취약점 진단시스템

팀 명 : J.S.P
팀 장 : 박지영(12)
팀 원 : 김태훈(09)
전동현(09)
담당교수 : 양환석 교수님

2015. 6
중부대학교 정보보호학과

목 차

요약

최근 한수원(한국 수력 원자력 발전소) 사건 등 빈번한 사이버 공격으로 인하여 컴퓨터 보안의 인식이 증가함에 따라 개인PC에 진단 프로그램인 알약,V3와 같이 국산 프로그램부터 어베스트같은 해외 프로그램도 많이 사용되고있다.
그러나 하드웨어의 파티션 별로 진단시 시간이 오래걸리고 업데이트를 하지않으면 구버전의 프로그램이 실행됨에 따라 이용자들의 많은 시간과 관심을 쏟아야 하는 상황이다. 그래서 툴의 업데이트가 필요없고 지속적인 업데이트가 가능한 웹페이지를 이용하여 간단한 진단 및 상태 확인을 빠르고 간단하게 사용가능한 시스템 설계 및 구현하였다.
웹페이지를 활용한 진단 시스템을 구현하기 위해서 웹페이지,진단프로그램,Dos 탐지프로그램을 구현하였다. JSP를 활용하여 웹페이지를 구현하였으며 관리자 페이지에서 Dos탐지를 위하여 Windump와winpcap을 이용하였으며 모든 진단 목록 조회 기능을 구현하였으며 Tomcat,MySQL,JSP를 이용해 서버와 데이터베이스를 구축했다. 그리고 진단 프로그램은 JAVA를 이용하여 구현하였다

1. 서론

최근 정보통신의 발전으로 여러 기술이 융합되고 다양한 서비스가 출현하였다.
그에 발맞춰 그것을 악용하여 사이버 공격하는 사례가 증가 하고 있는 추세이다.
예를 들어 한수원사건(찾아보기),777ddos공격 등 사이버 테러가 발생함에 따라 개인 사용자들도 컴퓨터 보안에 관심을 가지기 시작하였다. 그래서 개인pc에 백신 프로그램 1개정도는 설치되어있다. 하지만 진단 설정에 따른 소요 시간이 제각각이며 너무 오래 걸린다는 점에서 자주 사용하지 않는 실정이다. 그리고 빈번한 업데이트로 자동 업데이트 설정을 하지 않으면 구 버전의 진단 툴을 사용함으로써 공격에 대응 하지 못하는 사례가 빈번하다.
그에 따라 진단 시스템 사이트는 웹을 이용하여 사용자의 개인pc의 문제점을 진단 및 조회, 보고서 양식으로 출력 해줌으로써 사용자의 편의를 제공하며 간단한 조작으로 진단이 가능 하게 하며 웹사이트에 접속하는 모든 이용자가 간단한 진단을 받을 수 있도록 비로그인 인원도 진단이 가능하도록 지원 함 으로서 악의 적인 해킹에 노출되어 있는 문제를 해소하고자 진단 시스템 사이트를 설계 및 구현하였다.

2. 관련 연구

2.1 JAVA

JAVA언어는 오크(Oak)라는 언어로부터 탄생되었다. 오크언어는 1991년 미국 썬마이크로시스템사의 컴퓨터 과학자인 제임스 고슬링에 의해 개발된 언어로서 가전제품의 기능을 프로그램으로 제공하기 위해 개발 되었다. 처음에는 가전제품이나 PDA와 같은 소형기기에 사용될 목적이였으나 여러 종류의 운영체제를 사용하는 컴퓨터들이 통신하는 인터넷이 등장하자 운영체제에 독립적인 오크가 이에 적합하다고 판단하여 오크를 인터넷에 적합하도록 그 개발 방향을 바꾸면서 이름을 자바(JAVA)로 변경하였으며, 1996년 1월에 자바의 정식버전을 발표했다. 자바의 가장 중요한 특징은 운영체제(Operating System, 플랫폼)에 독립적이라는 것이다. 자바로 작성된 프로그램은 운영체제의 종류에 관계없이 실행이 가능하기 때문에, 운영체제에 따라 프로그램을 전혀 변

경하지 않고도 실행이 가능하다. 이러한 장점으로 인해 자바는 다양한 기종의 컴퓨터와 운영체제가 공존하는 인터넷 환경에 적합한 언어로써 인터넷의 발전과 함께 많은 사용자층을 확보할 수 있었다. 또한 객체지향개념과 기존의 다른 프로그래밍언어, 특히 C++의 장점을 채택하는 동시에 잘 사용되지 않는 부분은 과감히 제외시킴으로써 비교적 배우기 쉽고 이해하기 쉬운 간결한 표현이 가능하도록 했다. 자바는 풍부한 클래스 라이브러리(Java API)를 통해 프로그래밍에 필요한 요소들을 기본적으로 제공하기 때문에 자바 프로그래머는 단순히 이 클래스 라이브러리만을 잘 활용해도 강력한 기능의 자바 프로그램을 작성할 수 있다.

2.2 JSP

JSP는 Java Server Page의 약자로, 썬마이크로시스템즈 사의 잦바 서블릿(Servlet)기술을 확장시킨 웹 환경상에서 100% 순수한 자바만으로 서버 사이드 모듈을 개발하기 위한 기술이다. JSP도 서블릿과 마찬가지로 서버 사이드에서 DBMS와 같은 [1]백 엔드 서버(Back-end Server)와 연동하여 이들 백 엔드 서버의 데이터를 가공하여 화면에 표시할 수 있고, 여러 조건에 따라 표시할 수 있는 내용들을 동적으로 처리할 수 있는 기능을 제공하고 있다. JSP는 웹프로그래밍 언어 중의 하나로, 자바라는 언어를 기반으로 만들어졌다. 그래서 자바언어가 갖는 특징들을 그대로 이어 받고 있다.

- 객체 지향적이다.
- 네트워크 지향적이다.
- 멀티 쓰레드를 지원한다.
- 플랫폼에 독립적이다.
- 보안성이 뛰어나다.
- 코드가 친근하다.

2.3 Winpcap

WinDump는 Tcpdump를 Win32로 포팅한 것으로, 인기 있는 유닉스용 네트워크 툴이다. WinDump는 가장 유명한 유닉스용 스니퍼/네트웍 유틸리티 중 하나인 Tcpdump와 완전히 호환가능하다. Tcpdump와 마찬가지로 WinDump는 정규표현식에 맞는 패킷 헤더를 출력한다. Windump의 거의 모든 기능을 Tcpdump에서 사용할 수 있다.
WinDump는 네트워크 인터페이스를 정해져 있지 않은 모드(promiscuous mode)로 만든다.(드러나는 모든 패킷을 잡는다). WinDump로 애플리케이션의 응답 시간(response time)을 측정하며, 네트워크 문제가 발생했을 때 에러의 정확한 위치를 지정한다.비교환 이더넷(non-switched Ethernet)과같은 공유 액세스 네트워크에서 트래픽이 다른 호스트 사이에서 이동하는 것을 볼 때 유용하다.

2.4 Tomcat

톰켓 자체에 웹 서버 기능이 내장되어있어 JSP가 실행되는 웹 서버를 구성할 수 있다.
톰켓에 아파치를 연동하는 이유는 톰켓의 웹 서버 기능은 기본적인 기능이기 때문에 아파치와 연동하여 아파치가 가지고 있는 다양한 웹 서버 기능을 이용하기 위해서 이다
톰캣이란? JSP/Servlet Container 중에 하나로 사용자에게 JSP요청을 받으면 서블릿으로 바

꾸어 이를 실행하는 역할을 한다. JSP페이지를 웹 서버에 요청을 하면 이페이지를 해석하고 실행하는 역할을 하는 것이다.

아파치는 웹 서버로서 사용자의 요청을 받아 처리를 한다. 아파치가 요청을 받았는데 이것이 JSP문서 또는 서블릿이면 톰캣으로 넘기게 된다.

JSP코딩시에는 톰캣만 이용하여 충분히 가능하지만 톰캣의 웹 서버는 기능도 적고 많고 사용자가 요구를 할 때 부하가 많이 걸린다. 따라서 일반적인 목적 (JSP를 실행하는 웹 서버) 에서는 아파치를 웹 서버로 이용하고
 단지 톰캣은 JSP/서블릿 컨테이너 기능만 수행하게 하여 이용을 하는 것이다

2.5 MySQL

MySQL은 세계적으로 가장 널리 사용되고 있는 오픈소스 데이터베이스로 C/C++, java 등과 연결 가능한 API도 제공되며, 다양한 웹서버와도 연결이 용이하다. 이러한 오픈
소스 데이터베이스인 MySQL의 특징 몇 가지를 소개하겠다.

① MySQL은 관계형 데이터베이스 관리 시스템이다.

관계형 데이터베이스는 데이터를 하나의 커다란 저장 공간에 저장하지 않고 서로 별개의 테이블에 나누어서 저장을 하는 시스템으로 이를 통해 처리 속도와 유연성이 확보된다. SQL(Structured Query Language)은 ANSI/ISO표준에서 정의한 데이터베이스 접속을 위한 가장 일반적인 표준 언어이다.

② MySQL 소프트웨어는 오픈소스 이다.

MySQL 데이터베이스는 GPL(GNU Public License)를 준수하는 오픈소스 데이터베이스이며, GPL을 준수해서 사용하는 모든 사용자에게 무료로 배포되고 있다.

③ MySQL 서버는 클라이언트/서버 또는 임베디드 시스템에서 사용할 수 있다.

MySQL 데이터베이스 소프트웨어는 다중-쓰레드 SQL 서버로 구성된 클라이언트/서버 시스템이다. 또한, MySQL 서버를 임베디드 형태로도 다양한 용도로 사용할 수가 있다.

