CASTLE 사용자 설명서

(PHP Version)

2016. 12.

KISA 한국인터넷진흥원

버 전	계정 내용	개정일
V1.0	- 최초 작성	2014.7
V1.1	- 정책파일 권한변경(p42)추가 - 정책 모든 설정 후 관리자 페이지 접근 제한(p43, p44) 추가	2016.5
V2.0	- 개요(p4) 수정, 불필요한 내용 삭제	2016.12

< 목차 >

제 1 장 개요

최근 홈페이지를 통한 해킹사고가 많이 발생하고 있다. 홈페이지를 통한 해킹 공격은 비교적 어렵지 않은 기술로 해킹이 가능하지만 매우 큰 피해를 입힐 수 있어 공격자들이 홈페이지를 대상으로 많은 해킹시도를 하고 있다.

홈페이지를 통한 해킹사고를 예방하기 위해서는 웹취약점 점검을 통해 홈페이지의 취약점을 사전에 발견해서 조치해야 하며, 또한 방화벽 등의 보안장비를 통해 공격시도를 차단해야 한다.

하지만 많은 중소기업 홈페이지의 경우, 비용이 발생하는 웹취약점 점검 및 취약점 조치에 어려움이 있다. 한국인터넷진흥원에서는 중소기업의 홈페이지 해킹사고 예방을 위해 다양한 서비스를 제공하고 있으며, CASTLE 프로그램은 중소기업 등에 최소한의 보안장치를 제공하고자 한국인터넷진흥원에서 개발하여 배포하고 있다. CASTLE은 웹서버에 설치하여 홈페이지 취약점을 이용한 해킹공격을 차단하는 웹방화벽 기능을 제공한다.

본 문서는 공개 웹방화벽 CASTLE(PHP버전)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.

CASTLE은 가장 일반적인 웹 개발 환경에서 적용 가능하도록 제작하였다. 각 기관의 웹 개발 환경 및 서비스가 매우 다양하므로, 운용중인 서비스에 지장이 없도록 충분히 테스트하고 적용하기 바란다.

한국인터넷진흥원에서는 중소·영세 기업에 CASTLE을 보급하여 홈페이지를 통한 해킹사고를 줄일 수 있도록 노력하고 있다.

※ 해당 프로그램은 최소한의 웹방화벽 기능만을 제공하며, 상용 웹방화벽 제품의 사용을 권장합니다.

■ CASTLE의 주요기능

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

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

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

■ 기대효과

□ CASTLE 확산으로 국내 웹 어플리케이션의 보안성 향상

□ 개발자들은 개발 단계에서부터 CASTLE을 통합적으로 적용하여 보안성 강화

□ 서버 관리자들은 편리한 사용과정을 통해 기존 웹 어플리케이션 수정 용이

제 2 장 설치 및 적용

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

1. 지원 환경

CASTLE PHP 버전은 다음과 같은 환경에서 정상적으로 동작한다.

운영체제	Windows, Linux, Unix 계열
웹서버	Apache 모든 버전
PHP버전	4.1.x ~ 5.x.x

2. 설치 준비

■ 설치 사전 준비

설치를 위해 최신 버전의 CASTLE 패키지를 CASTLE 배포 공식 사이트에서 다운로드 받는다. CASTLE 패키지는 CASTLE ASP(castleasp), JSP(castlejsp), PHP(castlephp), DOTNET, Spring 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 > [다운로드] > [캐슬]
⇒ 주의. Krcert 홈페이지가 아닌 경우 정상적인 설치파일이 아닐 수 있음

3. 설치 과정

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

□ 설치 페이지 주소
- http://서버주소/CASTLE설치디렉토리/install.php

⇒ **주의. CASTLE 설치 디렉토리명은 임의로 변경해주시기 바랍니다.**
기본(castlephp) 디렉토리명 사용시 해킹 우려가 있음.

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

□ 테스트 설치 환경
- 기본 URL : http://test.com
- CASTLE 설치상대경로 : /castlephp
- CASTLE 설치전체경로 : http://test.com/castlephp/install.php

=> 주의. 기본(castlephp) 디렉토리명 사용시 해킹 우려가 있음으로, 변경하시기 바랍니다.

■ 설치 1단계 - 설치 동의 단계

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

※ 설치 전체 경로 : http://test.com/castlephp/install.php

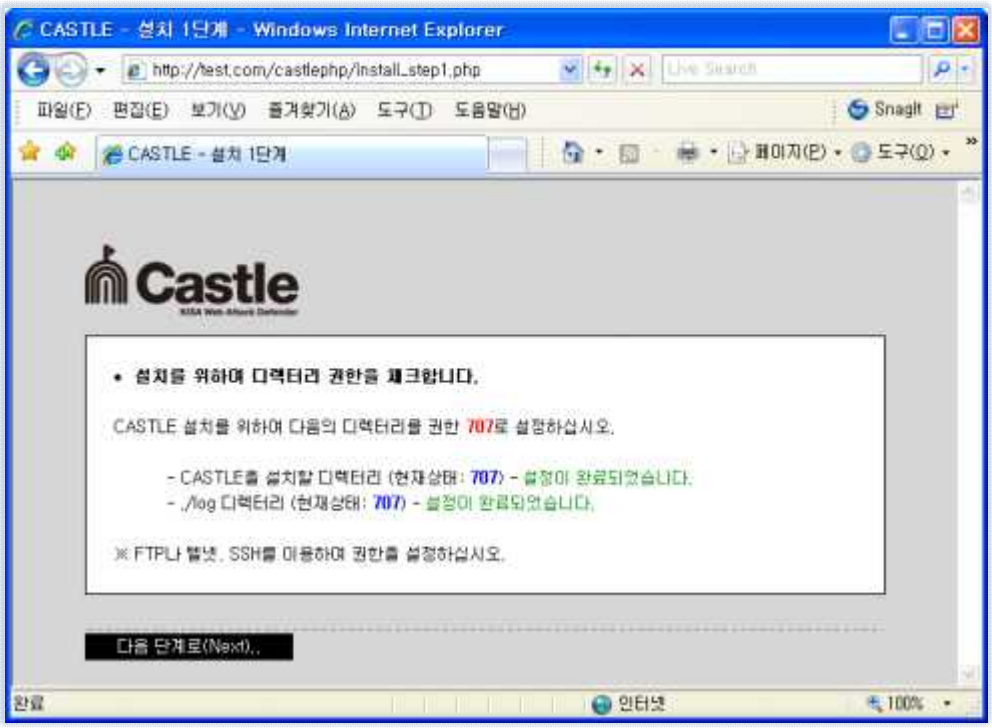
■ 설치 2단계 – 권한 설정 단계

권한 설정 단계는 설치하고자 하는 시스템에 쓰기 권한을 설정했는지 확인하는 단계이다. 정상적인 웹 서비스를 위해 쓰기 권한을 줘야 한다.

CASTLE를 설치하기 위해서는 『castlephp/』와 『castlephp/log』디렉토리 권한을 707로 설정해야 한다. 권한 설정을 제대로 설정하지 않으면 다음 단계를 진행할 수 없기 때문에 리눅스/유닉스 경우 서버에 터미널로 접속하여 아래와 같이 반드시 권한을 707로 설정해야한다.

