**사 용 권 한**

**Client Approval:**

본인은 서명으로써 본 문서가 본 프로젝트 범위 내에서 사용될 것을 인가함.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **승인자 :** | 한국저작권위원회 차태원 팀장 | (인) | **일자 :** | \_\_\_\_\_/\_\_/\_\_ |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **검토자 :** | 한국저작권위원회 문경도 선임 | (인) | **일자:** | \_\_\_\_/\_\_/\_\_ |

**주식회사 굿씽크 & 엘에스웨어Approval:**

본 문서에 대한 서명은 본 문서에 대하여 수행 및 유지관리의 책임이 있음을 인정하는 것임.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **승인자 :** | 주식회사 굿씽크 곽종 부장 | (인) | **일자:** | \_\_\_\_/\_\_/\_\_ |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **검토자 :** | 엘에스웨어㈜ 김민 책임 | (인) | **일자:** | \_\_\_\_/\_\_/\_\_ |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **작성자 :** | 엘에스웨어㈜ 신창권 상무 | (인) | **일자:** | 2018/10/12 |

**제.개정이력**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| 1.2 | 최종 단계 감리 시정 조치 반영 | 2018/11/13 |
| 1.1 | 설계 단계 감리 시정 조치 | 2018/10/12 |
| 1.0 | 제정 | 2018/05/29 |
| **개정번호** | **제.개정페이지및내용** | **제.개정일자** |

내용

[1 문서 개요 1](#_Toc493341111)

[1.1 제정 경위 1](#_Toc493341112)

[1.2 문서 범위 1](#_Toc493341113)

[2 보안 계획서의 대상 2](#_Toc493341114)

[3 주요 보안 관련 법령 3](#_Toc493341115)

[3.1 행정기관 및 공공기관 정보시스템 구축ㆍ운영지침(2013.8.27개정판) 3](#_Toc493341116)

[3.2 홈페이지개발보안안내서(제2010-11호) 3](#_Toc493341117)

[3.2.1 접근통제 취약점 3](#_Toc493341118)

[3.2.2 부적절한 파라미터 3](#_Toc493341119)

[3.2.3 취약한 세션 관리 (Cookie Injection) 3](#_Toc493341120)

[3.2.4 악의적인 명령 실행(XSS) 4](#_Toc493341121)

[3.2.5 버퍼 오버플로우 4](#_Toc493341122)

[3.2.6 악의적인 명령어 주입 공격 (SQL Injection) 4](#_Toc493341123)

[3.2.7 업로드 취약점 4](#_Toc493341124)

[3.2.8 다운로드 취약점 4](#_Toc493341125)

[3.2.9 개발 보안 관리 4](#_Toc493341126)

[3.2.10 부적절한 환경설정(서버 설정관련) 5](#_Toc493341127)

[3.3 홈페이지 보안관리 매뉴얼 (국가사이버안전센터) 5](#_Toc493341128)

[3.3.1 디렉토리리스팅 취약점 5](#_Toc493341129)

[3.3.2 파일 다운로드 취약점 5](#_Toc493341130)

[3.3.3 크로스 사이트 스크립트 취약점 5](#_Toc493341131)

[3.3.4 파일 업로드 취약점 6](#_Toc493341132)

[3.3.5 WebDAV 취약점 6](#_Toc493341133)

[3.3.6 테크노트(Technote) 취약점 6](#_Toc493341134)

[3.3.7 제로보드(Zeroboard) 취약점 6](#_Toc493341135)

[3.3.8 SQL Injection 취약점 6](#_Toc493341136)

[3.4 공공기관 홈페이지 개인 정보 노출 방지 가이드라인 6](#_Toc493341137)

[4 보안 사항 준수 대상 및 범위 8](#_Toc493341138)

[4.1 기술적인 보안 준수 8](#_Toc493341139)

[4.1.1 입력 데이터 검증 및 표현 8](#_Toc493341140)

[4.1.2 보안기능 8](#_Toc493341141)

[4.1.3 시간및상태 9](#_Toc493341142)

[4.1.4 에러처리 9](#_Toc493341143)

[4.1.5 코드오류 9](#_Toc493341144)

[4.2 홈페이지 개인정보 보호 적용 여부 및 방안 10](#_Toc493341145)

[5 암호화 정책 11](#_Toc493341146)

[5.1 암호화 대상 11](#_Toc493341147)

[5.2 암호화 적용 계획 11](#_Toc493341148)

[6 응용 시스템 보안 12](#_Toc493341149)

[6.1 사용자 계정 관리 12](#_Toc493341150)

[6.2 사용자 접근 제어 12](#_Toc493341151)

[6.3 웹 개발 보안 적용 계획 12](#_Toc493341152)

[6.4 웹 개발 보안 취약성 점검 계획 12](#_Toc493341153)

[7 개인정보보호 대책 12](#_Toc493341154)

[8 개발시스템 보안 대책 12](#_Toc493341155)

[9 보안대책 12](#_Toc493341156)

[9.1 관리적 보안 12](#_Toc493341157)

[9.2 물리적 보안 12](#_Toc493341158)

[9.3 기술적 보안 13](#_Toc493341159)

[10 취약점 점검 13](#_Toc493341160)

[10.1 OS 취약점 진단 항목 13](#_Toc493341161)

[10.2 Database 취약점 점검 항목 15](#_Toc493341162)

[10.3 OS 취약점 점검 항목 16](#_Toc493341163)

[10.4 WAS 취약점 점검 항목 17](#_Toc493341164)

[11 보안 점검 활동 계획 및 보고 19](#_Toc493341165)

[12 소스코드 취약점 점검 20](#_Toc493341166)

[12.1 취약점 점검 방법 20](#_Toc493341167)

[12.2 취약점 점검 대상 20](#_Toc493341168)

[12.3 취약점 점검 항목 20](#_Toc493341169)

[12.4 취약점 점검 일정 20](#_Toc493341170)

[12.5 취약점 점검 결과 보고 및 조치 20](#_Toc493341171)

[13 상세 보안 지침 내용 20](#_Toc493341172)

# 문서 개요

## 제정 경위

본 문서는 “저작권기술 성능평가 시스템 개선 및 고도화” 사업의 보안 서비스 적용과 관련되어 관련 지침을 만들기 위해서 제정된다.

## 문서 범위

본 “저작권기술 성능평가 시스템 개선 및 고도화” 사업 수행을 통해 획득하게 되는 각종 자료 및 정보 자산을 대상으로 함.