3. 연구내용

취약점 진단 시스템 사이트를 구현하기 위하여 Tomcat, MySQL, JSP, JAVA를 이용했다.
 웹 페이지는 관리자 페이지와 사용자 페이지 두 가지로 구현하였다. 사용자 페이지는 진단 및 조회, 다운로드 기능을 구현하였다.
손님으로 접속 시에는 진단 기능만 가능하고 로그인후 진단 시 서버는 받아온 정보를 MySQL과의 연동으로 DB에 저장한다. 진단 결과 다운로드는 MS word파일로 저장이 가능하다. 관리자 페이지에서는 관리자 ID로 로그인시 DOS공격 탐지 및 모든 저장된 정보를 확인 할 수 있다. Dos공격 탐지에는JAVA,WinDump,WinPcap을 이용하여 핑을 보내는 ip를 캡쳐후 지정된 횟수 이상시 DB에 저장되어 확인이 가능하도록 구현하였다.
그림1은 취약점 진단 시스템의 전체 구성도를 나타낸 것이다.

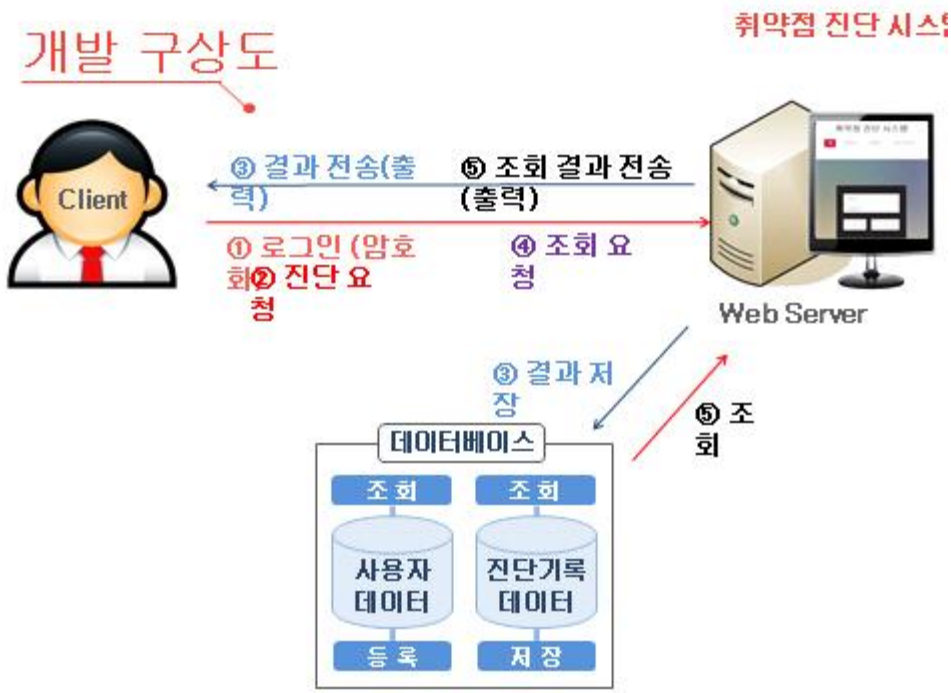


그림1. 취약점 진단 시스템의 구성도

3.1 프로그램 구현

그림 2는 웹페이지의 Main페이지다
회원가입 이후 로그인시 사용자 페이지에서 진단하기, 조회하기 기능을 이용 할 수 있으며 비로그인 시에는 진단하기만 사용 할 수 있다. 그리고 Main 페이지에서 관리자 페이지로 넘어갈 수 있다.

그림2. Main 페이지

그림 3은 사용자 페이지의 진단하기 기능이며 비 로그인 시에는 DB에 저장되지는 않는다.

그림3. 진단하기 페이지

그림 4는 진단하기 페이지에서 진단하기를 클릭 시 진단하여 보고서 형식으로 출력해주는 페이지 이다.

이름	root
이메일	ghainb@naver.com
진단 일자	2015-05-22
내용	호스트 이름: KIM-PC OS 이름: Microsoft Windows 7 Ultimate K OS 버전: 6.1.7601 Service Pack 1 빌드 7601 네트워크 카드: NIC 3개 설치됨 [01]: Bluetooth 장치(개인 영역 네트워크) 연결 이름: Bluetooth 네트워크 연결 상태: 미디어 연결이 끊어짐 [02]: Realtek PCIe GBE Family Controller 연결 이름: 로컬 영역 연결 DHCP 사용: 예 DHCP 서버: 192.168.10.1 IP 주소 [01]: 192.168.10.98 [02]: fe80::8537:4878:b144:344c [03]: Intel(R) Wireless-N 7260 연결 이름: 무선 네트워크 연결 상태: 미디어 연결이 끊어짐 방화벽 상태: ---------- 프로필 = 표준 작동 모드 = 사용 예외 모드 = 사용 멀티캐스트/브로드캐스트 응답 모드 = 사용 알림 모드 = 사용 그룹 정책 버전 = Windows 방화벽 원격 관리 모드 = 사용 안 함 KakaoTalk가 발견되었습니다. 1개의 이상프로세스가 발견되었습니다.

그림 4. 진단 페이지

그림 5는 진단페이지에서 MS Word 이미지 클릭 시 보고서파일을 다운받을 수 있다.

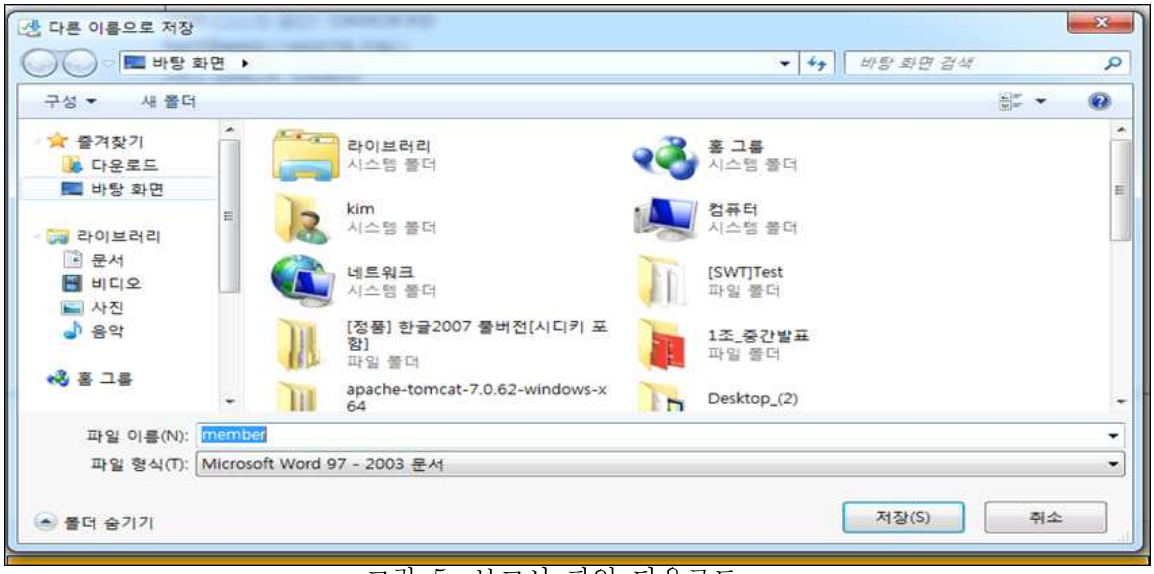


그림 5. 보고서 파일 다운로드

그림 6은 조회하기 페이지로 로그인 한 유저의 그동안의 진단했었던 정보를 찾아볼 수 있다.

그림 6. 조회하기 페이지

그림 7은 관리자 페이지로 Dos 공격을 탐지 가능하다.
MySQL에 일정 횟수가 넘으면 그 IP를 저장하고 저장된 값을 페이지에
출력해주는 형식이다.

그림 7. 관리자 페이지의 Dos 공격 의심 IP 캡쳐

그림8은 관리자 페이지에서 로그인후 진단하기를 사용했던 유저의 모든 정보를 볼 수 있다.

호스트 이름: KIM-PC OS 이름: Microsoft Windows 7 Ultimate K OS 버전: 6.1.7601 Service Pack 1 빌드 7601 네트워크...	2015-05-24
호스트 이름: KIM-PC OS 이름: Microsoft Windows 7 Ultimate K OS 버전: 6.1.7601 Service Pack 1 빌드 7601 네트워크...	2015-05-28
호스트 이름: KIM-PC OS 이름: Microsoft Windows 7 Ultimate K OS 버전: 6.1.7601 Service Pack 1 빌드 7601 네트워크...	2015-05-28

그림8. 관리자 페이지에서의 모든 정보

3.2 취약점 진단 시스템 소스

3.2.1 MAIN 페이지

```
%@ page language="java" contentType="text/html; charset=EUC-KR"
pageEncoding="EUC-KR"%>
<%@ page import="java.text.SimpleDateFormat" import="java.sql.*"
import="java.net.URLEncoder"%>

<head>
<title>J.S.P.-취약점진단시스템</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<meta name="description" content="" />
```

```
<meta name="keywords" content="" />
<script src="js/jquery.min.js"></script>
<script src="js/jquery.dropotron.min.js"></script>
<script src="js/skel.min.js"></script>
<script src="js/skel-layers.min.js"></script>
<script src="js/init.js"></script>
<link rel="shortcut icon" href="./images/1.ico">
<LINK REL="stylesheet" type="text/css" href="./css/style.css" />




</head>
<html>
<body class="homepage">
<!-- Header -->
<div id="header-wrapper">
<div id="header">
<!-- Logo -->
<h1>
<a href="main.jsp">취약점진단시스템</a>
</h1>

<!-- Nav -->
<nav id="nav">
<ul>
<li class="current"><a href="main.jsp">홈</a></li>
<li><a href="Check_menu.jsp">진단하기</a></li>
<li><a href="Search_menu.jsp">조회하기</a></li>
<li><a href="Rootmain.jsp">관리자페이지</a></li>
</ul>
</nav>

<!-- Banner -->
<section id="banner">
<header>
<%
//------------------------------- JSP CODE START ( 세션변수에따른문서선택)
String member_id = (String) session.getAttribute("member_id");
if (member_id == null || member_id == "") {
%>
<jsp:include page="./LoginForm.jsp" flush="false" />
<%
} else {
%>
<jsp:include page="./LoginState.jsp" flush="false" />
<%
}
//------------------------------- JSP CODE END
%>
</header>
</section>

<!-- Intro -->
<section id="intro" class="container">
<div class="row">
<div class="4u">
<section class="first">
<i class="icon featured fa-cog"></i>
<header>
<h2>진단</h2>
</header>
<p>진단을요청하면현재자신이사용중인컴퓨터의기본적인시스템정보, 보안정보등을진단받을수
```

```
있습니다.</p>
</section>
</div>
<div class="4u">
<section class="middle">
<i class="icon featured alt fa-file-pdf-o"></i>
<header>
<h2>보고서출력</h2>
</header>
<p>진단을요청한컴퓨터의진단결과를보고서형식으로다운로드하여출력할수있습니다.</p>
</section>
</div>
<div class="4u">
<section class="last">
<i class="icon featured alt2 fa-list"></i>
<header>
<h2>조회</h2>
</header>
<p>진단결과가저장되어있어개인의지난진단기록들을조회할수있습니다.</p>
</section>
</div>
</div>
</section>
</div>
</div>

<!-- Main -->
<div id="main-wrapper">
<div class="container">
<div class="row">
<div class="12u">
<!-- Portfolio -->
<section>
<header class="major">
<h2>J.S.P.</h2>
</header>
</section>
</div>
</div>
</div>
</div>

<!-- Footer -->
<div id="footer-wrapper">
<section id="footer" class="container">
<div class="row">
<div class="12u">
<!-- Copyright -->
<div id="copyright">
<ul class="links">
<li>&copy; J.S.P. - Coding is the realization of the
imagine.</li>
</ul>
</div>
</div>
</div>
</section>
</div>
</body>
</html>
```

