

# CASTLE 설치 가이드(ASP 홈페이지)

2009. 01.

인터넷침해대응센터 (KISC)



※ 본 보고서의 전부나 일부를 인용시 반드시 [자료: 한국인터넷진흥원(KISA)]를 명시하여 주시기 바랍니다.

## 설치 준비

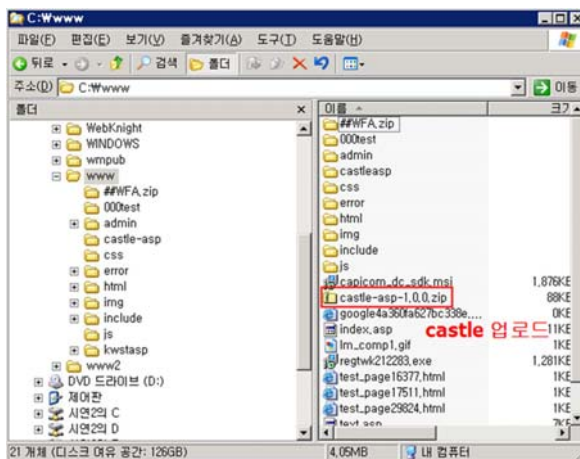
이 장에서는 본 가이드에서 예제로 적용할 홈페이지 정보와 시스템 정보, 그리고 CASTLE을 업로드해서 설치 준비하는 방법을 설명한다.

### 1.1 설치 환경

본 가이드에서 CASTLE을 적용할 홈페이지 정보와 시스템 정보는 아래와 같다.

- OS : Windows 2003 Enterprise, IIS 6.0
- 홈페이지 도메인: http://test.com
- 홈페이지 종류 : ASP 기업 홈페이지
- 쇼핑몰 홈 디렉터리 : C:\www

### 1.2 파일 업로드



test.com 홈페이지의 홈 디렉토리인 C:\www 에 CASTL ASP 버전을 업로드하고 홈 디렉토리에 압축을 해지하여, 설치 준비를 한다. 압축을 해제 후 그림의 "castle-asp" 폴더 명을 그대로 사용하면, 공격자들에게 CASTLE 사용여부를 노출할 수 있으므로 폴더명을 변경하여 설정하기 바란다.

## 2 설치

이 설치 장에서는 CASTLE 설치 페이지에 접근하여, 설치 하는 과정을 설명한다.

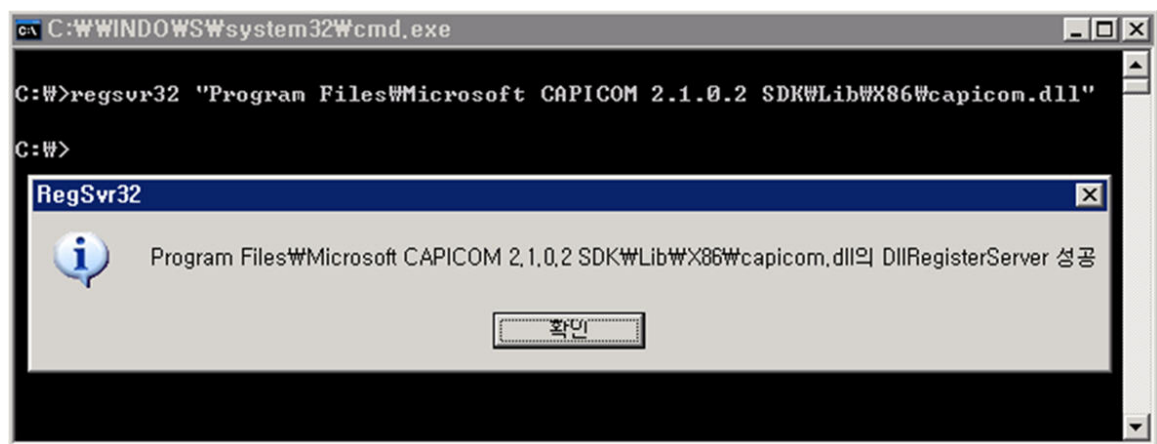
### 2.1 설치 준비

CASTLE ASP 버전을 윈도우에 설치하기 전에 CAPICOM 컴포넌트를 추가해야 한다. CAPICOM은 마이크로소프트사의 홈페이지에서 다운로드 하여, 레지스트리에 등록해야 한다. 다운로드 위치는 다음과 같다.

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

다운 받은 CAPICOM을 설치한 후 CMD 창에서 capicom.dll 파일이 존재하는 폴더로 이동해서 다음과 같은 명령어를 실행하여 레지스트리에 등록한다.

```
regsvr32 capicom.dll
```



또는 다운 받은 CAPICOM을 압축을 해제하여 capicom.dll 파일만 레지스트리에 추가해도 된다.

