CASTLE 사용자 설명서

(ASP 버전)

2009. 1.

KrCERT/CC
인터넷 침해 대응 센터

한국인터넷진흥원
Korea Internet & Security Agency

<목 차>

본 문서는 최근 해킹에 주로 이용되고 있는 주요 웹 보안 취약점으로 인한 피해 감소를 목적으로 한국인터넷진흥원 인터넷침해대응센터 해킹대응팀 연구원들과 국내 웹 보안 및 웹 어플리케이션 전문가의 참여를 통해 제작되었습니다.

2009년 1월

연구 책임자 : 팀　　장 최중섭
참여 연구원 : 선임연구원 서진원
주임연구원 한단송
주임연구원 주필환
외부 전문가 : 전남대학교 이재서
감　수 : 보안전문가 김종회

제 1 장 활용에 앞서

기존의 침해사고에서 공격자들은 운영체제 취약점이나 시스템 어플리케이션 취약점을 주로 공격에 이용하였다. 하지만 최근에는 홈페이지 운영에 필요한 웹 어플리케이션 취약점을 공격에 많이 사용하고 있다.

웹 어플리케이션 취약점은 다른 해킹 기법과 비교하여 상대적으로 낮은 수준의 기술로도 해킹이 가능하고, 이를 이용해 많은 사용자들을 대상으로 빠른 시간 내 악성코드의 전파가 가능하다.

웹 어플리케이션 취약점의 보완을 위해서는 취약점의 원인이 되는 소스코드 수정이 필요하나 대부분의 중소 홈페이지의 경우, 개발인력의 미비로 인해 침해사고가 지속적으로 재발하는 문제가 발생하고 있다. 이러한 문제점을 해결하기 위해서 KISA에서는 안전한 웹 어플리케이션의 소스코드를 제작해 보급하였으며 공개 웹방화벽을 보급하여 웹 어플리케이션의 취약점을 차단하고자 하는 많은 노력을 기울이고 있다.

본 문서는 ASP 환경에서 사용할 수 있는 CASTLE(“홈페이지를 보호하는 성벽“이라는 의미)의 사용법을 설명한다. 개발자들은 개발 단계부터 CASTLE을 적용하여, 웹 보안성을 강화를 할 수 있도록 한다. 웹 어플리케이션의 소스코드를 수정하기 힘든 관리자 또한 간단한 작업만으로도 본 도구를 적용할 수 있다.

CASTLE을 가장 일반적인 웹 개발 환경에서 적용 가능하도록 제작하였다. 각 기관의 웹 개발 환경 및 서비스가 매우 다양하므로, 정상적인 서비스에 지장이 없도록 충분히 최적화 작업 및 테스트를 해야 한다. 아무쪼록 본 프로그램이 국내 홈페이지에 대한 피해사고 감소와 홈페이지 관리자의 보안작업에 도움이 되길 바란다.

※ 한국인터넷진흥원에서는 CASTLE를 인터넷에서 공개된 WSM(Web Security Module)을 개발한 외부전문가와 함께 개발했다. 사용자의 편리성 및 보안성 강화 기능을 추가적으로 개발하여 기존 버전과 많은 변화를 보였다.

□ CASTLE의 주요기능

o 보안성 강화
- OWASP 10대 주요 취약점 해결
- 소스코드 수준의 웹 어플리케이션 보안성 강화

o 사용자 편리성 강화
- 관리기능으로 편리한 정책 설정 지원
- 운영 중인 프로그램 소스의 최소 수정으로도 적용 가능

o 높은 호환성 지원
- 다양한 웹 서버 환경과 웹 어플리케이션에서 동작할 수 있는 호환성 지원

□ 기대효과

o CASTLE 확산으로 국내 웹 어플리케이션의 보안성 향상
o 개발자들은 개발 단계에서부터 CASTLE을 통합적으로 적용하여 보안성 강화
o 서버 관리자들은 편리한 사용과정을 통해 기존 웹 어플리케이션 수정용이

제 2 장 설치 및 적용

2장 설치 및 적용에서는 CASTLE 설치 전 준비 사항과 단계별 설치 방법에 대해서 설명한 후 CASTLE 적용방법에 대해 설명한다.

1. 지원 환경

CASTLE ASP 버전은 다음과 같은 환경에서 정상적으로 동작한다.

운영체제	Windows 계열
웹서버	IIS 모든 버전
ASP버전	1.x ~ 2.0

2. 설치 준비

■ 설치 사전 준비

CASTLE ASP 버전을 윈도우에 설치하기 전에 미리 추가해야할 컴포넌트가 존재한다. 소스와 함께 CAPICOM 컴포넌트를 마이크로소프트사의 홈페이지에서 다운로드 하여, 윈도우 레지스트리에 등록하는 과정이 필요하다. CAPICOM은 윈도우에서 암호화에 관련 있는 라이브러리들을 COM 개체 형태로 제공 한다. 다운로드 위치는 다음과 같다.

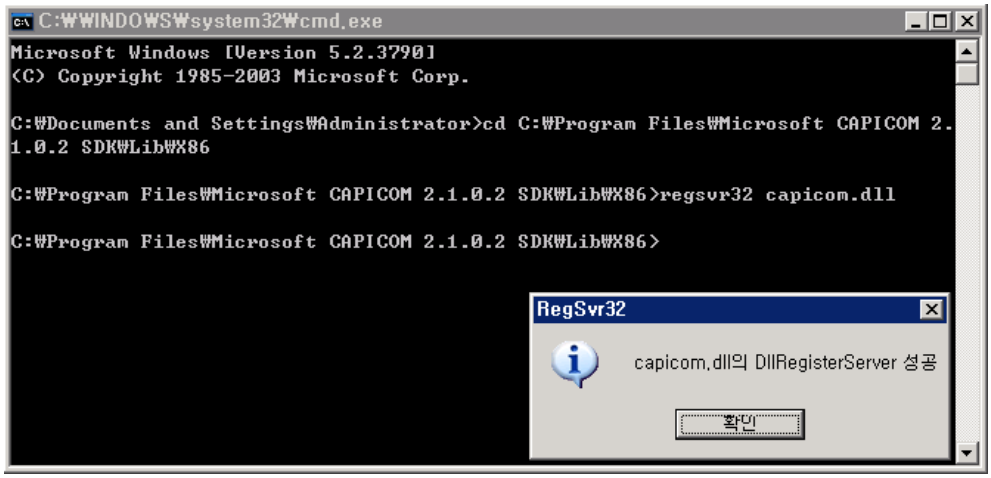
http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=860EE43A-A843-462F-ABB5-FF88EA5896F6

전체패키지를 설치하거나, 압축을 풀어서 『capicom.dll』만 등록하여

도 무방하다. 전체 패키지를 설치했다면, 『capicom.dll』 파일이 존재하는 폴더로 이동해서 이 파일을 레지스트리에 등록한다.

등록 절차는 다음과 같다. 윈도우 시작버튼 -> 실행 -> 'cmd' 명령을 통해서 『capicom.dll』 파일이 존재하는 디렉토리에서 다음과 같은 명령을 실행한다.

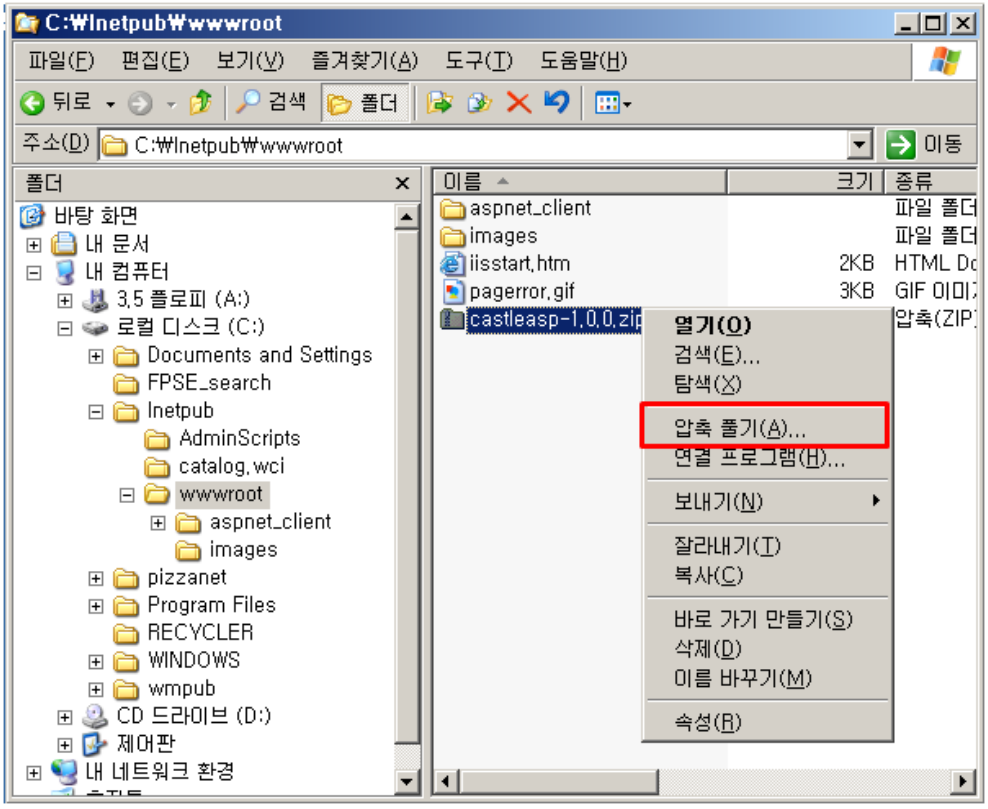
> regsvr32 capicom.dll Enter↵



■ 설치 준비

설치를 위해 최신 버전의 CASTLE 패키지를 CASTLE 배포 공식 사이트에서 다운로드 받는다. CASTLE 패키지는 CASTLE ASP(castleasp), JSP(castlejsp), PHP(castlephp) 버전을 모두 포함하고 있다. 적용하고자 하는 웹 사이트의 프로그래밍 언어에 따라 해당 버전을 웹 서버로 업로드 해야 한다.