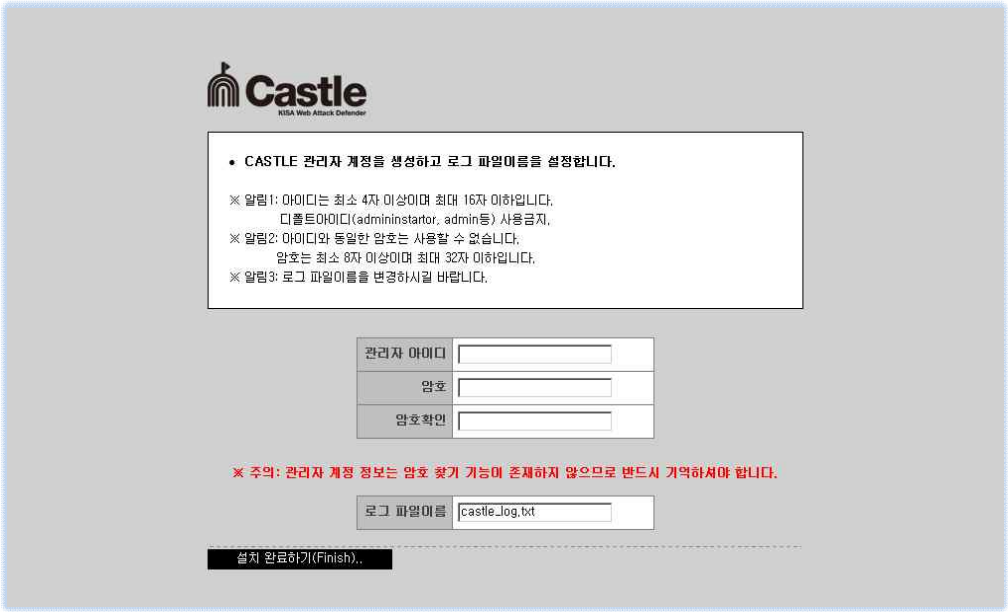
```
#chmod 707 castlephp/
#chmod 707 castlephp/log
```

권한 설정을 완료하면 다음 그림과 같이 녹색 글씨로 "**설정이 완료되었습니다.**"라는 메시지를 확인할 수 있다. 그리고 다음 단계를 눌러 관리자 계정 설정 단계로 진행한다.



■ 설치 3단계 - 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 생성해야 한다. **아이디와 암호는 찾기 기능이 없으므로 반드시 기억해야 하며 아이디와 암호를 잃어버린 경우에는 재설치 과정을 거쳐야 하므로 주의해야 한다.** 보안을 위해 로그 파일 이름을 관리자가 직접 설정하도록 하였으므로, **로그파일 이름을 다른 이름으로 변경한다.**



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

※ 아이디, 패스워드 생성 규칙

1. 디폴트아이디(administartor, admin등) 사용금지
2. 아이디는 최소 4자 이상이며 최대 16자 이하로 사용
3. 아이디와 동일한 암호는 사용 불가
4. 암호는 최소 8자 이상이며 영문, 숫자 특수문자를 조합해서 생성

4. 적용 과정

웹 어플리케이션 CASTLE을 각 웹 페이지나 프로그램에 적용하기 위해서는 CASTLE를 적용하고자 하는 대상 파일에 4줄로 구성된 코드를 추가한다.

예를 들어 『http://test.com/test.php』웹 프로그램에 CASTLE를 적용한다면 『test.php』파일의 첫 줄에 아래와 같은 코드를 추가해야 한다.

```
<?php
define("__CASTLE_PHP_VERSION_BASE_DIR__", "CASTLE 프로그램 위치 절대 경로");
include_once(__CASTLE_PHP_VERSION_BASE_DIR__ . "/castle_referee.php");
?>
```

추가할 소스코드의 내용은 위와 같다. 위 코드에서 **"CASTLE 프로그램 위치 절대 경로"** 부분을 CASTLE 프로그램이 설치된(압축 해제된) 경로로 수정해야 한다.

예를 들어 CASTLE이 『/var/www/html/castlephp』에 설치된 경우라면 다음과 같이 수정하고 설치할 웹 페이지 첫줄에 추가 한다.

```
<?php
define("__CASTLE_PHP_VERSION_BASE_DIR__", "/var/www/html/castlephp");
include_once(__CASTLE_PHP_VERSION_BASE_DIR__ . "/castle_referee.php");
?>
```

실제 예로 제로보드 4.18 버전에 CASTLE를 적용한다면 아래와 같이 추가한다. 이렇게 『lib.php』와 『_head.php』파일에 추가하면, 모든 제로보드 파일에 CASTLE를 적용 할 수 있다.

『lib.php』와 『_head.php』에 적용하는 것으로 모든 파일에 적용할 수 있는 이유는, 제로보드의 모든 파일이 『lib.php』또는 『_head.ph- 10 -p』를 참조하고 있기 때문이다.

```
<?php
define("__CASTLE_PHP_VERSION_BASE_DIR__" , "/var/www/html/castlephp");
include_once(__CASTLE_PHP_VERSION_BASE_DIR__ . "/castle_referee.php");
?>
<?
/*********************************************************************
 * Zeroboard library
 ... 중략 ...
```

제로보드의 경우는 프로그램 구성상 『lib.php』와 『_head.php』파일에만 추가하여 모든 파일에 적용시킬 수 있지만 모든 프로그램이 각각의 파일로 나뉘어져 있는 경우에는 적용하고자 하는 모든 웹 페이지나 프로그램을 모두 수정해야 한다. 위와 같이 CASTLE를 적용하기 위해서 PHP 소스를 수정할 때에는 PHP 문법적 에러가 발생하지 않도록 꼼꼼하게 해야 한다. 수정이 완료되면 다음과 같은 방법으로 에러가 없는지 확인하도록 한다.

```
#php lib.php
...
중략
...
```

위와 같이 실행하였을 때 경고나 에러가 발생하지 않으면 정상적으로 적용을 완료한 것이다.

※ 즉, CASTLE를 적용하고자 하는 웹사이트에 제로보드의 『 lib.php 』와 『 _head.php 』 같은 공통 참조 파일이 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.

□ 관리자 페이지 주소

- http://서버주소/CASTLE설치디렉토리/castle_admin.php

=> 주의. 기본 관리자 페이지명(castle_admin.php) 사용시 해킹 우려가 있음으로, 임의의 페이지명으로 변경하시기 바랍니다.

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

□ 테스트 관리자 페이지 환경

- 기본 URL : http://test.com
- CASTLE 설치상대경로 : /castlephp
- CASTLE 관리자 페이지 전체경로 : http://test.com/castlephp/castle_admin.php

■ 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/castlephp/castle_admin.php

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, 메뉴얼에 대한 링크가 있으며 왼쪽에 관리메뉴 링크가 있다.

■ 관리자 페이지 메뉴별 설명

관리자 페이지는 7개 메뉴로 구성되어 있다.

■ 관리자 페이지 접근 제한

모든 설정이 끝난 후, 외부에서 캐슬 관리자 페이지 접근 제한하기 위해 서버(Apache) 설정을 변경해야한다. 리눅스/유닉스 경우 서버에 터미널을 접속하여 etc/httpd/conf 설정을 변경시켜 준다.