# 보안 계획서의 대상

본 사업에 있어서의 보안 대상 항목은 다음과 같이 적용한다.

* 서버, 응용 및 데이터에 대한 보안 진단 및 점검을 수행․조치하고, 보안 계획을 수립 한다.
* 시스템을 운영하기 위하여 물리적 보안 대책, 관리적 보안 대책, 기술적 보안 대책 등 안전 및 보안 관리에 대한 운영 지침을 마련한다.
* 주관사업자는 본 사업 수행 중 취득한 지식에 대하여 과업 수행 중은 물론 사업이 완료된 후에라도 비밀 보안을 준수하여야 한다.
* 본 사업에 종사하는 모든 인원은 별도 양식에 의한 보안 각서를 반드시 제출하도록 한다.
* 개발시스템 관리자를 지정하고, 프로그램 소스코드 및 관련 S/W의 유출을 방지하기 위해 디스크, CD, 출력물은 별도 관리하도록 한다.
* 정보시스템의 상호운용성, 사용자편의성, 보안성 등 최소한의 품질 확보 및 시스템 구축 표준화 방안 추진(정보시스템구축․운영지침, 행정안전부고시 2012-25호)
* 웹 표준 준수 및 윈도우 7/8/11 버전 이상과 상호 호환성 유지
* 웹 개발 사업의 경우 홈페이지 개발보안 가이드(한국인터넷진흥원) 및 홈페이지 보안관리 매뉴얼(국가사이버안전센터)을 준수
* 가능한 S/W를 모듈화하여 시스템 유지보수가 용이하도록 개발
* 「공공기관 웹사이트 개인정보 노출방지 가이드라인(2011)」적용

# 주요 보안 관련 법령

본 사업에 있어서의 보안은 주요 정부 기관에서 배포하고 있는 가이드 라인 및 법령을 준수하여 보안을 고려하여 시스템을 구축하고 개발을 수행한다.

## 행정기관 및 공공기관 정보시스템 구축ㆍ운영지침(2013.8.27개정판)

본 가이드 라인은 정보시스템을 구축ㆍ운영 함에 있어서 준수해야 할 기준, 표준 및 절차와 같은 법 제 49조제1항에 따른 상호운용성 기술평가에 관한 사항을 정의하고 있다.

* 사업계획 수립
* 정보화사업 발주
* 사업자선정 및 계약
* 사업수행
* 소프트웨어 개발 보안
* 검사 및 운영

## 홈페이지개발보안안내서(제2010-11호)

홈페이지 개발자가 웹 어플리케이션이나 웹 컨텐츠를 개발시의 보안 취약점에 대해 중점적으로 다루고 있으며, 홈페이지 운영자가 주요 공개 웹 어플리케이션의 취약점 정보를 파악함으로써 안전한 운영을 하는데도 활용할 수 있도록 하고 있다.

본 사업에서는 한국인터넷진흥원에서 권고하고 있는 홈페이지개방보안안내서에 의거하여 웹개발에 대한 보안을 준수하며, 각각의 항목별로 아래와 같이 준수하도록 한다.

### 접근통제 취약점

* 적용 여부 : 적용함
* 적용 방법
  1. 관리자 페이지에 대해서는 정해진 사용자만이 접근할 수 있도록 IP 구간을 지정하여 접근되도록 한다.
  2. 관리자 페이지 URL은 일반적으로 유추하기 쉬운 경로를 사용하지 않는다.  
     (현재의 경로 /copyright/jsp/ctismng\_login.jsp )
  3. 관리자 페이지 매 세션마다 관리자 계정에 대한 세션 활성 여부를 확인한다.
  4. 관리자 페이지에 대한 로그인 정보는 암호화 하여 관리한다.

### 부적절한 파라미터

* 적용 여부 : 부분 적용함
* 부분 적용 사유 : 인수 변조를 방지하기 위한 별도의 프레임웍(라이브러리 혹은 컴포넌트)이 현재 구성되어 있지 않으나, 웹서버내의 Filter를 사용하여 악위적인 문자열에 대해서는 기본적인 필터링을 현재 구성되어 있다.
* 적용 방법

1. 프로그램상에서의 최대한 입력 값에 대해 검증한다.
2. 데이터 유형, 허용된 문자 여부, 최대 / 최소 길이, 숫자의 범위 등을 검증한다.

### 취약한 세션 관리 (Cookie Injection)

* 적용 여부 : 적용함
* 적용 방법

1. 중요한 정보가 전송되는 경우에는 SSL을 사용하여 통신한다.
2. Client측의 Cookie보다는 Server Side Session을 사용한다.

### 악의적인 명령 실행(XSS)

* 적용 여부 : 적용함
* 적용 방법

1. 입력된 내용중에 스크립트 혹은 HTML문법이 포함되어 있는 경우는 특별한 경우를 제외하고는 입력을 허용하지 않는다.
2. 필요한 경우에는 서버측에 전송되어 저장될 경우 HTML encoding을 수행하여 저장하도록 한다.
3. 일반 입력 문자 중에서도 <, > 등과 같은 특수 문자는 &lt;,&gt;와 같이 변환하여 처리한다.

### 버퍼 오버플로우

* 적용 여부 : 적용함
* 적용 방법

1. 웹서버 및 웹어플리케이션 서버에 대한 버그 패치를 지속적으로 참고하고, 최신의 패치를 적용한다.
2. 입력 값에 대한 검증 로직을 구현한다.
3. 필요시 ITS4와 같은 코드검사 출을 사용하여 버퍼 오버플로우가 발생 가능한지 여부를 수행한다. (http://www.cigital.com/its4/)

### 악의적인 명령어 주입 공격 (SQL Injection)

* 적용 여부 : 적용함
* 적용 방법

1. 데이터베이스와 연동하는 스크립트에 대한 모든 파라미터를 점검하여 SQL injection이 발생되지 않도록 한다.
2. 허용된 특수문자 이외에는 입력을 받지 않도록 한다.
3. 서버 에러 메시지가 나타나지 않도록 별도의 오류 페이지를 출력한다.

### 업로드 취약점

* 적용 여부 : 적용함
* 적용 방법

1. 업로드되는 경로에 대한 실행 금지 설정을 적용한다.
2. 업로드 되는 파일에 대한 확장자를 지정하며, 서버측에서도 검사하도록 한다.