3.2.2. 회원가입 페이지

```
%@ page language="java" contentType="text/html; charset=EUC-KR"
pageEncoding="EUC-KR"%>
<%@ page import="java.text.SimpleDateFormat" import="java.sql.*"
import="java.net.URLEncoder"%>

<head>
<title>J.S.P.-취약점진단시스템</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<meta name="description" content="" />
<meta name="keywords" content="" />
<script src="js/jquery.min.js"></script>
<script src="js/jquery.dropotron.min.js"></script>
<script src="js/skel.min.js"></script>
<script src="js/skel-layers.min.js"></script>
<script src="js/init.js"></script>
<link rel="shortcut icon" href="./images/1.ico">
<LINK REL="stylesheet" type="text/css" href="./css/style.css" />




</head>
<html>
<body class="homepage">
<!-- Header -->
<div id="header-wrapper">
<div id="header">
<!-- Logo -->
<h1>
<a href="main.jsp">취약점진단시스템</a>
</h1>

<!-- Nav -->
<nav id="nav">
<ul>
<li class="current"><a href="main.jsp">홈</a></li>
<li><a href="Check_menu.jsp">진단하기</a></li>
<li><a href="Search_menu.jsp">조회하기</a></li>
<li><a href="Rootmain.jsp">관리자페이지</a></li>
</ul>
</nav>

<!-- Banner -->
<section id="banner">
<header>
<%
//------------------------------- JSP CODE START ( 세션변수에따른문서선택)
String member_id = (String) session.getAttribute("member_id");
if (member_id == null || member_id == "") {
%>
<jsp:include page="./LoginForm.jsp" flush="false" />
<%
} else {
%>
<jsp:include page="./LoginState.jsp" flush="false" />
<%
}
//------------------------------- JSP CODE END
%>
</header>
</section>
```

```
<!-- Intro -->
<section id="intro" class="container">
<div class="row">
<div class="4u">
<section class="first">
<i class="icon featured fa-cog"></i>
<header>
<h2>진단</h2>
</header>
<p>진단을요청하면현재자신이사용중인컴퓨터의기본적인시스템정보, 보안정보등을진단받을수
있습니다.</p>
</section>
</div>
<div class="4u">
<section class="middle">
<i class="icon featured alt fa-file-pdf-o"></i>
<header>
<h2>보고서출력</h2>
</header>
<p>진단을요청한컴퓨터의진단결과를보고서형식으로다운로드하여출력할수있습니다.</p>
</section>
</div>
<div class="4u">
<section class="last">
<i class="icon featured alt2 fa-list"></i>
<header>
<h2>조회</h2>
</header>
<p>진단결과가저장되어있어개인의지난진단기록들을조회할수있습니다.</p>
</section>
</div>
</div>
</section>
</div>
</div>

<!-- Main -->
<div id="main-wrapper">
<div class="container">
<div class="row">
<div class="12u">
<!-- Portfolio -->
<section>
<header class="major">
<h2>J.S.P.</h2>
</header>
</section>
</div>
</div>
</div>
</div>

<!-- Footer -->
<div id="footer-wrapper">
<section id="footer" class="container">
<div class="row">
<div class="12u">
<!-- Copyright -->
<div id="copyright">
<ul class="links">
<li>&copy; J.S.P. - Coding is the realization of the
imagine.</li>
</ul>
</div>
</div>
```

```
</div>
</section>
</div>
</body>
</html>
```

3.2.3 진단 페이지

```
<%@ page language="java" contentType="text/html; charset=EUC-KR"
    pageEncoding="EUC-KR"%>
<%@ page import="java.sql.*"
import = "java.text.SimpleDateFormat"
import = "java.util.Date"
import = "java.io.*" %>

<%
int member_RcdNo = 0;
String name = null
String mail = null

Connection conn = null
PreparedStatement pstmt = null
Statement stmt = null
ResultSet rs1 = null
ResultSet rs2 = null

String Query1 = ""
String Query2 = ""
String Query3 = ""

String jdbcUrl = "jdbc:mysql://localhost:3306/web_db"
String jdbcId = "root"
String jdbcPw = "1234"

Class.forName("com.mysql.jdbc.Driver");
conn = DriverManager.getConnection(jdbcUrl,jdbcId,jdbcPw);

String member_id ="손님"
String member_name ="손님"
String member_mail=""
String member_pwd=""

if( session.getAttribute("member_id") != null ) {
member_id = (String) session.getAttribute("member_id");
}
try {
Query1 = "select count(RcdNo) from list"
pstmt = conn.prepareStatement(Query1);
rs1 = pstmt.executeQuery();

while( rs1.next() ) {
member_RcdNo = rs1.getInt(1) + 2;
}

Date d = new Date();
SimpleDateFormat day = new SimpleDateFormat("yyyy-MM-dd");

int cnt = 0;
String result = null
String s = null
String msg = null
String strLine = null
String[] command = {"systeminfo","netsh firewall show state", "chkdsk" ,"tasklist"};
```

```
for( int i = 0; i < command.length i++ ) {
Process oProcess = new ProcessBuilder("cmd", "/c", command[i]).start();

// 외부프로그램출력읽기
BufferedReader stdOut    = new BufferedReader(new
InputStreamReader(oProcess.getInputStream()));

while( (s = stdOut.readLine()) != null ) { result += (s + "\n"); }

//systeminfo 명령문
if(result != null && i == 0 ) {
BufferedReader reader = new BufferedReader(new StringReader(result));
try {
while( (strLine = reader.readLine() ) != null) {
if( strLine.matches("호스트이름.*") ) {
msg += strLine + "\n"
msg = msg.replace("null", "");
} else if( strLine.matches("OS 이름.*") ) {
msg += strLine + "\n"
} else if( strLine.matches("OS 버전.*") ) {
msg += strLine + "\n"
} else if( strLine.matches("네트워크카드.*") ) {
msg += strLine + "\n"
while( (strLine = reader.readLine()) != null ) {
if( !(strLine.matches("Hyper.*")) ) {
msg += strLine + "\n"
} else {
break
}
}
}
}
} catch( IOException e ) {
// TODO Auto-generated catch block
e.printStackTrace();
}
}

//netsh firewall show state 명령문
if( result != null && i == 1 ) {
BufferedReader reader = new BufferedReader(new StringReader(result));
try {
while( (strLine = reader.readLine()) != null ) {
if ( strLine.matches("방화벽상태.*") ) {
msg += "\n" + strLine + "\n"
while( (strLine = reader.readLine()) != null ) {
if( !(strLine.matches("현재모든네트워크.*")) ) {
msg += strLine + "\n"
} else {
break
}
}
} else{}
}
} catch( IOException e ) {
// TODO Auto-generated catch block
e.printStackTrace();
}
}//chkdsk 명령문
if(result != null && i == 2 ) {
BufferedReader reader = new BufferedReader(new StringReader(result));
try {
while( (strLine = reader.readLine() ) != null) {
if( strLine.matches("Windows에서파일시스템에문제가없음을확인했습니다.*") ) {
```

```
msg += strLine + "\n"
msg = msg.replace("null", "");
while( (strLine = reader.readLine()) != null ) {
if( !(strLine.matches("Hyper.*")) ) {
msg += strLine + "\n"
} else {
break
}
}
}
}
} catch( IOException e ) {
// TODO Auto-generated catch block
e.printStackTrace();
}
}

//tasklist 명령문
if( result != null && i == 3 ) {
BufferedReader reader = new BufferedReader(new StringReader(result));
try {
while( (strLine = reader.readLine()) != null ) {
if( strLine.matches("Back orifice1.2.exe.*") ) {
msg += "\n Back orifice가검출되었습니다. \n"
cnt++;
} else if( strLine.matches("netbus1.70.exe.*") ) {
msg += "\n netbus1.70이검출되었습니다.\n"
cnt++;
} else if( strLine.matches("KakaoTalk.exe.*") ) {
msg += "\n KakaoTalk가발견되었습니다.\n"
cnt++;
}
}
msg += cnt + "개의이상프로세스가발견되었습니다."
msg=msg.replaceAll("\n", "<br>");
if( !member_id.equals("손님") ) {
Query2 = "select PWD, NAME, MAIL from member where ID=?;"
pstmt = conn.prepareStatement(Query2);
pstmt.setString(1, member_id);
rs2 = pstmt.executeQuery();
while( rs2.next() ) {
member_pwd = rs2.getString("PWD");
member_name = rs2.getString("NAME");
member_mail = rs2.getString("MAIL");
}
Query3 = "insert into list(RcdNo, UsrId, UsrDate, UsrContent, UsrName, UsrMail,
UsrPwd) values('" + member_RcdNo + "','" + member_id + "','" + day.format(d) +
"','" + msg + "','" + member_name + "','" + member_mail +"','"+ member_pwd+"')"
stmt = conn.createStatement();
stmt.executeUpdate(Query3);
rs2.close();
}

/* request.setAttribute("msg", msg);
request.setAttribute("member_mail", member_mail);
request.setAttribute("member_name", member_name);
request.setAttribute("day", day.format(d)); */
session.setAttribute("msg", msg);
session.setAttribute("member_mail", member_mail);
session.setAttribute("member_name", member_name);
session.setAttribute("day", day.format(d));

} catch( IOException e ) {
// TODO Auto-generated catch block
e.printStackTrace();
```

```
} finally {
if( stmt != null ) try { stmt.close(); } catch( SQLException ex) {}
if( conn != null ) try { conn.close(); } catch( SQLException ex) {}
}
}
}
%>
<head>
<title>J.S.P.-취약점진단시스템</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<link rel="shortcut icon" href="images/1.ico">
<script src="js/jquery.min.js"></script>
<script src="js/jquery.dropotron.min.js"></script>
<script src="js/skel.min.js"></script>
<script src="js/init.js"></script>
<script src="js/jquery.lazyload.js"></script>
<LINK REL="stylesheet" type="text/css" href="./css/loader.css" />
<script language=javascript>
function hidePreload() {
  preload.style.visibility = "hidden"
}
function makePreload(msg) {
  document.write("<div id=\"preload\" style=\"",
    "position:absolute;top:0;left:0;width:100%;height:100%;",
    "background-color:white;color:black;",
    "text-align:center;z-index:1\">",
    "<table border='0' height='100%'><tr><td>",
    msg,
    "</td></tr></table></div>");
}
makePreload("페이지로딩중. 잠시만기다려주세요.");
self.onload=hidePreload
</script>

</head>

<html>
<body>
<!-- Header -->
<div id="header-wrapper">
<div id="header">
<!-- Logo -->
<h1>취약점진단시스템</h1>
</div>
</div>
<div id="main-wrapper">
<div class="container">
<section class="box">
<table width=510 height=40 border=0 cellspacing=1 cellpadding=1 align=center>
<tr bgcolor=#A0A0A0>
<td align=center><font size=4><b>진단내용</b></font></td>
</tr>
</table>
<table width=510 border=1 cellspacing=0 cellpadding=1 align=center>
<tr>
<td width=120 align=center><b>이름</b></td>
<td width=500><%=member_name %></td>
</tr>

<tr>
<td width=120 align=center><b>이메일</b></td>
<td width=500><%=member_mail %></td>
</tr>

<tr>
```

```
<td width=120 align=center><b>진단일자</b></td>
<td width=500><%=day.format(d) %></td>
</tr>

<tr>
<td width=120 align=center><b>내용</b></td>
<td width=500><%=msg %></td>
</tr>
</table>

<table width=510 height=50 border=0 cellspacing=1 cellpadding=1 align=center>
<tr align=center>
<td width="310" align=center>
<a href="go12.jsp"><img src="./images/Copy of btn_pdf.png"
style=cursor:hand></a>
</td>
</tr>
</table>

<%
} catch( SQLException e ) {
e.printStackTrace();
} finally {
rs1.close();
pstmt.close();
conn.close();
}

%>
</section>
</div>
</div>
<%
String gogo = request.getParameter("msg");
request.setAttribute("msg",gogo);
%>
</body>
</html>
<FORM ACTION ="go12.jsp" METHOD=POST>
NAME1 ="name"
```