□ httpd.conf 파일 vi 편집

```
#cd etc/httpd/conf
#vi httpd.conf
```

```
DocumentRoot "/var/www/html"

#
# Each directory to which Apache has access can be configured with respect
# to which services and features are allowed and/or disabled in that
# directory (and its subdirectories).
#
# First, we configure the "default" to be a very restrictive set of
# features.
#
<Directory "var/www/html/test/php/castle_admin_login.php">
    Options FollowSymLinks
    AllowOverride None
    Order deny,allow
    Deny from all
    Allow from localhost
</Directory>

#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
```

□ Directory 태그에 설정 수정.

```
<Directory “캐슬경로/castle_admin_login.php”>
  options FollowSymLinks
  AllowOverride None
  order deny,allow
  Deny from all
  Allow From localhost
</Directory>
```

□ 로컬 접속 시 캐슬 접속 화면.

□ 외부에서 캐슬 접속 화면.

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

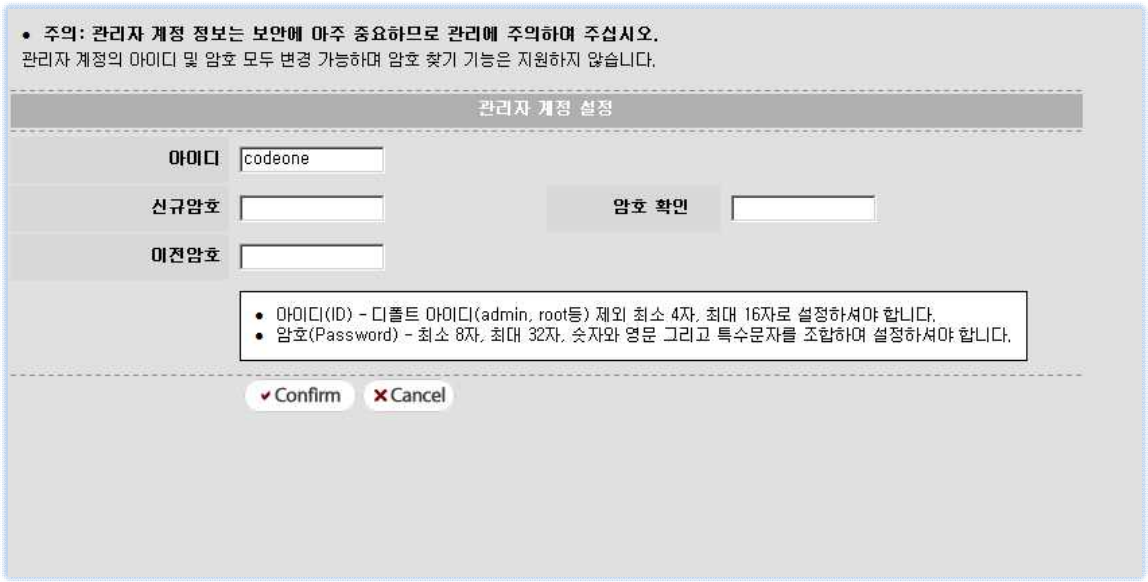
아이디는 최소 4자, 최대 16자의 문자열 또는 숫자로 구성해야 한다.

※ 디폴트아이디(administrator, admin등) 사용금지

■ 암호 설정 규칙

암호는 최소 8자, 숫자, 영어, 특수 문자열을 조합하여 구성해야 한다.

※ 아이디와 동일한 암호 사용금지



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

제 5 장 기본 설정

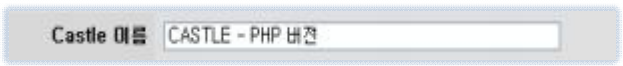
5장 기본 설정에서는 CASTLE에 대한 가장 중요한 부분으로 기본설정, 사이트 설정, 적용대상 등 운영에 관련된 정책 설정에 대하여 설명한다.

1. 기본 설정

기본 설정에서는 이름, 차단모드 그리고 알림방식에 대해서 설정한다.

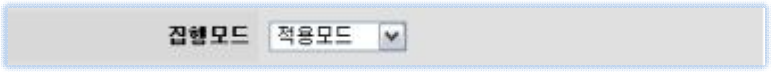
■ 이름 설정

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



■ 차단모드 설정 (*설정상 주의필요)

차단모드 설정은 CASTLE 설정에 있어서 가장 중요한 부분으로 설치한 CASTLE를 실제 차단할 것인지 혹은 설치만하고 차단하지 않을 것인지 등을 설정한다. 차단모드에는 총 3개의 모드가 있으며 **적용모드**, **감사모드** 그리고 **비 적용모드**가 있다.



□ 적용모드(enforcing)

- 차단모드를 적용모드로 설정할 경우, CASTLE에서 정의한 정책들에 의해 탐지를 수행하고, 차단 또는 허용

□ 감사모드(permissive) - 기본 설정 상태

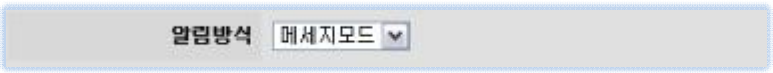
- 감사모드로 설정한 경우에는 적용모드와 마찬가지로 CASTLE에서 정의한 정책들에 의해 탐지를 수행하지만 무조건 허용함
- 설치 초기에 정책을 작성하는 과정에 감사모드로 정책의 안정화하는 것이 좋음
- 정의한 정책에 의해 탐지한 것들은 로그 파일로 기록하므로, 로그를 확인하여 운영하는 사이트 환경에 맞게 정책 수정이 필요

□ 비적용모드(disabled)

- 비적용모드로 설정되어 있을 경우에는 CASTLE이 적용되지 않음

■ 알림방식 설정

알림방식 설정은 차단모드를 적용모드로 설정했을 때 비정상적인 행위로 탐지되어 사용자의 접근이 차단할 필요가 있을 경우 어떻게 차단할 것인지에 대한 설정이다. 알림방식에는 경고모드, 알림모드 그리고 스텔스모드가 있다.



□ 경고모드(alert)

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

□ 메시지모드(message)

- 차단 결과를 메시지로 알림

□ 스텔스모드(stealth)

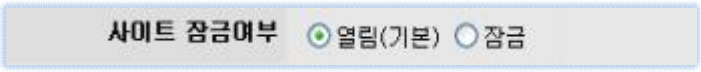
- 빈 페이지를 출력한다.
- CASTLE 운영 사실을 숨기고자 할 때에 유용함

2. 사이트 설정

사이트 설정에서는 현재 운영 중인 사이트에 대한 전반적인 설정으로 현재 운영 중인 사이트를 잠글 것인지 서비스할 것인지에 대한 설정과 사이트의 문자 셋이 무엇인지를 설정한다. 지원하는 문자 셋으로는 UTF-8과 EUC-KR이 있다.

■ 사이트 잠금 여부 설정

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



☐ 열림

- 사이트를 정상적으로 운영함

☐ 잠금

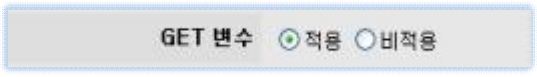
- 사이트를 잠그고 운영하지 않음, 다음의 그림은 사이트가 잠긴 화면

3. 적용대상 설정

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

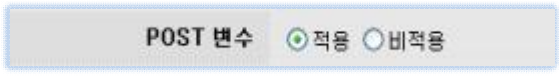
■ GET 변수 설정

- GET 변수들을 대상으로 탐지 수행 여부를 설정한다.