### 다운로드 취약점

* 적용 여부 : 적용함
* 적용 방법

1. 다운로드 되는 파일에 대해서는 URL 경로상에 해당 파일의 위치나 파일명이 나타나지 않도록 처리한다.
2. 다운로드 받을 수 있는 디렉토리는 특정 디렉토리로 한정한다.

### 개발 보안 관리

* 적용 여부 : 적용함
* 적용 방법

1. 사용자에게 전달된 값(HIDDEN form 필드, parameter)를 재사용할 경우 해당 값에 대한 변조를 주의한다.
2. 최종 통제 메커니즘은 반드시 서버에서 수행되도록 한다.
3. 클라이언트에게 중요 정보를 전달하지 않는다.
4. 중요 정보 전송 시 POST Method 및 SSL을 적용한다.
5. 중요한 트렌젝션이 일어나는 프로세스에 사용자의 비밀번호를 재확인한다.
6. 중요 정보를 보여주는 페이지는 캐쉬를 사용하지 못하도록 설정한다.
7. 적절한 방법으로 암호화한다

### 부적절한 환경설정(서버 설정관련)

* 적용 여부 : 적용함
* 적용 방법

1. 운영서버에는 백업파일이나 텍스트 파일 등 불필요한 파일이 올라가지 않도록 한다.
2. 디렉토리 리스팅이 되지 않도록 설정한다.

## 홈페이지 보안관리 매뉴얼 (국가사이버안전센터)

본 지침에서는 홈페이지 해킹에 많이 악용되었던 보안취약점으로 8종을 선정하고, 어떠한 피해를 초래할 수 있는지 설명한데 이어 홈페이지 운영자가 따라하기 방식으로 점검 및 조치할 수 방법에 대해 다루고 있다.

### 디렉토리리스팅 취약점

* 적용 여부 : 적용함
* 문제점 : 홈페이지의 속성을 설정하는 ‘웹사이트 등록정보’에 특정 디렉토리에 대하여 ‘디렉토리 검색’ 항목이 체크되어 있거나(IIS 웹서버),‘httpd.conf 파일’에서 ‘Indexes’ 옵션이 ON되어 있는 경우(아파치 웹서버)에 인터넷 사용자에게 모든 디렉토리 및 파일목록이 보여지게 되고, 파일의 열람 및 저장도 가능하게 되어 비공개 자료가 유출될 수 있다.

### 파일 다운로드 취약점

* 적용 여부 : 적용함
* 문제점 : 게시판 등에 저장된 자료에 대해 ‘다운로드 스크립트’를 이용하여 다운로드 기능을 제공하면서, 대상 자료파일의 위치 지정에 제한조건을 여하지 않았을 경우에 URL칸의다운로드스크립트의인수값에 ‘../’ 문자열등을 입력하여 시스템 디렉토리 등에 있는 /etc/passwd와 같은 비공개 자료들이 유출될 수 있다.특히, 리눅스 및 유닉스 계열의 웹서버에 각별한 주의가 필요하다.

### 크로스 사이트 스크립트 취약점

* 적용 여부 : 적용함
* 문제점 : 게시판에 새 게시물을 작성하여 등록할 때와 같이 사용자의 입력을 받아 처리하는 웹 응용프로그램에서 입력 내용에 대해 실행코드인 스크립트의 태그를 적절히 필터링하지 않을 경우에 악의적인 스크립트가 포함된 게시물을 등록 할 수 있어 해당게시물을 열람하는 일반 사용자의 PC로부터 개인정보인 쿠키를 유출할 수 있는 등의 피해를 초래할 수 있다.

### 파일 업로드 취약점

* 적용 여부 : 적용함
* 문제점 : 첨부파일 업로드를 허용하는 홈페이지 게시판에서 .php, .jsp 등의 확장자 이름의 스크립트 파일의 업로드를 허용할 경우에 해커가 악성 실행프로그램을 업로드 한 후에 홈페이지 접속방식으로 원격에서 서버컴퓨터의 시스템 운영 명령어를 실행시킬 수 있다.

### WebDAV 취약점

* 적용 여부 : 적용함
* 문제점 : 윈도우 서버 컴퓨터에서 기본으로 설치되는 원격관리기능인 WebDAV가 계속 사용가능 하도록 설정되어 있고, WebDAV 라이브러리 파일의 속성 및 홈페이지 디렉토리에 쓰기 권한이 모두 허용되어 있는 경우에 해커가 WebDAV 도구를 사용, 원격에서 홈페이지 디렉토리에 임의의 파일을 삽입하여 화면을 변조할 수 있다.

### 테크노트(Technote) 취약점

* 적용 여부 : 적용함
* 문제점 : 국내에서 개발되어 무료 배포중인 게시판 제작 프로그램 ‘테크노트’의 일부 CGI프로그램들에서 인수값 처리시에 ‘|’문자 이후에 나오는 컴퓨터 운영 명령어가 실행될 수 있는 결함이 있어 해커는 홈페이지 접속방식으로 컴퓨터명령어를 실행하여 화면을 변조하거나 컴퓨터를 조작할 수 있다. ‘테크노트’는 리눅스 및 유닉스 계열의 홈페이지 서버컴퓨터에 주로 사용되고, 윈도우 계열의 홈페이지에서도 ‘Perl’이 지원될 경우에 사용될 수 있다..

### 제로보드(Zeroboard) 취약점

* 적용 여부 : 적용함
* 문제점 : 국내에서 개발되어 무료 배포중인 게시판 제작 프로그램 ‘제로보드’의 일부 PHP프로그램이 원격에 있는 PHP파일을 실행할 수 있는 결함이 있어 해커는 홈페이지 접속방식으로 컴퓨터 명령어를 실행하여 화면을 변조하거나 컴퓨터를 조작할 수 있다. ‘제로보드’는 리눅스 및 유닉스 계열의 홈페이지 서버컴퓨터에 주로 사용되고, 윈도우 계열의 홈페이지에서도 ‘PHP’가 지원될 경우에 사용될 수 있다..

### SQL Injection 취약점

* 적용 여부 : 적용함
* 문제점 :웹브라우저 주소(URL)창 또는 사용자 ID 및 패스워드 입력화면 등에서 데이터베이스 SQL문에 사용되는 문자기호(‘ 및 “)의 입력을 적절히 필터링 하지 않은 경우에 해커가 SQL문으로해석될수있도록조작한입력으로데이터베이스를인증절차없이 접근, 자료를 무단 유출하거나 변조할 수 있다.