※ CASTLE 배포 공식 사이트: http://www.krcert.or.kr



3. 설치 과정

CASTLE 설치 과정은 총 4단계로 1. 설치 동의, 2. 권한 설정, 3. 문자셋(charset) 설정, 4. 관리자 계정 설정으로 이루어진다.

o 설치 페이지 주소 http://서버주소/CASTLE설치디렉터리/install.asp

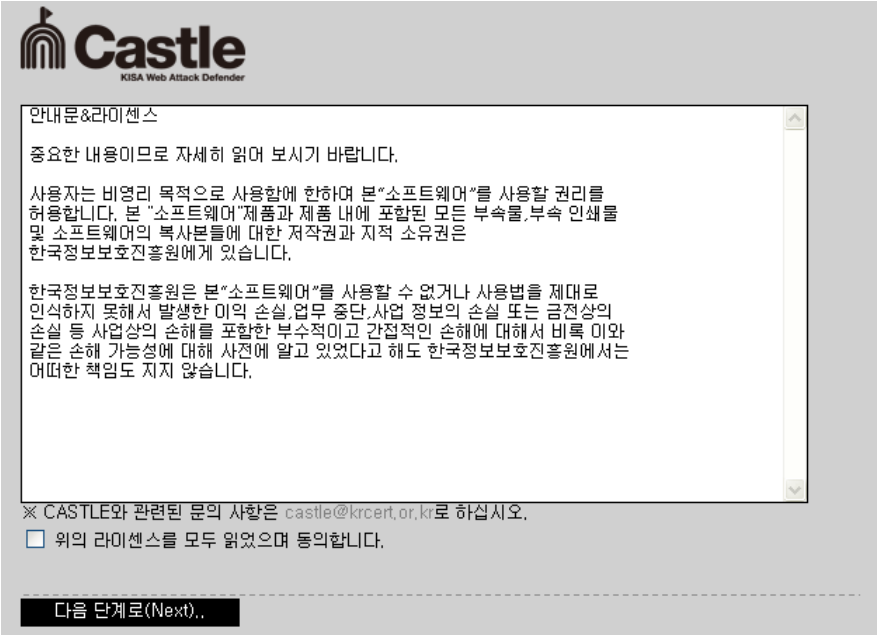
CASTLE 설치 초기 페이지는 위와 같이 install.asp 파일이다. 앞의 설치 준비 과정을 통해 압축 해제한 위치를 웹 브라우저를 통해 연결할 수 있다.

o 테스트 설치 환경
- 기본 URL : http://test.com
- CASTLE 설치상대경로 : /castleasp
- CASTLE 설치전체경로 : http://test.com/castleasp/install.asp

■ 설치 1단계 - 설치 동의 단계

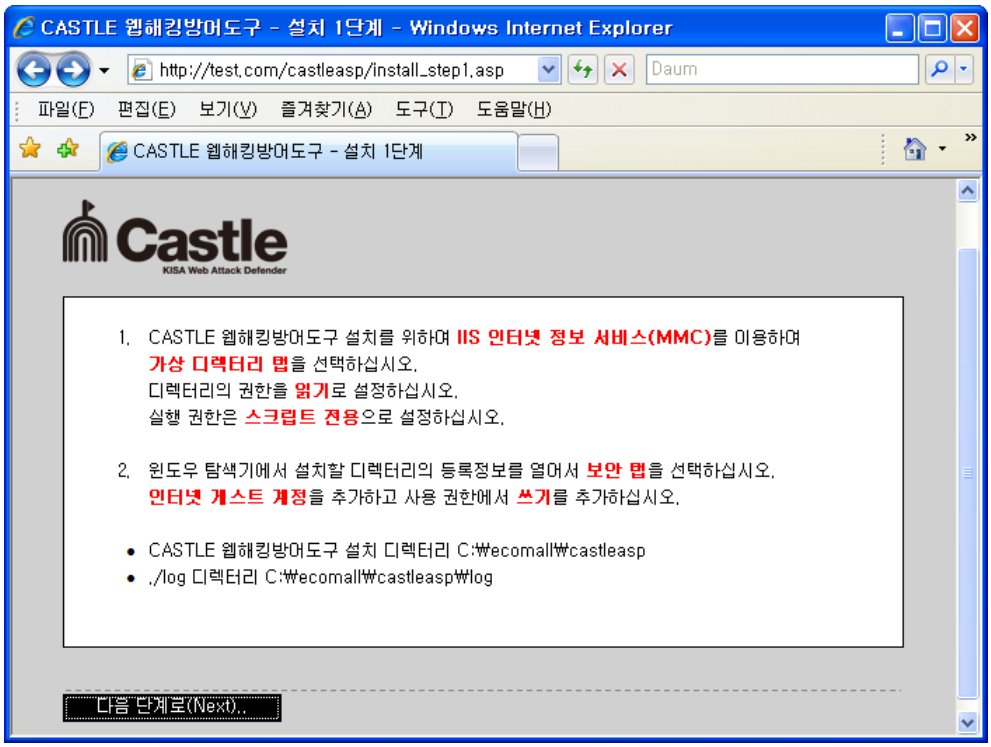
설치를 위해서 웹 브라우저를 이용하여 위의 설치전체경로에 접근하면 아래의 그림과 같이 안내문과 라이센스를 확인하는 화면이 나타난다. 현재 CASTLE를 무료로 공개하기 때문에 바로 "**위의 라이센스를 모두 읽었으며 동의합니다.**"를 클릭하고 다음 단계로 진행한다.

※ 설치 전체 경로 : http://test.com/castleasp/install.asp

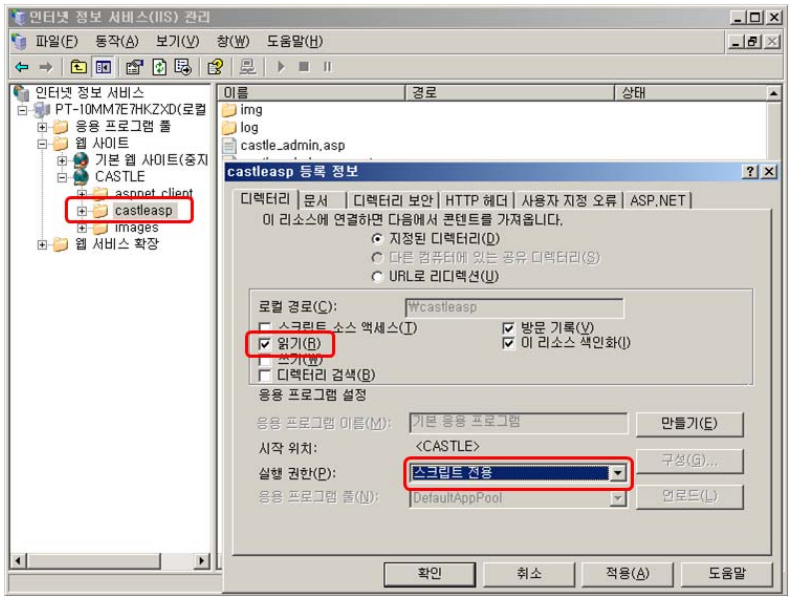


■ 설치 2단계 - 권한 설정 단계

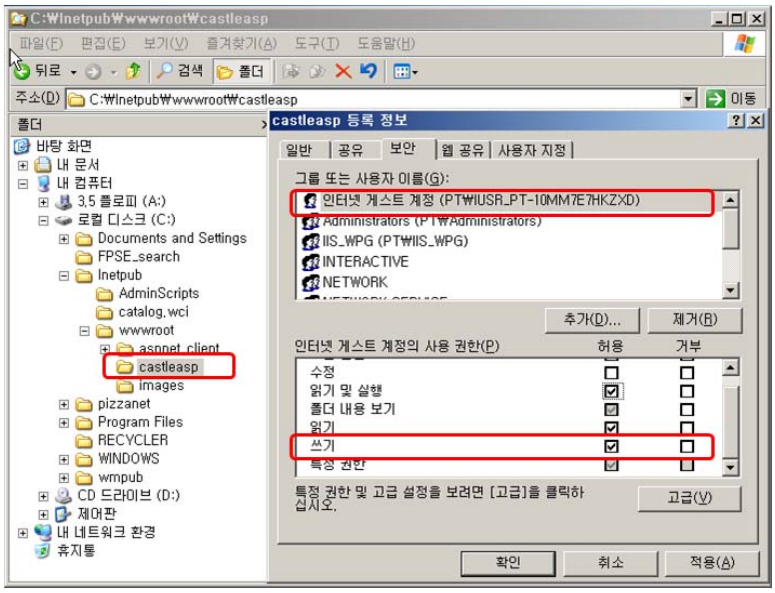
권한 설정 단계는 설치하고자 하는 시스템에 쓰기 권한을 설정했는지 확인하는 단계이다. 정상적인 웹 서비스를 위해 IIS 인터넷 정보 서비스 관리의 대화상자에서 쓰기 권한을 줘야 한다.



