웹 어플리케이션 보안템플릿 (PHP 버전)

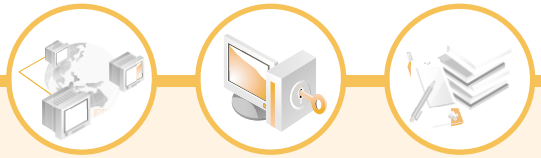
– 웹 어플리케이션 보안템플릿 개정판 –

2007. 9

정보통신부

한국정보보호진흥원
Korea Information Security Agency

www.kisa.or.kr



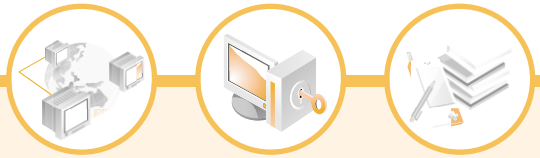
본 문서는 최근 해킹에 주로 이용되고 있는 주요 웹 보안 취약점으로 인한 피해 감소를 목적으로 한국정보보호진흥원 인터넷침해사고대응지원센터 해킹대응팀 연구원들과 국내 웹 보안 및 웹 어플리케이션 전문가의 참여를 통해 제작되었습니다.

2007년 9월

사업 책임자 : 본 부 장 **김우한**
연구 책임자 : 팀 장 **최중섭**
참여 연구원 : 선임연구원 **서진원**
주임연구원 **한단송**
주임연구원 **주필환**
연 구 원 **김영직**
외부 전문가 : 전남대학교 **이재서**
감 수 : 보안전문가 **김종회**

목 차

www.kisa.or.kr



www.kisa.or.kr

제 1 장

활용에 앞서

제 1 장 | 활용에 앞서

기존의 침해사고는 운영체제의 취약점이나 어플리케이션 취약점이 주로 이용되었으나, 최근에는 홈페이지에 존재하는 웹 어플리케이션 취약점이 공격에 많이 사용되고 있다.

홈페이지에 존재하는 웹 어플리케이션 취약점은 다른 해킹 기법과 비교하여 상대적으로 낮은 수준의 기술로도 해킹이 가능하고, 이를 이용해 많은 사용자들을 대상으로 빠른 시간 내 악성코드의 전파가 가능하다. 또한 홈페이지를 방문하는 고객을 대상으로 악성코드가 전파되므로, 공격자의 입장에서는 특정 분야 사용자를 목표로 한 공격이 가능하다는 장점이 있다.

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

본 문서에서는 PHP 환경에서 사용할 수 있는 보안모듈(KWST-KISA Web Security Template, 이하 KWST)를 제공한다. KWST는 웹 어플리케이션의 소스코드를 수정하지 못하는 곳이나 공개 웹 방화벽의 설치가 어려운 홈페이지 등에서 사용할 수 있으며 간단한 작업만으로 홈페이지에 적용이 가능한 보안 모듈 형태로 제공된다.

KWST은 가장 일반적인 웹 개발 환경에서 적용 가능하도록 제작되었지만, 각 기관의 웹 개발 환경 및 서비스가 매우 다양하므로, 정상적인 서비스에 지장이 없도록 충분한 최적화 작업 및 테스트를 하기 바란다. 향후, 추가로 ASP, JSP 보안모듈을 제작, 배포할 예정이며 모든 보안모듈 프로그램 및 관련자료는 한국정보보호진흥원 KrCERT 홈페이지에서 다운로드가 가능하다.

모쪼록 본 프로그램이 국내 홈페이지에 대한 피해사고 감소와 홈페이지 관리자의 보안작업에 도움이 되길 바란다.

※ KWST는 인터넷에서 공개된 WSM(Web Security Module)을 개발한 외부전문가에게 의뢰하여 개발되었으며, 사용자의 편리성 및 보안성 강화 기능을 추가적으로 개발하여 기존 버전과 많은 변화를 보였다.

■ KWST의 주요기능

- **보안성 강화**
  - OWASP 10대 취약점 중 주요 취약점을 해결
  - 웹 해킹 탐지 우회 차단 기능 추가
  - 소스코드 차원의 웹 어플리케이션 보안성 강화

- **사용자 편리성 강화**
  - 관리자 페이지를 이용해 편리한 정책 설정 지원
  - 운영 중인 프로그램 소스의 최소 수정만으로 적용 가능

- **높은 호환성 지원**
  - 다양한 웹 서버 환경과 웹 어플리케이션에서 동작할 수 있는 호환성 지원
  - 각 웹 어플리케이션 서버 버전에서 동작할 수 있도록 호환성 지원

■ 기대효과

- 웹 어플리케이션 개발과정에서의 보안성 강화 확보
- 웹 보안 템플릿 확산으로 국내 웹 어플리케이션의 보안성 향상
- 편리한 사용과정을 통해 기존 웹 어플리케이션 수정용이

제 2 장

설치 및 적용

제 2 장 | 설치 및 적용

제2장에서는 KWST 설치 전에 준비할 사항과 단계별 설치 방법을 알아보고, 설치 후 적용방법에 대해서 설명한다.

1. 설치 준비

KWST 설치를 위해서 설치할 시스템에 최신 버전의 KWST 프로그램 소스를 제공된 CD에서 복사한다.

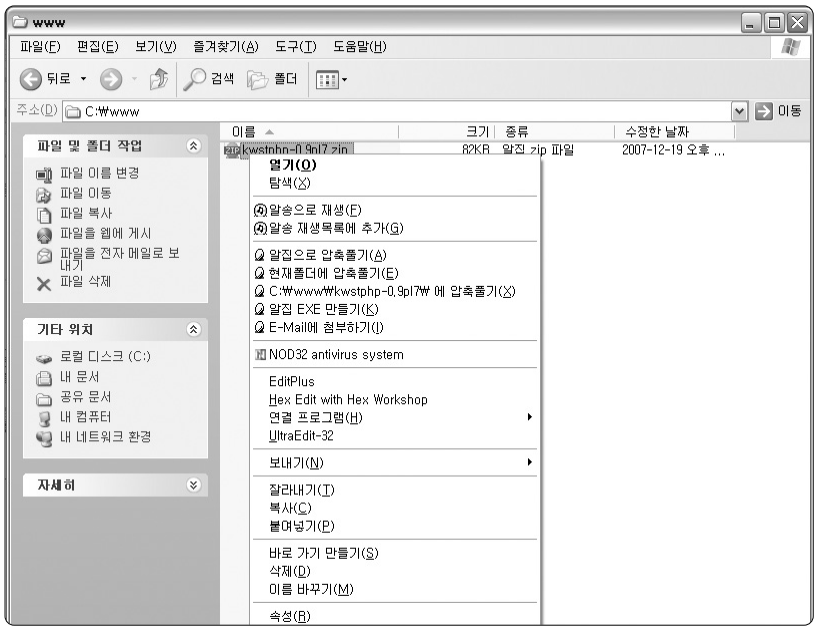
■ 리눅스 & 유닉스 계열에서의 설치 준비

리눅스 및 유닉스 계열에서는 다음의 방법에 따라 설치 준비를 한다.

```
# tar zxvf kwstphp-0.9pl7.tar.gz
kwstphp/
kwstphp/install.php
kwstphp/kwst_version.php
kwstphp/kwst_admin_bottom.php
kwstphp/kwst_admin_download.php
kwstphp/kwst_admin_login_submit.php
kwstphp/install_step3.php
kwstphp/kwst_admin_policy_submit.php
...
중략
...
```

■ 윈도우즈 계열에서의 설치 준비

윈도우 계열 시스템에서 KWST를 설치하고자 하는 경우에는 파일을 받아 알집 등의 압축 해제 프로그램을 이용하여 압축을 해제한다. 압축 해제 후에는 마찬가지로 웹상에서 이후 설치 과정을 진행하면 된다.



2. 설치 과정

웹 어플리케이션 보안 템플릿(KWST) 설치 과정은 총 4단계로 0. 설치 동의, 1. 권한 설정, 2. 문자셋(charset) 설정, 3. 관리자 계정 설정으로 이루어진다. 윈도우 계열에서는 2. 권한 설정 과정은 거치지 않는다.

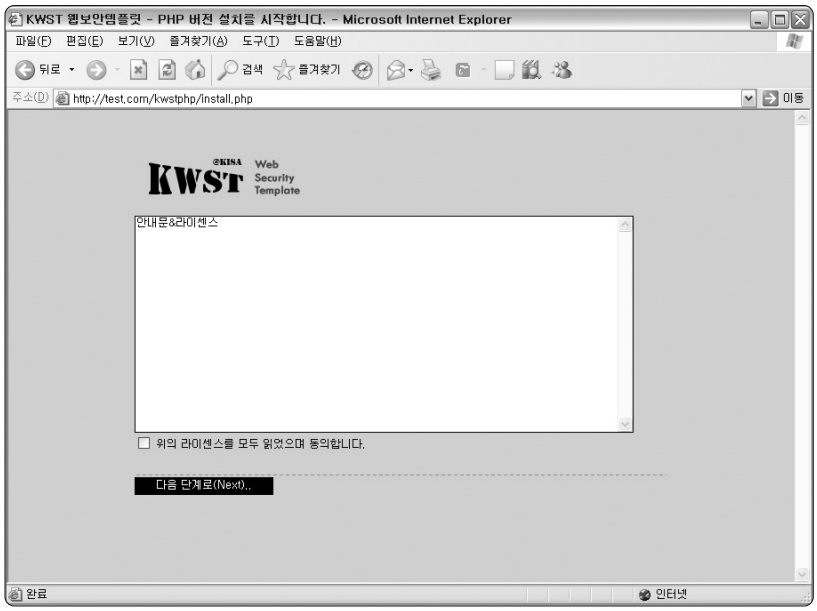
- **설치 페이지 주소**
  http://서버주소/KWST설치디렉터리/install.php

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

- **테스트 설치 환경**
  - 기본 URL : http://test.com
  - KWST 설치상대경로 : /kwstphp
  - KWST 설치전체경로 : http://test.com/kwstphp/install.php

