500번대(오류 페이지 → 정보 획득)

5 맞춤형 오류페이지 생성하기

1 IIS에서 제공하는 오류 페이지 확인

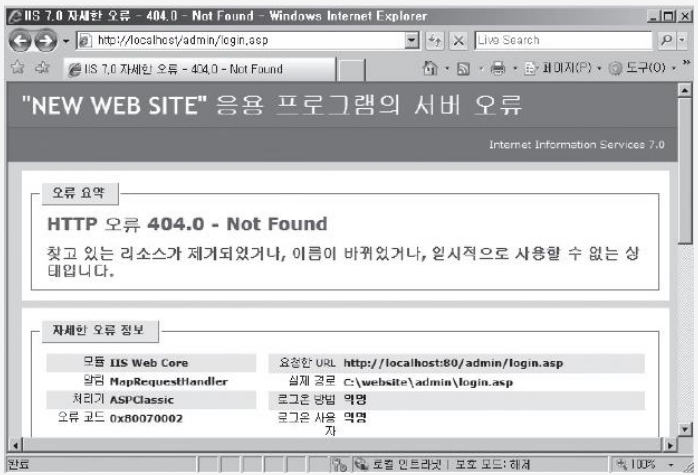


※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

5 맞춤형 오류페이지 생성하기

2 해당 파일이 존재하지 않을 때의 오류 메시지 확인

- http://localhost/admin/login.asp에 접속 후 확인

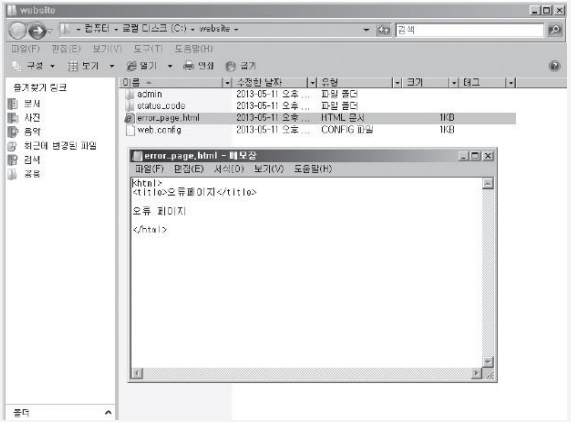


※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

5 맞춤형 오류페이지 생성하기

3 오류 메시지를 보여주기 위한 별도의 파일 생성

- 웹 사이트에서 오류가 발생했을 때 원하는 오류 메시지를 보여주기 위해 별도의 파일을 생성



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

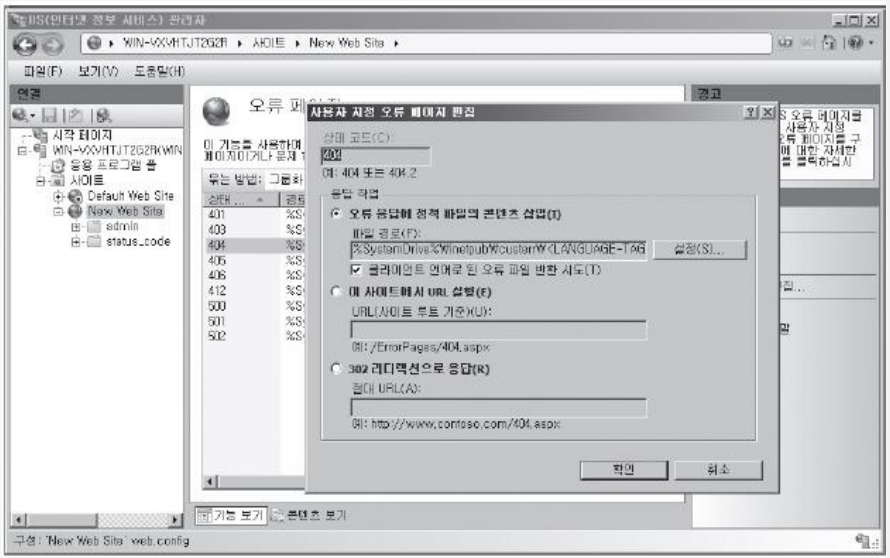
5 맞춤형 오류페이지 생성하기

4 오류 메시지 편집 화면

- IIS 관리자 도구에서 새로 생성한 New Web Site를 클릭하고 오류 페이지 기능을 열어 변경하고자 하는 코드를 더블클릭