먼저 IIS 인터넷 정보 서비스(IIS) 관리 대화상자에서 왼쪽창의 리스트에서 '**웹 사이트**'의 트리를 확장하여, '**기본 웹 사이트**' 하위의 『castleasp』에 폴더의 등록 정보를 열다. castleasp 등록 정보 대화상자에서 디렉터리 탭을 선택한다. 각각의 설정 값 중에서 로컬 경로(C)의 '**읽기**', 실행 권한(P)가 '**스크립트 전용**'에 체크되어 있는지 확인한다. 대부분 디폴트 값으로 설정되어 있다.



또한, 윈도우 탐색기에서 등록정보의 보안 탭을 이용하여 인터넷 게스트 계정이나 Everyone 계정에 쓰기 권한을 추가해야 한다.



권한 설정이 완료되면 다음단계인 문자셋 설정 단계로 진행한다.

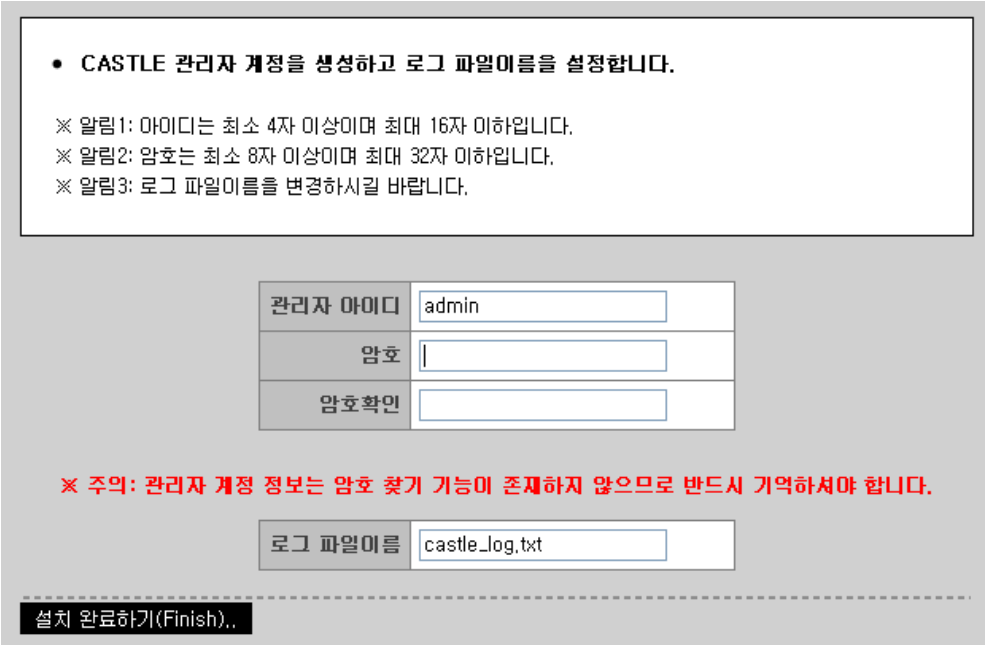
■ 설치 3단계 - 문자셋 설정 단계

문자셋 설정은 CASTLE를 적용하고자 하는 서버나 웹 페이지의 문자셋에 맞추어 설정한다. 제대로 설정하지 않은 경우, CASTLE 메시지를 확인할 때 글자들을 깨진 상태로 출력할 수 있다. 다음과 같은 방법으로 웹 페이지의 문자셋을 정확한 문자셋으로 설정하고, 다음 단계인 관리자 계정 설정 단계로 진행한다.

ASP 버전의 경우, IIS 웹 서버에서, CASTLE을 적용하는 각 웹 페이지들의 문자 인코딩 저장 방식과 관련이 있다. 적용하고자 하는 웹 페이지들의 문자셋에 맞게 설정한다. CASTLE ASP 버전은 한글 지원을 위해, EUC-KR과 UTF-8 인코딩 방식을 지원한다.

■ 설치 4단계 - 관리자 계정 설정 및 로그 파일 이름 설정 단계

관리자 계정은 CASTLE 관리자 페이지에 인증을 하기 위한 관리자 계정이다. 아이디와 암호는 보안상 아주 중요하기 때문에 쉽지 않은 암호로 생성하길 바란다. **아이디와 암호는 찾기 기능이 없으므로 반드시 기억해야 하며 아이디와 암호를 잃어버린 경우에는 재설치 과정을 거쳐야 하므로 주의하길 바란다.** 보안을 위해 로그 파일 이름을 관리자가 직접 설정하도록 하였으므로, **로그파일 이름을 다른 이름으로 변경한다.**



아이디와 **암호, 암호확인**을 정확히 입력하고, 로그 파일명을 변경 후 "**설치 완료하기(Finish)**" 버튼을 누르면 "**설치가 완료되었습니다.**"라는 메시지와 함께 설치를 완료한다.

4. 적용 과정

CASTLE을 각 웹 페이지나 프로그램에 적용하기 위해서는 적용하고자 하는 대상 파일에 아래와 같은 코드를 추가해야 된다. 예를 들어 『http://test.com/test.asp』웹 프로그램에 CASTLE를 적용한다면 『test.asp』파일의 첫 줄에 아래와 같은 코드를 추가해야 한다. 주로 모든 페이지에서 include하여 사용하는 설정파일, 『config.asp』와 같은 헤더 파일에 아래와 같이 적용하면, 각각의 페이지에 추가해야 하는 수고를 덜 수 있다.

```
<%
Application("CASTLE_ASP_VERSION_BASE_DIR") = "CASTLE 설치 URL 절대 경로"
Server.Execute(Application("CASTLE_ASP_VERSION_BASE_DIR") &
"/castle_referee.asp")
%>
```

추가할 소스코드의 내용은 위와 같다. 위 코드에서 "**CASTLE 설치 URL 절대 경로**" 부분을 CASTLE 프로그램을 도메인 이후의 경로로 수정해야 한다. 예를 들어 CASTLE의 첫 설치 페이지가 "http://test.com/castleasp/install.asp"이라면 CASTLE 설치 URL 절대 경로는 "/castleasp"로 수정하고, 설치할 웹 페이지 첫줄에 추가한다.

※ 즉, CASTLE를 적용하고자 하는 웹사이트에 공통으로 참조하는 파일(헤더파일)이 있다면 그 파일에만 적용하면 모든 적용을 완료할 수 있다.

제 3 장 관리자 페이지 설명

3장 관리자 페이지 설명에서는 CASTLE 관리자 페이지의 화면구성을 차례대로 설명한다. 관리자 페이지는 웹 브라우저를 통해 다음과 같이 입력하여 접근할 수 있다.

o 관리자 페이지 주소:
http://서버주소/CASTLE설치디렉터리/castle_admin.asp

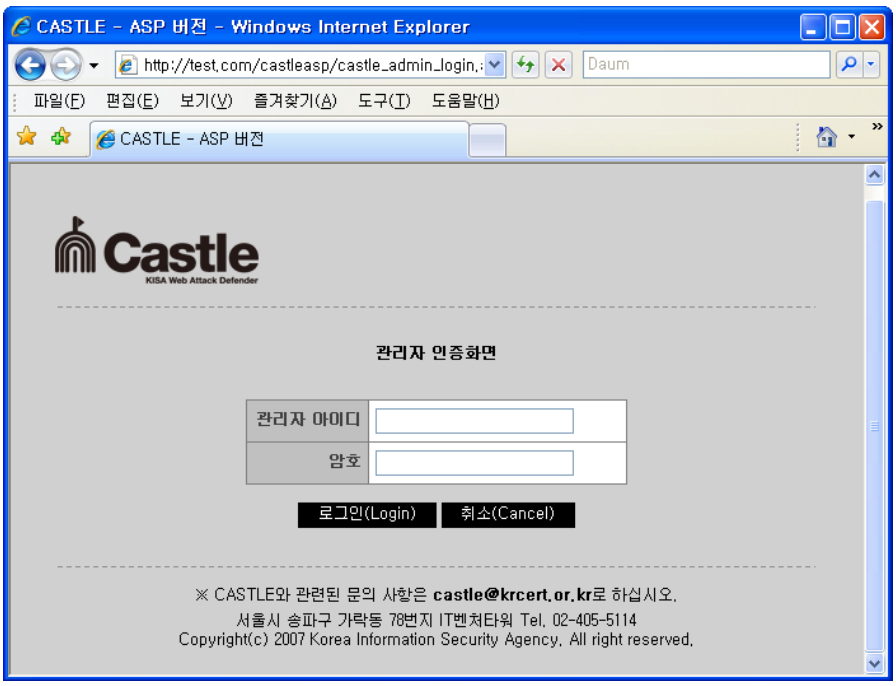
로그인을 하지 않고 관리자 페이지에 연결하는 경우, 인증 화면으로 이동한다.

o 테스트 관리자 페이지 환경
- 기본 URL : http://test.com
- CASTLE 설치상대경로 : /castleasp
- CASTLE 관리자 페이지 전체경로 : http://test.com/castleasp/castle_admin.asp

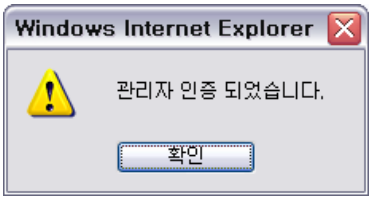
■ 관리자 인증

관리자 페이지에 인증하기 위해서는 반드시 로그인 과정을 통해 인증을 거쳐야 한다. 인증하지 않은 경우, 바로 다음 그림과 같은 인증 페이지로 이동한다.