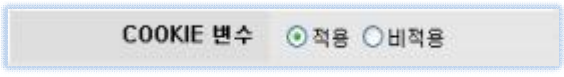
■ POST 변수 설정

- POST 변수들을 대상으로 탐지 수행 여부를 설정한다.



■ COOKIE 변수 설정

- COOKIE 변수들을 대상으로 탐지 수행 여부를 설정한다.



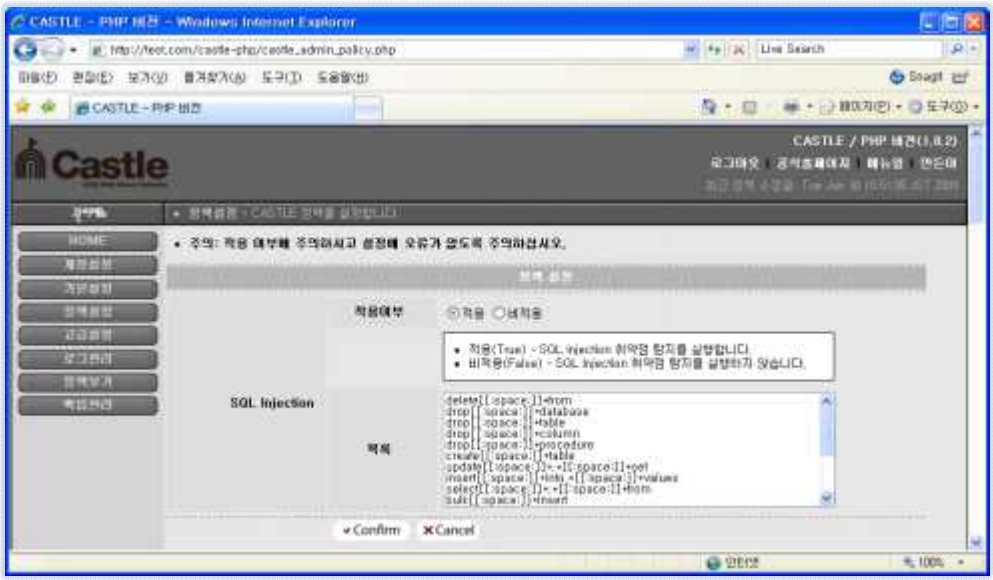
제 6 장 정책 설정

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

※ 초기 설정되어 있는 정책만으로는 모든 공격을 탐지할 수 없습니다.

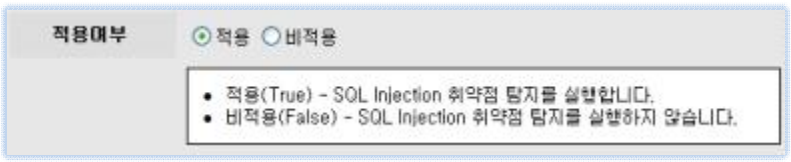
1. SQL Injection 정책 설정

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



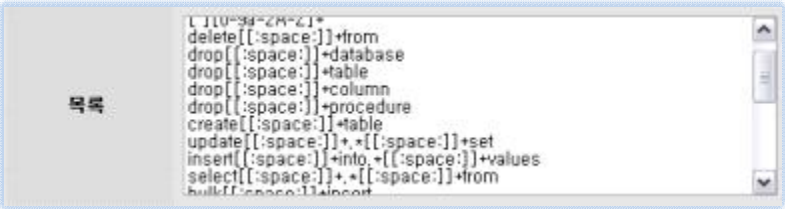
□ 적용여부

- SQL Injection 공격 탐지 수행 여부를 설정한다.



□ 목록

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



■ SQL Injection 공격 탐지 차단

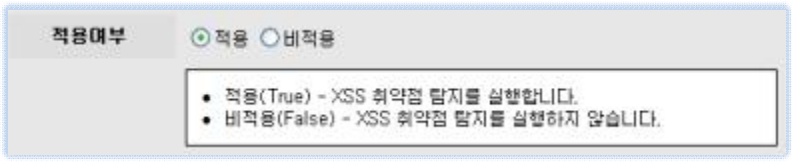
변수에 "1 or 1 --"와 같이 목록에 포함된 형태의 SQL Injection 공격 코드를 넣었을 때 다음과 같이 탐지하고, 차단한다.

2. XSS 정책 설정

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

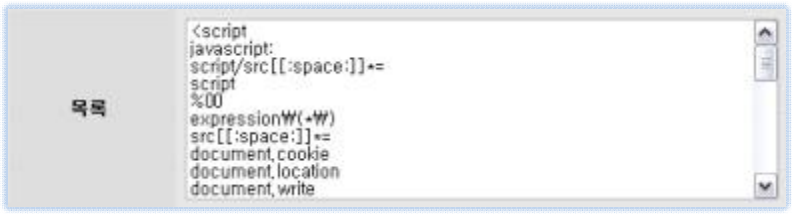
□ 적용여부

- XSS 공격 탐지 수행 여부를 설정한다.



□ 목록

- XSS 공격 형태를 정규표현식으로 설정한다.



■ XSS 공격 탐지 차단

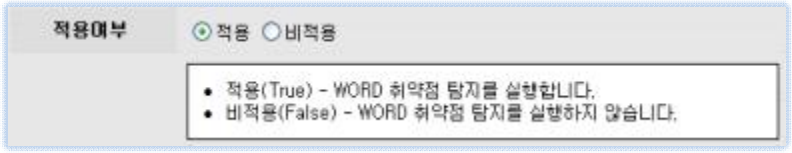
변수에 “javascript:”와 같이 목록에 포함된 형태의 XSS 공격 코드를 넣었을 때 다음과 같이 탐지하고 차단한다.

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.

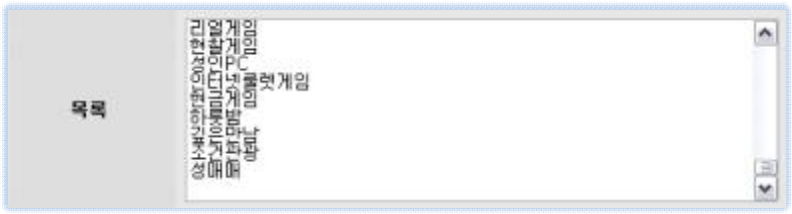
□ 적용여부

- 금칙어 탐지 수행 여부를 설정한다.



□ 목록

- 금칙어 형태를 정규표현식으로 설정한다.