5 맞춤형 오류페이지 생성하기

4 오류 메시지 편집 화면



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

5 맞춤형 오류페이지 생성하기

5 오류 메시지 편집 기능 선택

- '이 사이트에서 URL 실행'을 선택 후 error_page.html을 입력

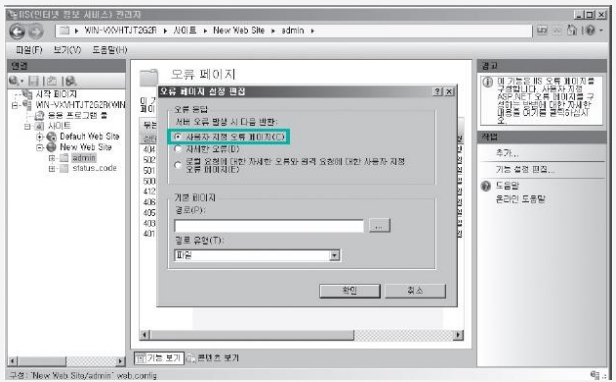
5 맞춤형 오류페이지 생성하기

6 '사용자 지정 오류 페이지' 선택

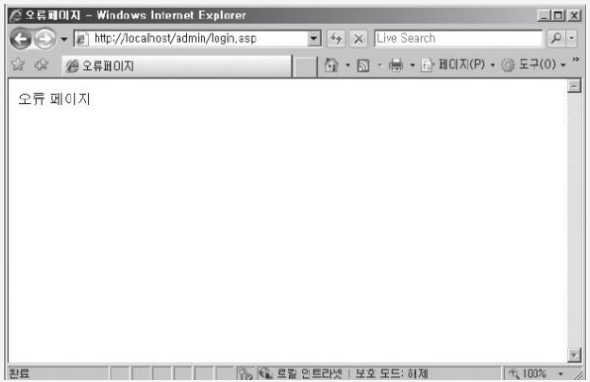
- [기능 설정 편집]을 클릭하여
  [오류 페이지 설정 편집] 대화상자가 나타나면
  '사용자 지정 오류 페이지' 선택
- 브라우저를 통해 존재하지 않는 페이지를 요청하면
  다음과 같이 error_page.html의 내용이 화면에
  나타남

5 맞춤형 오류페이지 생성하기

6 '사용자 지정 오류 페이지' 선택



[오류 페이지 설정 편집]



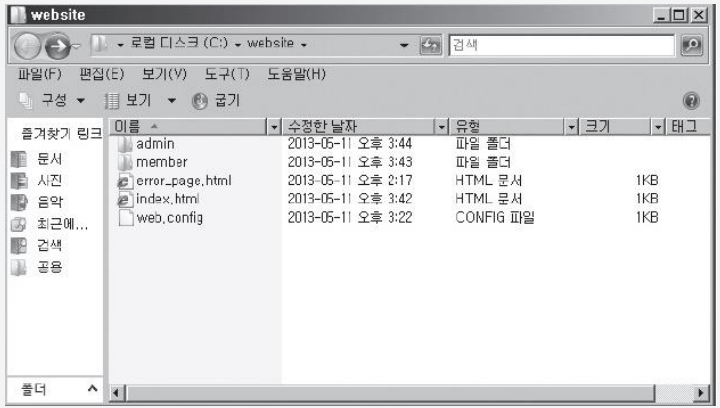
[맞춤형 오류 페이지]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