※ 관리자 페이지 전체경로 : http://test.com/castleasp/castle_admin.asp

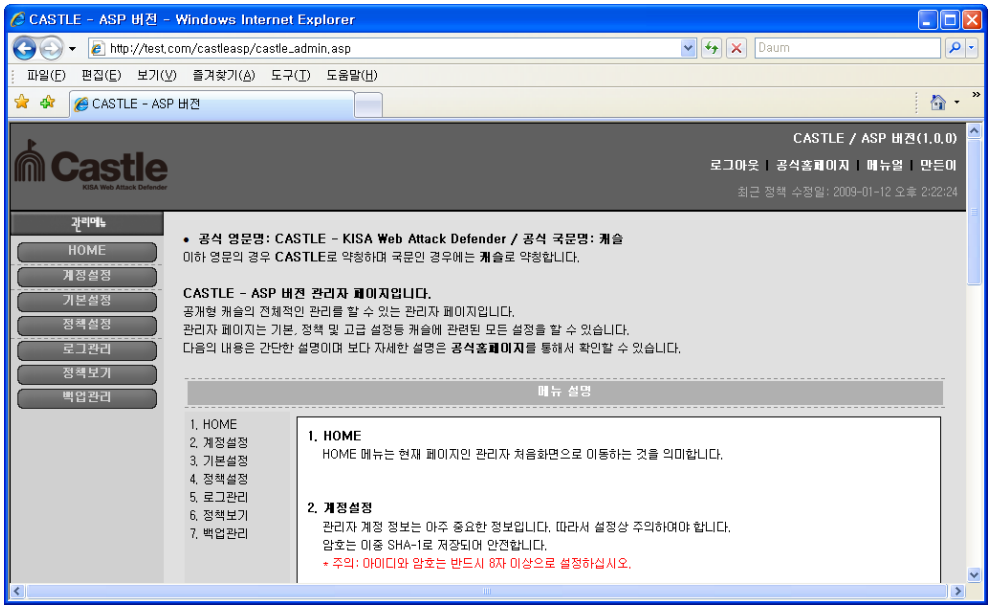


설치 과정에서 생성한 관리자 계정 정보를 통해 인증을 수행할 수 있다. 정확히 아이디와 암호를 입력하고 "**로그인(Login)**" 버튼을 누르면 다음과 같이 "**관리자 인증 되었습니다.**" 라는 메시지와 함께 인증된다.



■ 관리자 페이지 초기 화면

관리자 페이지 초기 화면은 다음 그림과 같이 각 관리 메뉴별로 간단한 설명을 담고 있다. 관리자 페이지는 윗부분에 **공식홈페이지**, **메뉴얼**에 대한 링크가 있으며 왼쪽에 **관리메뉴** 링크가 있다.



■ 관리자 페이지 메뉴별 설명

관리자 페이지는 7개 메뉴로 구성되어 있다.

o HOME
- HOME 메뉴는 현재 페이지인 관리자 처음화면으로 이동
- 링크: castle_admin.asp

o 계정설정
- 관리자 계정 아이디와 암호를 설정함
- 링크: castle_admin_account.asp

o 기본설정
- CASTLE 이름, 적용 여부, 메시지 방식 등 기본적인 운영에 관련된 정책을 설정
- 링크: castle_admin_config.asp

o 정책설정
- 실제 공격을 탐지 및 차단하는 정책
- 각 정책은 정규표현식을 지원함
- 링크: castle_admin_policy.asp

o 로그관리

- 정책에 의해 공격을 탐지한 로그들을 관리
- 링크: castle_admin_log.asp

o 정책보기
- 관리자가 설정한 모든 정책을 확인함
- 링크: castle_admin_policy_view.asp

o 백업관리
- 현재 모든 정책을 관리자 PC에 저장
- 링크: castle_admin_backup.asp

제 4 장 관리자 계정 관리

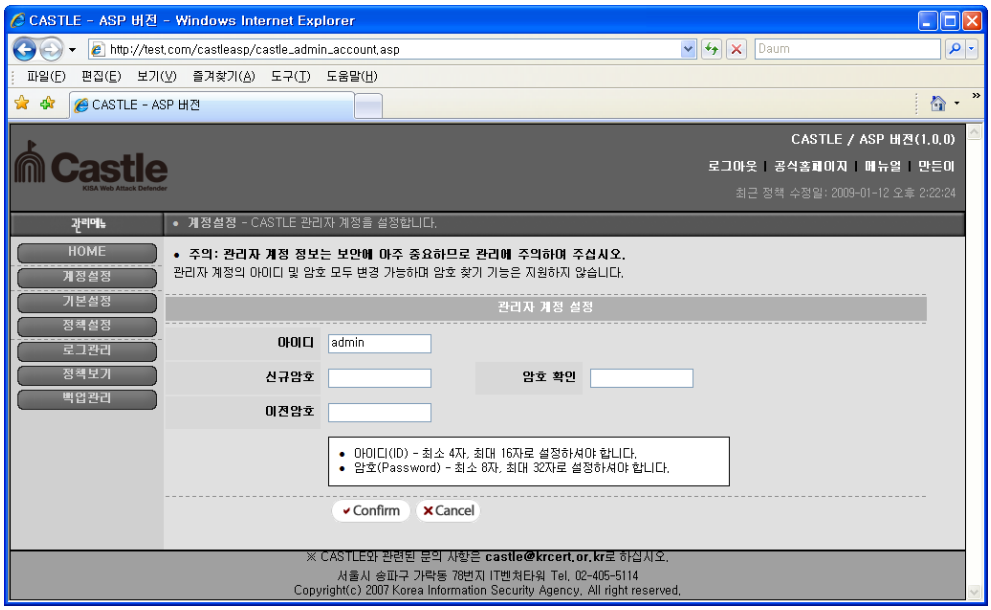
4장 관리자 계정 관리에서는 관리자 페이지 인증을 위한 아이디, 암호를 설정하는 "**계정설정**" 메뉴를 설명한다. 관리자 계정의 아이디와 암호는 보안상의 이유로 상당히 긴 문자열로 구성하도록 하였다.

■ 아이디 설정 규칙

아이디는 최소 4자, 최대 16자의 문자열 또는 숫자로 구성해야 한다.

■ 암호 설정 규칙

암호는 최소 8자, 최대 32자의 문자열 또는 숫자로 구성해야 한다.
(MD5 해쉬 구조로 암호화되어 저장)



새로운 관리자 아이디와 암호, 암호 확인을 입력하고 이전 암호를 정확히 입력하면 "**관리자 계정 정보가 수정되었습니다.**" 메시지와 함께 설정을 완료한다.

제 5 장 기본 설정

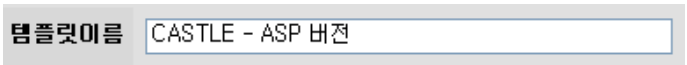
5장 기본 설정에서는 CASTLE에 대한 가장 중요한 부분으로 **기본설정, 사이트 설정, 적용대상** 등 운영에 관련된 정책 설정에 대하여 설명한다.

1. 기본 설정

기본 설정에서는 **이름, 집행모드** 그리고 **알림방식**에 대해서 설정한다.

■ 이름 설정

설치한 CASTLE 관리자 페이지의 이름을 설정한다. 설정된 CASTLE 이름을 각 관리자 페이지의 타이틀(title)에 표시하며 관리자가 임의대로 이름을 설정할 수 있다.



■ 집행모드 설정 (*설정상 주의필요)

집행모드 설정은 CASTLE 설정에 있어서 가장 중요한 부분으로 설치한 CASTLE를 실제 집행할 것인지 혹은 설치만하고 집행하지 않을 것인지 등을 설정한다. 집행모드에는 총 3개의 모드가 있으며 **적용모드**, **감사모드** 그리고 **비적용모드**가 있다.

o 적용모드(enforcing)

- 집행모드를 적용모드로 설정할 경우, CASTLE에서 정의한 정책들에 의해 탐지를 수행하고, 차단 또는 허용한다.

o 감사모드(permissive) - 기본 설정 상태

- 감사모드로 설정한 경우에는 적용모드와 마찬가지로 CASTLE에서 정의한 정책들에 의해 탐지를 수행하지만 **무조건 허용함**
- 설치 초기에 정책을 작성하는 과정에 감사모드로 정책의 안정화하는 것이 좋음
- 정의한 정책에 의해 탐지한 것들은 로그 파일로 기록하므로, 로그를 확인하여 운영하는 사이트 환경에 맞게 정책 수정이 필요

o 비적용모드(disabled)

- 비적용모드로 설정되어 있을 경우에는 CASTLE이 적용되지 않음

■ 알림방식 설정

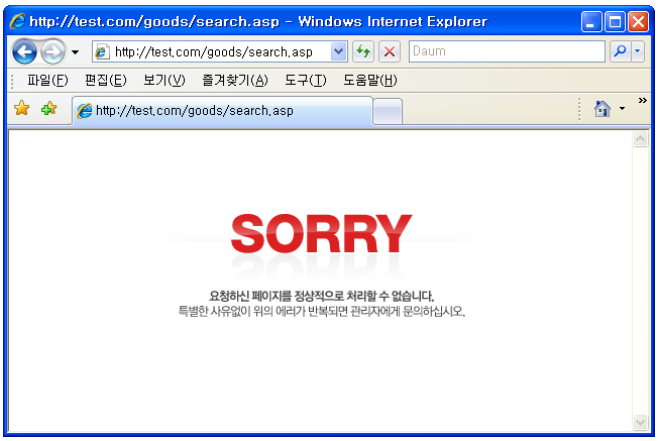
알림방식 설정은 **집행모드를 적용모드**로 설정했을 때 비정상적인 행위로 탐지되어 사용자의 접근이 차단할 필요가 있을 경우 어떻게 차단할 것인지에 대한 설정이다. 알림방식에는 **경고모드**, **알림모드** 그리고 **스텔스모드**가 있다.