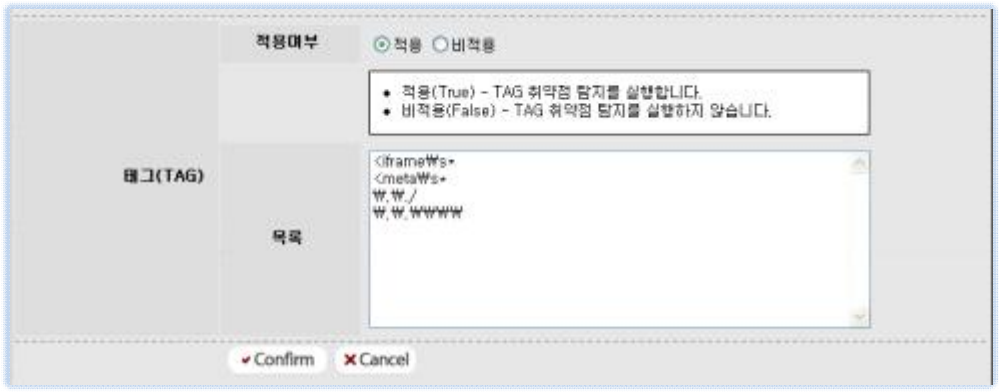


■ 금칙어 차단

변수에 목록에 포함된 금칙어를 넣었을 때 다음과 같이 탐지하고, 차단한다.

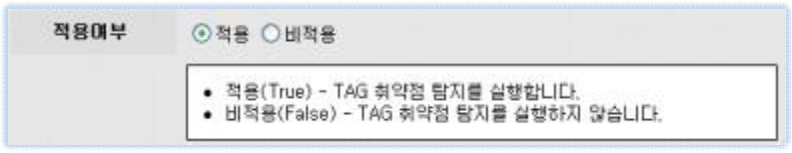
4. 불량태그 정책 설정

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



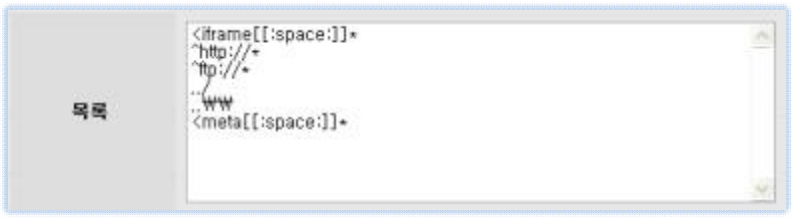
□ 적용여부

- 불량태그 공격의 탐지 수행 여부를 설정한다.



□ 목록

- 불량태그 공격 형태를 정규표현식으로 설정한다.

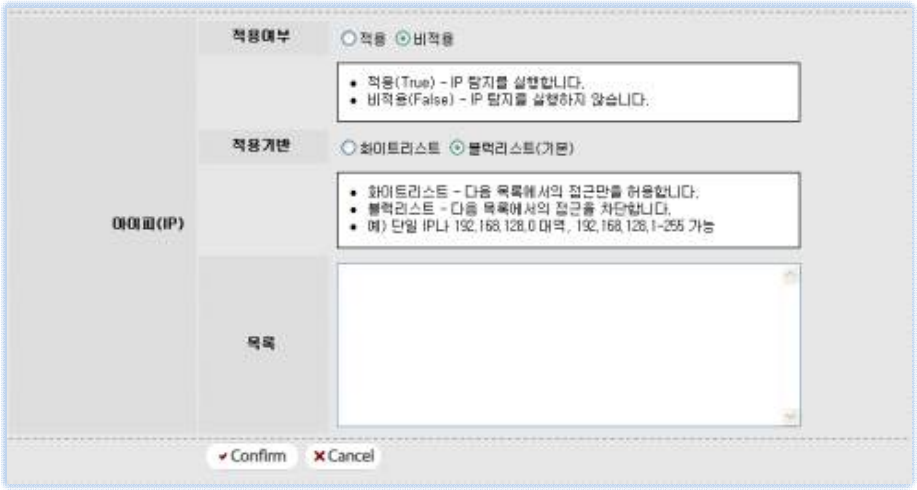


■ 불량태그 공격 탐지 차단

변수에 “<iframe”와 같이 목록에 포함된 형태의 불량태그를 넣었을 때 다음과 같이 탐지하고 차단한다.

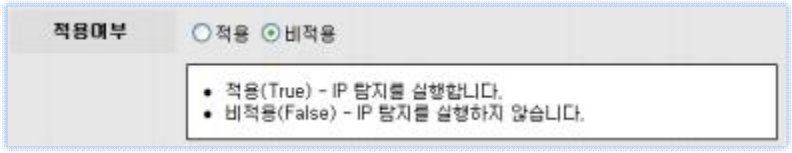
5. IP 정책 설정

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



□ 적용여부

- IP 탐지 수행 여부를 설정한다.



□ 적용기반

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

□ 목록

- IP를 정규표현식으로 설정한다.

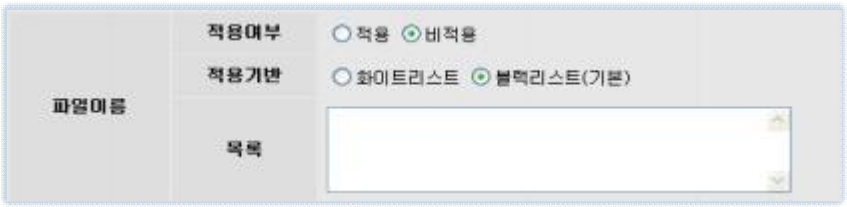
■ 아이피 탐지 차단

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

6. 파일 정책 설정

파일 정책은 업로드하는 파일들에 이름, 타입, 크기로 허용할 것인지 차단할 것인지를 설정한다. 이 정책으로 파일 업로드 공격을 탐지 할 수 있다.

■ 파일이름



□ 적용여부

- 파일이름 탐지 수행 여부를 설정한다.

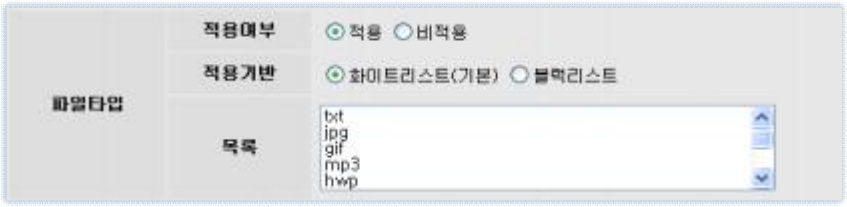
□ 적용기반

- 화이트리스트 : 목록에 포함된 파일이름만 업로드를 허용함
- 블랙리스트 : 목록에 포함된 파일이름은 업로드를 차단함

□ 목록

- 파일이름을 정규표현식으로 설정한다.

■ 파일타입



□ 적용여부

- 파일타입 탐지 수행 여부를 설정한다.

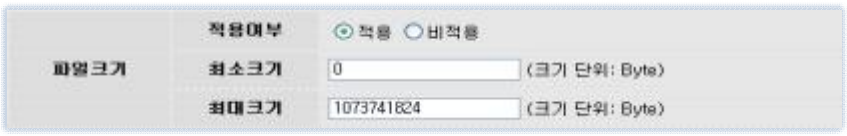
□ 적용기반

- 화이트리스트 : 목록에 포함된 파일타입만 업로드를 허용함
- 블랙리스트 : 목록에 포함된 파일타입은 업로드를 차단함

□ 목록

- 파일타입을 정규표현식으로 설정한다.

■ 파일크기



□ 적용여부

- 파일크기 탐지 수행 여부를 설정한다.