6 IPv4 주소 및 도메인 제한하기

1 admin과 member 디렉터리 생성

- 웹 디렉터리 상단에 admin과 member 디렉터리를 생성하고, 각 디렉터리에 내용을 간단히 설명하는 index 파일을 만듦



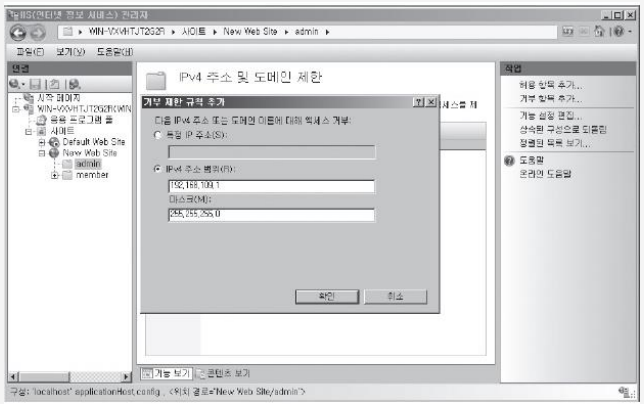
[관리자와 일반 사용자 디렉터리 생성]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

6 IPv4 주소 및 도메인 제한하기

2 차단할 IP 주소 입력(black list)

- admin 디렉터리를 선택하고 'IPv4 주소 및 도메인 제한 기능'을 선택
- 오른쪽의 [거부 항목 추가]를 클릭하여 차단할 IP 주소 입력

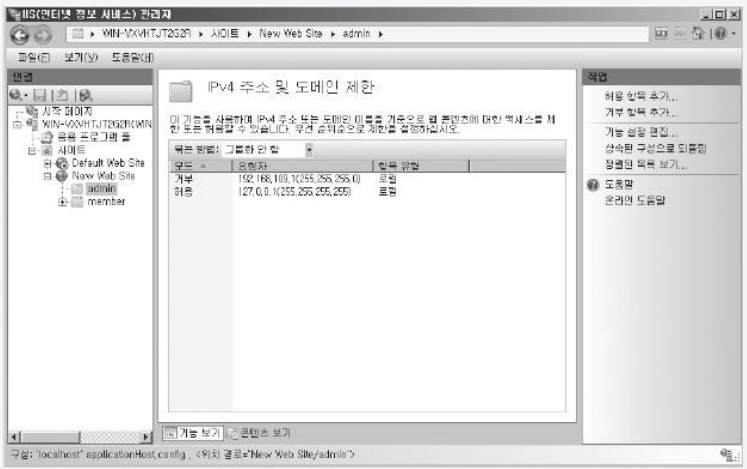


※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

6 IPv4 주소 및 도메인 제한하기

3 허용할 IP 주소 입력(white list)

- [허용 항목 추가]를 클릭하여 특정 IP 주소에 '127.0.0.1'을 입력



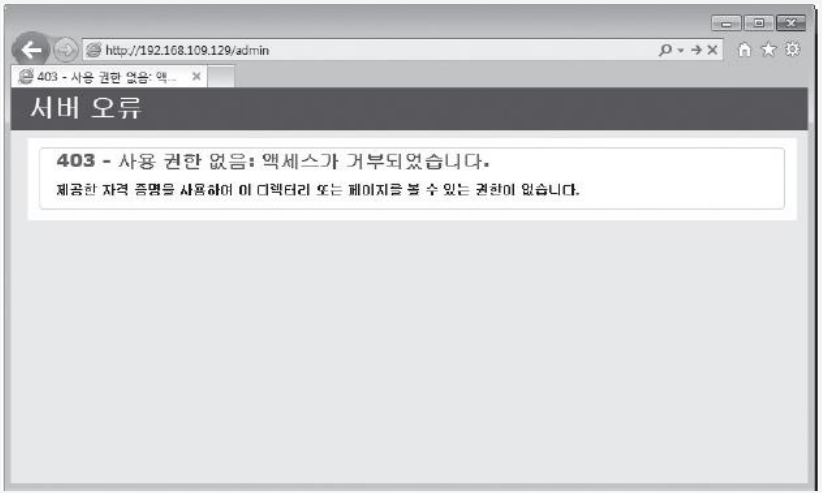
[관리자 디렉터리에 설정된 IP 허용 및 거부 목록]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