o 경고모드(alert)

- 집행 결과를 **경고창**으로 알리며, 차단 사유에 대해 상세한 정보를 관리자에게 곧바로 결과를 알리고자 할 때 설정
- 관리자가 디버깅 할 때 유용하게 사용할 수 있음

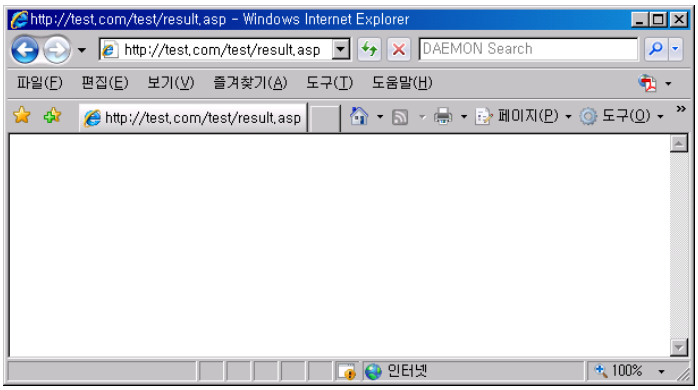
o 메시지모드(message)

- 집행 결과를 메시지로 알림



o 스텔스모드(stealth)

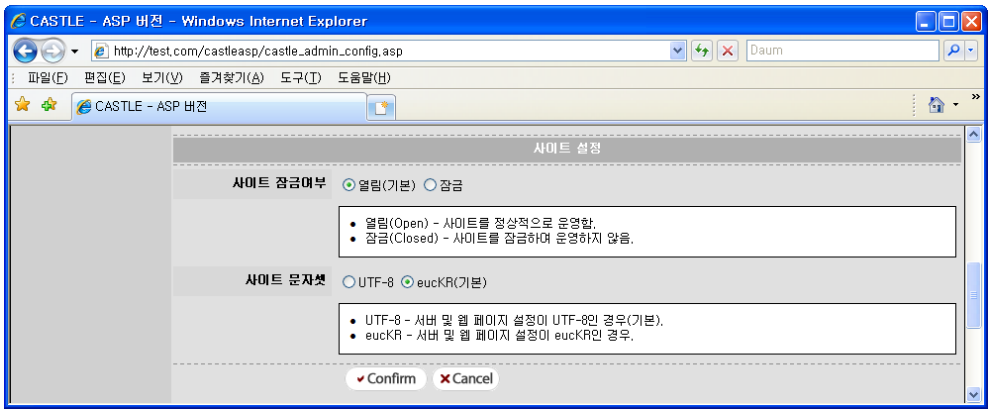
- 빈 페이지를 출력한다.
- CASTLE 운영 사실을 숨기고자 할 때에 유용함



2. 사이트 설정

사이트 설정에서는 현재 운영 중인 사이트에 대한 전반적인 설정으로 현재 운영 중인 사이트를 잠글 것인지 서비스할 것인지에 대한 설정과 사이트의 문자셋이 무엇인지를 설정한다. 지원하는 문자셋으로는 **UTF-8**

과 **EUC-KR**이 있다.



■ 사이트 잠금여부 설정

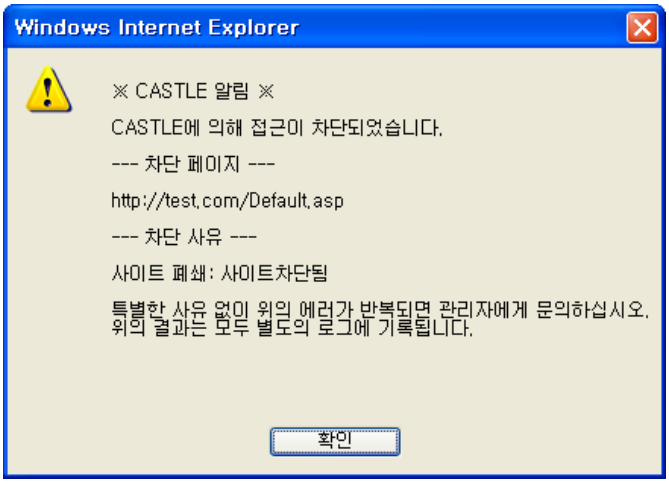
CASTLE 설치되어 운영 중인 사이트를 일시적으로 또는 영구적으로 차단할 수 있다.

o 열림

- 사이트를 정상적으로 운영함

o 잠금

- 사이트를 잠그고 운영하지 않음, 다음의 그림은 사이트가 잠긴 화면



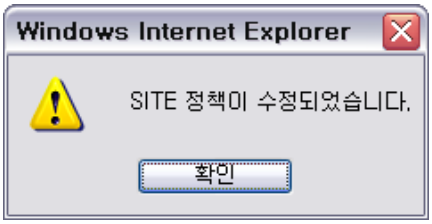
■ 사이트 문자셋 설정

CASTLE를 설치 운영하고자 하는 웹 페이지나 웹 서버의 설정에 따라 문자셋(charset)을 설정한다. 국내에서 주로 사용되는 UTF-8와 EUC-KR 두 개의 문자셋 만을 제공하며 문자셋이 잘못 설정될 경우에 각 에러 메시지들이 깨져서 보이게 되므로 정확하게 설정해야 한다.

o UTF-8
- 서버 및 웹 페이지 설정이 UTF-8인 경우

o EUC-KR(CP949)
- 서버 및 웹 페이지 설정이 EUC-KR(CP949)인 경우

정상적으로 문자셋을 설정했을 경우에는 다음의 그림과 같이 문제없이 알림 메시지를 볼 수 있다.



※ CASTLE ASP 버전은 문자셋 설정과 상관없이 에러 메시지는 정상적으로 동작하도록 작성하였다.

3. 적용대상 설정

적용대상 설정은 CASTLE 에 의해서 탐지할 대상들에 대한 설정이다. 기본으로 GET, POST, COOKIE 등에 전역변수들을 대상으로 탐지를 수행할 수 있다.

■ GET 변수 설정

GET 변수들을 대상으로 탐지 수행 여부를 설정한다.

■ POST 변수 설정

POST 변수들을 대상으로 탐지 수행 여부를 설정한다.

■ COOKIE 변수 설정

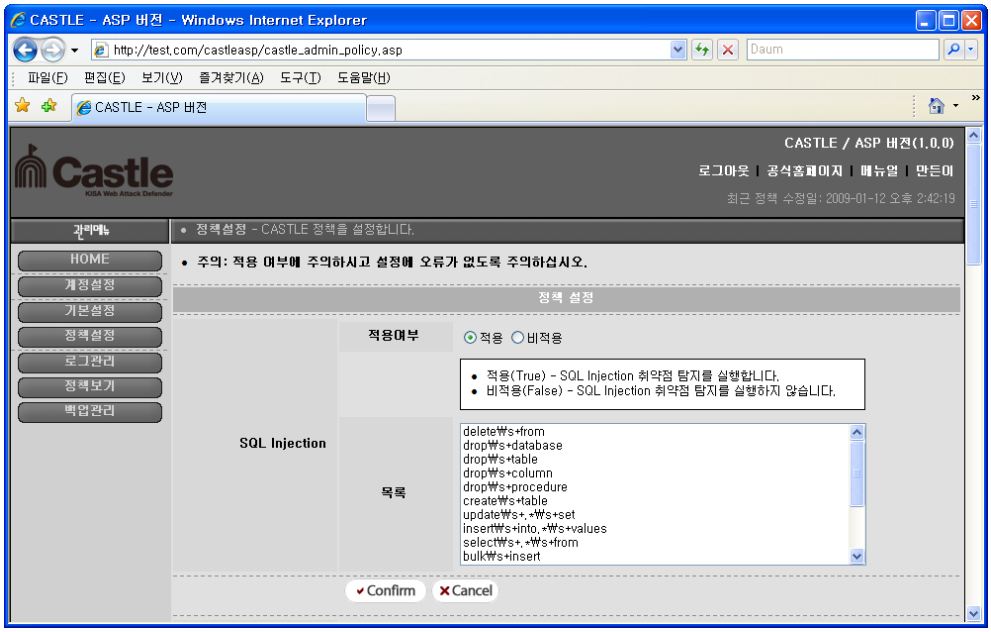
COOKIE 변수들을 대상으로 탐지 수행 여부를 설정한다.

제 6 장 정책 설정

6장 정책 설정에서는 CASTLE에서 탐지할 공격 형태들을 유형별로 설정한다. 대표적인 공격들인 **SQL Injection, XSS, 금칙어(WORD), 불량태그(TAG), IP, 파일**별로 정책을 설정할 수 있다.

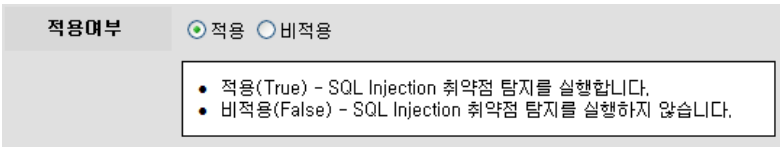
1. SQL Injection 정책 설정

SQL Injection 공격 형태를 정규표현식 형태로 설정할 수 있다. 이렇게 설정한 정규표현식 규칙에 포함되는 모든 공격을 탐지할 수 있다.