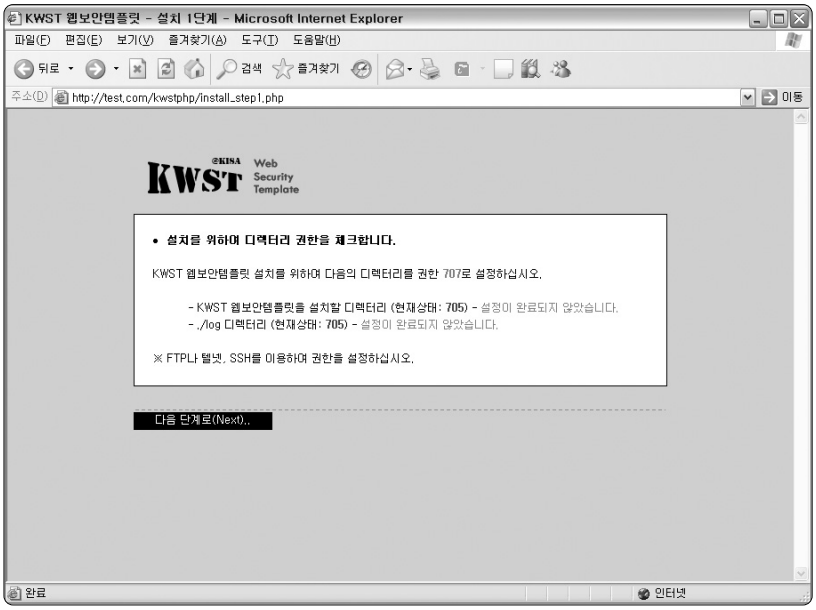
■ 설치 1단계 – 설치 동의 단계

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



■ 설치 2단계 – 권한 설정 단계

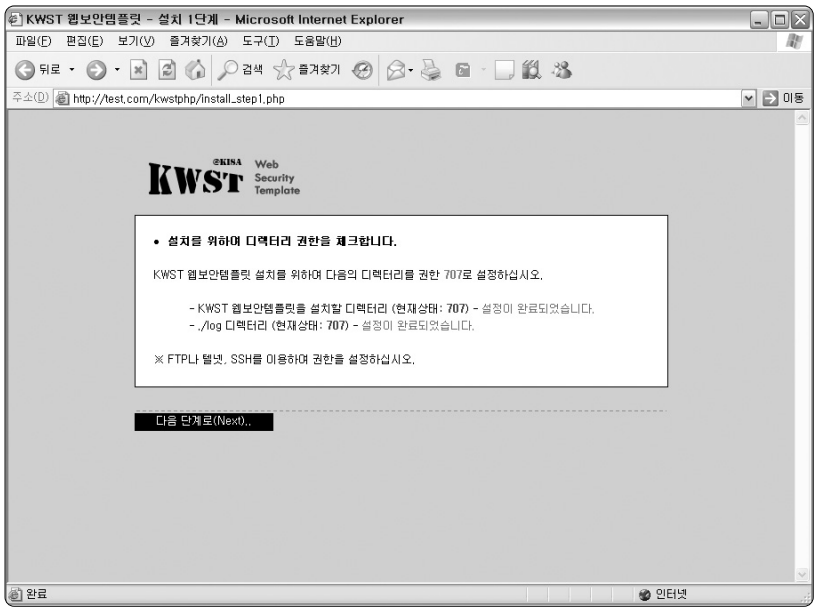
권한 설정 단계는 설치하고자 하는 시스템에 쓰기 권한이 정상적으로 설정되어 있는지를 확인하는 단계이다. 윈도우즈 계열에서는 기본적으로 쓰기 권한이 주어져 있기 때문에 권한 설정 단계를 거치지 않고 바로 문자셋 설정 단계로 바로 진행된다.



KWST를 설치하기 위해서는 kwstphp/와 kwstphp/log 디렉터리 권한이 707로 설정되어 있어야 한다. 권한 설정이 완전히 이루어지지 않으면 다음 단계로 진행되지 않기 때문에 시스템에 터미널로 접속하여 다음의 방법으로 반드시 권한을 707로 설정해야한다.

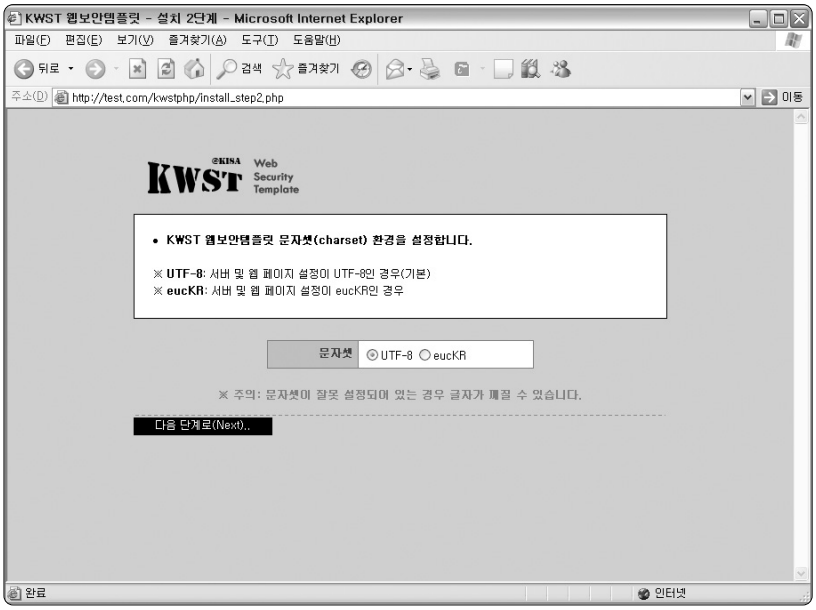
```
#chmod 707 kwstphp/
#chmod 707 kwstphp/log
```

권한 설정이 완료되면 다음의 그림과 같이 녹색 글씨로 "설정이 완료되었습니다."라는 메시지를 확인할 수 있다. 그리고 다음 단계를 눌러 문자셋 설정 단계로 진행한다.



■ 설치 3단계 – 문자셋 설정 단계

문자셋 설정은 KWST를 적용하고자 서버나 웹 페이지의 문자셋에 맞추어 설정하여야 한다. 그렇지 않은 경우 KWST 메시지를 확인할 때에 글씨가 깨진 상태로 출력되게 된다. 다음의 방법으로 시스템 상태를 확인하고 반드시 정확한 문자셋으로 설정하고 다음 단계인 관리자 계정 설정 단계로 진행한다.

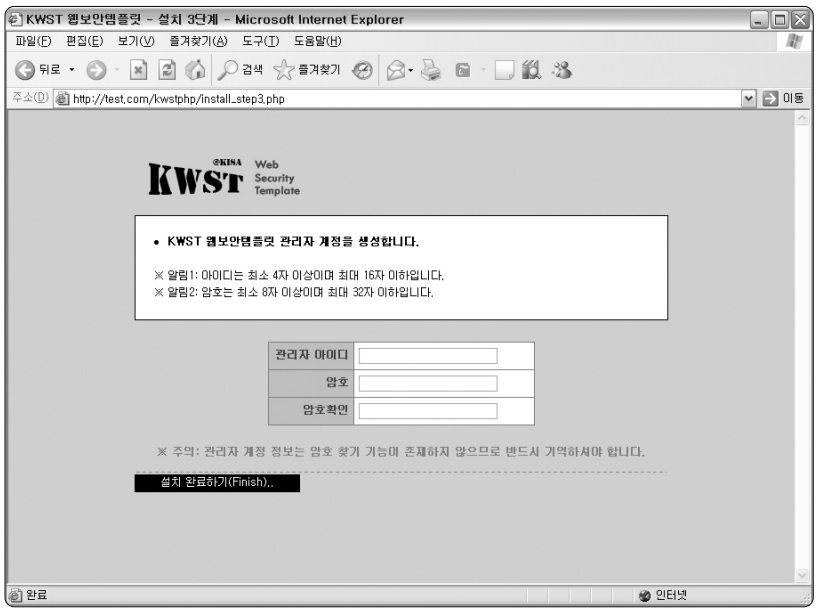


아래의 방법은 Apache 웹 서버에서 문자셋이 어떻게 설정되어 있는가를 확인하는 방법이다. 본인의 시스템에 따라 확인하기 바란다. 위의 경우에는 UTF-8로 웹 서버가 문자셋을 설정하고 있는 것을 나타낸다.

```
#grep AddDefaultCharset /etc/httpd/conf/httpd.conf
AddDefaultCharset UTF-8
```

■ 설치 4단계 – 관리자 계정 설정 단계

관리자 계정은 KWST 관리자 페이지에 인증을 하기 위한 관리자 계정이다. 아이디와 암호는 보안상 아주 중요하기 때문에 쉽지 않은 암호로 생성하길 바란다. **아이디와 암호는 찾기 기능이 없으므로 반드시 기억**해야 하며 아이디와 암호를 잃어버린 경우에는 재설치 과정을 거쳐야 하므로 주의하길 바란다.



아이디와 **암호**, **암호확인**을 정확히 입력한 후 "설치 완료하기(Finish)" 버튼을 누르면 "설치가 완료되었습니다."라는 메시지와 함께 설치가 완료된다.

3. 적용 과정

웹 어플리케이션 보안모듈을 각 웹 페이지나 프로그램에 적용하기 위해서는 KWST를 적용하고자 하는 대상 파일에 4줄로 구성된 코드를 추가해야 된다. 예를 들어 http://test.com/test.php 웹 프로그램에 KWST를 적용한다면 test.php 파일의 첫 줄에 아래와 같이 추가해야 된다.

```
<?php // WEB Security Module
define("__KWST_PHP_VERSION_BASE_DIR__", "KWST 프로그램 위치 절대 경로");
include_once(__KWST_PHP_VERSION_BASE_DIR__."/kwst_referee.php");
?>
```

추가할 소스코드의 내용은 위와 같다. 위의 코드에서 "KWST 프로그램 위치 절대 경로" 부분을 KWST 프로그램이 설치된(압축 해제된) 경로로 수정해야 한다. 예를 들어 KWST가 "/var/www/html/kwstphp"에 설치된 경우라면 다음과 같이 수정하고 설치할 웹 페이지 첫줄에 추가하면 된다.

```
<?php // KISA WEB Security Template
define("__KWST_PHP_VERSION_BASE_DIR__", "/var/www/html/kwstphp");
include_once(__KWST_PHP_VERSION_BASE_DIR__."/kwst_referee.php");
?>
```

실제 예로 제로보드에 lib.php 파일에 KWST를 적용한다면 다음과 같이 추가하면 된다. 이렇게 추가되면 제로보드 lib.php 파일에 KWST가 적용되게 된다.

```
<?php // KISA WEB Security Template
define("__KWST_PHP_VERSION_BASE_DIR__", "./kwstphp");
include_once(__KWST_PHP_VERSION_BASE_DIR__."/kwst_referee.php");
?>
<?
/*****************************************************************************
 * Zeroboard library
 *
 ... 중략 ...
```


이처럼 적용하고자 하는 웹 페이지나 프로그램을 모두 수정하면 된다. 그러나 위 과정은 상당히 번거로우며 수정할 때에 PHP 문법적 에러가 발생하지 않도록 꼼꼼하게 하여야 한다. 수정이 완료되면 다음과 같은 방법으로 정상적으로 에러가 없는지 확인하도록 한다.

```
#php lib.php
...
중략
...
```

위와 같이 실행하였을 때에 경고나 에러가 발생하지 않으면 정상적으로 수정이 완료된 것이다.

www.kisa.or.kr

제 3 장

관리자 페이지 설명

웹 어플리케이션 보안템플릿
(PHP 버전)

제 3 장 | 관리자 페이지 설명

제3장에서는 KWST 관리자 페이지의 화면구성을 차례대로 설명한다. 각 화면 구성별 기능에 대한 자세한 설명은 다음 3장부터 차례대로 설명한다. 관리자 페이지로의 접근은 웹 브라우저를 통해 접근할 수 있으며 웹 브라우저 주소 입력란에 다음과 같이 입력하여 관리자 페이지로 접근할 수 있다.