6 IPv4 주소 및 도메인 제한하기

4 접근 제어 메시지 확인

[관리자 디렉터리 접근 제어 화면]



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

7 WebKnight 방화벽

- AQTRONIX(http://www.aqtronix.com/?PageID=99)에서 제공하는 IIS 기반의 공개 웹 애플리케이션 방화벽(WAF)
- 한국인터넷진흥원에서 운영하는 'WebKnight 자료실'에 상세한 설명과 사용법이 나와 있음
- http://toolbox.krcert.or.kr/MMBF/MMBFBBS_S.aspx?MENU_CODE=37&BOARD_ID=8

8 WAF

- 웹방화벽(Web Application Firewall, WAF)은, 일반적인 네트워크 방화벽 (Firewall)과는 달리 웹 애플리케이션 보안에 특화되어 개발된 솔루션임

  웹방화벽의 기본 역할은 그 이름에서도 알 수 있듯, SQL Injection, Cross-Site Scripting(XSS)등과 같은 웹 공격을 탐지하고 차단하는 것인데, 직접적인 웹 공격 대응 이 외에도, 정보유출방지솔루션, 정로그인방지솔루션, 웹사이트위변조방지솔루션 등으로 활용이 가능함(SQL Injection, XSS)

8 WAF

- 정보유출방지솔루션으로 웹방화벽을 이용할 경우, 개인정보가 웹 게시판에 게시되거나 개인 정보가 포함된 파일 등이 웹을 통해 업로드 및 다운로드 되는 경우에 대해서 탐지하고 이에 대응하는 것이 가능함(업로드, 다운로드 오류)
- 부정 로그인 방지 솔루션으로서는, 추정 가능한 모든 경우의 수를 대입하여 웹사이트에 로그인을 시도하는 경우와 같은 비정상적인 접근에 대한 접근 제어 기능을 함(Password crack)

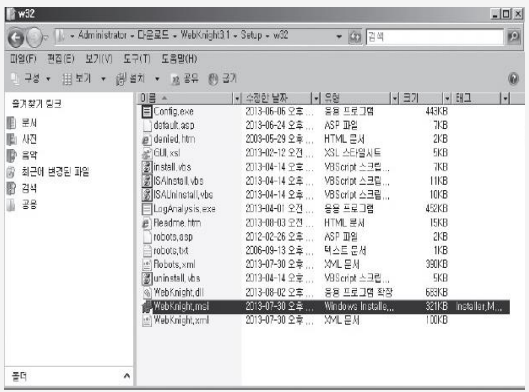
8 WAF

- 웹사이트 위변조 방지 솔루션은 주로 해커가 해킹을 한 후에 과시하는 것이 목적인 웹사이트 위변조가 발생했을 경우, 이에 대해 탐지하고 대응 함(무결성 검사)

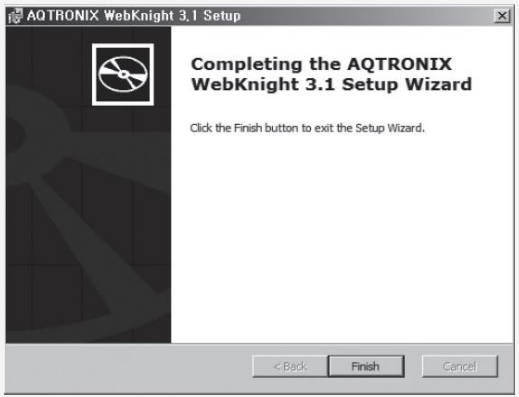
- 즉, 웹방화벽은 위에서 기술한 4 가지 웹 보안 기능을 제공하면서, 웹 애플리케이션이라는 [집]을 미처 예상하지 못했던 외부의 공격으로부터 지켜내고, 사전에 발견하지 못했던 내부의 위험 요소로부터 지켜내는 [울타리] 역할을 수행하는 존재라고 할 수 있음