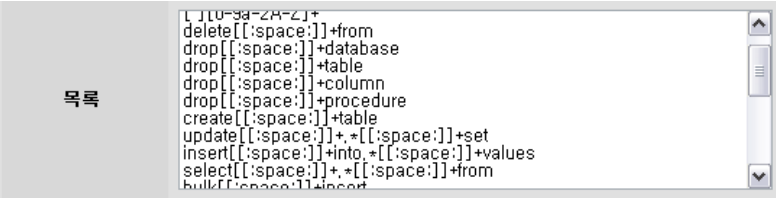
o 적용여부

- SQL Injection 공격 탐지 수행 여부를 설정한다.



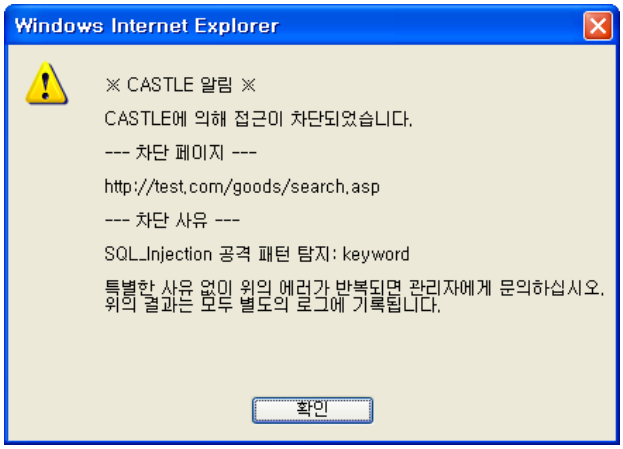
o 목록

- SQL Injection 공격 형태를 정규표현식으로 설정한다.
- 필요한 경우 목록에 정규표현식으로 룰을 추가하고 'Confirm' 버튼을 누르면 새로운 룰을 추가한다.



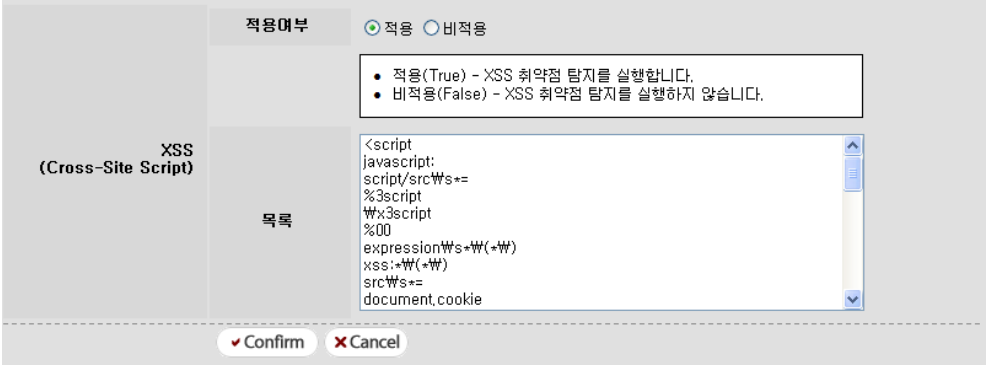
■ SQL Injection 공격 탐지 차단

변수에 "1 or 1 --"와 같이 목록에 포함된 형태의 SQL Injection 공격 코드를 넣었을 때 다음과 같이 탐지하고, 차단한다.



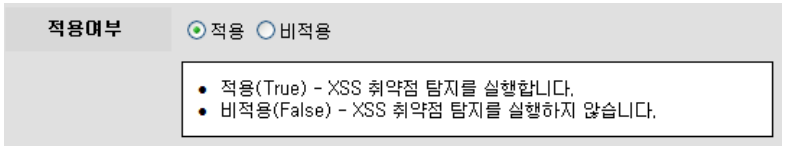
2. XSS 정책 설정

XSS 공격 형태를 정규표현식 형태로 설정할 수 있다. 이렇게 설정된 정규표현식 규칙에 포함되는 모든 공격을 탐지한다.



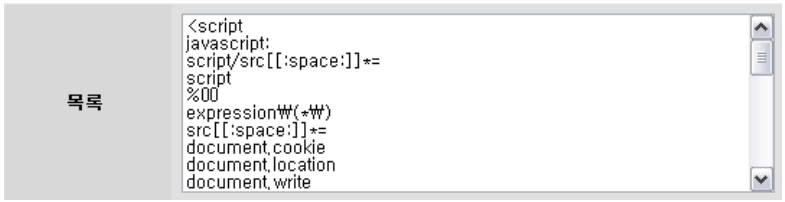
o 적용여부

- XSS 공격 탐지 수행 여부를 설정한다.



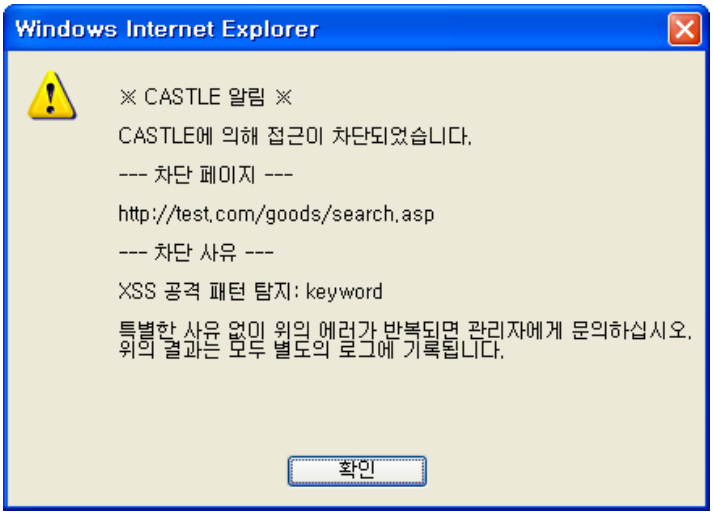
o 목록

- XSS 공격 형태를 정규표현식으로 설정한다.



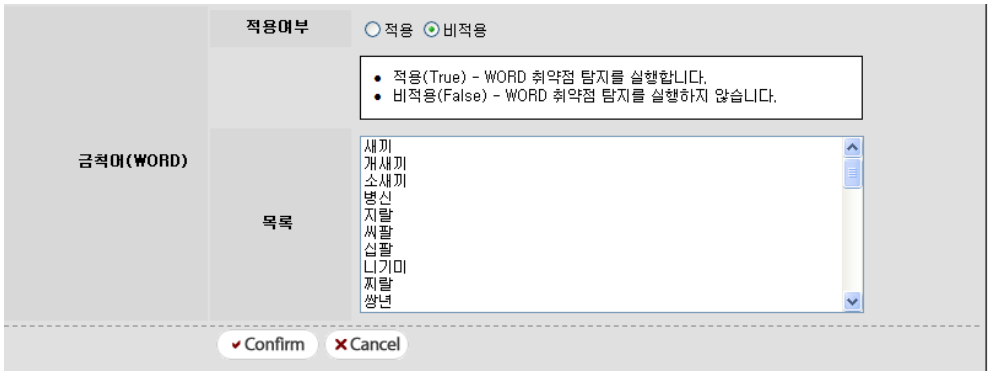
■ XSS 공격 탐지 차단

변수에 “javascript:“와 같이 목록에 포함된 형태의 XSS 공격 코드를 넣었을 때 다음과 같이 탐지하고 차단한다.



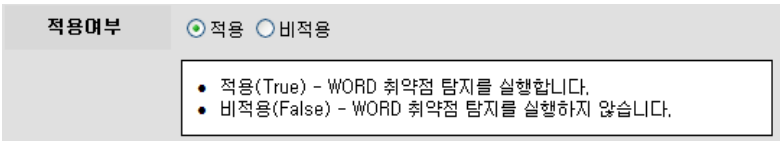
3. 금칙어 정책 설정

금칙어 형태를 정규표현식 형태로 설정할 수 있다. 이렇게 설정된 정규표현식 규칙에 포함되는 모든 공격을 탐지한다. 금칙어는 스팸성 글이나 악성 댓글을 차단하는데 유용하다.



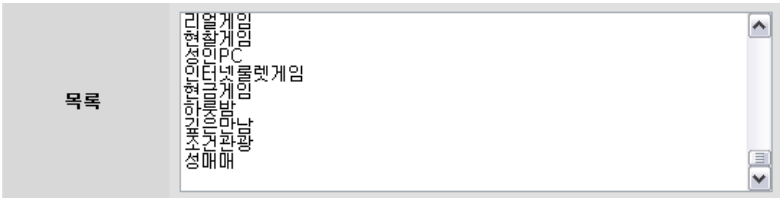
o 적용여부

- 금칙어 탐지 수행 여부를 설정한다.