## 공공기관 홈페이지 개인 정보 노출 방지 가이드라인

* 홈페이지 보안 취약점 및 기술적 보안 조치

1. 인젝션(SQL Injection)
2. 크로스사이트 스크립트(XSS)
3. 취약한 인증과 세션관리
4. 불안전한 직접객체 참조
5. 크로스사이트 변조요청(CSRF)
6. 보안상 잘못된 구성
7. 불안전한 암호화 저장
8. URL 접근 제한 실패
9. 불안전한 통신
10. 검증되지 않은 리다이렉트와 포워드

# 보안 사항 준수 대상 및 범위

본 사업을 위한 기술적인 보안 준수 사항 및 그 범위에 대해 기술한다.

## 기술적인 보안 준수

### 입력 데이터 검증 및 표현

|  |  |  |
| --- | --- | --- |
| 번호 | 보안약점 | 설 명 |
| 1 | SQL 삽입 | 사용자의 입력값 등 외부 입력값이 SQL 쿼리에 삽입되어 공격자가 쿼리를 조작해 공격할 수 있는 보안약점 |
| 2 | 자원 삽입 | 외부 입력값에 대한 검증이 없거나 혹은 잘못된 검증을 거쳐서 시스템 자원에 접근하는 경로 등의 정보로 이용될 때 발생하는 보안약점 |
| 3 | 크로스사이트스크립트 | 검증되지 않은 외부 입력값에 의해 브라우저에서 악의적인 코드가 실행되는 보안약점 |
| 4 | 운영체제 명령어 삽입 | 운영체제 명령어를 구성하는 외부 입력값이 적절한 필터링을 거치지 않고 쓰여져서 공격자가 운영체제 명령어를 조작할 수 있는 보안약점 |
| 5 | 위험한 형식 파일 업로드 | 파일의 확장자 등 파일형식에 대한 검증없이 업로드를 허용하여 발생하는 보안약점 |
| 6 | 신뢰되지 않는 URL 주소로 자동 접속 연결 | 사용자의 입력값 등 외부 입력값이 링크 표현에 사용되고, 이 링크를 이용하여 악의적인 사이트로 리다이렉트(redirect)되는 보안약점 |
| 7 | XQuery 삽입 | 사용자의 입력값 등 외부 입력값이 XQuery 표현에 삽입되어 악의적인 쿼리가 실행되는 보안약점 |
| 8 | XPath 삽입 | 사용자의 입력값 등 외부 입력값이XPath 표현에 삽입되어 악의적인 쿼리가 실행되는 보안약점 |
| 9 | LDAP 삽입 | 검증되지 않은 입력값을 사용해서 동적으로 생성된 LDAP문에 의해 악의적인 LDAP 명령이 실행되는 보안약점 |
| 10 | 크로스사이트 요청 위조 | 검증되지 않은 외부 입력값에 의해 브라우저에서 악의적인 코드가 실행되어 공격자가 원하는 요청(Request)이 다른 사용자(관리자 등)의 권한으로 서버로 전송되는 보안약점 |
| 11 | 디렉토리 경로 조작 | 지정된 경로 밖의 파일시스템 경로에 접근하게 되는 보안약점 |
| 12 | HTTP 응답분할 | 사용자의 입력값 등 외부 입력값이 HTTP 응답헤더에 삽입되어 악의적인 코드가 실행되는 보안약점 |
| 13 | 정수 오버플로우 | 정수를 사용한 연산의 결과가 정수값의 범위를 넘어서는 경우 프로그램이 예기치 않은 동작될 수 있는 보안약점 |
| 14 | 보호메커니즘을 우회할 수 있는 입력값 변조 | 사용자에 의해 변경될 수 있는 값을 사용하여 보안결정(인증/인가/권한부여 등)을 수행하여 보안 메커니즘이 우회될 수 있는 보안약점 |

### 보안기능

|  |  |  |
| --- | --- | --- |
| 번호 | 보안약점 | 설 명 |
| 1 | 적절한 인증 없는 중요기능 허용 | 적절한 인증없이 중요정보(계좌이체 정보, 개인정보 등)를 열람(또는 변경)할 수 있게 하는 보안약점 |
| 2 | 부적절한 인가 | 적절한 접근제어 없이 외부 입력값을 포함한 문자열로 서버자원에 접근(혹은 서버 실행 인가)을 할 수 있게 하는 보안약점 |
| 3 | 중요한 자원에 대한 잘못된 권한설정 | 중요자원(프로그램 설정, 민감한 사용자 데이터 등)에 대한 적절한 접근권한을 부여하지 않아, 의도하지 않는 사용자에 의해 중요정보가 노출․수정되는 보안약점 |
| 4 | 취약한 암호화 알고리즘 사용 | 중요정보(패스워드, 개인정보 등)의 기밀성을 보장할 수 없는 취약한 암호화 알고리즘을 사용하여 정보가 노출될 수 있는 보안약점 |
| 5 | 사용자 중요정보 평문 저장(또는 전송) | 중요정보(패스워드, 개인정보 등) 저장(또는 전송)시 암호화 하지 않아 공격자에게 누출될 수 있는 보안약점 |
| 6 | 하드코드된 패스워드 | 소스코드내에 비밀번호를 하드코딩함에 따라 관리자 비밀번호가 노출되거나, 주기적 변경 등 수정(관리자 변경 등)이 용이하지 않는 보안약점 |
| 7 | 충분하지 않은 키 길이 사용 | 데이터의 기밀성, 무결성 보장을 위해 사용되는 키의 길이가 충분하지 않아 기밀정보 누출, 무결성이 깨지는 보안약점 |
| 8 | 적절하지 않은 난수 값 사용 | 예측 가능한 난수사용으로 공격자로 하여금 다음 숫자 등을 예상하여 시스템 공격이 가능한 보안약점 |
| 9 | 패스워드 평문 저장 | 기밀정보인 비밀번호를 암호화하지 않아 노출될 수 있는 보안약점 |
| 10 | 하드 코드된 암호화 키 | 소스코드 내에 암호화키를 하드코딩 하는 경우, 향후 노출될 수 있으며, 키 변경 등 수정이 용이하지 않는 보안약점 |
| 11 | 취약한 패스워드 허용 | 비밀번호 조합규칙(영문, 숫자, 특수문자 등) 및 길이가 충분하지 않아 노출될 수 있는 보안약점 |
| 12 | 사용자 하드디스크에 저장되는 쿠키를 통한 정보노출 | 쿠키(세션 ID, 사용자 권한정보 등 중요정보)를 사용자 하드디스크에 저장함으로써 개인정보 등 기밀정보가 노출될 수 있는 보안약점 |
| 13 | 보안속성 미적용으로 인한 쿠키 노출 | 쿠키에 보안속성을 적용하지 않을 경우, 쿠키에 저장된 중요데이터가 공격자에 노출될 수 있는 보안약점 |
| 14 | 주석문 안에 포함된 패스워드 등 시스템 주요정보 | 소스코드내의 주석문에 비밀번호가 하드코딩되어 비밀번호가 노출될 수 있는 보안약점 |
| 15 | 솔트 없이 일방향해쉬 함수사용 | 공격자가 솔트없이 생성된 해쉬값을 얻게 된 경우, 미리 계산된 레인보우 테이블을 이용하여 원문을 찾을 수 있는 취약점 |
| 16 | 무결성검사없는 코드 다운로드 | 원격으로부터 소스 코드 또는 실행파일을 무결성검사없이 다운로드 받고 이를 실행하는 경우 공격자가 악의적인 코드를 실행 할 수 있는 보안약점 |