□ 최소크기

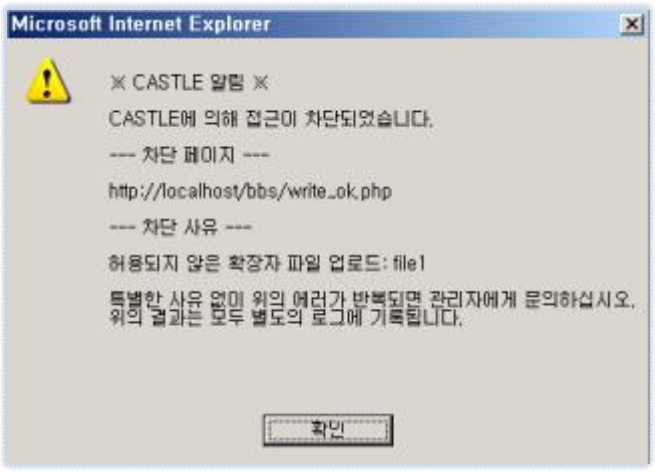
- 업로드를 허용할 최소크기 값 설정

□ 최대크기

- 업로드를 허용할 최대크기 값 설정

■ 파일 업로드 탐지 차단

허용하지 않은 확장자인 “*.php”를 가진 파일을 업로드 할 때에 다음과 같이 탐지되고 차단 된다.



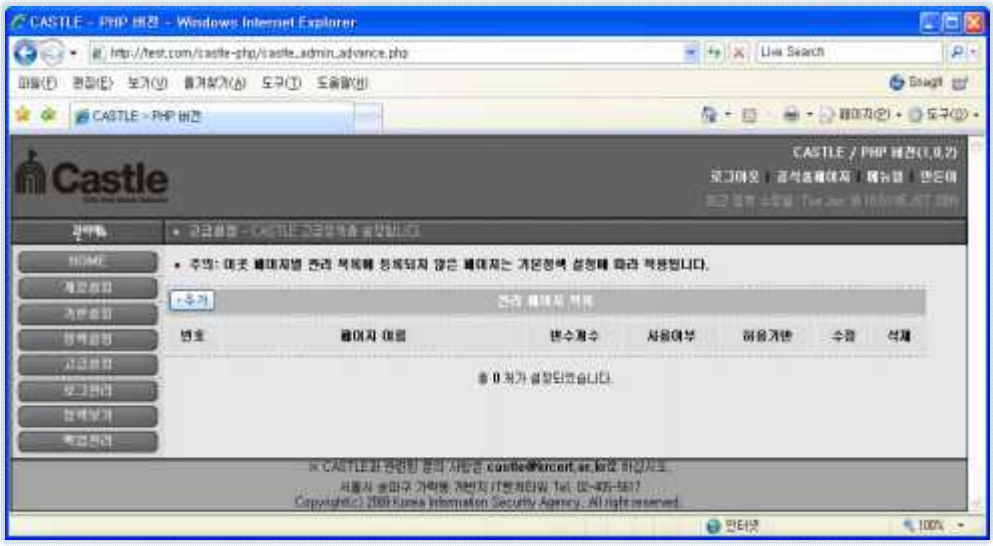
■ 정책 모든 설정 후 권한 변경

정책 설정 후 생성되는 castle_policy.php (정책파일) 변조 또는 변조를 통한 해킹을 예방하기 위해 운영단계에서는 권한 변경 리눅스/유닉스 경우 서버에 터미널로 접속하여 아래와 같이 반드시 권한을 400으로 설정해야한다.

```
#chmod 400 castle_policy.php
```

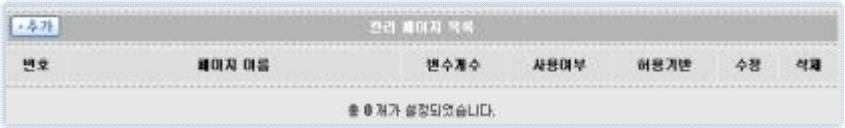
제 7 장 고급 설정

7장 고급 설정에서는 각 페이지별로 정책을 설정한다. 이때 설정된 페이지 정책들은 기본설정 정책보다 우선적으로 탐지된다.



1. 신규 페이지 추가

위의 그림은 어떤 정책도 설정되지 않은 초기 상태의 고급 설정 페이지의 화면이다. “추가” 버튼을 클릭하면 아래와 같이 관리할 페이지를 추가할 수 있다.



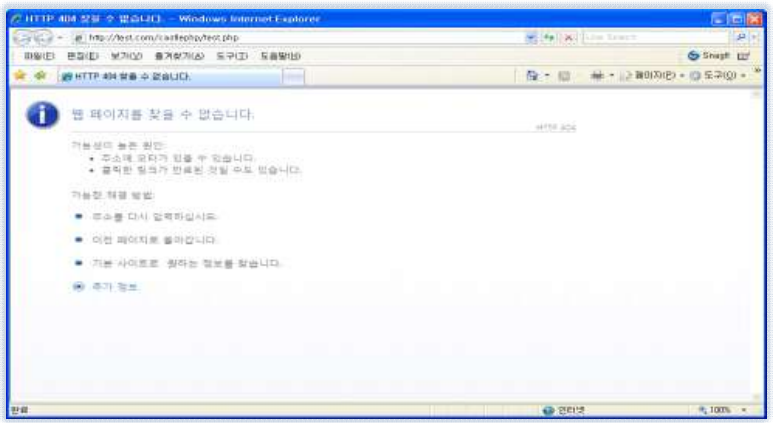
■ 페이지 추가

페이지 추가 버튼을 누르면 다음과 같은 폼이 나타난다.

□ 페이지 이름

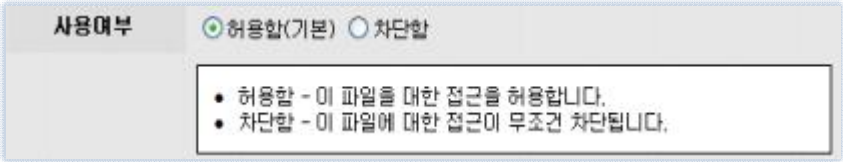
- 추가할 페이지 이름으로 http://host/path에서 /path 입력
- ex) http://testcom/test.php일 경우 “/test.php” 이 부분을 입력하면 됨
- 반드시 “**페이지보기**” 버튼을 클릭하여 정상적으로 /path를 적었는지를 확인해 보아야 다음으로 진행이 됨

다음의 그림은 “**페이지보기**“ 클릭 후 페이지 이름을 잘못 입력하였을 때 내용으로 “**웹 페이지를 찾을 수 없습니다.**” 라고 표시된다.



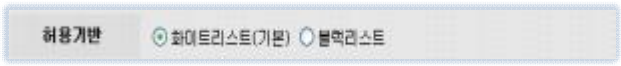
□ 사용여부

- 현재 추가할 페이지에 대한 접근을 허용 여부를 설정한다.
  이때 차단으로 설정할 경우 해당 페이지에 대한 접근은 무조건 차단된다.