3.2.4 파일 다운로드

```
<%@ page language="java" contentType="application/vnd.word;charset=UTF-8"
pageEncoding="UTF-8"%>
<%@ page import="java.sql.*"
import = "java.text.SimpleDateFormat"
import = "java.util.Date"
import = "java.io.*"
%>
<%
String list_content = (String) session.getAttribute("msg");
String date = (String) session.getAttribute("day");
%>


<%

    // MS word로다운로드/실행, filename에저장될파일명을적어준다.
  response.setHeader("Content-Disposition", "attachment;filename=member.doc");
  response.setHeader("Content-Description", "JSP Generated Data");
```

```
%>

<%
int member_RcdNo = 0;
String name = null
String mail = null

Connection conn = null
PreparedStatement pstmt = null
Statement stmt = null
ResultSet rs1 = null
ResultSet rs2 = null

String Query1 = ""
String Query2 = ""
String Query3 = ""

String jdbcUrl = "jdbc:mysql://localhost:3306/web_db"
String jdbcId = "root"
String jdbcPw = "1234"

Class.forName("com.mysql.jdbc.Driver");
conn = DriverManager.getConnection(jdbcUrl,jdbcId,jdbcPw);

String member_id ="손님"
String member_name ="손님"
String member_mail=""
String member_pwd=""

if( session.getAttribute("member_id") != null ) {
member_id = (String) session.getAttribute("member_id");
}
try {
Query1 = "select count(RcdNo) from list"
pstmt = conn.prepareStatement(Query1);
rs1 = pstmt.executeQuery();

while( rs1.next() ) {
member_RcdNo = rs1.getInt(1) + 2;
}

Date d = new Date();
SimpleDateFormat day = new SimpleDateFormat("yyyy-MM-dd");


if( !member_id.equals("손님") ) {
Query2 = "select PWD, NAME, MAIL from member where ID=?;"
pstmt = conn.prepareStatement(Query2);
pstmt.setString(1, member_id);
rs2 = pstmt.executeQuery();
while( rs2.next() ) {
member_pwd = rs2.getString("PWD");
member_name = rs2.getString("NAME");
member_mail = rs2.getString("MAIL");
}
stmt = conn.createStatement();

rs2.close();
}

/* request.setAttribute("msg", msg);
request.setAttribute("member_mail", member_mail);
request.setAttribute("member_name", member_name);
request.setAttribute("day", day.format(d)); */
```

```
session.setAttribute("member_mail", member_mail);
session.setAttribute("member_name", member_name);
session.setAttribute("day", day.format(d));


} finally {
if( stmt != null ) try { stmt.close(); } catch( SQLException ex) {}
if( conn != null ) try { conn.close(); } catch( SQLException ex) {}
}


%>
<body>
<!-- Header -->
<div id="header-wrapper">

</div>
<div id="main-wrapper">
<div class="container">
<section class="box">
<table width=510 height=40 border=0 cellspacing=1 cellpadding=1 align=center>
<tr bgcolor=#A0A0A0>
<td align=center><font size=4><b>진단내용</b></font></td>
</tr>
</table>
<table width=510 border=1 cellspacing=0 cellpadding=1 align=center>
<tr>
<td width=120 align=center><b>이름</b></td>
<td width=500><%=member_name %></td>
</tr>

<tr>
<td width=120 align=center><b>이메일</b></td>
<td width=500><%=member_mail %></td>
</tr>

<tr>
<td width=120 align=center><b>진단일자</b></td>
<td width=500><%=date %></td>
</tr>

<tr>
<td width=120 align=center><b>내용</b></td>
<td width=500><%=list_content %></td>
</tr>
</table>

<table width=510 height=50 border=0 cellspacing=1 cellpadding=1 align=center>
<tr align=center>
<td width="310" align=center>

</td>
</tr>
</table>


</section>
</div>
</div>
</body>
</html>
```