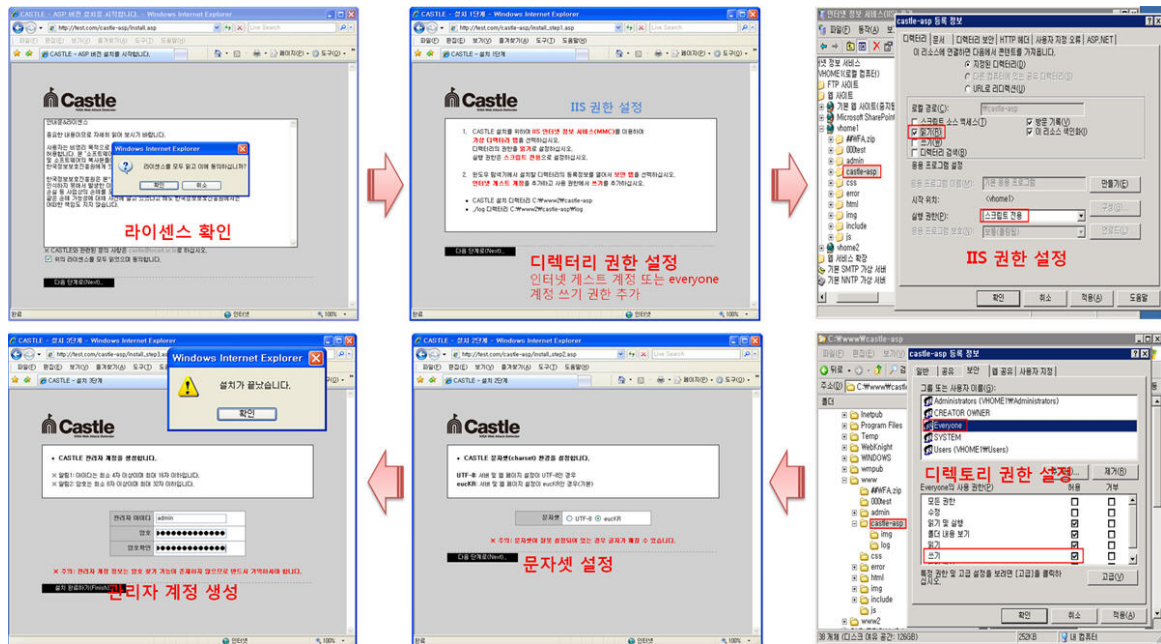
## 2.2 설치 과정

인터넷 브라우저를 실행하여 아래 주소로 접속한 후, 아래 그림과 같이 설정하여 설치를 완료한다.

- 설치 페이지 : <http://test.com/castle-asp/install.asp>

만약 홈 디렉토리에 압축을 해제한 폴더명이 변경 되었다면 설치 페이지의 접근 주소는 "castle-php"가 변경된 폴더명으로 수정하여 CASTLE 설치 페이지에 접근 해야 한다. 이후 본 가이드에서 나오는 castle-php는 현재 적용된 홈페이지에서 설치된 CASTLE의 홈 디렉토리이다.

- 설치 페이지 : [http://test.com/변경된\\_폴더명/install.asp](http://test.com/변경된_폴더명/install.asp)



※ CASTLE은 패스워드를 찾는 기능이 없기 때문에 패스워드를 반드시 기억해야 한다.

### 3 적용

이 장에서는 홈페이지 파일들이 공통으로 사용하는 헤더 파일을 찾고, 해당 파일에 CASTLE을 적용하는 방법에 대해 설명한다.

#### 3.1 공통파일에 적용

홈페이지의 소스 파일들을 확인하여 대다수 파일들에서 참조해서 사용하는 공통파일(헤더)을 찾는다. 현재 적용중인 홈페이지의 fsboard.asp를 확인한 결과 다음과 같은 내용을 확인할 수 있다.

<중략...>

```
<object id="objRs" runat="Server" progid="ADODB.Recordset"> </object>
<object id="fs" runat="Server" progid="Scripting.FileSystemObject"> </object> <%
```

```
'/////기본 포함파일 %>
```

```
<!-- #include file = "lib/lib.asp" -->
```

```
<!-- #include file = "lib/dbConn.asp" -->
```

```
<!-- #include file = "lib/common.asp" -->
```

```
<!-- #include file = "lib/conf.asp" --> <%
```

```
'//디자인파일 적용 확인
```

```
strFullPath = Request.ServerVariables("URL")
```

<중략...>

위의 include된 파일들을 살펴 보면 대부분의 파일에서 공통적으로 참조하는 것을 알 수 있다. 이렇게 적용할 홈페이지에서 공통적으로 참조하는 파일들을 찾아서 현재 설치된 CASTLE을 적용하기 위하여 공통적으로 참조하는 파일들에 아래와 내용을 입력한다.

```
<% 'KISA WEB Security Template
Application("CASTLE_ASP_VERSION_BASE_DIR") = "castle 설치 경로"
Server.Execute(Application("CASTLE_ASP_VERSION_BASE_DIR") & "/castle_referee.asp")
%>
```