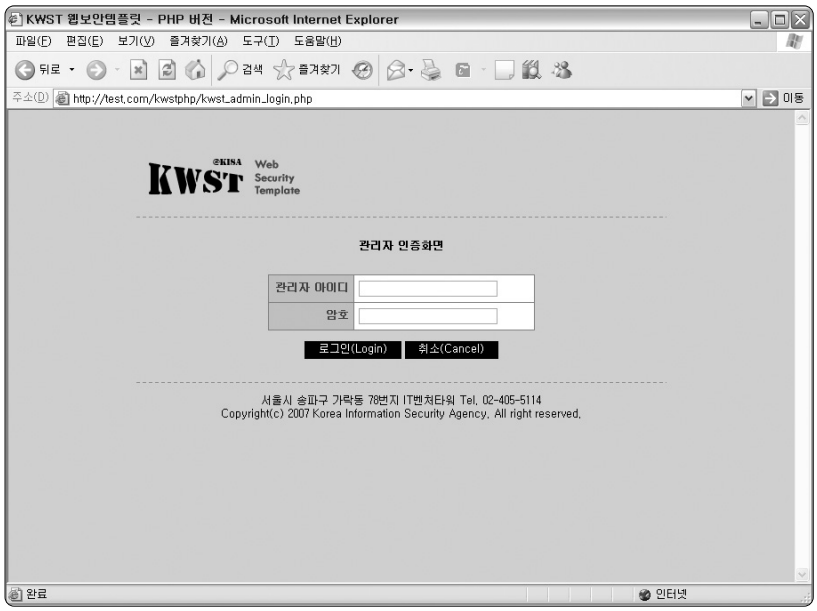
- **관리자 페이지 주소:**
  http://서버주소/KWST설치디렉터리/kwst_admin.php

인증을 거치지 않고 처음 관리자 페이지에 연결하는 경우에는 인증 화면으로 자동으로 이동된다.

- **테스트 관리자 페이지 환경**
  - 기본 URL : http://test.com
  - KWST 설치상대경로 : /kwstphp
  - KWST 관리자 페이지 전체경로 : http://test.com/kwstphp/kwst_admin.php

■ 관리자 인증

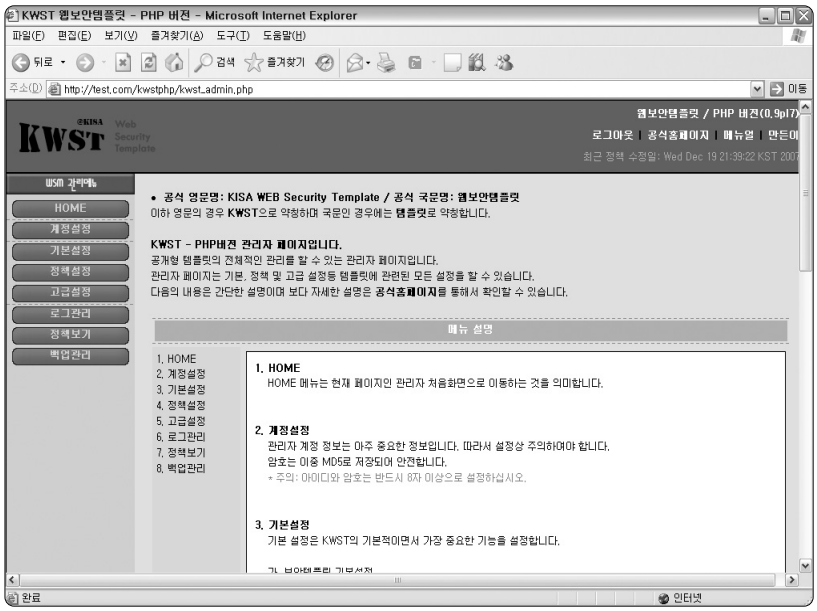
관리자 페이지에 인증하기 위해서는 반드시 로그인 과정을 통해 인증을 거쳐야 한다. 인증되지 않은 경우는 바로 다음 그림과 같이 인증 페이지로 이동된다.



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 다음의 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 페이지 메뉴는 8개로 구성되어 있다. 각 메뉴별 간략 설명은 앞의 초기화면에서 설명하고 있다. 이곳에서는 간단히 메뉴별 설명을 한다.

- **HOME**
  - HOME 메뉴는 현재 페이지인 관리자 처음화면으로 이동
  - 링크: kwst_admin.php

- **계정설정**
  - 관리자 계정 아이디와 암호를 설정함
  - 링크: kwst_admin_account.php

- **기본설정**
  - KWST 이름, 적용 여부, 메시지 방식 등 기본적인 운영에 관련된 정책을 설정
  - 링크: kwst_admin_config.php

- **정책설정**
  - 실제 악성코드를 탐지하는 정책을 설정함
  - 각 정책은 정규표현식을 지원함

– 링크: kwst_admin_policy.php

- **고급설정**
  – 각 페이지별 세부 정책 설정함
  – 각 페이지별로 허용하는 변수와 허용하지 않은 변수 등 상세히 설정이 가능함
  – 링크: kwst_admin_advance.php

- **로그관리**
  – 탐지되어 기록되는 로그들을 관리
  – 링크: kwst_admin_log.php

- **정책보기**
  – 현재 설정되어 있는 정책을 확인함
  – 링크: kwst_admin_policy_view.php

- **백업관리**
  – 현재 설정되어 있는 정책에 대하여 관리자 PC에 저장할 수 있음
  – 링크: kwst_admin_backup.php

제 4 장

관리자 계정 관리

제 4 장 | 관리자 계정 관리

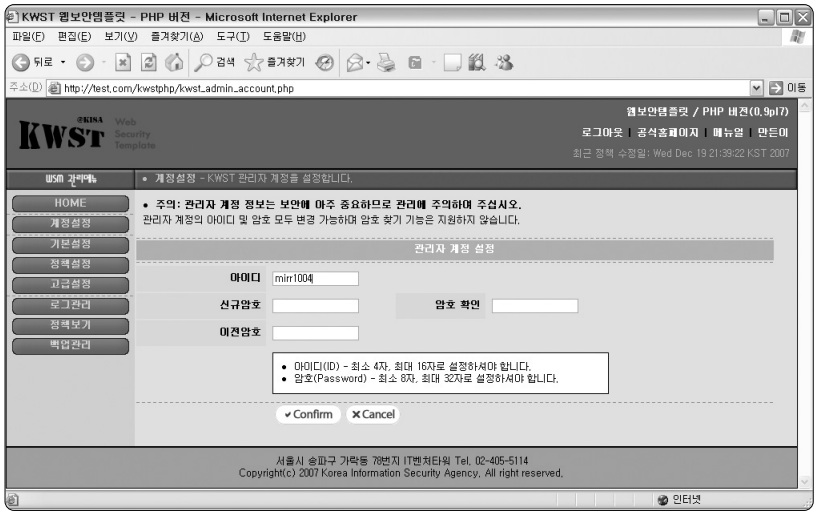
제4장에서는 KWST 관리자 페이지 인증을 위한 아이디와 암호를 설정하는 것을 설명한다. 관리자 계정의 아이디와 암호는 보안상의 이유로 상당히 긴 문자열로 구성되도록 하였다.

■ 아이디 설정 규칙

아이디는 최소 4자, 최대 16자의 문자열 또는 숫자로 구성된다.

■ 암호 설정 규칙

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



새로운 관리자 아이디와 암호, 암호 확인을 입력하고 이전 암호를 정확히 입력하게 되면 "관리자 계정 정보가 수정되었습니다." 메시지와 함께 설정된다.

www.kisa.or.kr

제 5 장

기본 설정

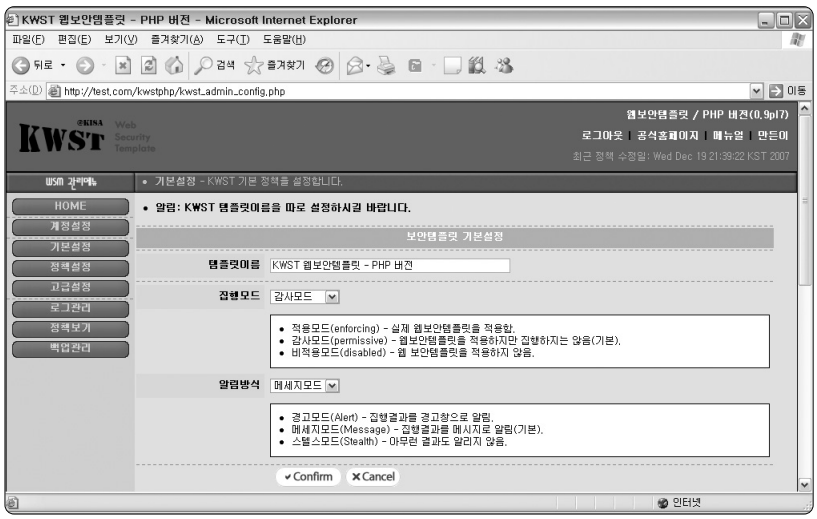
1. 보안 모듈 기본 설정
2. 사이트 설정
3. 보안모듈 적용대상 설정

제 5 장 | 기본 설정

제5장 기본 설정에서는 KWST에 대한 가장 중요한 부분으로 보안모듈 기본설정, 사이트 설정, 보안모듈 적용대상 등 운영에 관련된 정책 설정에 대하여 설명한다.

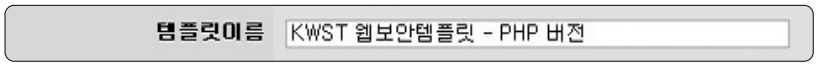
1. 보안 모듈 기본 설정

보안 모듈 기본 설정에서는 모듈이름, 집행모드 그리고 알림방식에 대해서 설정한다.



■ 모듈이름 설정

설치한 KWST 관리자 페이지의 이름을 설정한다. 설정된 모듈이름은 각 관리자 페이지의 타이틀(title)에 표시되며 관리자가 임의대로 모듈이름을 설정하면 된다.



■ 집행모드 설정 (*설정상 주의필요)

집행모드 설정은 KWST 설정에 있어서 가장 중요한 부분으로 설치한 KWST를 실제 집행할 것인지 혹은 설치만하고 집행하지 않을 것인지 등을 설정한다. 집행모드에는 총 3개의 모드가 있으며 적용모드, 감사모드 그리고 비적용모드가 있다.

- **적용모드(enforcing)**
  - 집행모드가 적용모드로 설정되어 있을 경우에는 KWST에서 정의한 정책들에 의해 탐지를 수행하고 차단 또는 허용된다.