□ 허용기반

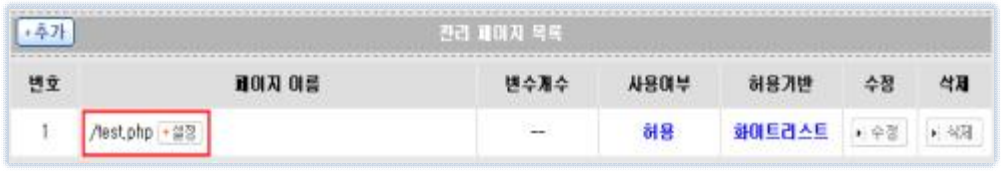
- 추가할 페이지에서 사용하는 변수들에 대하여 화이트리스트 방식으로 설정할 것인지 아니면 블랙리스트 방식으로 설정할 것인지를 나타낸다. 화이트리스트로 설정할 경우에는 정해진 변수 이외에는 어떠한 변수 사용도 차단되며 블랙리스트 방식의 경우에는 지정된 변수의 사용이 무조건 차단된다.



페이지 이름 부분에 “/test.php“로 입력하고 페이지보기를 실행하였을 때 다음과 같이 관리할 대상이 제대로 표시되면 ”Confirm“ 버튼을 클릭하고 페이지를 추가한다.

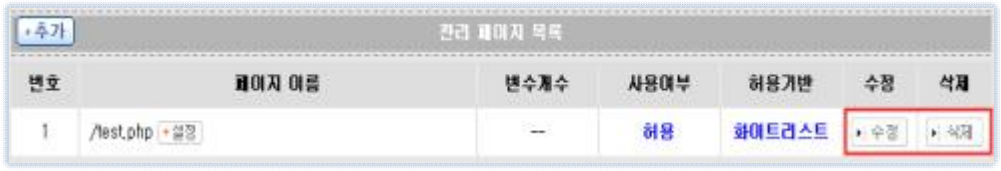
만약 현재 정책을 설정하는 test.php에 CASTLE이 적용되어 있지 않다면 /test.php의 소스 상단에 CASTLE을 적용할 소스 4줄을 입력해 줘야 한다.

다음과 같이 정상적으로 페이지가 추가되면 관리 대상 페이지 목록에 나타난다. 앞서 입력한 “test.php“가 추가되어 있는 것을 볼 수 있다.



2. 관리 페이지 수정과 삭제

고급 설정에서 관리할 페이지 목록별 각 표시줄에 오른쪽 부분에는 “수정”, “삭제” 버튼이 있다. 이 버튼을 클릭함으로써 수정 및 삭제가 가능하다.



■ 페이지 수정

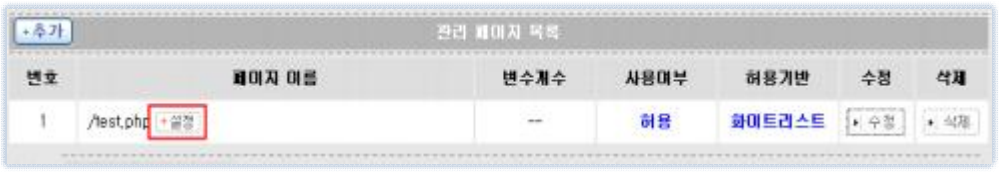
수정 버튼을 클릭하면 아래 그림과 같이 수정할 페이지 목록 바로 밑에 수정할 수 있는 폼이 나타난다. 페이지 추가와 마찬가지로 사용여부와 허용기반을 수정할 수 있다. 현재에는 페이지 이름에 대한 수정 기능은 지원하지 않는다.

■ 페이지 삭제

페이지 삭제는 삭제 버튼을 클릭하면 삭제 여부를 확인한다. “확인”을 클릭하게 되면 해당 페이지는 페이지별 관리 대상에서 삭제할 수 있다.

3. 각 페이지별 변수 설정

각 페이지별 변수 설정은 관리 페이지 목록에서 페이지 이름 부분에 “설정” 버튼을 클릭하여 설정할 수 있다.



아래 그림은 페이지별 변수 설정 화면이다. 아랫부분에 변수 관리 설정 부분에 허용하거나 차단할 변수들에 목록이 표시된다. 관리할 변수를 추가하려면 중간에 있는 “**추가**” 버튼을 클릭하면 다음의 그림과 같이 변수 정보 입력 폼이 표시되고 변수 정보 입력 폼을 작성하고 “Confirm”을 클릭하면 된다.

■ 변수 추가

변수 추가 버튼을 누르면 아래와 같은 폼이 나타난다. 입력 폼에 추가할 변수 정보를 입력하고 “Confirm”을 클릭하면 변수가 추가된다.

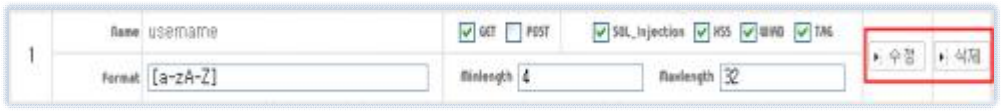
□ 입력 폼별 설명

- Name: 변수명
- Format: 변수값 입력 형태(정규표현식)
- GET: GET 메소드에 대한 허용 여부
- POST: POST 메소드에 대한 허용 여부
- SQL Injection: SQL Injection 공격 탐지 여부
- XSS: XSS 공격 탐지 여부
- WORD: 불량 단어 탐지 여부
- TAG: 불량 태그 탐지 여부
- Minlength: 변수 최소 길이
- Maxlength: 변수 최대 길이

“test.php“ 페이지에서 변수 username과 password를 사용하고 username 변수는 알파벳으로만 구성, 길이는 최소 4에서 최대 32이고 password변수는 숫자로 구성, 길이가 최소 1에서 최대 32로 구성된다고 할 때에 해당 변수들에 정책을 추가한다면 다음의 그림과 같이 설정한다.

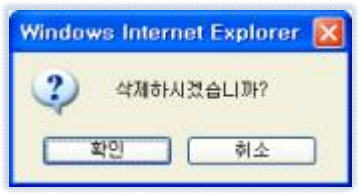
■ 변수 수정과 삭제

변수 수정과 삭제 기능은 각 변수 목록에 오른쪽에 위치한 수정과 삭제 버튼을 통해서 수행한다.



o 수정 클릭시의 확인 창

o 삭제 클릭시의 확인 창



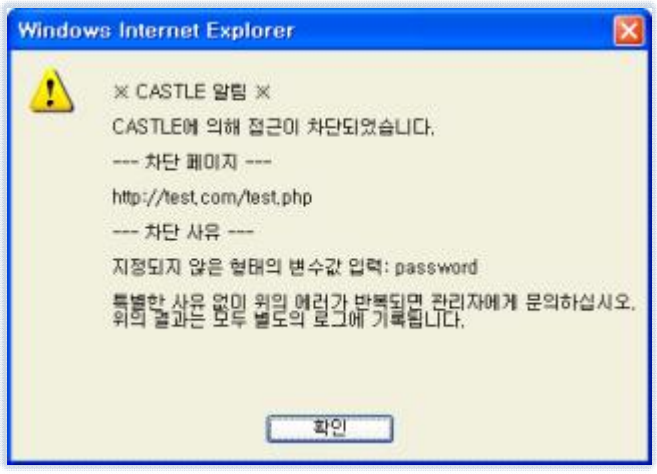
4. 페이지별 정책 테스트

■ 설정하지 않은 username 사용

변수 username은 허용되지 않았기 때문에 다음의 그림과 같이 차단된다.

■ 잘못된 형태의 값을 입력

변수 password는 [0-9] 정규표현식에 따라 숫자로만 구성되어야 한다.