9 Webkinght 설치

1 Setup₩w32₩WebKnight.msi 파일 실행



[Webknight 설치 파일]

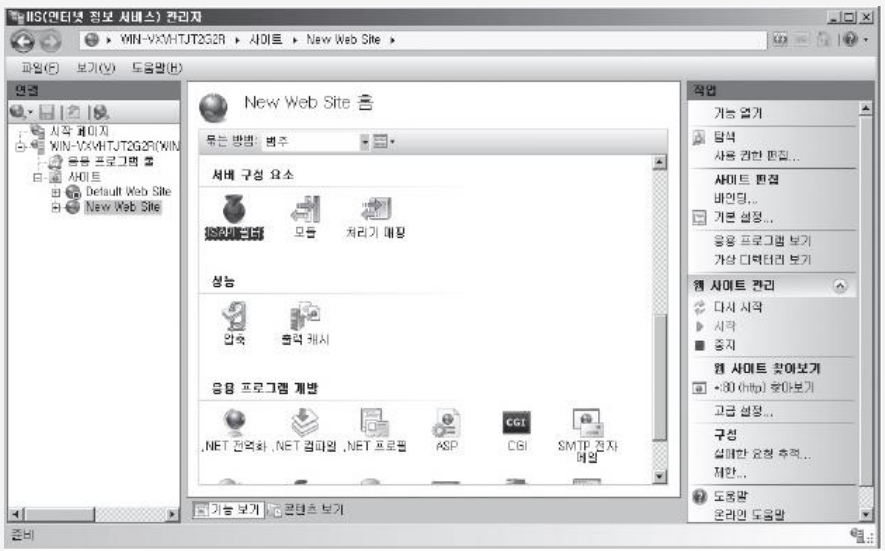


[Webknight 설치 완료]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

9 Webkinght 설치

2 ISAPI 필터 기능 실행



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

9 Webkinght 설치

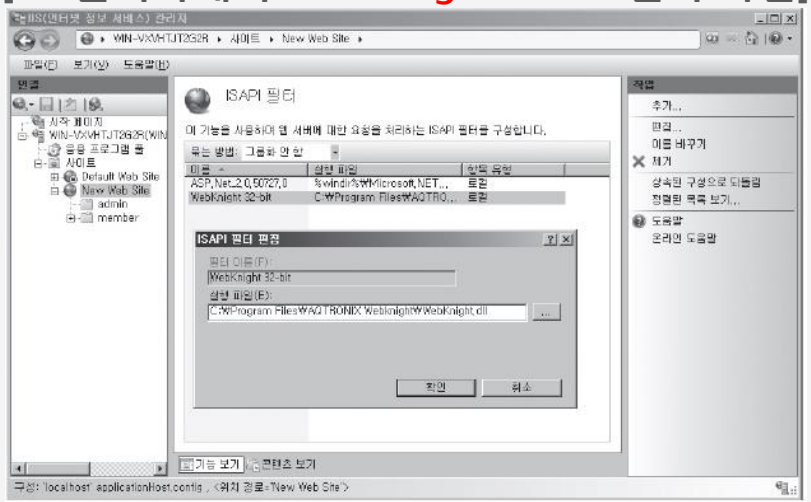
3 WebKnight ISAPI 추가

- 자동으로 WebKnight가
  보이지 않을 경우 아래와 같이 입력
- 필터 이름 : WebKnight 32-bit
- 실행 파일 : C:₩Program Files₩AQTRONIX
  Webknight₩WebKnight.dll

9 Webkinght 설치

3 WebKnight ISAPI 추가

[IIS 관리자에서 Webknight ISAPI 설치 확인]