- **감사모드(permissive) – 기본 설정 상태**
  - 감사모드로 설정되어 있을 경우에는 적용모드와 마찬가지로 KWST에서 정의한 정책들에 의해 탐지를 수행하지만 무조건 허용됨
  - 설치 초기에 정책을 작성하는 과정에 감사모드로 정책의 안정화하는 것이 좋음

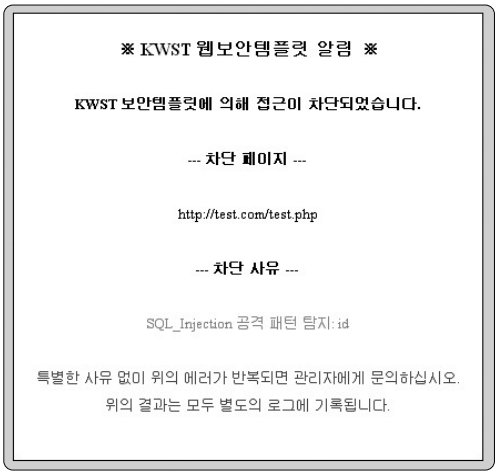
- **비적용모드(disabled)**
  - 비적용모드로 설정되어 있을 경우에는 KWST 프레임워크에서 바로 빠져나와 아무런 탐지도 적용도 되지 않음

■ 알림방식 설정

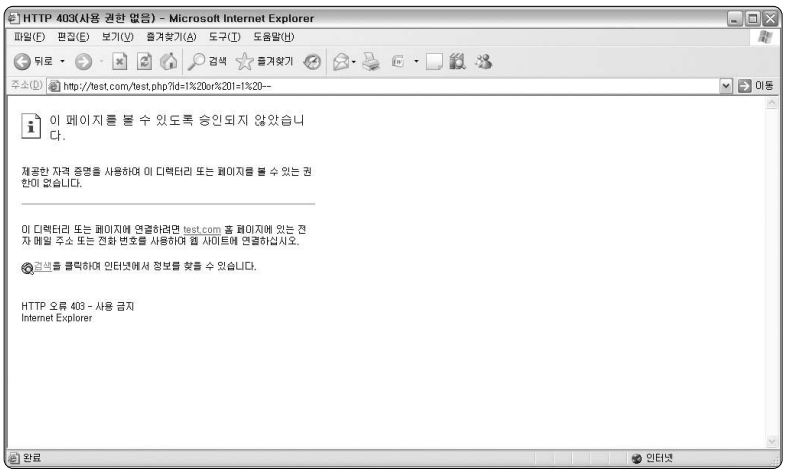
알림방식 설정은 **집행모드**가 **적용모드**로 설정되어 있을 때 비정상적인 행위로 탐지되어 사용자의 접근이 차단할 필요가 있을 경우 어떻게 차단할 것인지에 대한 설정이다. 알림방식에는 **경고모드**, **알림모드** 그리고 **스텔스모드**가 있다.

- **경고모드(alert)**
  - 집행 결과를 **경고창**으로 알리며 사용자에게 곧바로 결과를 알리고자 할 때 설정

- **메시지모드(message)**
  - 집행 결과를 메시지로 알림, 일반적인 에러 메시지처럼 알림



- **스텔스모드(stealth)**
  - 권한이 없다는 403 접근 거부 페이지를 보여줌
  - KWST 웹보안모듈이 설치되어 운영하고 있다는 것을 숨기고자 할 때에 유용함

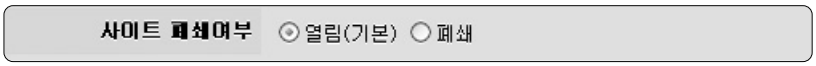


2. 사이트 설정

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

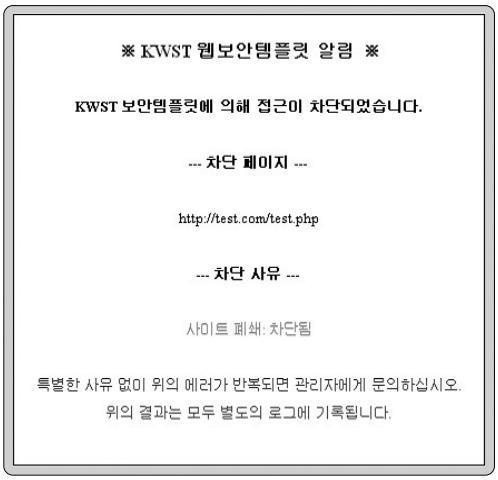
■ 사이트 폐쇄여부 설정

KWST 설치되어 운영 중인 사이트를 일시적으로 또는 영구적으로 차단하고자 한다면 사이트를 폐쇄 할 수 있다.



- **열림**
  – 사이트를 정상적으로 운영함

- **폐쇄**
  – 사이트를 폐쇄하여 운영하지 않음, 다음의 그림은 사이트가 폐쇄된 화면



■ 사이트 문자셋 설정

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

- UTF-8
  - 서버 및 웹 페이지 설정이 UTF-8인 경우

- eucKR(CP949)
  - 서버 및 웹 페이지 설정이 eucKR(CP949)인 경우

정상적으로 문자셋이 설정되어 있을 경우에는 다음의 그림과 같이 제대로 된 알림 메시지를 볼 수 있다.

다음의 그림은 문자셋이 잘못 설정된 경우의 알림 메시지이다. 글씨가 깨어져 정확히 확인할 수 없게 된다.

3. 보안모듈 적용대상 설정

보안모듈 적용대상 설정은 KWST 웹보안모듈에 의해서 탐지할 대상들에 대한 설정이다. 기본으로 GET, POST, FILE, COOKIE 등에 전역변수들을 대상으로 탐지를 수행하도록 설정되어 있다.

GET 변수 설정

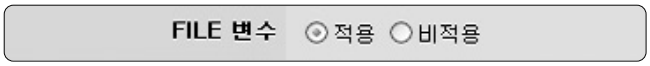
GET 변수들을 대상으로 탐지를 수행할지 안할지를 설정한다.

POST 변수 설정

POST 변수들을 대상으로 탐지를 수행할지 안할지를 설정한다.

FILE 변수 설정

FILE 변수들을 대상으로 탐지를 수행할지 안할지를 설정한다.



COOKIE 변수 설정

COOKIE 변수들을 대상으로 탐지를 수행할지 안할지를 설정한다.

www.kisa.or.kr

제 6 장

정책 설정

웹 어플리케이션 보안템플릿
(PHP 버전)

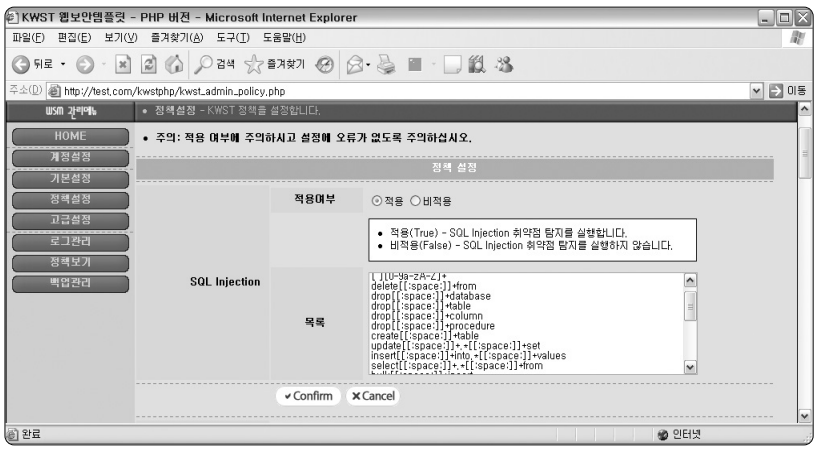
1. SQL Injection 정책 설정
2. XSS 정책 설정
3. 불량단어 정책 설정
4. 불량태그 정책 설정
5. 아이피 정책 설정
6. 파일 정책 설정

제 6 장 | 정책 설정

제6장 정책 설정에서는 KWST에서 탐지할 공격 형태들을 유형별로 설정한다. 대표적인 공격들인 SQL Injection, XSS, 불량단어(WORD), 불량태그(TAG), 아이피주소, 파일별로 정책을 설정할 수 있다.

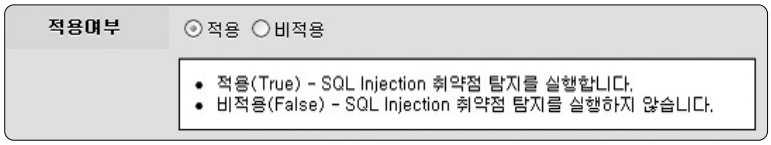
1. SQL Injection 정책 설정

SQL Injection 공격 형태를 정규표현식 형태로 설정할 수 있다. 이렇게 설정된 정규표현식 규칙에 포함되는 모든 공격은 탐지된다.



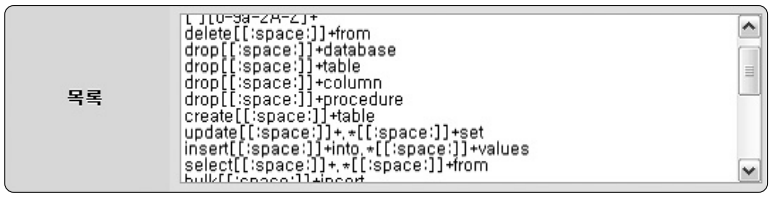
● **적용여부**

– SQL Injection 공격 탐지를 수행할지 안할지를 설정한다.



● **목록**

– SQL Injection 공격 형태를 정규표현식으로 설정한다.

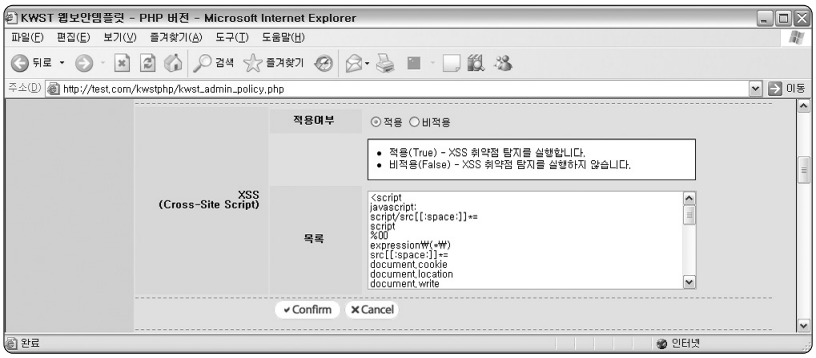


■ SQL Injection 공격 탐지 차단

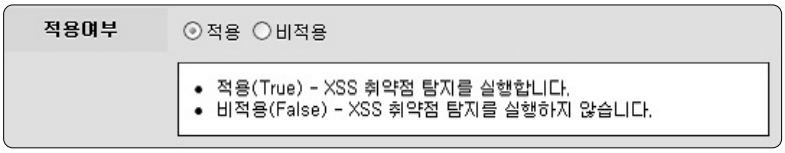
변수에 “1 or 1 --”와 같이 목록에 포함된 형태의 SQL Injection 공격 코드를 넣었을 때 다음과 같이 탐지되고 차단된다.