### 시간및상태

|  |  |  |
| --- | --- | --- |
| 번호 | 보안약점 | 설 명 |
| 1 | 경쟁조건: 검사시점과사용시점(TOCTOU) | 멀티 프로세스 상에서 자원을 검사하는 시점과 사용하는 시점이 달라서 발생하는 보안약점 |
| 2 | 제어문을 사용하지 않는 재귀함수 | 적절한 제어문 사용이 없는 재귀함수에서 무한재귀가 발생하는 보안약점 |

### 에러처리

|  |  |  |
| --- | --- | --- |
| **번호** | **보안약점** | **설 명** |
| 1 | 오류메시지통한 정보노출 | 개발시 활용을 위한 오류정보의 출력메시지를 배포될 버전의 SW에 포함시킬 때 발생하는 보안약점 |
| 2 | 오류상황 대응 부재 | 시스템에서 발생하는 오류상황을 처리하지 않아 프로그램 다운 등 의도하지 않은 상황이 발생할 수 있는 보안약점 |
| 3 | 적절하지않은 예외처리 | 예외에 대한 부적절한 처리로 인해 의도하지 않은 상황이 발생될 수 있는 보안약점 |

### 코드오류

|  |  |  |
| --- | --- | --- |
| **번호** | **보안약점** | **설 명** |
| 1 | 널(Null) 포인터 역참조 | Null로 설정된 변수의 주소값을 참조했을 때 발생하는 보안약점 |
| 2 | 부적절한 자원 해제 | 사용된 자원을 적절히 해제 하지 않으면 자원의 누수 등이 발생하고, 자원이 모자라 새로운 입력에 처리 못하게 되는 보안약점 |

## 홈페이지 개인정보 보호 적용 여부 및 방안

|  |  |  |  |
| --- | --- | --- | --- |
| **구 분** | **점 검 항 목** | **적용**  **여부** | **비고** |
| 정책 | 개인정보 보호를 위한 책임자를 지정하여 운영 | 적용 |  |
| 개인정보 보호를 위한 정책 또는 관리계획(침해사고 대응계획 포함)을 수립․운영 | 적용 | 저작권위원회  홈페이지 |
| 외주인력 보안관리를 위해 보안서약서 집행, 비밀번호 노출 예방 등 조치 수행 | 적용 | 보안서약서 |
| DB 서버에 접속하는 장비(PC, 노트북 등)에서 불법 또는 비인가된 S/W 사용을 방지하고 정품 S/W만 사용하도록 하는 정책을 수립․운영 | 적용 | 위원회서버 및 성능평가 PC에서만 접근 가능 |
| DB서버에 접근 가능한 자(내부직원, 위탁인력, 개발자 등) 대상으로 개인정보보호 관련 교육을 연2회 이상 실시 | 적용 | 정보화관리팀의 내부 정책에 따름 |
| 네트워크 | 상시적으로 비인가 IP주소의 접근을 통제 | 적용 |  |
| 상시적으로 불필요한 서비스 포트 사용을 통제 | 적용 |  |
| 상시적으로 불법적인 해킹시도를 방지하고, 이에 대해 모니터링을 실시 | 적용 | 정보화관리팀에서 수행 |
| 상시적으로 바이러스, 웜 등의 네트워크 유입을 차단 | 적용 | 정보화관리팀에서 수행 |
| 주기적으로 네트워크 접속에 대한 로그를 관리하고, 분석 | 적용 | 정보화관리팀에서 수행 |
| 네트워크 장비 및 정보보호시스템의 보안패치 발생시 지체없이 업데이트를 수행 | 적용 | 정보화관리팀에서 수행 |
| DB 및 Application | 상시적으로 네트워크를 통한 비인가자의 DB 접근을 통제 | 적용 |  |
| DB서버내에 불필요한 서비스 포트를 차단 | 적용 |  |
| 상시적으로 DB 접속자 및 개인정보취급자의 접속기록 보존 | 미적용 | 해당 정책은 적용되지 않음 |
| DB 접속기록을 주기적으로 모니터링하여 통제 | 미적용 | 해당 정책은 적용되지 않음 |
| DB서버에 접속하는 관리자 PC가 인터넷 접속되는 내부망의 네트워크와 분리 | 적용 |  |
| 개인정보취급자의 역할에 따라 DB 접근권한을 차등화하여 부여 | 적용 |  |
| 개인정보취급자의 전보, 이직, 퇴사 등 인사 이동 발생시 지체없이 DB 접근권한을 변경 | 적용 |  |
| DB접속자 및 개인정보취급자의 DB 로그인 비밀번호를 최소 3개월마다 변경 | 적용 |  |
| DB접속자 및 개인정보취급자의 비밀번호 입력시 5회 이상 연속 입력오류가 발생한 경우계정잠금 등 접근을 제한 | 적용 |  |
| DB 및 DB접속 어플리케이션 서버에 대한 물리적 접근을 인가된 자로 한정 | 적용 | 정보화관리팀을 통한 접근 가능 |
| DB 및 DB접속 어플리케이션 서버에서 보조기억매체(USB 등) 사용시 관리자 승인 후 사용 | 적용 |  |
| DB서버 및 DB접속 어플리케이션 서버에 접속하는 모든 개인정보취급자의 단말기(PC, 노트북 등)의 운영체제 보안패치를 제조사 공지 후 지체없이 수행 | 적용 |  |
| HDD등 DB 저장매체의 불용처리시(폐기, 양여, 교체 등) 저장매체에 저장된 개인정보는 모두 파기 | 적용 | 정보화관리팀에서 수행 |
| 웹(Web) | 신규 웹 취약점 및 알려진 주요 웹(Web) 취약점 진단/보완을년1회 이상 실시하거나, 상시적으로 비인가자에 의한 웹서버 접근, 홈페이지 위․변조 등을 자동으로 차단할 수 있는 보호 조치를 수행 | 적용 |  |
| 웹서버 프로그램과 운영체제 보안패치를 제조사 공지 후 지체없이 수행 | 적용 | 정보화관리팀에서 수행 |

# 암호화 정책

## 암호화 대상

중요한 개인 혹은 기관 정보에 대해서는 Database에 저장시 반드시 암호화를 하여 보관하며, 적용 범위에 다음과 같다.