3.2.5 조회하기 페이지

```
<%@ page language="java" contentType="text/html; charset=EUC-KR"
pageEncoding="EUC-KR"%>
<%@ page import="java.text.SimpleDateFormat"
 import="java.sql.*"
 import="java.net.URLEncoder"
 import="java.net.URLEncoder" %>

<%
request.setCharacterEncoding("euc-kr");

Connection conn = null
PreparedStatement pstmt = null
ResultSet rs1 = null
ResultSet rs2 = null

int TotalRecords = 0;

int CurrentPage = 0;
int Number = 0;
int TotalPages = 0;
int TotalPageSets = 0;
int CurrentPageSet = 0;

int PageRecords = 10;
int PageSets = 10;

if( request.getParameter("CurrentPage") == null) {
CurrentPage = 1;
} else {
CurrentPage = Integer.parseInt(request.getParameter("CurrentPage"));
}

String Query1 = ""
String Query2 = ""
String encoded_key = ""

int FirstRecord = PageRecords * (CurrentPage-1);

String column = request.getParameter("column");
if( column == null ) column = ""

String key = request.getParameter("key");
if( key != null ) {
encoded_key = URLEncoder.encode(key, "euc-kr");
} else {
key = ""
}

try {
String jdbcUrl = "jdbc:mysql://localhost:3306/web_db"
String jdbcId = "root"
String jdbcPw = "1234"

Class.forName("com.mysql.jdbc.Driver");
conn = DriverManager.getConnection(jdbcUrl,jdbcId,jdbcPw);

if( column.equals("") || key.equals("") ) {
Query1 = "select count(RcdNo) from list"
Query2 = "select RcdNo, UsrContent, UsrDate from list order by RcdNo desc limit
" + FirstRecord + "," + PageRecords
} else {
Query1 = "select count(RcdNo) from list where " + column + "like '%" + key + "%'"
Query2 = "select RcdNo, UsrContent, UsrDate from list where" + column + "like
'%" + key + "%'" + "order by RcdNo desc limit " + FirstRecord + "," + PageRecords
```

```
}

pstmt = conn.prepareStatement(Query1);
rs1 = pstmt.executeQuery();
pstmt = conn.prepareStatement(Query2)
rs2 = pstmt.executeQuery();

rs1.next();
TotalRecords = rs1.getInt(1);

Number = TotalRecords - (CurrentPage - 1) * PageRecords
%>

<head>
<title>J.S.P.-취약점진단시스템</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<link rel="shortcut icon" href="./images/1.ico">
<script src="js/jquery.min.js"></script>
<script src="js/jquery.dropotron.min.js"></script>
<script src="js/skel.min.js"></script>
<script src="js/skel-layers.min.js"></script>
<script src="js/init.js"></script>
</head>

<html>
<body>
<!-- Header -->
<div id="header-wrapper">
<div id="header">
<!-- Logo -->
<h1><a href="main.jsp">취약점진단시스템</a></h1>
<!-- Nav -->
<nav id="nav">
<ul>
<li><a href="main.jsp">홈</a></li>
<li><a href="Check_menu.jsp">진단하기</a></li>
<li class="current"><a href="Search_menu.jsp">조회하기</a></li>
</ul>
</nav>
</div>
</div>

<!-- Main -->
<div id="main-wrapper">
<div class="container">
<!-- Content -->
<article class="box post">
<table width=510 height=40 border=0 cellspacing=1 cellpadding=1 align=center>
<tr bgcolor=#A0A0A0>
<td align=center><font size=4><b>진단목록</b></font></td>
</tr>
</table>

<table width=510 border=1 cellspacing=0 cellpdding=1 align=center>
<tr align=center>
<td width=800><b>진단내용</b></td>
<td width=100><b>진단일자</b></td>
</tr>
<%
while(rs2.next()) {
int rno = rs2.getInt("RcdNo");
String subject = rs2.getString("UsrContent");
String date = rs2.getString("UsrDate");

int max_length = 150;
```

```
if (subject.length() > max_length) {
subject = subject.substring(0, max_length);
subject = subject + "..."
}
%>
<tr>
<td width=800 align=left><a
href="SearchContent.jsp?rno=<%=rno%>"><%=subject%></a></td>
<td align=center><%=date %></td>
</tr>
<%
Number--;
}
%>
</table>

<form name="Search_menu" method=post action="TestList.jsp">
<table width=510 height=50 border=0 cellspacing=1 cellpadding=1 align=center>
<tr>
<td align=left width=100></td>
<td width=320 align=center>
<%
TotalPages = (int)Math.ceil((double)TotalRecords/PageRecords);
TotalPageSets = (int)Math.ceil((double)TotalPages/PageSets);
CurrentPageSet = (int)Math.ceil((double)CurrentPage/PageSets);

String bf_block = "./images/btn_bf_block.png"
String bf_page = "./images/btn_bf_page.png"
String nxt_page = "./images/btn_nxt_page.png"
String nxt_block = "./images/btn_nxt_block.png"

if( CurrentPageSet > 1 ) {
int BeforePageSetLastPage = PageSets * (CurrentPageSet - 1);
String retUrl = "TestLsit.jsp?CurrentPage=" + BeforePageSetLastPage + "&column="
+ column + "&key=" + encoded_key

String click = "javascript:location.replace('" + retUrl + "')"
out.println("<img src=" + bf_block + " onClick=" + click + " style=cursor:hand>");
} else {
out.println("<img src=" + bf_block + ">");
}

if( CurrentPage > 1 ) {
int BeforePage = CurrentPage - 1;
String retUrl = "TestList.jsp?CurrentPage=" + BeforePage + "&column=" + column +
"&key=" +encoded_key

String click = "javascript:location.replace('" + retUrl + "')"
out.println("<img src=" + bf_page + " onClick=" + click + " style=cursor:hand>");
} else {
out.println("<img src=" + bf_page + ">");
}

int FirstPage = PageSets * (CurrentPageSet - 1);
int LastPage = PageSets * CurrentPageSet

if( CurrentPageSet == TotalPageSets ) {
LastPage = TotalPages
}

for( int i = FirstPage + 1; i <= LastPage i++ ) {
if( CurrentPage == i ) {
out.println("<b>" + i + "</b>");
} else {
```

```
String retUrl = "TestList.jsp?CurrentPage=" + i + "&column=" + column + "&key=" +
encoded_key
out.println("<a href=" + retUrl + ">" + i + "</a>");
}
}

if( TotalPages > CurrentPage ) {
int NextPage = CurrentPage + 1;
String retUrl = "TestList.jsp?CurrentPage=" + NextPage + "&column=" + column +
"&key=" + encoded_key

String click = "javascript:location.replace('" + retUrl + "')"
out.println("<img src=" + nxt_page + " onClick=" + click + " style=cursor:hand>");
} else {
out.println("<img src=" + nxt_page + ">");
}

if( TotalPages > CurrentPageSet ) {
int NextPageSet = PageSets * CurrentPageSet + 1;
String retUrl = "TestList.jsp?CurrentPage=" + NextPageSet + "&column=" + column
+ "&key=" + encoded_key

String click = "javascript:location.replace('" + retUrl + "')"
out.println("<img src=" + nxt_block + ">");
} else {
out.println("<img src=" + nxt_block + ">");
}
%>
</td>
<td width=120 align=right>
<select name="column" size=1>
<option value="" selected>선택</option>
<option value="UsrContent">진단내용</option>
<option value="UsrDate">진단일자</option>
</select>
<input type=text name="key" size=10 maxlength=20>
<img src="./images/btn_search.png" align=absmiddle style=cursor:hand
onClick="javascript:submit()">
</td>
</tr>
</table>
</form>
<%
} catch( SQLException e ) {
e.printStackTrace();
} finally {
rs2.close();
rs1.close();
pstmt.close();
conn.close();
}
%>
</article>
</div>
</div>

<!-- footer -->
<div id="footer-wrapper">
<section id="footer" class="container">
<!-- Copyright -->
<div id="copyright">
<ul class="links">
<li>&copy; J.S.P. - Coding is the realization of the imagine.</li>
</ul>
</div>
```

```
</section>
</div>
<!--
<%
//로그인한사용자가아닌경우로그인페이지로이동
String retURL = "'main.jsp'"
String member_id = (String) session.getAttribute("member_id");
if ( member_id == null || member_id == "" ) {
out.println("<script type = \"text/javascript\">");
out.println("alert('로그인후사용하실수있습니다.')");
out.println("location.replace(" + retURL + ")");
out.println("</script>");
return
}
%>
-->
</body>
</html>
```

3.2.6 기록 삭제 소스

```
<%@ page language="java" contentType="text/html; charset=EUC-KR"
    pageEncoding="EUC-KR"%>
<%@ page import="java.sql.*"
import="java.net.URLEncoder"
import="java.util.Date" %>

<%
int rno = Integer.parseInt(request.getParameter("rno"));


String encoded_key = ""

String column = request.getParameter("column");
if( column != null ) {
String key = request.getParameter("key");
if( key != null ) {
encoded_key = URLEncoder.encode(key, "euc-kr");
} else {
key = ""
}
}

%>
<head>
<title>J.S.P.-취약점진단시스템</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<link rel="shortcut icon" href="images/1.ico">
<script src="js/jquery.min.js"></script>
<script src="js/jquery.dropotron.min.js"></script>
<script src="js/skel.min.js"></script>
<script src="js/init.js"></script>

<style>
<!--
form input[type=password] {
width: 50%
}
-->
</style>

<script type="text/javascript">
```

```
function CheckPwd(form) {
if( !form.pw.value ){
alert("비밀번호를입력하세요.");
form.pw.focus();
return
}
}

function Back() {
window.history.back();
}
</script>
</head>

<html>
<body>

<!-- Header -->
<div id="header-wrapper">
<div id="header">
<!-- Logo -->
<h1>취약점진단시스템</h1>
</div>
</div>
<div id="main-wrapper">
<div class="container">
<section class="box">
<center><i class="icon featured alt fa-trash-o"></i></center>
<form name="pwd" method="post"
action="DeleteProc.jsp?rno=<%=rno%>&column=<%=column%>&key=<%=encoded_ke
y%>">
<center><input type="password" id="pw" name="pw" maxlength="16" title="비밀번호"
placeholder="비밀번호" class="int"></center>
<ul class="actions" align="center">
<li><input type="submit" value="삭제" STYLE=CURSOR:HAND
onClick="javascript:CheckPwd(pwd)"></li>
<li><input type="button" value="취소"
onclick="javascript:location.replace('SeachContent.jsp?rno=<%=rno%>&column=<%=c
olumn%>&key=<%=encoded_key%>')"></li>
</ul>
</form>
</section>
</div>
</div>

</body>
</html>
```