2. XSS 정책 설정

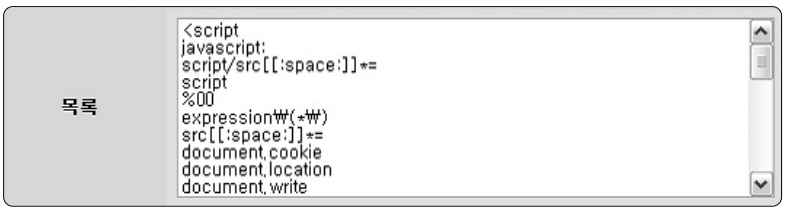
XSS 공격 형태를 정규표현식 형태로 설정할 수 있다. 이렇게 설정된 정규표현식 규칙에 포함되는 모든 공격은 탐지된다.



- **적용여부**
  - XSS 공격 탐지를 수행할지 안할지를 설정한다.

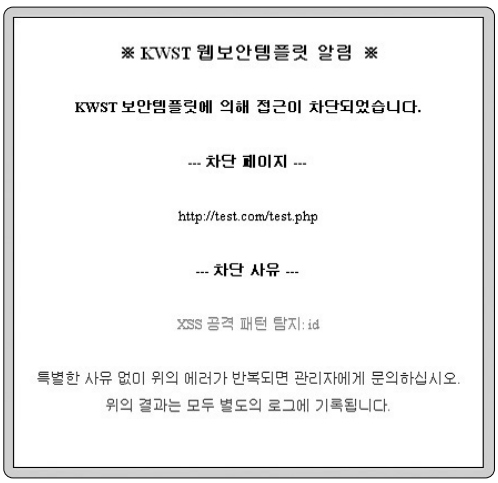


- **목록**
  - XSS 공격 형태를 정규표현식으로 설정한다.



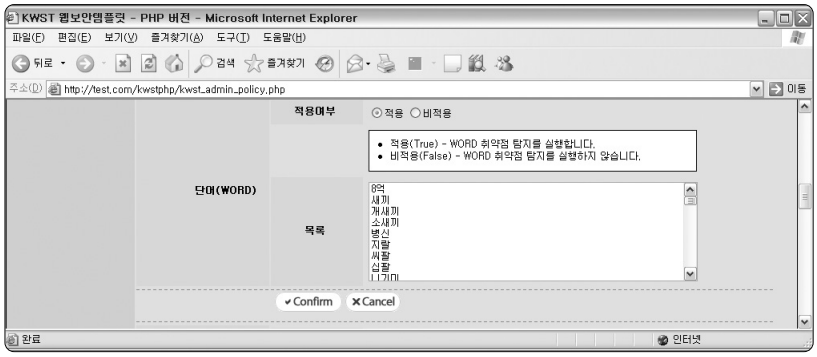
■ XSS 공격 탐지 차단

변수에 "javascript:"와 같이 목록에 포함된 형태의 XSS 공격 코드를 넣었을 때 다음과 같이 탐지되고 차단된다.



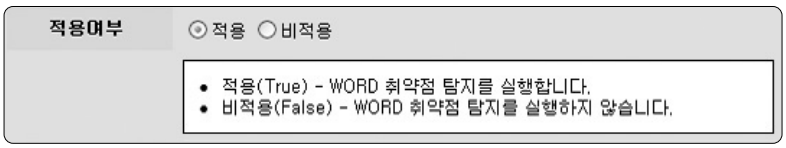
3. 불량단어 정책 설정

불량단어 형태를 정규표현식 형태로 설정할 수 있다. 이렇게 설정된 정규표현식 규칙에 포함되는 모든 공격은 탐지된다. 불량단어는 스팸성 글이나 악성 댓글을 차단하는데 유용하다.



- **적용여부**

  – 불량단어 탐지를 수행할지 안할지를 설정한다.

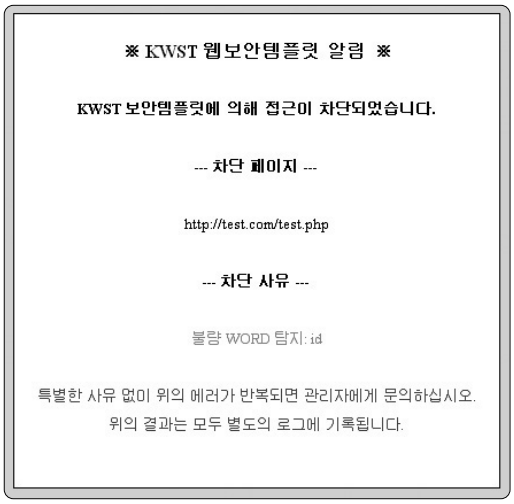


- **목록**

  – 불량단어 형태를 정규표현식으로 설정한다.

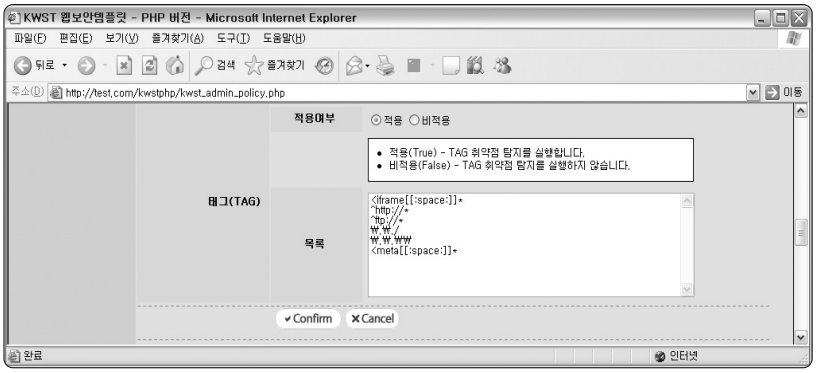
■ 불량단어 공격 탐지 차단

변수에 "현찰게임과 같이 목록에 포함된 형태의 불량단어를 넣었을 때 다음과 같이 탐지되고 차단된다.

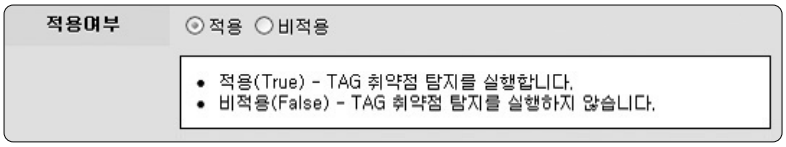


4. 불량태그 정책 설정

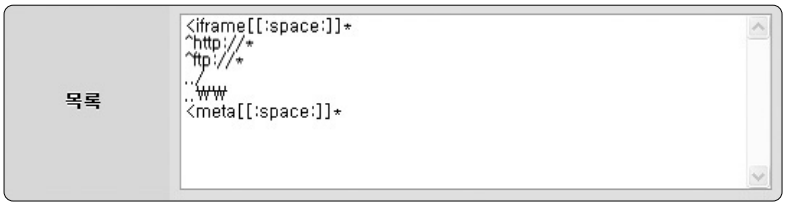
불량태그 형태를 정규표현식 형태로 설정할 수 있다. 이렇게 설정된 정규표현식 규칙에 포함되는 모든 공격은 탐지된다.



- **적용여부**
  - 불량태그 공격 탐지를 수행할지 안할지를 설정한다.

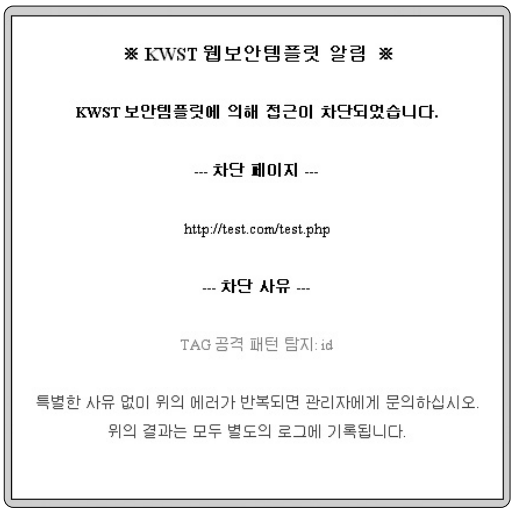


- **목록**
  - 불량태그 공격 형태를 정규표현식으로 설정한다.



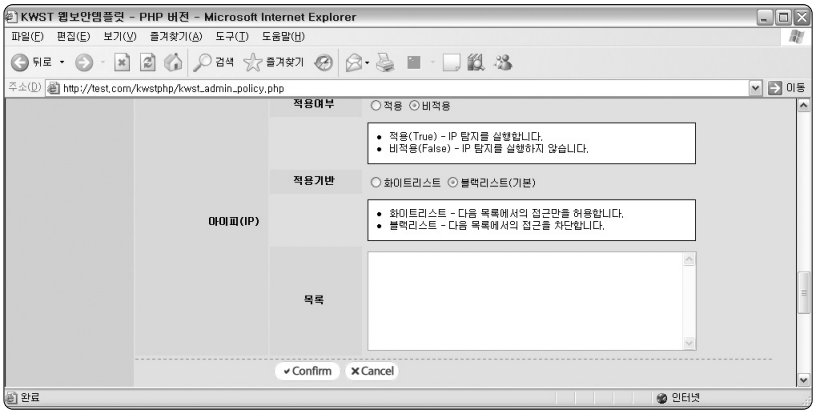
■ 불량태그 공격 탐지 차단

변수에 “<iframe”와 같이 목록에 포함된 형태의 불량태그를 넣었을 때 다음과 같이 탐지되고 차단된다.



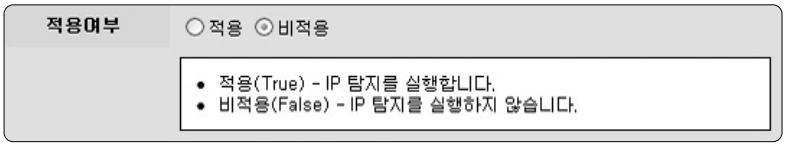
5. 아이피 정책 설정

아이피 정책 설정에서는 아이피 주소를 정규표현식 형태로 설정하여 접근 통제할 정책을 설정한다. 이렇게 설정된 정규표현식 규칙에 포함되는 모든 아이피는 적용기반에 따라 차단되거나 허용된다.



● **적용여부**

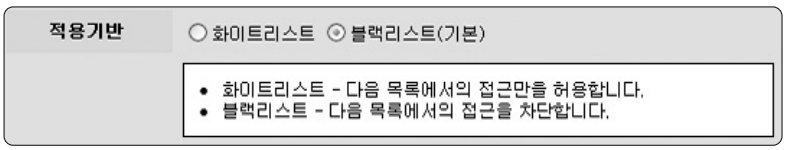
아이피 탐지를 수행할지 안할지를 설정한다.