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

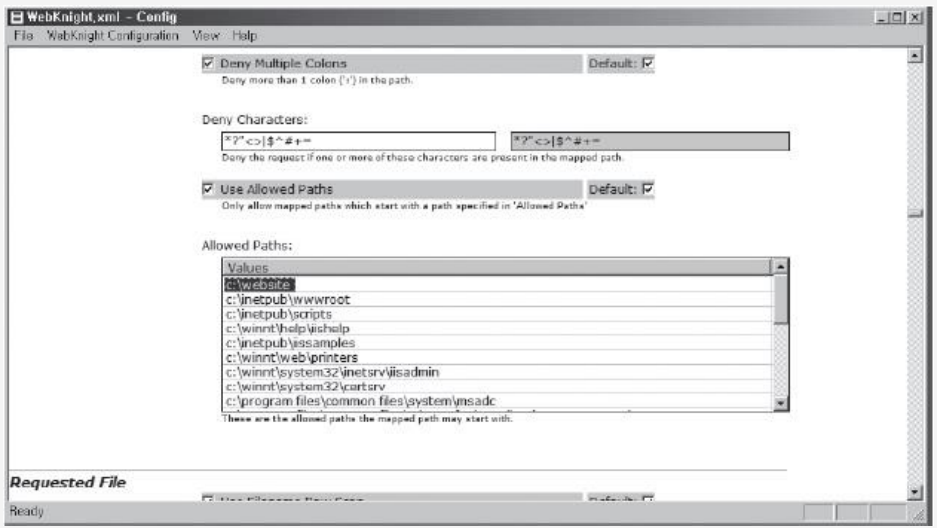
9 Webkinght 설치

4 ~ 5 웹 사이트 경로 설정 후 생성 폴더 추가

- [시작]-[모든 프로그램]-[AQTRONIX Webknight][WebKnight Configuration]을 실행하고 WebKnight.xml을 선택
- Allowed Paths 부분에 라인을 추가하여 'C:₩website'를 입력

9 Webkinght 설치

4 ~ 5 웹 사이트 경로 설정 후 생성 폴더 추가

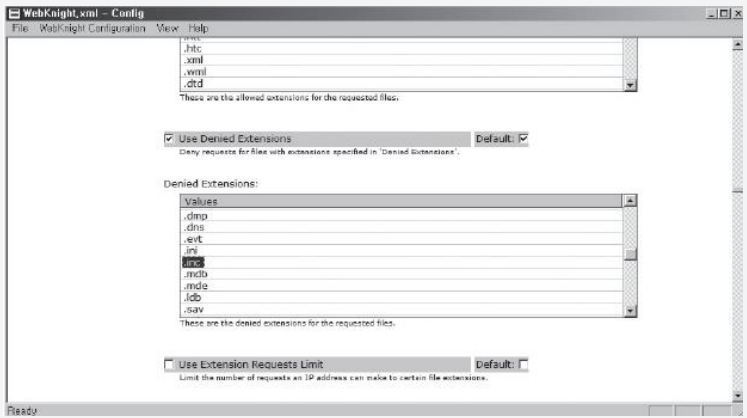


※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

9 Webkinght 설치

6 특정 확장자를 요청하지 못하도록 하는 옵션 추가

- [WebKnight Configuration] 메뉴에서 [Requested File]을 선택하고 Denied Extensions 부분에 '.inc'를 추가