3.2.7 프린트 소스

```
<%@ page language="java" contentType="text/html; charset=EUC-KR"
    pageEncoding="EUC-KR"%>
<%@ page import="java.sql.*"
import="java.net.URLEncoder"
import="java.util.Date" %>

<%
int rno = Integer.parseInt(request.getParameter("rno"));

Connection conn = null
PreparedStatement pstmt = null
ResultSet rs = null
PreparedStatement pstmt2 = null
```

```
ResultSet rs2 = null

String encoded_key = ""

String column = request.getParameter("column");
if( column == null ) {
column = ""
}

String key = request.getParameter("key");
if( key != null ) {
encoded_key = URLEncoder.encode(key, "euc-kr");
} else {
key = ""
}

try {
String jdbcUrl = "jdbc:mysql://localhost:3306/web_db"
String jdbcId = "root"
String jdbcPw = "1234"

Class.forName("com.mysql.jdbc.Driver");
conn = DriverManager.getConnection(jdbcUrl,jdbcId,jdbcPw);

String Query = "select UsrName, UsrMail, UsrDate, UsrContent from list where
RcdNo=?"
pstmt = conn.prepareStatement(Query);
pstmt.setInt(1, rno);
rs = pstmt.executeQuery();
rs.next();

String name = rs.getString(1);
String mail = rs.getString(2);
String date = rs.getString(3);
String content = rs.getString(4).trim();
content = content.replaceAll("\r\n","<br>");

%>
<script type="text/javascript">
function Print() {
document.body.innerHTML = selectArea.innerHTML
    window.print();
}

function popupDelete() {
var popUrl = "./Delete.jsp"//팝업창에출력될페이지URL
var popOption = "width=500, height=500, resizable=no, scrollbars=no, status=no;"
//팝업창옵션(optoin)
window.open(popUrl,"",popOption);
}
</script>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<link rel="shortcut icon" href="./images/1.ico">
<script src="js/jquery.min.js"></script>
<script src="js/jquery.dropotron.min.js"></script>
<script src="js/skel.min.js"></script>
<script src="js/skel-layers.min.js"></script>
<script src="js/init.js"></script>
</head>

<html>
<body>
<!-- Header -->
<div id="header-wrapper">
```

```
<div id="header">
<!-- Logo -->
<h1><a href="main.jsp">취약점진단시스템</a></h1>
<!-- Nav -->
<nav id="nav">
<ul>
<li><a href="main.jsp">홈</a></li>
<li><a href="Check_menu.jsp">진단하기</a></li>
<li class="current"><a href="Search_menu.jsp">조회하기</a></li>
</ul>
</nav>
</div>
</div>

<div id="main-wrapper">
<div class="container">
<div id="selectArea">
<!-- Content -->
<article class="box post">
<center><i class="icon featured alt2 fa-list"></i></center>
<table width=510 height=40 border=0 cellspacing=1 cellpadding=1 align=center>
<tr bgcolor=#A0A0A0>
<td align=center><font size=4><b>진단내용</b></font></td>
</tr>
</table>

<table width=510 border=1 cellspacing=0 cellpadding=1 align=center>
<tr>
<td width=120 align=center><b>이름</b></td>
<td width=500><%=name%></td>
</tr>

<tr>
<td width=120 align=center><b>이메일</b></td>
<td width=500><%=mail%></td>
</tr>

<tr>
<td width=120 align=center><b>진단일자</b></td>
<td width=500><%=date%></td>
</tr>

<tr>
<td width=120 align=center><b>내용</b></td>
<td width=500><%=content%></td>
</tr>
</table>

<table width=510 height=50 border=0 cellspacing=1 cellpadding=1 align=center>
<tr align=center>
<td width="310" align=right>
<img src="./images/btn_print.png" style=cursor:hand
onClick="javascript:Print()"> 
<img src="./images/btn_del.png" style=cursor:hand
onClick="javascript:location.replace('Delete.jsp?rno=<%=rno%>&column=<%=column
%>&key=<%=encoded_key%>')">
</td>
</tr>
</table>
<%
} catch( SQLException e ) {
e.printStackTrace();
} finally {
rs.close();
pstmt.close();
```

```
conn.close();
}
%>
</article>
</div>
</div>
</div>

<!-- footer -->
<div id="footer-wrapper">
<section id="footer" class="container">
<!-- Copyright -->
<div id="copyright">
<ul class="links">
<li>&copy; J.S.P. - Coding is the realization of the imagine.</li>
</ul>
</div>
</section>
</div>
</body>
</html>
```

3.2.8 관리자 페이지

```
<%@ page language="java" contentType="text/html; charset=EUC-KR"
pageEncoding="EUC-KR"%>
<%@ page import="java.text.SimpleDateFormat"
import="java.sql.*"
import="java.net.URLEncoder" %>

<head>
<title>J.S.P.-취약점진단시스템</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<meta name="description" content="" />
<meta name="keywords" content="" />
<script src="js/jquery.min.js"></script>
<script src="js/jquery.dropotron.min.js"></script>
<script src="js/skel.min.js"></script>
<script src="js/skel-layers.min.js"></script>
<script src="js/init.js"></script>
<link rel="shortcut icon" href="./images/1.ico">
<LINK REL="stylesheet" type="text/css" href="./css/style.css" />




</head>
<html>
<body class="homepage">
<!-- Header -->
<div id="header-wrapper">
<div id="header">
<!-- Logo -->
<h1><a href="Rootmain.jsp">관리자페이지</a></h1>

<!-- Nav -->
<nav id="nav">
<ul>
<li class="current"><a href="main.jsp">사용자페이지</a></li>
```

```
<li><a href="dos.jsp">dos 의심ip</a></li>
<li><a href="all_search_menu.jsp">모든진단조회</a></li>

</ul>
</nav>

<!-- Banner -->
<section id="banner">
<header>
<%
//------------------------------ JSP CODE START ( 세션변수에따른문서선택)
String member_id = (String) session.getAttribute("member_id1");
if ( member_id == null || member_id == "" ) {
%>
<jsp:include page="./RootLoginForm.jsp" flush="false" />
<%
} else {
%>
<jsp:include page="./RootLoginState.jsp" flush="false" />
<%
}
//------------------------------ JSP CODE END
%>
</header>
</section>

<!-- Intro -->
<section id="intro" class="container">
<div class="row">
<div class="4u">
<section class="first">
<i class="icon featured fa-cog"></i>
<header>
<h2>진단</h2>
</header>
<p> 진단을요청하면현재자신이사용중인컴퓨터의기본적인시스템정보,
보안정보등을진단받을수있습니다.</p>
</section>
</div>
<div class="4u">
<section class="middle">
<i class="icon featured alt fa-file-pdf-o"></i>
<header>
<h2>보고서출력</h2>
</header>
<p> 진단을요청한컴퓨터의진단결과를보고서형식으로다운로드하여출력할수있습니다.</p>
</section>
</div>
<div class="4u">
<section class="last">
<i class="icon featured alt2 fa-list"></i>
<header>
<h2>조회</h2>
</header>
<p> 진단결과가저장되어있어개인의지난진단기록들을조회할수있습니다.</p>
</section>
</div>
</div>
</section>
</div>
</div>

<!-- Main -->
<div id="main-wrapper">
<div class="container">
```

```
<div class="row">
<div class="12u">
<!-- Portfolio -->
<section>
<header class="major">
<h2>J.S.P.</h2>
</header>
</section>
</div>
</div>
</div>
</div>

<!-- Footer -->
<div id="footer-wrapper">
<section id="footer" class="container">
<div class="row">
<div class="12u">
<!-- Copyright -->
<div id="copyright">
<ul class="links">
<li>&copy; J.S.P. - Coding is the realization of the imagine.</li>
</ul>
</div>
</div>
</div>
</section>
</div>
</body>
</html>
```

3.2.9 Dos 탐지 소스

```
package dos1;

import java.io.IOException;
import java.io.SequenceInputStream;
import java.util.HashMap;
import java.util.Scanner;
import java.sql.*;
import java.net.*;
import java.io.*;

public class test_windump {
	Connection conn = DBConnect.Connect();
	PreparedStatement pstmt = null;
	HashMap<String, String> map = new HashMap<String, String>();

	public static void main(String[] args) {
		new test_windump();
	}

	public test_windump() {
		// 실행 커맨드
		String[] cmd = { "cmd", "/c", "windump", "-i 2","-a","-E", "-t"
,"-v", "-p" };

		Process process = null;

		try {
			// 프로세스빌더 실행
			process = new ProcessBuilder(cmd).start();

			SequenceInputStream seqIn = new SequenceInputStream(
```

```
                                        process.getInputStream(),
process.getErrorStream());

                        // 스캐너클래스를 사용해 InputStream을 스캔함
                        // Scanner s = new Scanner(process.getInputStream());
                        // Scanner s = new Scanner(process.getErrorStream());
                        Scanner s = new Scanner(seqIn);
                        String full_data = " ";// 모든 데이터
                        String cutt_data = " ";// 필요한 부분만큼 자른것
                        String b = " ";

                        while (s.hasNextLine() == true) {
                                try {
                                        full_data = (s.nextLine());
                                        System.out.println(full_data);
                                        String sql2 = "insert into test2(name)
values('"
                                                        + full_data + "')";
                                        pstmt = conn.prepareStatement(sql2);
                                        pstmt.executeUpdate();
                                        int full_data_elngth = full_data.length();
                                        map.put("kim-PC: icmp", "있다");// icmp
잡아내는것 if문으로 확인불가능

                        // map으로 있다는true 일시 진행

                                        if (full_data_elngth > 57) {
                                                cutt_data = (full_data.substring(57,
full_data_elngth));// 길이

                                                                                //
짤라서

                                                                                //
받아오기
                                                b =
full_data.substring(full_data_elngth - 12,
                                                                full_data_elngth);
                                                if (map.containsKey(b) == true) {
                                                        String sql = "insert into
go(name) values('"
                                                                                +
cutt_data + "')";
                                                        pstmt =
conn.prepareStatement(sql);
                                                        pstmt.executeUpdate();
                                                }

                                        }
                                } catch (SQLException e) {
                                        e.printStackTrace();
                                }
                                try {
                                        if (map.containsKey(b) == true) {
                                                int cutt_data_len =
cutt_data.length();
                                                String dab =
cutt_data.substring(cutt_data_len - 31,
                                                                cutt_data_len -
15);

                                                String sql1 = "select count(*) from
go where name = '"
                                                                + cutt_data + "'";
                                                Statement st =
```

```
conn.createStatement();
                                                        ResultSet rs =
st.executeQuery(sql1);

                                                        while (rs.next()) {
                                                                int name =
rs.getInt("count(*)");
                                                                System.out.format(
                                                                        "\n\t ip:
%s일정 패킷데이터가 초과하는 패킷을 보내셨습니다.\n",
                                                                        dab);
                                                                if (name > 500) {

System.out.format("\n\t ip: %s는 dos 공격이 의심됩니다",

dab);
                                                                }

                                                        }

                                                }
                                        } catch (SQLException se) {
                                                se.printStackTrace();
                                        }
                                }

                        } catch (IOException e) {
                                e.printStackTrace();
                        }
                }

}
```