● **적용기반**

– 화이트리스트 : 목록에 포함된 아이피 주소에서만 접근을 허용함

– 블랙리스트 : 목록에 포함된 아이피 주소에서의 접근은 차단함

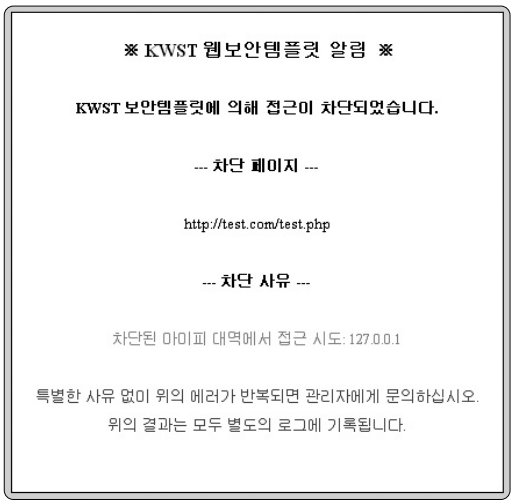


● 목록

– 아이피 주소를 정규표현식으로 설정한다.

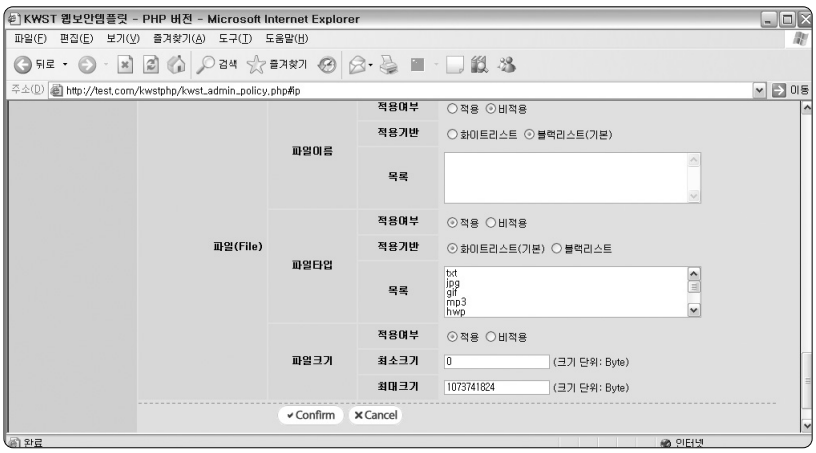
■ 아이피 탐지 차단

위의 그림과 같이 아이피 설정 부분에 블랙리스트 방식으로 "127.0.0.1"를 설정하고 접근했을 때 아래의 그림과 같이 탐지된다.

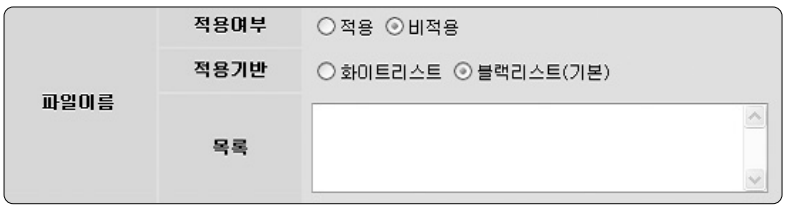


6. 파일 정책 설정

파일 정책은 업로드하는 파일들에 이름과 타입 그리고 크기로 허용할 것인지 차단할 것인지를 설정한다.



■ 파일이름



- **적용여부**
  - 파일이름 탐지를 수행할지 안할지를 설정한다.

● **적용기반**

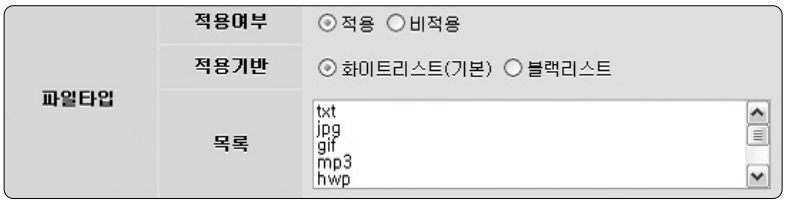
– 화이트리스트 : 목록에 포함된 파일이름만 업로드를 허용함

– 블랙리스트 : 목록에 포함된 파일이름은 업로드를 차단함

● **목록**

– 파일이름을 정규표현식으로 설정한다.

■ 파일타입



● **적용여부**

– 파일타입 탐지를 수행할지 안할지를 설정한다.

● **적용기반**

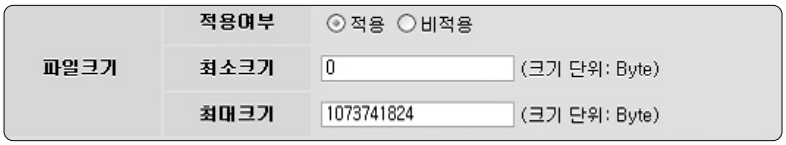
– 화이트리스트 : 목록에 포함된 파일타입만 업로드를 허용함

– 블랙리스트 : 목록에 포함된 파일타입은 업로드를 차단함

● **목록**

– 파일타입을 정규표현식으로 설정한다.

■ 파일크기



- **적용여부**
  – 파일크기 탐지를 수행할지 안할지를 설정한다.

- **최소크기**
  – 업로드를 허용할 최소크기 값을 설정

- **최대크기**
  – 업로드를 허용할 최대크기 값을 설정

■ 파일 업로드 탐지 차단

허용하지 않은 확장자인 "*.php"를 가진 파일을 업로드할 때에 다음과 같이 탐지되고 차단된다.

※ KWST 웹보안템플릿 알림 ※

KWST 보안템플릿에 의해 접근이 차단되었습니다.

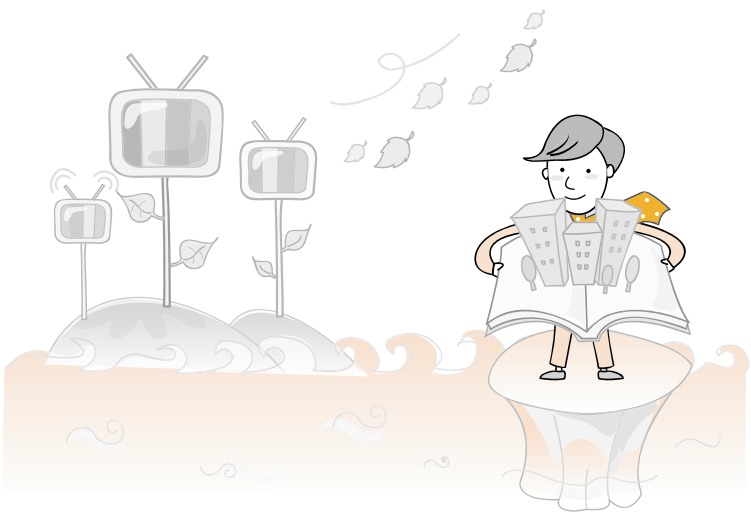
--- 차단 페이지 ---

http://test.com/test.php

--- 차단 사유 ---

허용되지 않은 확장자 파일 업로드: file

특별한 사유 없이 위의 에러가 반복되면 관리자에게 문의하십시오.
위의 결과는 모두 별도의 로그에 기록됩니다.



www.kisa.or.kr

제 7 장

고급 설정

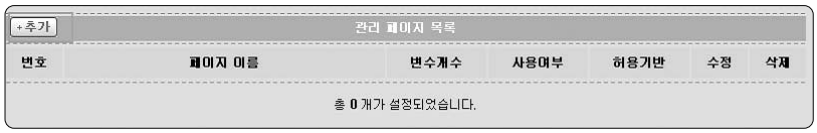
1. 신규 페이지 추가
2. 관리 페이지 수정과 삭제
3. 각 페이지별 변수 설정
4. 페이지별 정책 테스트

제 7 장 | 고급 설정

제7장 고급 설정에서는 각 페이지별로 정책 설정한다. 이때에 설정된 페이지들은 정책 설정에서 설정한 정책보다 우선 탐지된다.

1. 신규 페이지 추가

위의 그림은 아무런 페이지별 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**

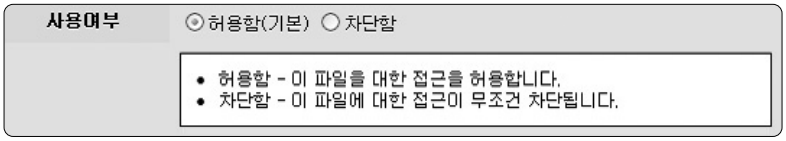
– 추가할 페이지 이름으로 http://host/path에서 /path 입력

– ex) http://testcom/test.php일 경우"/test.php" 이 부분을 입력하면 됨

– 반드시 "페이지보기" 버튼을 클릭하여 정상적으로 /path를 적었는지를 확인해 보아야 다음으로 진행이 됨

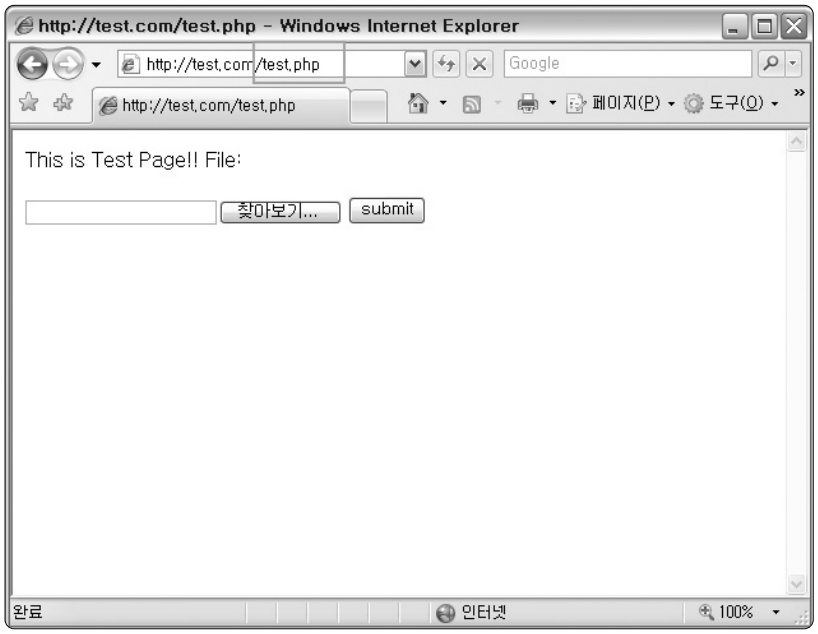
다음의 그림은 "페이지보기" 클릭 후 페이지 이름을 잘못 입력하였을 때의 내용으로 "웹 페이지를 찾을 수 없습니다."라고 표시된다.

- **사용여부**
  - 현재 추가할 페이지에 대한 접근을 허용할 것인지 차단할 것인지를 설정한다. 이때에 차단으로 설정할 경우 해당 페이지에 대한 접근은 무조건 차단된다.