1. 로그인 비밀번호
2. 이메일
3. 핸드폰번호
4. 연락처

## 암호화 적용 계획

현재의 중요한 개인정보 에 대해서는 SHA-2 (SHA256) 암호화 알고리즘을 사용하여 암호화가 되어 있으며, 사용자 비밀번호 등에 대해서는 일방향 암호화가 되어 있고, 그 이외의 항목에 대해서는 양방향 암호화가 되어 있다.

\* 사용자 테이블 암호화 예(현재)

|  |  |  |
| --- | --- | --- |
| 컬럼ID | 자릿수 | 컬럼명칭 |
| USERPWD | VARCHAR2(200 BYTE) | 비밀번호 |
| PHONE | VARCHAR2(200 BYTE) | 전화번호 |
| BIZ\_NO | VARCHAR2(200 BYTE) | 사업자번호 |
| OFC\_EM | VARCHAR2(200 BYTE) | 대표이메일 |
| OFC\_TEL | VARCHAR2(200 BYTE) | 회사연락처 |
| OFC\_CEL | VARCHAR2(200 BYTE) | 담당자핸드폰 |
| TCH\_EM | VARCHAR2(200 BYTE) | 기술책임자이메일 |
| TCH\_TEL | VARCHAR2(200 BYTE) | 기술책임자전화번호 |
| TCH\_CEL | VARCHAR2(200 BYTE) | 기술책임자핸드폰 |

# 응용 시스템 보안

## 사용자 계정 관리

본 시스템의 관리 사이트에 접속을 위한 계정은 정해진 사용자만이 접속할 수 있도록 하며, 반드시 로그인을 거쳐야만 접속이 가능하도록 구성한다.

접근하는 계정에 대한 비밀번호는 암호화하여 관리한다.

## 사용자 접근 제어

본 시스템의 관리 사이트에 접근하기 위해서는 반드시 정해진 IP (내부IP 및 한국저작권위원회 에서만 접속이 기술적인조치 관련 서버IP 로 한정)만 접속이 가능하도록 접근제어를 수행한다.

## 웹 개발 보안 적용 계획

안전한 시스템 개발을 위하여 시큐어 코딩에 근거한 개발 규칙 및 개발 보안 가이드 라인을 교육을 통하여 개발자에게 숙지시키도록 한다.

## 웹 개발 보안 취약성 점검 계획

웹 개발 결과물에 대하여 취약성 점검 툴을 활용하여 점검을 수행한다.

# 개인정보보호 대책

본 시스템에서는 개인이 회원가입을 직접 하지 않고, 기업 및 단체의 정보를 입력하여 관리되고 는 있으나, 기업 및 단체의 정보에 대해서도 기본적으로 홈페이지 개인정보 노출 가이드라인에 준하여 적용하도록 한다.

# 개발시스템 보안 대책

개발시스템에 대한 보안을 강화하기 위하여 관리자를 지정하며, 소스 및 관련 S/W등의 유출방지를 위해 디스크, CD, 출력물은 별도로 관리하도록 한다.

* 개발 시스템 관리자 : 엘에스웨어(주) 신창권 이사

# 보안대책

## 관리적 보안

현재 운영되고 있는 서버 들에 대하여 정보화관리팀을 통해 운영 및 관리되도록 하며, 서버실 자체는 사전에 승인을 받은 경우에만 입실이 가능하도록 하고, 입실 후 입 출입 대장을 기록하여 관리한다.

## 물리적 보안

본 사업에 있어서 사용되는 서버는 시건장치가 구비되어 있는 별도의 서버실에 위치하여 관리되도록 하며, 성능평가를 수행하고 있는 성능평가실의 경우 해당 성능평가 PC에 결과 로그 및 각종 평가 툴 등에 접근이 가능하므로, 출입자체를 엄격히 제한한다.

출입문에는 지문 인식 등의 시건 장치를 통하여 외부인으로부터 접근을 차단한다.

|  |  |  |
| --- | --- | --- |
| 구분 | 내용 | 비고 |
| 네트워크 | - 통신장비의 보호, 방화벽, IPS, VPN 보호 등  - 네트워크 장비에 대한 관리적, 물리적 보안  - 방화벽을 활용한 보안 적정성 유지 | 정보화관리팀 업무 영역 |
| 서버 | - 서버에서 제공하는 기본 보안 기능 적용  - 백신 설치 운영 및 최신의 업데이트를 유지  - 서버 보안 툴 적용  - OS 및 AP 취약점 점검을 통한 취약점 패치 적용 | 정보화관리팀 업무 영역 |
| DB | - 중요 개인정보 항목에 대한 암호화  - DB 암호화 솔루션을 통한 DB 보안 체계 유지  - 테이블 별 접근 권한 세분화 | 정보화관리팀 및 저작권 기술팀 |

## 기술적 보안

기술적인 보안에 있어서는 접근에 대한 보안 및 취급하고 있는 자료에 대한 보안 등으로 관리될 수 있도록 하며, 해당 내용은 본 계획서 4장 암호화 정책, 5장 응용 시스템 보안, 6장 개인 정보 보호 대책에 준하여 적용한다.