3.2.10 Dos 탐지 페이지 소스

```
<%@page import="java.sql.SQLException"%>
<%@page import="java.sql.DriverManager"%>
<%@page import="java.sql.ResultSet"%>
<%@page import="java.sql.PreparedStatement"%>
<%@page import="java.sql.Connection"%>
<%@ page language="java" contentType="text/html; charset=UTF-8"
pageEncoding="UTF-8"%>
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<head>
<title>J.S.P.-취약점진단시스템</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<meta name="description" content="" />
<meta name="keywords" content="" />
<script src="js/jquery.min.js"></script>
<script src="js/jquery.dropotron.min.js"></script>
<script src="js/skel.min.js"></script>
<script src="js/skel-layers.min.js"></script>
<script src="js/init.js"></script>
<link rel="shortcut icon" href="./images/1.ico">
<LINK REL="stylesheet" type="text/css" href="./css/style.css" />




</head>
<html>
```

```
<body class="homepage">
<!-- Header -->
<div id="header-wrapper">
<div id="header">
<!-- Logo -->
<h1><a href="Rootmain.jsp">관리자페이지</a></h1>

<!-- Nav -->
<nav id="nav">
<ul>
<li><a href="main.jsp">홈</a></li>
<li class="current"><a href="dos.jsp">dos 의심ip</a></li>
<li><a href="all_search_menu.jsp">모든진단조회</a></li>
</ul>
</nav>









</html>

<%
//로그인한사용자가아닌경우로그인페이지로이동
String retURL = "'Rootmain.jsp'"
String member_id = (String) session.getAttribute("member_id1");
if ( member_id == null || member_id == "" ) {
out.println("<script type = \"text/javascript\">");
out.println("alert('로그인후사용하실수있습니다.')");
out.println("location.replace(" + retURL + ")");
out.println("</script>");
return
}
%>
    <%
        Class.forName("com.mysql.jdbc.Driver");
        Connection conn = null
        PreparedStatement pstmt = null
        ResultSet rs = null

        try{
            String jdbcDriver = "jdbc:mysql://localhost:3306/test"
            String dbUser = "root"
            String dbPwd = "1234"

            conn = DriverManager.getConnection(jdbcDriver, dbUser, dbPwd);

            pstmt = conn.prepareStatement("select * from test2");

            rs = pstmt.executeQuery();
            out.println("<script>alert('DOS공격의심IP');</script>");
            while(rs.next()){
    %>
         <tr>
         <table width=510 height=40 border=0 cellspacing=1 cellpadding=1
align=center>
<tr bgcolor=#A0A0A0>
<td align=center><font size=4><b>DOS 의심IP</b></font></td>
</tr>
</table>
            <br><td><%="IP:"+ rs.getString("name") %></td></br>
```

```
        </tr>
    <%
            }
        }catch(SQLException se){
            se.printStackTrace();
        }finally{
            if(rs != null) rs.close();
            if(pstmt != null) pstmt.close();
            if(conn != null) conn.close();
        }
    %>

     <!-- Main -->
<div id="main-wrapper">
<div class="container">
<div class="row">
<div class="12u">
<!-- Portfolio -->
<div id="copyright">
<ul class="links">
<li>&copy; J.S.P. - Coding is the realization of the imagine.</li>
</ul>
</div>
</section>
</div>
</div>
</div>
</div>

</body>

</html>
    </tbody>
</table>
</body>
</html>
```

3.2.11 모든 유저 조회 정보

```
<%@ page language="java" contentType="text/html; charset=EUC-KR"
pageEncoding="EUC-KR"%>
<%@ page import="java.text.SimpleDateFormat"
 import="java.sql.*"
 import="java.net.URLEncoder" %>

<%
//로그인한사용자가아닌경우로그인페이지로이동
String retURL = "'Rootmain.jsp'"
String member_id = (String) session.getAttribute("member_id1");
if ( member_id == null || member_id == "" ) {
out.println("<script type = \"text/javascript\">");
out.println("alert('로그인후사용하실수있습니다.')");
out.println("location.replace(" + retURL + ")");
out.println("</script>");
return
}

request.setCharacterEncoding("euc-kr");

Connection conn = null
PreparedStatement pstmt = null
PreparedStatement pstmt1 = null
ResultSet rs1 = null
```

```
ResultSet rs2 = null

int TotalRecords = 0;

int CurrentPage = 0;
int Number = 0;
int TotalPages = 0;
int TotalPageSets = 0;
int CurrentPageSet = 0;

int PageRecords = 5;
int PageSets = 5;

if( request.getParameter("CurrentPage") == null) {
CurrentPage = 1;
} else {
CurrentPage = Integer.parseInt(request.getParameter("CurrentPage"));
}

String Query1 = ""
String Query2 = ""
String encoded_key = ""

int FirstRecord = PageRecords * (CurrentPage-1);

String column = request.getParameter("column");
if( column == null ) column = ""

String key = request.getParameter("key");
if( key != null ) {
encoded_key = URLEncoder.encode(key, "euc-kr");
} else {
key = ""
}

try {
String jdbcUrl = "jdbc:mysql://localhost:3306/web_db"
String jdbcId = "root"
String jdbcPw = "1234"

Class.forName("com.mysql.jdbc.Driver");
conn = DriverManager.getConnection(jdbcUrl,jdbcId,jdbcPw);

if( column.equals("") || key.equals("") ) {
Query1 = "select count(*) from list"
Query2 = "select RcdNo, UsrContent, UsrDate from list"

}

pstmt = conn.prepareStatement(Query1);
rs1 = pstmt.executeQuery();
pstmt1 = conn.prepareStatement(Query2);
rs2 = pstmt1.executeQuery();
while( rs1.next() ) {
TotalRecords = rs1.getInt(1);

Number = TotalRecords - (CurrentPage - 1) * PageRecords
}

%>

<head>
<title>J.S.P.-취약점진단시스템</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<link rel="shortcut icon" href="./images/1.ico">
```

```
<script src="js/jquery.min.js"></script>
<script src="js/jquery.dropotron.min.js"></script>
<script src="js/skel.min.js"></script>
<script src="js/skel-layers.min.js"></script>
<script src="js/init.js"></script>
</head>

<html>
<body>
<!-- Header -->
<div id="header-wrapper">
<div id="header">
<!-- Logo -->
<h1><a href="Rootmain.jsp">관리자페이지</a></h1>
<!-- Nav -->
<nav id="nav">
<ul>
<li><a href="Rootmain.jsp">홈</a></li>
<li><a href="dos.jsp">dos 의심ip</a></li>
<li class="current"><a href="all_search_menu.jsp">모든진단조회</a></li>
</ul>
</nav>
</div>
</div>

<!-- Main -->
<div id="main-wrapper">
<div class="container">
<!-- Content -->
<article class="box post">
<table width=510 height=40 border=0 cellspacing=1 cellpadding=1 align=center>
<tr bgcolor=#A0A0A0>
<td align=center><font size=4><b>진단목록</b></font></td>
</tr>
</table>

<table width=510 border=1 cellspacing=0 cellpdding=1 align=center>
<tr align=center>
<td width=800><b>진단내용</b></td>
<td width=100><b>진단일자</b></td>
</tr>
<%
while(rs2.next()) {
int rno = rs2.getInt("RcdNo");
String subject = rs2.getString("UsrContent");
String date = rs2.getString("UsrDate");

int max_length = 150;

if (subject.length() > max_length) {
subject = subject.substring(0, max_length);
subject = subject + "..."
}
%>
<tr>
<td width=800 align=left><a href="as.jsp?rno=<%=rno%>"><%=subject%></a></td>
<td align=center><%=date %></td>
</tr>
<%
Number--;
}
%>
</table>

<form name="count" method=post action="aaaaa.jsp">
```

```
<table width=510 height=50 border=0 cellspacing=1 cellpadding=1 align=center>
<tr>
<td align=left width=100></td>
<td width=320 align=center>
<%
TotalPages = (int)Math.ceil((double)TotalRecords/PageRecords);
TotalPageSets = (int)Math.ceil((double)TotalPages/PageSets);
CurrentPageSet = (int)Math.ceil((double)CurrentPage/PageSets);

String bf_block = "./images/btn_bf_block.png"
String bf_page = "./images/btn_bf_page.png"
String nxt_page = "./images/btn_nxt_page.png"
String nxt_block = "./images/btn_nxt_block.png"

if( CurrentPageSet > 1 ) {
int BeforePageSetLastPage = PageSets * (CurrentPageSet - 1);
String retUrl = "count.jsp?CurrentPage=" + BeforePageSetLastPage + "&column=" +
column + "&key=" + encoded_key

String click = "javascript:location.replace('" + retUrl + "')"
out.println("<img src=" + bf_block + " onClick=" + click + " style=cursor:hand>");
} else {
out.println("<img src=" + bf_block + ">");
}

if( CurrentPage > 1 ) {
int BeforePage = CurrentPage - 1;
String retUrl = "count.jsp?CurrentPage=" + BeforePage + "&column=" + column +
"&key=" +encoded_key

String click = "javascript:location.replace('" + retUrl + "')"
out.println("<img src=" + bf_page + " onClick=" + click + " style=cursor:hand>");
} else {
out.println("<img src=" + bf_page + ">");
}

int FirstPage = PageSets * (CurrentPageSet - 1);
int LastPage = PageSets * CurrentPageSet

if( CurrentPageSet == TotalPageSets ) {
LastPage = TotalPages
}

for( int i = FirstPage + 1; i <= LastPage i++ ) {
if( CurrentPage == i ) {
out.println("<b>" + i + "</b>");
} else {
String retUrl = "count.jsp?CurrentPage=" + i + "&column=" + column + "&key=" +
encoded_key
out.println("<a href=" + retUrl + ">" + i + "</a>");
}
}

if( TotalPages > CurrentPage ) {
int NextPage = CurrentPage + 1;
String retUrl = "count.jsp?CurrentPage=" + NextPage + "&column=" + column +
"&key=" + encoded_key

String click = "javascript:location.replace('" + retUrl + "')"
out.println("<img src=" + nxt_page + " onClick=" + click + " style=cursor:hand>");
} else {
out.println("<img src=" + nxt_page + ">");
}

if( TotalPages > CurrentPageSet ) {
```

```
int NextPageSet = PageSets * CurrentPageSet + 1;
String retUrl = "count.jsp?CurrentPage=" + NextPageSet + "&column=" + column +
"&key=" + encoded_key

String click = "javascript:location.replace('" + retUrl + "')"
out.println("<img src=" + nxt_block + ">");
} else {
out.println("<img src=" + nxt_block + ">");
}
%>
</td>
<td width=120 align=right>
<select name="column" size=1>
<option value="" selected>선택</option>
<option value="UsrContent">진단내용</option>
<option value="UsrDate">진단일자</option>
</select>
<input type=text name="key" size=10 maxlength=20>
<img src="./images/btn_search.png" align=absmiddle style=cursor:hand
onClick="javascript:submit()">
</td>
</tr>
</table>
</form>
<%
} catch( SQLException e ) {
e.printStackTrace();
} finally {
rs1.close();
rs2.close();
pstmt.close();
pstmt1.close();
conn.close();
}
%>
</article>
</div>
</div>

<!-- footer -->
<div id="footer-wrapper">
<section id="footer" class="container">
<!-- Copyright -->
<div id="copyright">
<ul class="links">
<li>&copy; J.S.P. - Coding is the realization of the imagine.</li>
</ul>
</div>
</section>
</div>
</body>
</html>
```

4. 결론

취약점 진단시스템을 툴 개념에서 웹사이트 차원으로 전환한 시스템을 개발
웹 접속방식으로 유해신호등을 탐지/진단함으로써 시스템 ugrade시 매번 재 다운로드 해야하는 문제점을 해소하였다
특히 PC 기동시 자동 실행방식으로 운영할 경우 최신 진단시스템을 가동, 최적의 진단체제 운영이 가능하며 백신 툴의 문제점을 보완해줄 수 있다.
취약 진단 시스템은 JSP, Tomcat, MySQL을 이용해 서버와 데이터 베이스를 구축하였으며
사용자가 사용자 페이지를 이용하여 진단하기 ,조회하기, 보고서 파일 다운로드를 이용할 수 있다.
관리자는 관리자 페이지에서 Winpcap, windump를 이용한 dos공격 탐지와 모든 유저 들의 진단 목록들을 조회할 수 있도록 구현하였다.