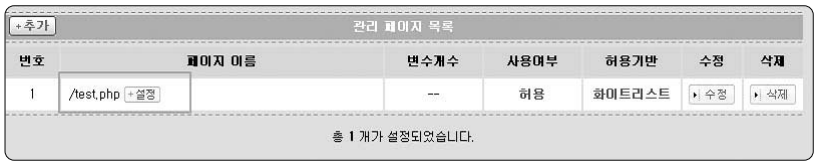


- **허용기반**
  - 추가할 페이지에서 사용하는 변수들에 대하여 화이트리스트 방식으로 설정할 것인지 아니면 블랙리스트 방식으로 설정할 것인지를 나타낸다. 화이트리스트로 설정할 경우에는 정해진 변수 이외에는 어떠한 변수에 사용도 차단되며 블랙리스트 방식의 경우에는 지정된 변수의 사용이 무조건 차단된다.

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

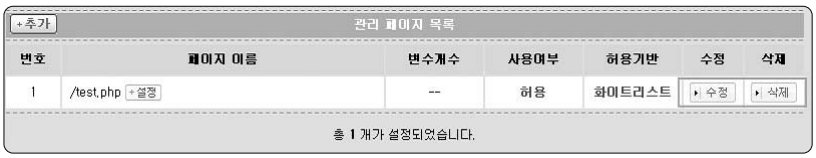


다음과 같이 정상적으로 페이지를 추가되면 관리 대상 페이지 목록에 나타난다. 앞서 입력한 “test.php”가 추가되어 있는 것을 볼 수 있다.



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 위의 그림과 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.

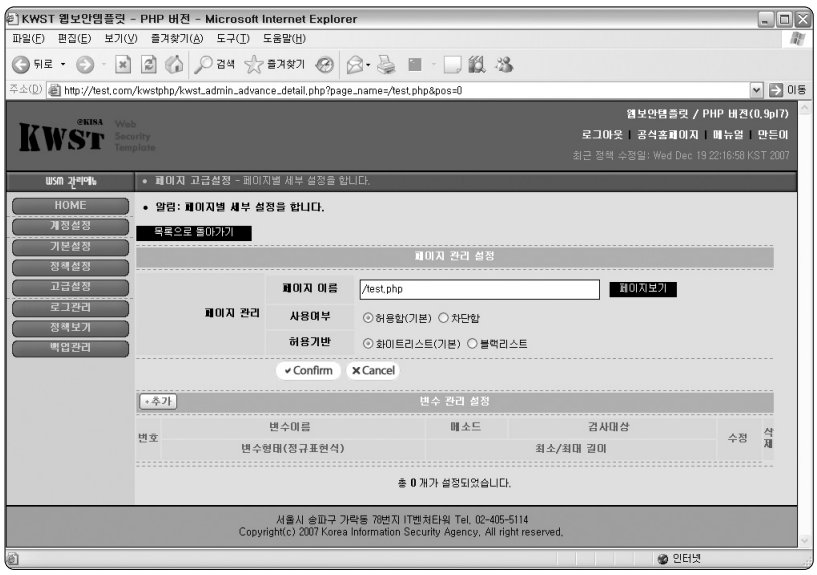
■ 페이지 삭제

페이지 삭제는 삭제 버튼을 클릭하면 다음의 그림과 같이 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.

아래의 그림은 페이지별 변수 설정 화면이다. 아랫부분에 변수 관리 설정 부분에 허용하거나 차단할 변수들에 목록이 표시된다. 관리할 변수의 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

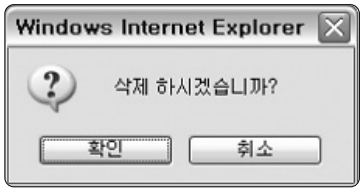
"test.php" 페이지에서 변수 id와 no를 사용하고 id 변수는 알파벳으로만 구성되고 길이는 최소 4에서 최대 32이고 no변수는 숫자로만 구성되어지며 길이가 최소 1에서 최대 32로 구성된다고 할 때에 해당 변수들에 정책을 추가한다면 다음의 그림과 같이 설정한다.

■ 변수 수정과 삭제

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

- 수정 클릭시의 확인 창

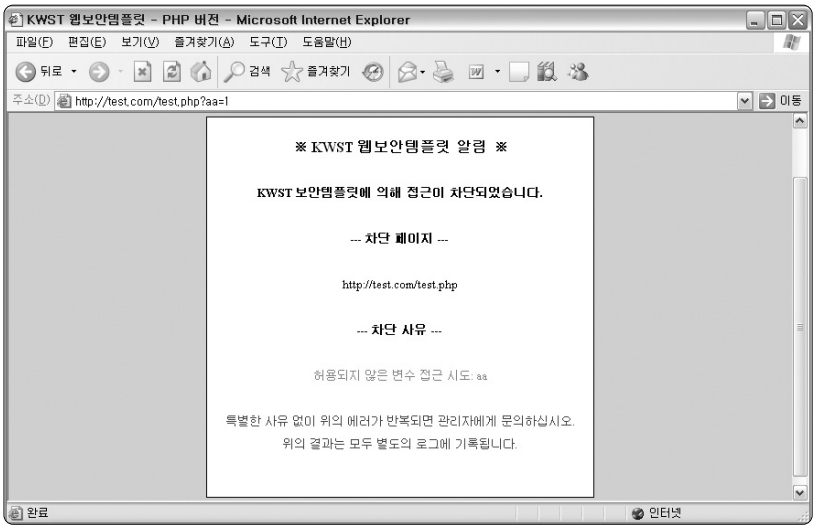
- 삭제 클릭시의 확인 창



4. 페이지별 정책 테스트

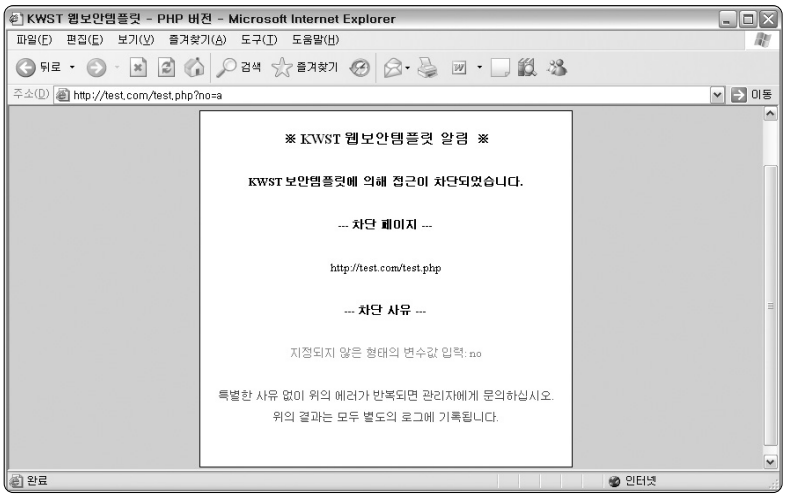
■ 설정하지 않은 id 사용

변수 aa는 허용되지 않았기 때문에 다음의 그림과 같이 차단된다.



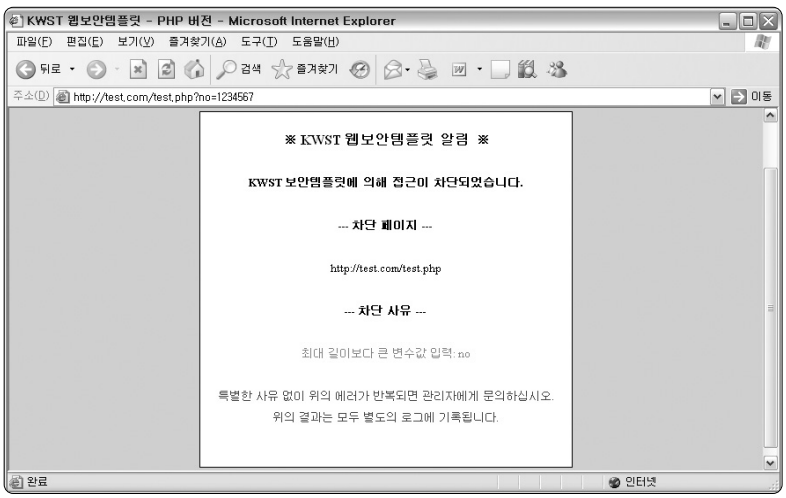
■ 잘못된 형태의 값을 입력

변수 no는 [0-9] 정규표현식에 따라 숫자로만 구성되어야 한다.



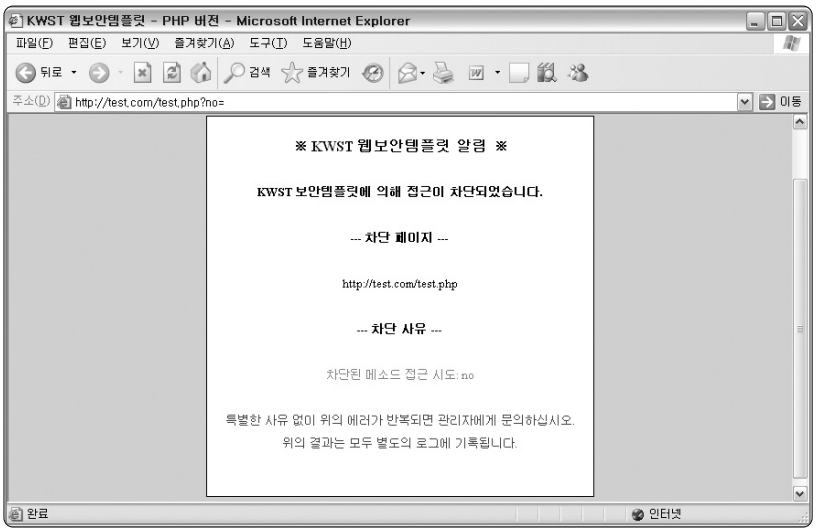
■ 최소, 최대 길이 범위를 벗어난 입력

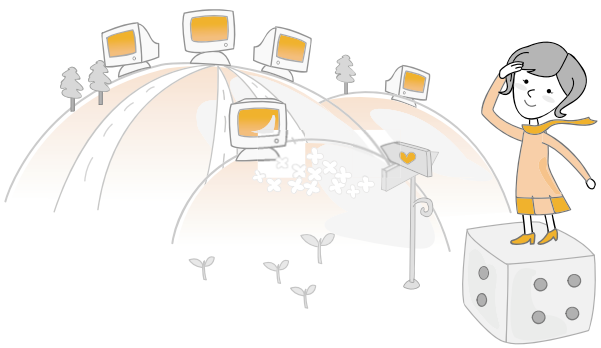
변수 no는 최소 1에서 최대 6 자리만 허용되도록 정책이 설정되어 있어 7자리 이상입력하면 다음과 같이 차단된다.



■ 허용되지 않은 메소드 접근

GET 메소드가 허용되지 않았을 때 GET으로의 접근은 차단된다.





제 8 장

로그 관리

웹 어플리케이션 보안템플릿
(PHP 버전)

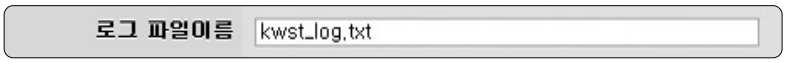
제 8 장 | 로그 관리

제8장 로그 관리는 KWST에 의해서 탐지된 결과를 저장할 로그 파일에 대한 설정이다. 로그 파일이름과 기록여부 그리고 기록방식 등을 설정한다.