# 취약점 점검

취약점 점검은 OW, WAS, DB에 대하여 점검을 수행하며 수행 대상 서버 및 점검 서비스는 아래와 같다.

|  |  |  |
| --- | --- | --- |
| 점검구분 | 대상서버 | 대상서비스 |
| OS | TMIS 웹서버 | REDHAT 6.2 |
| TMIS DB 서버 | Windows 2008 Standard |
| WAS | TMIS 웹서버 | JBoss 6.2 |
| DB | TMIS DB 서버 | ORACLE 11g Standard |

## OS 취약점 진단 항목

|  |  |  |
| --- | --- | --- |
| 구분 | 진단항목 | 위험도 |
| 1. 네트워크 서비스 | 불필요한 서비스 제거 | 중 |
| 터미널 서비스 환경 설정 | 중 |
| 2. 계정 관리 | Administrator 계정 관리 | 중 |
| GUEST 계정 관리 | 상 |
| 무자격 사용자 ID 제거 | 중 |
| 계정 잠금 정책 설정 | 중 |
| 암호 정책 설정 | 상 |
| Trivial Password | 상 |
| 사용자 계정 컨트롤 설정 | 상 |
| 3. 파일시스템 | CMD 파일 권한 설정 | 중 |
| 사용자 디렉터리 접근 제한 | 중 |
| 파일 및 디렉토리 보호 | 상 |
| 하드디스크 기본 공유 제거 | 중 |
| SAM 파일 접근 통제 | 중 |
| 4. 보안 패치 | 최신 서비스팩 적용 | 상 |
| 최신 HOT FIX 적용 | 상 |
| 5. 주요 응용 설정 | Telnet 서비스 보안 설정 | 중 |
| DNS 보안 설정 | 상 |
| SNMP 서비스 설정 | 중 |
| WebDAV | 상 |
| Web Client 서비스 취약점 점검 | 중 |
| Server 서비스 RPC 처리 취약점 점검 | 중 |
| TCP/IP IGMP MLD 원격 처리 취약점 점검 | 중 |
| 6. 시스템 보안 설정 | 원격 로그파일 접근 진단 | 하 |
| 공유권한 및 사용자 그룹 설정 | 중 |
| 로그오프나 워크스테이션 잠김 | 중 |
| 이벤트 뷰어 설정 | 상 |
| 로그온 메시지 출력 진단 | 하 |
| 마지막 로그온 사용자 계정 숨김 | 중 |
| 로그온 하지 않은 사용자 시스템 종료 방지 | 상 |
| 보안로그의 감사 기능 설정 | 상 |
| 7. 바이러스 진단 | 백신 프로그램 설치 | 상 |
| 최신 엔진 업데이트 | 상 |
| 8. 레지스트리 보안 설정 | SAM 보안 감사 설정 | 하 |
| Null Session 설정 | 상 |
| 레지스트리 보호 진단 | 중 |
| RDS 제거 | 중 |
| AutoLogon 기능제어 | 중 |

## Database 취약점 점검 항목

|  |  |  |
| --- | --- | --- |
| **구분** | **진단항목** | **위험도** |
| 1. 계정 관리 | 기본 계정의 패스워드, 정책 등을 변경하여 사용 | 상 |
| scott 등 Demonstration 및 불필요 계정을 제거하거나 잠금설정 후 사용 | 상 |
| 패스워드의 사용기간 및 복잡도를 기관의 정책에 맞도록 설정 | 상 |
| 데이터베이스 관리자 권한을 꼭 필요한 계정 및 그룹에 대해서만 허용 | 상 |
| 패스워드 재사용에 대한 제약이 설정 | 중 |
| DB 사용자 계정을 개별적으로 부여하여 사용 | 중 |
| 2. 접근 관리 | 원격에서 DB 서버로의 접속 제한 | 상 |
| DBA이외의 인가되지 않은 사용자가 시스템 테이블에 접근할 수 없도록 설정 | 상 |
| 오라클 데이터베이스의 경우 리스너의 패스워드를 설정하여 사용 | 상 |
| 불필요한 ODBC/OLE-DB 데이터 소스와 드라이브를 제거하고 사용 | 중 |
| 일정 횟수의 로그인 실패 시 이에 대한 잠금정책 설정 | 중 |
| 데이터베이스의 주요 파일 보호 등을 위해 DB 계정의 umask를 022 이상으로 설정 | 하 |
| 데이터베이스의 주요 설정파일, 패스워드 파일 등과 같은 주요 파일들의 접근 권한이 적절하게 설정 | 중 |
| 관리자 이외의 사용자가 오라클 리스너의 접속을 통해 리스너 로그 및 trace 파일에 대한 변경이 가능하지 않게 설정 | 하 |
| 3. 옵션 관리 | 응용프로그램 또는 DBA 계정의 Role이 Public으로 설정되지 않도록 조정 | 상 |
| OS\_ROLES, REMOTE\_OS\_AUTHENTICATION, REMOTE\_OS\_ROLES를 FALSE로 설정 | 상 |
| 패스워드 확인함수가 설정되어 적용 | 중 |
| 인가되지 않은 Object Owner가 존재하지 않도록 설정 | 하 |
| grant option이 role에 의해 부여되도록 설정 | 중 |
| 데이터베이스의 자원 제한 기능을 TRUE로 설정 | 하 |
| 4. 패치 관리 | 데이터베이스에 대해 최신 보안패치와 밴더 권고사항을 모두 적용 | 상 |
| 데이터베이스의 접근, 변경, 삭제 등의 감사기록이 기관의 감사기록 정책에 적합하도록 설정 | 상 |
| 보안에 취약하지 않은 버전의 데이터베이스를 사용 | 중 |
| 5. 로그 관리 | Audit Table은 데이터베이스 관리자 계정에 속해 있도록 설정 | 하 |

## OS 취약점 점검 항목

|  |  |  |
| --- | --- | --- |
| **구분** | **진단항목** | **위험도** |
| 1. 접근 제어 | 관리자 콘솔 관리 | 중 |
| 관리자 계정명 변경 | 중 |
| 관리자 패스워드 관리 | 중 |
| 패스워드 파일 관리 | 중 |
| 2. 설정 | 데몬관리 | 상 |
| 디렉토리 쓰기 권한 관리 | 중 |
| 소스/설정파일 권한 관리 | 중 |
| 로깅 디렉토리/파일 권한 관리 | 중0 |