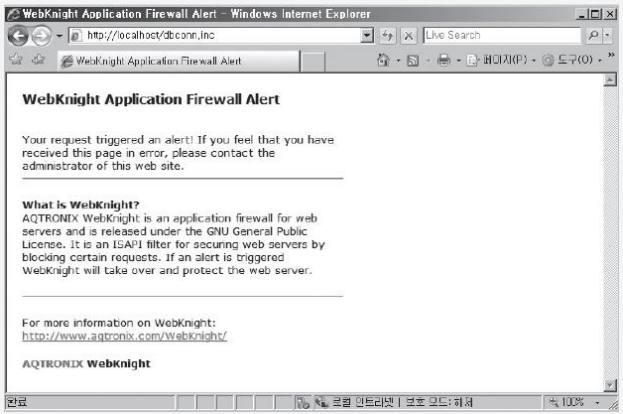


※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

9 Webkinght 설치

6 신규 규칙 실행 확인

- 브라우저를 통해 http://localhost/dbconn.inc 파일을 요청하면 WebKnight 에 의해 차단된 화면이 나타남



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

10 IIS7 웹 서버에서 이용 가능한 대표적인 로그 형식

- Microsoft IIS 로그 파일 형식
- NCSA 공통 로그 파일 형식
- W3C 확장 로그 파일 형식
  (IIS 웹 서버의 기본 설정이며 가장 널리 이용)

11 NCSA

- NCSA (National Center for Supercomputing Applications)는 슈퍼컴퓨터망에서 이용하게 될 각종 프로그램과 통신 규약을 연구하는 국립 슈퍼 컴퓨터 응용 센터임,

  미국 국립 수퍼컴퓨팅 응용 연구소,
  전미 슈퍼컴퓨터 응용 연구소라고도 함,

  1986년에 설립되었으며
  NSF의 5개 슈퍼컴퓨터 센터 중의 하나임

11 NCSA

- 미국 일리노이 대학교 어배너-샘페인 부설 연구소임, NCSA가 중점을 두고 있는 일은 일반 기업들이 개발하기 힘든 프로그램을 공익을 위해 연구하고 개발해내는 것,

  멀리 떨어져 있는 컴퓨터와 원활하게 통신하기 위해 생겨난 텔넷과 FTP도 NCSA에서 만들어낸 것임, (Telnet, FTP)

  또한 그래픽 기반의 웹 브라우저인 모자이크 웹 브라우저를 개발하기도 했음 (GUI 웹 브라우저)

12 W3C

- W3C(World Wide Web Consortium)는 월드 와이드 웹을 위한 표준을 개발하고 장려하는 조직으로 팀 버너스 리를 중심으로 1994년 10월에 설립되었음, W3C는 회원기구, 정직원, 공공기관이 협력하여 웹 표준을 개발 하는 국제 컨소시엄, W3C의 설립취지는 웹의 지속적인 성장을 도모하는 프로토콜과 가이드 라인을 개발하여 월드 와이드 웹의 모든 잠재력을 이끌어 내는 것(프로토콜)

12 W3C

- W3C는 설립목적인 웹 표준과 가이드라인 개발을 수행하고 있으며, 지금까지의 결과로 지난 10년간 80여개의 W3C 권고안을 발표, W3C는 또한 교육과 소프트웨어 개발에 관여해 왔고, 그리고 웹에 관하여 토론할 수 있는 열린 포럼을 개최해 왔음

12 W3C

- 웹의 모든 잠재력을 이끌어내기 위해서 가장 기본적인 웹 기술은 상호 간의 호환성이 있어야 한다는 것, 그리고 어떤 소프트웨어나 하드웨어에서도 웹에 접근할 수 있어야 한다는 것, W3C의 이러한 목표를 "웹 상호운용성 (Web Interoperability)" 이라고 함,