■ 로그 파일이름 설정

로그 파일이름은 기본으로 kwst_log.txt로 설정되어 있다. 기본 파일이름을 이용할 경우

에는 로그 정보가 유출되므로 관리자만 아는 이름으로 수정하여 사용하길 추천한다.



- **로그 파일 이름 규칙**
  - Year.Month.Day-로그파일이름(ex. 20071016-kwst_log.txt)

■ 로그 기록여부 설정

로그를 기록할 것인가 기록하지 않을 것인가를 설정한다.

- **기록**
  - 로그를 기록함

- **무기록**
  - 로그를 기록하지 않음

■ 로그 기록방식 설정

기록할 로그의 방식을 설정한다. 설정에 따라 간략하게 또는 상세하게 로그가 기록된다. 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] /~mirr1004/bbs/write_ok.php:
memo = 인터넷룰렛게임,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] /~mirr1004/bbs/write_ok.php:
memo = 인터넷룰렛게임,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 따라 설정하면 된다. 이것을 제대로 설정하지 않으면 나중에 로그를 확인할 때에 글씨가 깨질 수 있으므로 정확히 설정하도록 한다.

■ 로그 목록개수 설정

로그 관리에서 출력할 로그의 개수를 설정한다. 기본 20개로 설정되어 있다.

■ 로그 목록

일별로 로그를 출력하며 가장 최근의 로그 파일이 제일 위에 놓인다.

번호	로그파일	파일크기	최근시간	삭제
1	20071219-kwst_log.txt 다운로드	2,592 Bytes	December 19 2007 22:29:46	삭제
2	20071218-kwst_log.txt 다운로드	5,982 Bytes	December 18 2007 21:29:48	삭제
3	20071217-kwst_log.txt 다운로드	5,465 Bytes	December 17 2007 21:38:58	삭제
4	20071216-kwst_log.txt 다운로드	3,137 Bytes	December 16 2007 23:12:53	삭제
5	20071201-kwst_log.txt 다운로드	11,929 Bytes	December 01 2007 23:48:08	삭제
6	20071130-kwst_log.txt 다운로드	6,191 Bytes	November 30 2007 23:50:52	삭제
7	20071129-kwst_log.txt 다운로드	12,220 Bytes	November 29 2007 23:49:40	삭제

www.kisa.or.kr

제 9 장

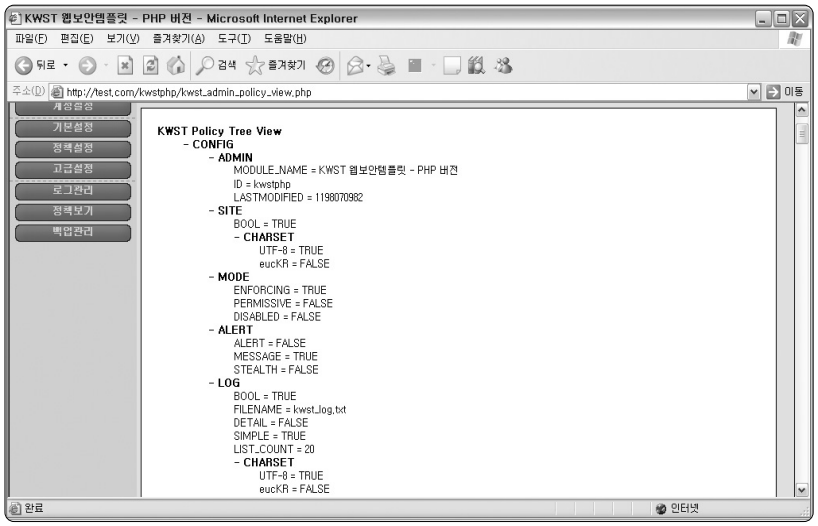
정책 보기

웹 어플리케이션 보안템플릿
(PHP 버전)

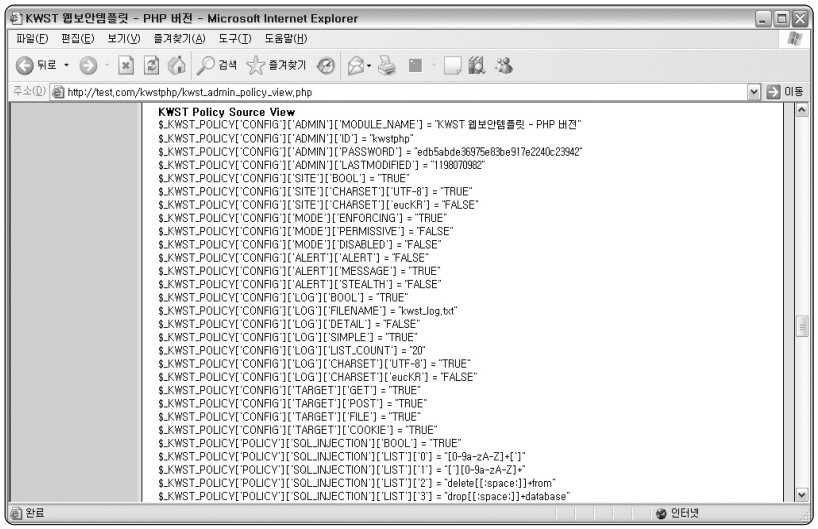
제 9 장 | 정책 보기

제9장 정책 보기는 현재 설정된 정책 정보를 트리 구조와 소스 형태로 일괄적으로 확인할 수 있는 기능이다.

■ 트리구조 정책 보기



■ 소스형태 정책 보기


KWST 웹보안템플릿 - PHP 버전 - Microsoft Internet Explorer
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
뒤로 검색 즐겨찾기
주소(D) http://test.com/kwstphp/kwst_admin_policy_view.php
이동
KWST Policy Source View
$_KWST_POLICY['CONFIG']['ADMIN']['MODULE_NAME'] = "KWST 웹보안템플릿 - PHP 버전"
$_KWST_POLICY['CONFIG']['ADMIN']['ID'] = "kwstphp"
$_KWST_POLICY['CONFIG']['ADMIN']['PASSWORD'] = "edb5abde36975e83be917e2240c23942"
$_KWST_POLICY['CONFIG']['ADMIN']['LASTMODIFIED'] = "1198070982"
$_KWST_POLICY['CONFIG']['SITE']['BOOL'] = "TRUE"
$_KWST_POLICY['CONFIG']['SITE']['CHARSET']['UTF-8'] = "TRUE"
$_KWST_POLICY['CONFIG']['SITE']['CHARSET']['eucKR'] = "FALSE"
$_KWST_POLICY['CONFIG']['MODE']['ENFORCING'] = "TRUE"
$_KWST_POLICY['CONFIG']['MODE']['PERMISSIVE'] = "FALSE"
$_KWST_POLICY['CONFIG']['MODE']['DISABLED'] = "FALSE"
$_KWST_POLICY['CONFIG']['ALERT']['ALERT'] = "FALSE"
$_KWST_POLICY['CONFIG']['ALERT']['MESSAGE'] = "TRUE"
$_KWST_POLICY['CONFIG']['ALERT']['STEALTH'] = "FALSE"
$_KWST_POLICY['CONFIG']['LOG']['BOOL'] = "TRUE"
$_KWST_POLICY['CONFIG']['LOG']['FILENAME'] = "kwst_log.txt"
$_KWST_POLICY['CONFIG']['LOG']['DETAIL'] = "FALSE"
$_KWST_POLICY['CONFIG']['LOG']['SIMPLE'] = "TRUE"
$_KWST_POLICY['CONFIG']['LOG']['LIST_COUNT'] = "20"
$_KWST_POLICY['CONFIG']['LOG']['CHARSET']['UTF-8'] = "TRUE"
$_KWST_POLICY['CONFIG']['LOG']['CHARSET']['eucKR'] = "FALSE"
$_KWST_POLICY['CONFIG']['TARGET']['GET'] = "TRUE"
$_KWST_POLICY['CONFIG']['TARGET']['POST'] = "TRUE"
$_KWST_POLICY['CONFIG']['TARGET']['FILE'] = "TRUE"
$_KWST_POLICY['CONFIG']['TARGET']['COOKIE'] = "TRUE"
$_KWST_POLICY['POLICY']['SQL_INJECTION']['BOOL'] = "TRUE"
$_KWST_POLICY['POLICY']['SQL_INJECTION']['LIST']['0'] = "[0-9a-zA-Z]+['|"]"
$_KWST_POLICY['POLICY']['SQL_INJECTION']['LIST']['1'] = "['|"][0-9a-zA-Z]+"
$_KWST_POLICY['POLICY']['SQL_INJECTION']['LIST']['2'] = "delete[[:space:]]+from"
$_KWST_POLICY['POLICY']['SQL_INJECTION']['LIST']['3'] = "drop[[:space:]]+database"
완료
인터넷

www.kisa.or.kr

제 10 장

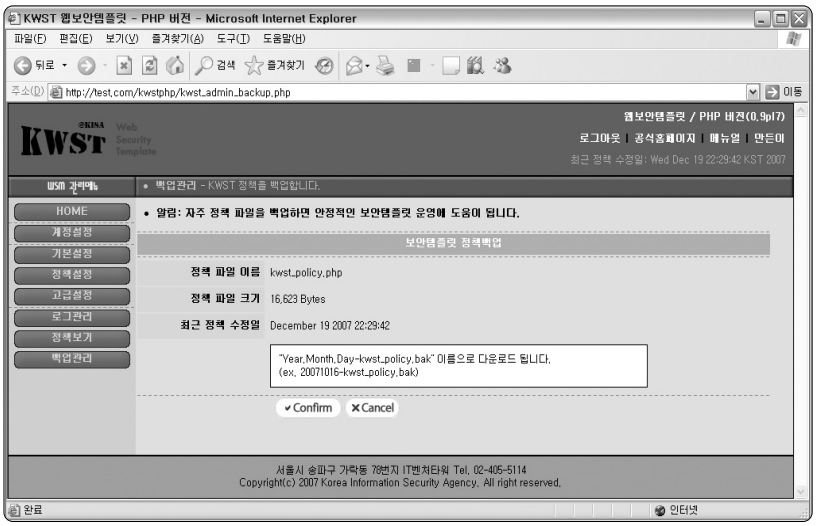
백업 관리

웹 어플리케이션 보안템플릿
(PHP 버전)

제 10 장 | 백업 관리

제10장 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.

www.kisa.or.kr

제 11 장

마치며...

제 11 장 | 마치며...

본 문서를 통해 많은 웹어플리케이션 사용자나 개발자들이 자신의 소중한 웹 서버, 웹 프로그램 나아가서 개인 정보의 보안성을 강화하여 보다 안전한 환경에서 영위하길 바란다.

웹 어플리케이션 보안템플릿(PHP 버전)

2007년 9월 인쇄
2007년 9월 발행

발행인 황중연
발행처 한국정보보호진흥원
서울시 송파구 중대로 135 IT벤처타워(서관)
TEL. (02)4055-114, http://www.kisa.or.kr
인쇄처 호정씨앤피(Tel 02-2277-4718)