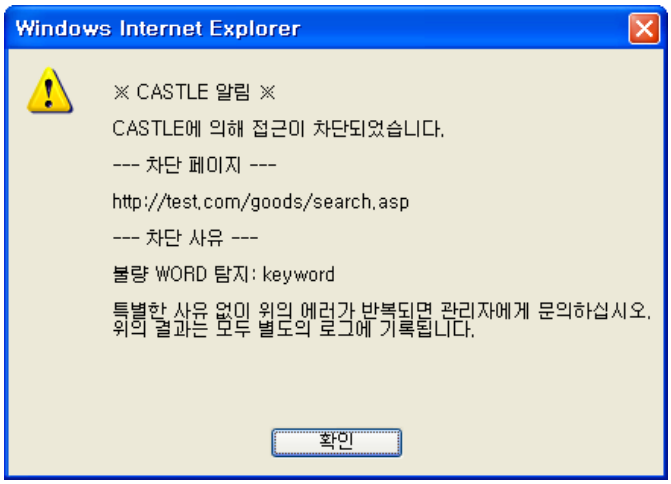
o 목록

- 금칙어 형태를 정규표현식으로 설정한다.



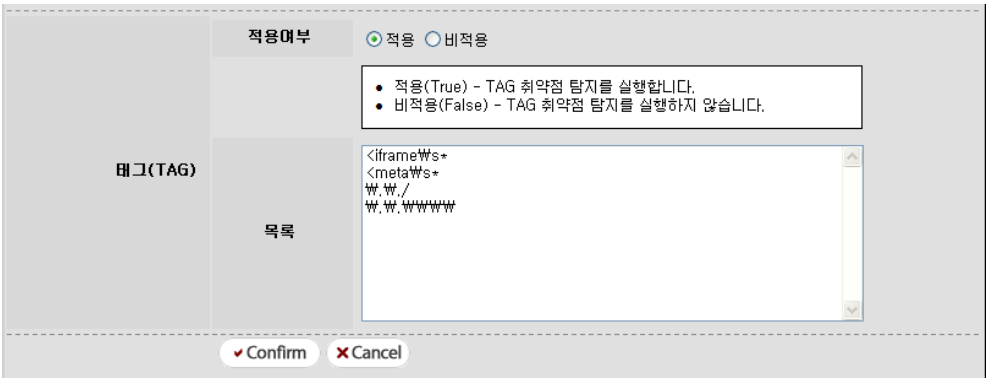
■ 금칙어 차단

변수에 "**현찰게임**와 같이 목록에 포함된 형태의 금칙어를 넣었을 때 다음과 같이 탐지하고, 차단한다.



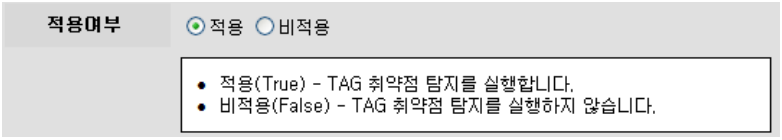
4. 불량태그 정책 설정

불량태그는 악의적인 용도로 자주 쓰이는 태그(tag)를 의미한다. 불량태그 형태를 정규표현식 형태로 설정할 수 있다. 이렇게 설정된 정규표현식 규칙에 포함되는 모든 공격을 탐지한다.



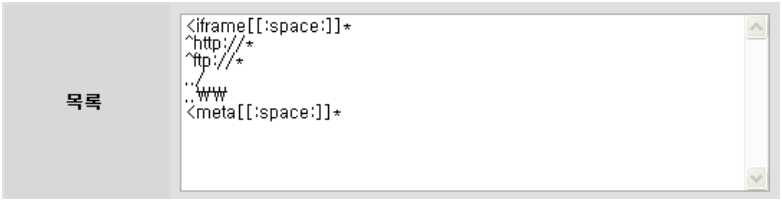
o 적용여부

- 불량태그 공격의 탐지 수행 여부를 설정한다.



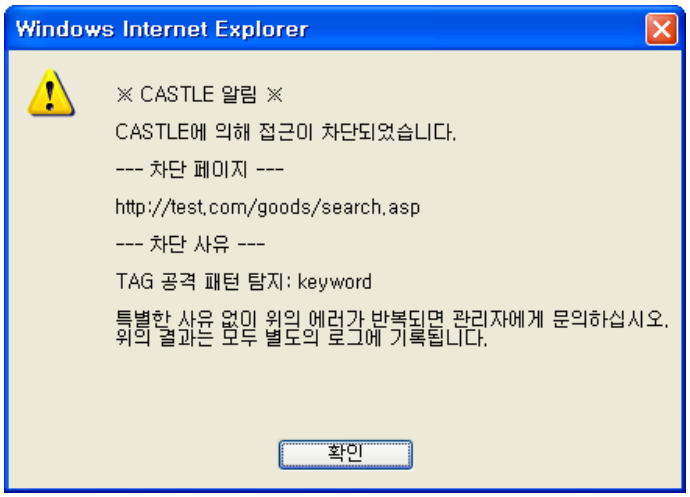
o 목록

- 불량태그 공격 형태를 정규표현식으로 설정한다.



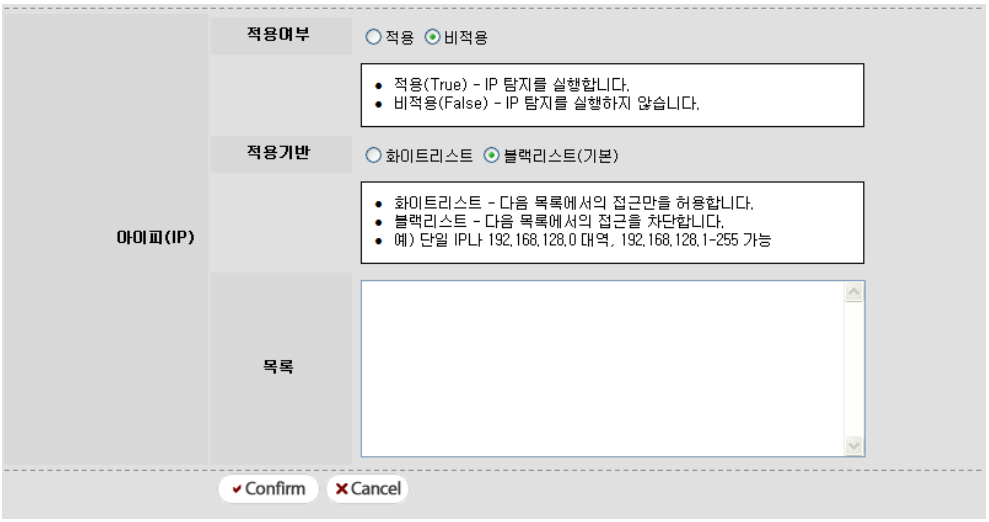
■ 불량태그 공격 탐지 차단

변수에 "**<iframe**"와 같이 목록에 포함된 형태의 불량태그를 넣었을 때 다음과 같이 탐지하고 차단한다.



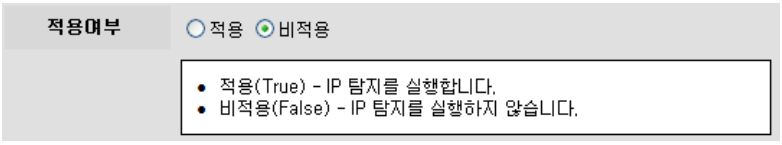
5. IP 정책 설정

IP 정책 설정에서는 IP를 정규표현식 형태로 설정하여 접근 통제한다. 이렇게 설정된 정규표현식 규칙에 포함되는 모든 아이피를 적용기반에 따라 차단하거나 허용한다.



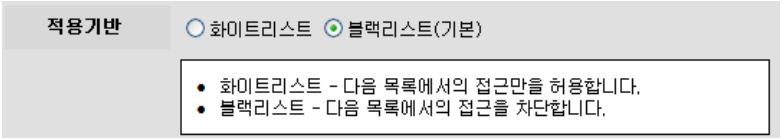
o 적용여부

IP 탐지 수행 여부를 설정한다.



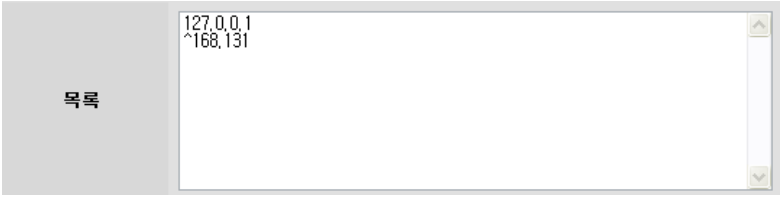
o 적용기반

- 화이트리스트 : 목록에 포함된 IP만 접근을 허용함
- 블랙리스트 : 목록에 포함된 IP 접근을 차단함



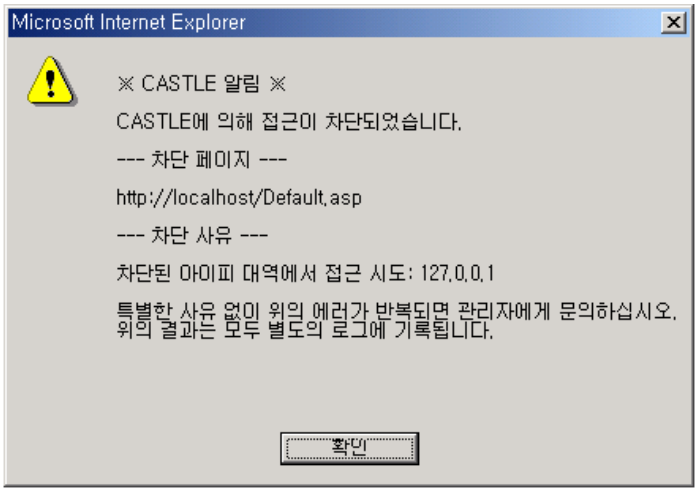
o 목록

- IP를 정규표현식으로 설정한다.