  W3C는 웹 언어와 프로토콜에 대한 공개(반독점적인) 표준을 제정하여 시장 분열과 웹의 분열을 피하고자 함

12 W3C

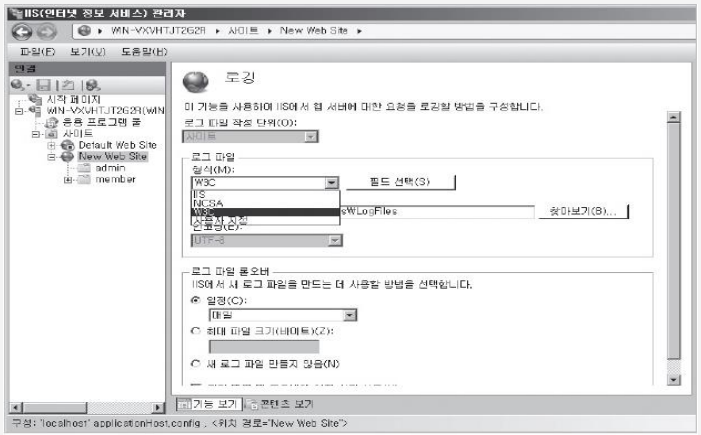
- 팀 버너스리(Tim Berners-Lee)와 운영진은 W3C를 웹 기술에 대한 컨센서스를 이끌어내는 산업 컨소시엄으로 발전시켜왔음, 유럽 핵물리 연구기관(European Organization for Nuclear Research, CERN)에서 근무하던 1989년에 월드 와이드 웹을 개발한 팀 버너스리는 W3C가 창립된 1994년부터 현재까지 W3C Director 직책을 맡고 있음,

  W3C는 2004년 12월에 창립 10주년을 기념하여 웹과 W3C의 과거와 미래에 관한 심포지엄을 보스턴에서 개최했음

13 윈도우 로그 형식 살펴보기

1 웹 로그 파일 형식 설정

- IIS 관리자에서 [사이트]-[New Web Site]를 선택하고 '상태 및 진단'에 있는 로깅을 더블클릭



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

13 윈도우 로그 형식 살펴보기

2 세부 필드 값 선택

- 〈필드 선택〉을 클릭하면 로그를 남기고 싶은 세부 필드 값을 선택할 수 있음

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

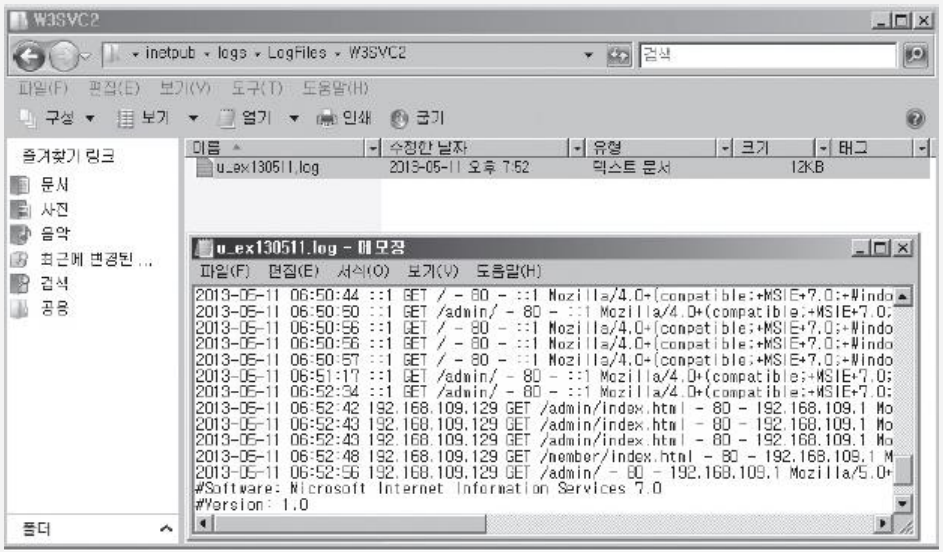
13 윈도우 로그 형식 살펴보기

3 로깅 기능

- 로그 파일의 형식과 로그 파일을 만드는 주기, 최대 파일 크기와 같은 옵션 을 선택할 수 있음
- 기본 설정은 매일 단위의 생성이며, 현재 날짜와 시간을 기반으로 C:₩inetpub₩logs₩LogFiles 디렉터리에 u_exyymmdd.log와 같은 파일 형태로 기록됨

13 윈도우 로그 형식 살펴보기

3 로깅 기능



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017