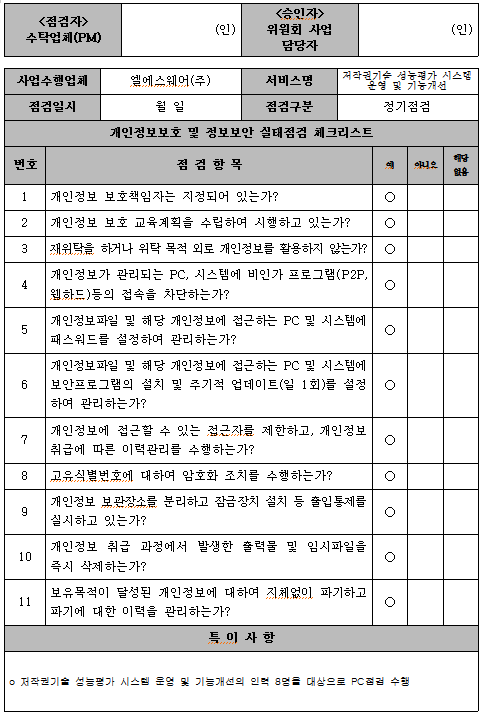
## WAS 취약점 점검 항목

|  |  |  |
| --- | --- | --- |
| **번호** | **구분** | **취약점 항목** |
| 1 | 입력데이터 검증 및 표현  (15개) | SQL 삽입 |
| 2 | 경로 조작 및 자원 삽입 |
| 3 | 크로스사이트 스크립트 |
| 4 | 운영체제 명령어 삽입 |
| 5 | 위험한 형식 파일 업로드 |
| 6 | 신뢰되지 않는 URL 주소로 자동접속 연결 |
| 7 | XQuery 삽입 |
| 8 | XPath 삽입 |
| 9 | LDAP 삽입 |
| 10 | 크로스사이트 요청 위조 |
| 11 | HTTP 응답 분할 |
| 12 | 정수형 오버플로우 |
| 13 | 보안 기능 결정에 사용되는 부적절한 입력값 |
| 14 | 메모리 버퍼 오버플로우 |
| 15 | 포맷 스트링 삽입 |
| 16 | 보안기능  (16개) | 적절한 인증 없는 중요기능 허용 |
| 17 | 부적절한 인가 |
| 18 | 중요한 자원에 대한 잘못된 권한 설정 |
| 19 | 취약한 암호화 알고리즘 사용 |
| 20 | 중요정보 평문 저장 |
| 21 | 중요정보 평문 전송 |
| 22 | 하드코드된 비밀번호 |
| 23 | 충분하지 않은 키 길이 사용 |
| 24 | 적절하지 않은 난수 값 사용 |
| 25 | 하드코드된 암호화키 |
| 26 | 취약한 비밀번호 허용 |
| 27 | 사용자 하드디스크에 저장되는 쿠키를 통한 정보노출 |
| 28 | 주석문 안에 포함된 시스템 주요정보 |
| 29 | 솔트 없이 일방향 해쉬 함수 사용 |
| 30 | 무결성 검사 없는 코드 다운로드 |
| 31 | 반복된 인증시도 제한 기능 부재 |
| 32 | 시간 및 상태  (2개) | 경쟁조건 : 검사시점과 사용시점(TOCTOU) |
| 33 | 종료되지 않는 반복문 또는 재귀 함수 |
| 34 | 에러처리  (3개) | 오류 메시지를 통한 정보노출 |
| 35 | 오류 상황 대응 부재 |
| 36 | 부적절한 예외 처리 |
| 37 | 코드오류  (4개) | 널포인터 역참조 |
| 38 | 부적절한 자원 해제 |
| 39 | 해제된 자원 사용 |
| 40 | 초기화되지 않은 변수 사용 |
| 41 | 캡슐화  (5개) | 잘못된 세션에 의한 데이터 정보 노출 |
| 42 | 제거되지 않고 남은 디버거 코드 |
| 43 | 시스템 데이터 정보 노출 |
| 44 | Public 메서드로부터 반환된 private 배열 |
| 45 | Private 배역에 Public 데이터 할당 |
| 46 | API 오용(2개) | DNS lookup에 의존한 보안결정 |
| 47 | 취약한 API 사용 |

# 보안 점검 활동 계획 및 보고

본 사업의 관리적, 물리적 보안 요건에 따라 정기적으로 보안 점검을 실시하고 점검 결과를 보고한다.

* 보안 점검 일정: 매월 마지막 주 월요일
* 보안 점검 대상: 본 사업에 참여하는 모든 인력에 대하여 점검
* 보안 점검 방식: 개인정보보호 및 정보보안 실태점검 체크리스트를 기반으로 점검
* 점검 결과 보고: 보안 점검 결과는 주관 기관 담당자에게 월간 보고 시 제출
* 개인정보보호 및 정보보안 실태점검 체크리스트



# 소스코드 취약점 점검

## 취약점 점검 방법

소스코드에 대한 취약점은 “소프트웨어 개발 보안(시큐어 코딩) 가이드”를 준수하는 인증된 취약점 점검 툴을 활용하여 점검을 수행한다.

## 취약점 점검 대상

소스코드에 대한 취약점 점검은 본 사업을 통해 수정되거나, 추가된 소스에 한하여 검사를 수행하며, 그 이외의 부분에 대해서는 고객과의 협의를 통하여 수행하도록 한다.

해당되는 소스로는 포렌식마크 기술 성능평가 도구(C#), 필터링 기술 성능평가 도구(C%), 저작권기술 관리 시스템(JAVA), 공정이요 포털(JAVA)이 해당 된다.

## 취약점 점검 항목

점검항목은 “소프트웨어 개발 보안(시큐어 코딩) 가이드”에 명시된 항목에 대한 점검을 수행한다.

## 취약점 점검 일정

* 1차 취약점 점검 수행 : 11/6
* 1차 취약점에 대한 조치 : 11/7 ~ 11/8
* 2차 취약점 점검 수행 : 11/9
* 2차 취약점에 대한 조치 : 11/10

## 취약점 점검 결과 보고 및 조치

발견된 취약점에 대한 보고서는 취약점 점검 툴에서 출력되는 보고서를 기준으로 고객에게 보고를 하며, 중요 취약점에 대해서는 반드시 시정 조치를 취하고, 재 점검을 받도록 한다.

# 상세 보안 지침 내용

본 문서는 다음 문서와 동일한 내용의 보안계획을 세워 처리한다.  
(참고 사이트 : <http://www.kisa.or.kr/public/laws/laws3.jsp> )

* [3.1]행정기관 및 공공기관 정보시스템 구축·운영 지침(안전행정부고시 제2014-51호)
* [3.2]홈페이지 개발 보안 안내서(KISA안내·해설 제 2010-11호)
* [3.3]홈페이지 개인정보 노출방지 가이드라인(행정자치부-2014.12)
* [3.4]소프트웨어 개발보안 가이드(안전행정부-2013.11)
* [3.5]Java 시큐어코딩 가이드(안전행정부-2012.09)