현재 적용할 홈페이지에 공통으로 참조하는 파일중 하나인 lib/conf.asp 시작 부분에 위 내용을 적용하도록 한다. 아래내용의 **"/castle-asp"**는 CASTLE를 업로드한 홈페이지 경로이다.

```
<% 'KISA WEB Security Template
Application("CASTLE_ASP_VERSION_BASE_DIR") = "/castle-asp"
Server.Execute(Application("CASTLE_ASP_VERSION_BASE_DIR") & "/castle_referee.asp")
%>
<%
'-----
'
' FSBOARD Configuration 0.6
<중략...>
```

## 4 관리

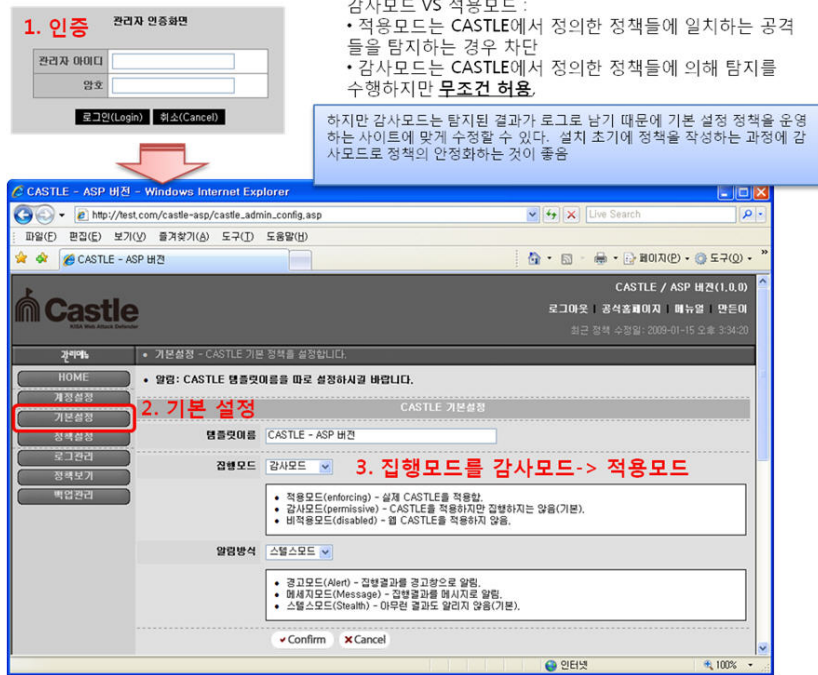
이 장에서는 CASTLE 관리페이지에 접속하여 적용 모드로 설정하고, CASTLE이 제대로 설정되었는지 확인하는 방법에 대해 설명하도록 한다.

### 4.1 적용모드 설정

다음과 같은 경로로 관리자 페이지에 접속한다.

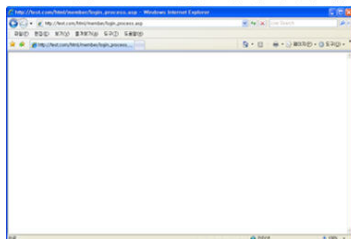
- 관리자 페이지 : [http://test.com/castle-asp/castle\\_admin.asp](http://test.com/castle-asp/castle_admin.asp)

관리자 페이지로 접속을 하면, 관리자 인증을 하지 않은 경우는 인증 과정을 진행한 후, 관리자 페이지에 접속한다. 기본 설정에서 **감사 모드와 적용모드의 차이점을 이해**하고(아래 그림에서 설명), 충분히 감사모드를 통해 정책이 안정화가 되었다면 **적용모드로 설정**한다.



알림 방식은 설정모드에 따라 아래와 같은 메시지를 출력한다. 원하는 방식을 선택하여 사용할 수 있다.

#### 1. 스텔스 모드 (빈 페이지 출력)



#### 2. 메시지 모드



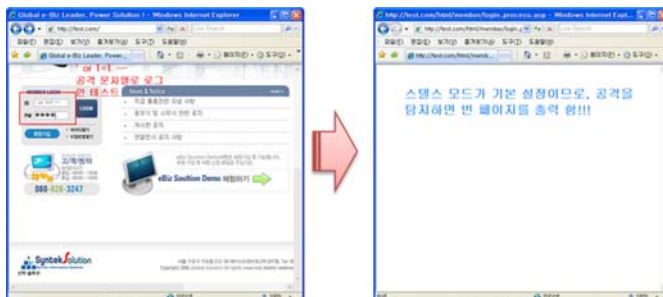
#### 3. 경고 모드(디버깅 모드)



## 4.2 적용여부 확인

앞서 설명한 모든 과정을 마쳤다면 사이트에서 사용자 데이터 입력 부분에 아래와 같은 공격 문자열을 입력하여 정상적으로 적용을 했는지 확인한다.

공격 테스트 문자열(sql injection) : ' or 1=1--



그림과 같은 화면이 출력하면 CASTLE의 적용이 완료된 상태이다. 이 후 정책설정, 고급설정, 로그관리, 정책보기, 백업관리 등 더 자세한 기능은 **CASTLE-ASP 사용자 설명서**를 참고 하기 바란다.