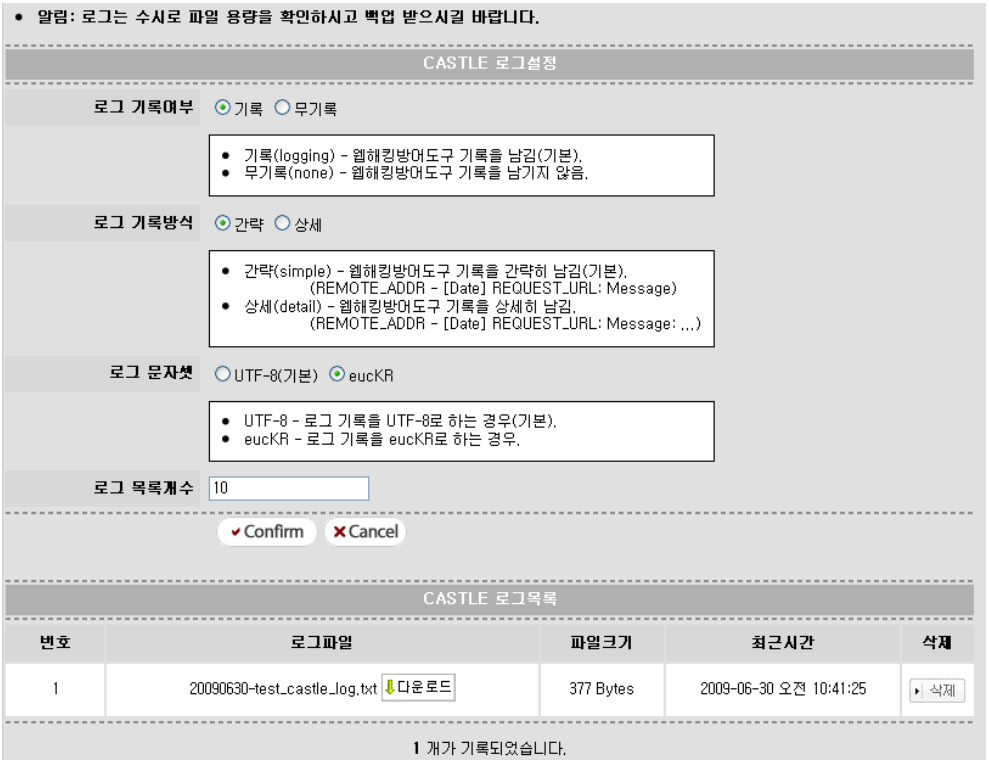
■ 아이피 탐지 차단

위의 그림과 같이 아이피 설정 부분에 블랙리스트 방식으로 "**127.0.0.1**"를 설정하고 접근했을 때 아래 그림과 같이 탐지한다.



제 7 장 로그 관리

7장 로그 관리는 CASTLE에 의해서 탐지된 결과를 저장할 로그 파일에 대한 설정이다. **로그 파일이름**과 **기록여부** 그리고 **기록방식** 등을 설정한다.



■ 로그 파일이름

로그 파일이름은 설치시 관리자가 직접등록 한다.

o 로그 파일 이름 규칙

- Year.Month.Day-로그파일이름(ex. 20071016-castle_log.txt)

■ 로그 기록여부 설정

로그 기록 여부를 설정한다.

o 기록
- 로그를 기록함

o 무기록
- 로그를 기록하지 않음

■ 로그 기록방식 설정

기록할 로그의 방식을 설정한다. 설정에 따라 간략하게 또는 상세하게 로그를 기록할 수 있다. 시스템 디스크 용량이 충분하다면 상세하게 기록하도록 설정할 것을 추천한다.

o 간략
- 로그를 간략하게 기록함

REMOTE_ADDR - [Date] REQUEST_URL: Key = Value: Message
ex)
125.24.15.196 - [19/Nov/2007:15:44:32 +0900] /test/test.asp: memo = 인터넷룰렛 게임,리얼PC게임,성인게임... : 불량 WORD 탐지

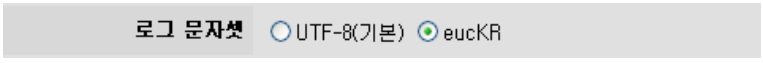
o 상세

- 로그를 상세하게 기록함

```
REMOTE_ADDR - [Date] REQUEST_URL: Key = Value: Message
   --> [Method: method]
   --> [Policy: policy]
   --> [Pattern: pattern]
   --> [Method: method]
   --> [Offset: offset] [Matched-Content: content]
ex)
  125.24.15.196 - [19/Nov/2007:15:44:32 +0900] /test/test.asp: memo = 인터넷룰렛
  게임,리얼PC게임,성인게임... : 불량 WORD 탐지
    -> [Method: POST]
    -> [Policy: 기본정책]
    -> [Pattern: 현금]
    -> [Offset: 123] [Matched-Content: 현금]
    -> [Offset: 231] [Matched-Content: 현금]
    -> [Offset: 472] [Matched-Content: 현금]
    -> [Offset: 921] [Matched-Content: 현금]
    -> [Offset: 2134] [Matched-Content: 현금]
```

■ 로그 문자셋 설정

기록할 로그의 문자셋을 설정한다. 각 시스템의 환경에 맞게 설정한다. 이것을 제대로 설정하지 않으면 나중에 로그를 확인할 때에 글씨가 깨질 수 있으므로 정확히 설정하도록 한다.



■ 로그 목록개수 설정

로그 관리에서 출력할 로그의 개수를 설정한다. 디폴트 20개이다.

■ 로그 목록

일별로 로그를 출력하며 가장 최근의 로그 파일이 제일 위에 놓인다.

CASTLE 로그목록

번호	로그파일	파일크기	최근시간	삭제
1	20090115-castle_log.txt 다운로드	112 Bytes	2009-01-15 오후 3:02:21	삭제
2	20090114-castle_log.txt 다운로드	112 Bytes	2009-01-14 오후 3:02:08	삭제
3	20090113-castle_log.txt 다운로드	112 Bytes	2009-01-13 오후 3:01:47	삭제
4	20090112-castle_log.txt 다운로드	612 Bytes	2009-01-12 오후 2:54:55	삭제

4 개가 기록되었습니다.

제 8 장 정책 보기

8장 정책 보기는 현재 설정된 정책 정보를 트리 구조와 소스 형태로 일괄적으로 확인할 수 있는 기능이다.

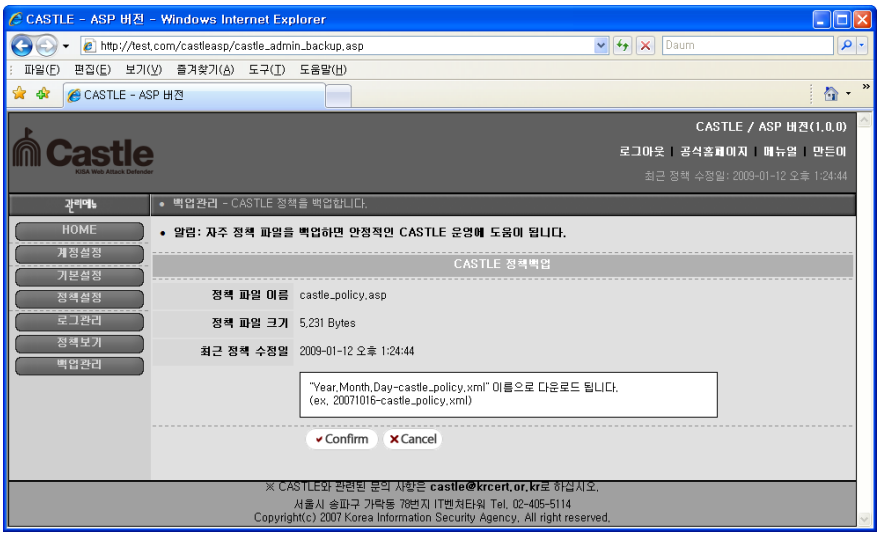
■ 트리구조 정책 보기

정책을 쉽게 확인할 수 있도록 XML 형식의 트리 구조로 구성하였다.

제 9 장 백업 관리

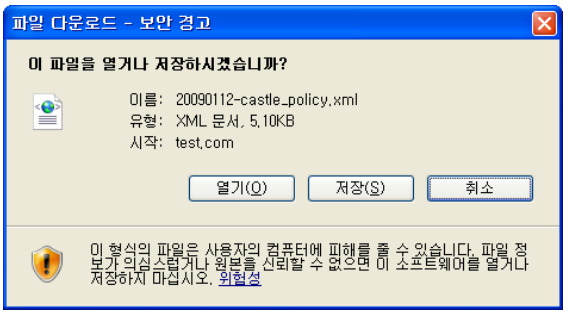
9장 백업 관리는 현재 설정된 정책을 관리자의 개인 PC로 백업하기 위한 기능이다. 현재 **정책 파일의 이름**, **파일 크기** 그리고 "**최근 정책 수정일**"을 확인할 수 있으며 정책을 다운로드 받을 수 있다.

■ 정책 정보 보기



■ 정책 다운로드

"**Confirm**" 버튼을 클릭하면 다음과 같이 정책을 다운로드 받을 수 있다. 정책은 수시로 백업하여 만일의 사태에 대비하기 바란다.



제 10장 마치며...

본 CASTLE를 사용하는 많은 웹 서버 관리자나 개발자들이 웹어플리케이션의 보안성을 강화하고, 보다 안전한 환경에서 사이트를 운영하여 여러분의 소중한 자산을 지켰으면 한다.