■ 최소, 최대 길이 범위를 벗어난 입력

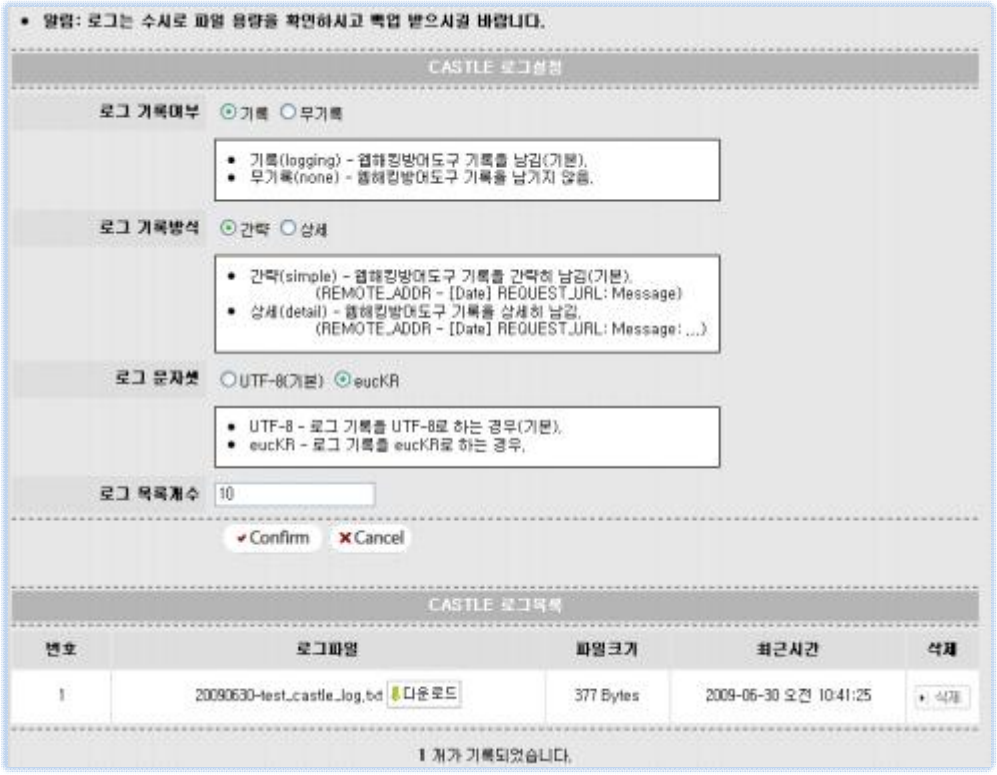
변수 password는 최소 1에서 최대 6자리만 허용되도록 정책이 설정되어 있어 7자리 이상입력하면 다음과 같이 차단된다.

■ 허용되지 않은 메소드 접근

GET 메소드가 허용되지 않았을 때 GET으로의 접근은 차단된다.

제 8 장 로그 관리

8장 로그 관리는 CASTLE에 의해서 탐지된 결과를 저장할 로그 파일에 대한 설정이다. 로그 파일이름과 기록여부 그리고 기록방식 등을 설정한다.



■ 로그 파일이름

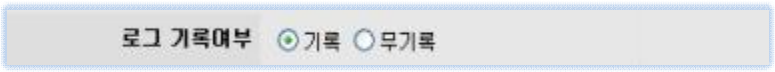
로그 파일이름은 설치시 관리자가 직접등록 한다.

□ 로그 파일 이름 규칙

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

■ 로그 기록여부 설정

로그 기록 여부를 설정한다.



□ 기록

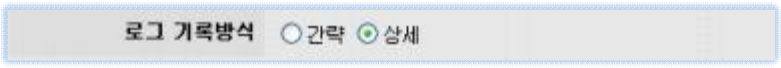
- 로그를 기록함

□ 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.



□ 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.php: memo = 인터넷룰렛
게임,리얼PC게임,성인게임... : 불량 WORD 탐지

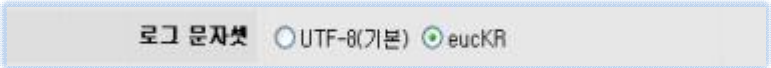
□ 상세

- 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.php:
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]
```

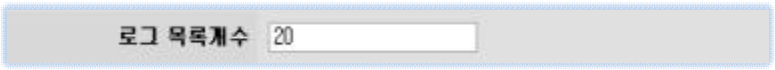
■ 로그 문자셋 설정

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.

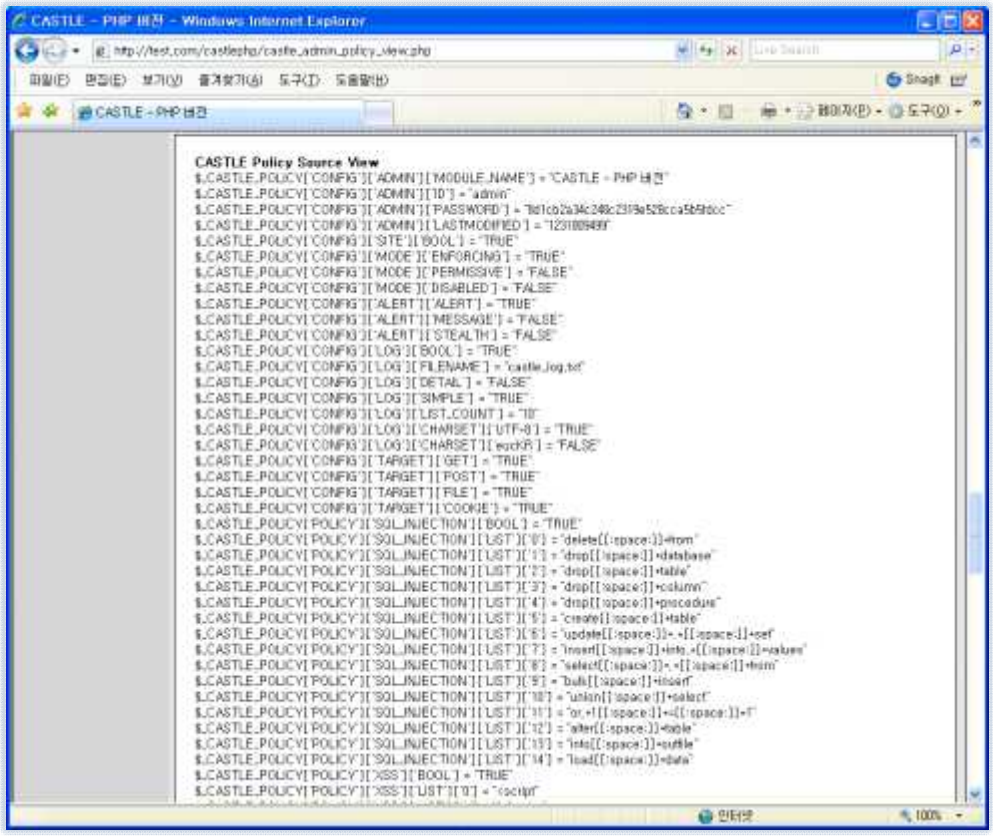
제 9 장 정책 보기

9장 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.

■ 소스형태 정책 보기



제 10 장 백업 관리

10장 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.