5. 참고문헌

(1)자바의정석(JAVA자바의 정석)-도우 출판사
(2)windump 사용법 -http://kaspyx.kr/19
(3)은노기의 JSP 2.3 웹프로그래밍" -삼양미디어
(4)최범균의 JSP 2.2웹 프로그래밍 기초부터 중급까지 -가메 출판사
(5)서블릿 JSP 웹 프로그래밍 with HTML CSS XML 자바스크립트 -프리렉 출판사

6. 발표 PPT 자료


조원
소개
결론
개발
결과
개발
구상도
추진
경과
개발
방향
주제
선정이유
About
Us


조원 소개
J.S.P.(Java Solution People)
박지영 (팀장)
- 프로그램 개발 및 총괄
김태훈
- 프로그램 개발
전동현
- 자료조사

주제 선정 이유

❖ 취약점 진단시스템은 통상 툴로 개발 보급되어 개별 PC 등에 다운로드하여 활용

❖ 이러한 시스템을 웹사이트화하여 필요한 경우 수시 접속, 유해 신호 등 컴퓨터의 취약점을 진단하는 시스템을 구현

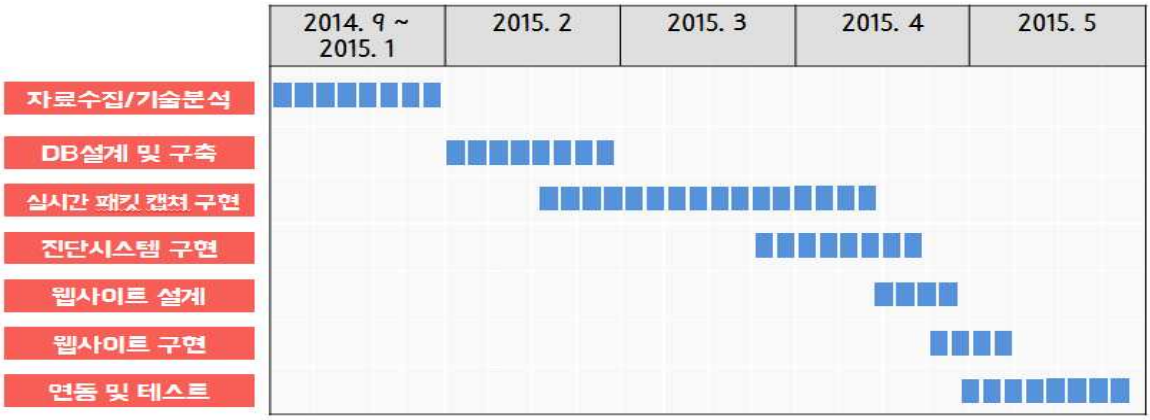
⇨ 시스템 Upgrade시 후속 다운로드없이 항상 최신 버전 활용을 자

개발 방향

접 근 성	인터넷이 가능한 어디서든 제약 없이 진단이 가능
간 편 화	프로그램과 툴이 아닌 웹사이트를 이용한 간편한 취약점 진단
출 력	날짜와 함께 DB에 저장된 분석기록을 보고서형식으로 출력가능

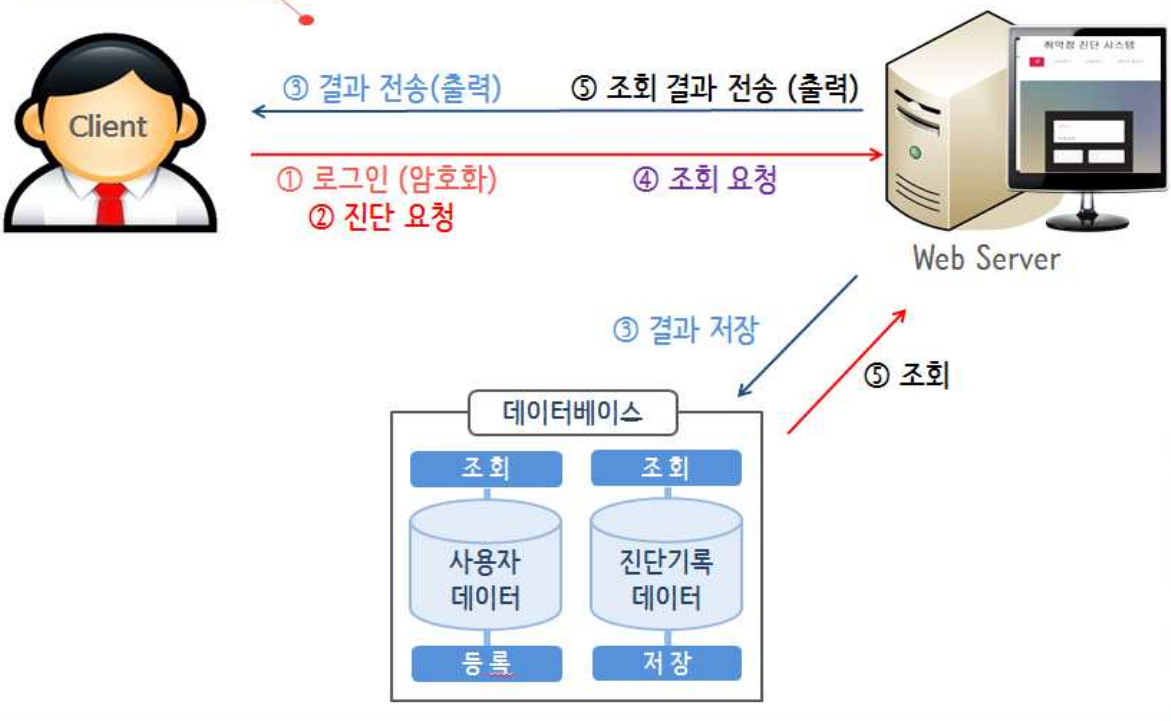
취약점 진단 시스템

추진 경과



취약점 진단 시스템

개발 구상도



개발 환경

❖ 개발 도구

- JAVA JDK 1.8
- Eclipse
- Windump & WinPcap

❖ 개발 환경

- Windows 7
- Tomcat & Mysql

개발 결과

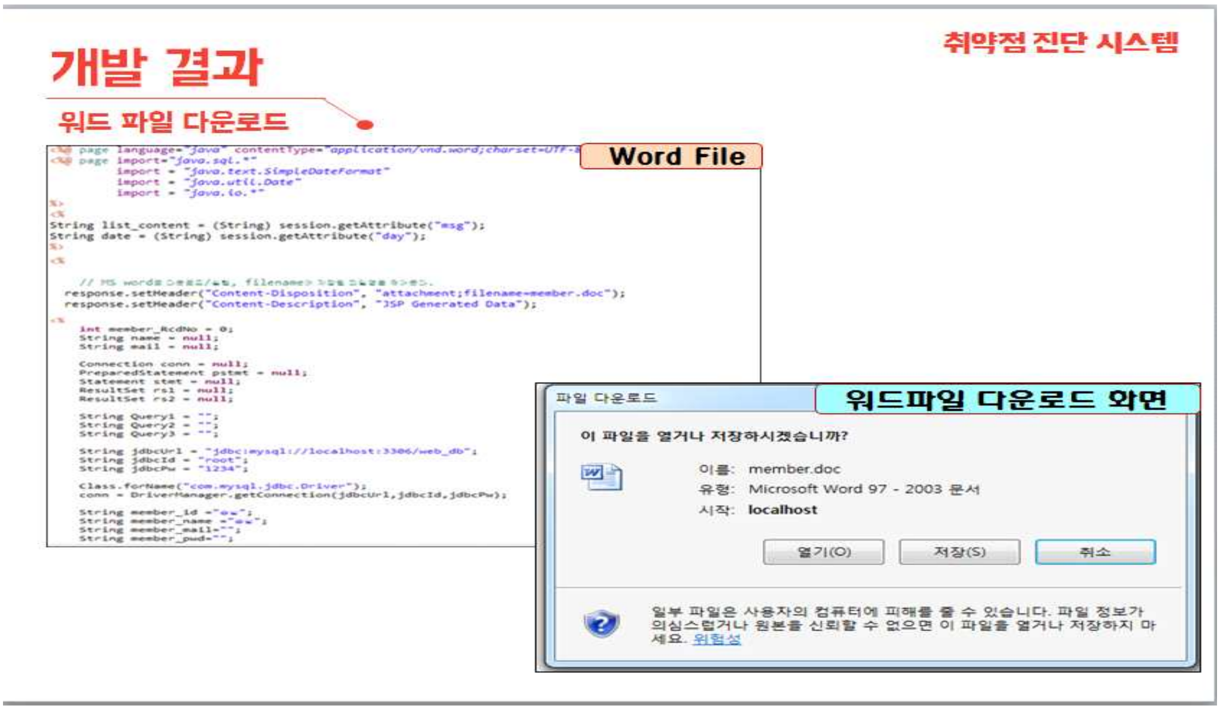
실시간 패킷 캡쳐

WinDump

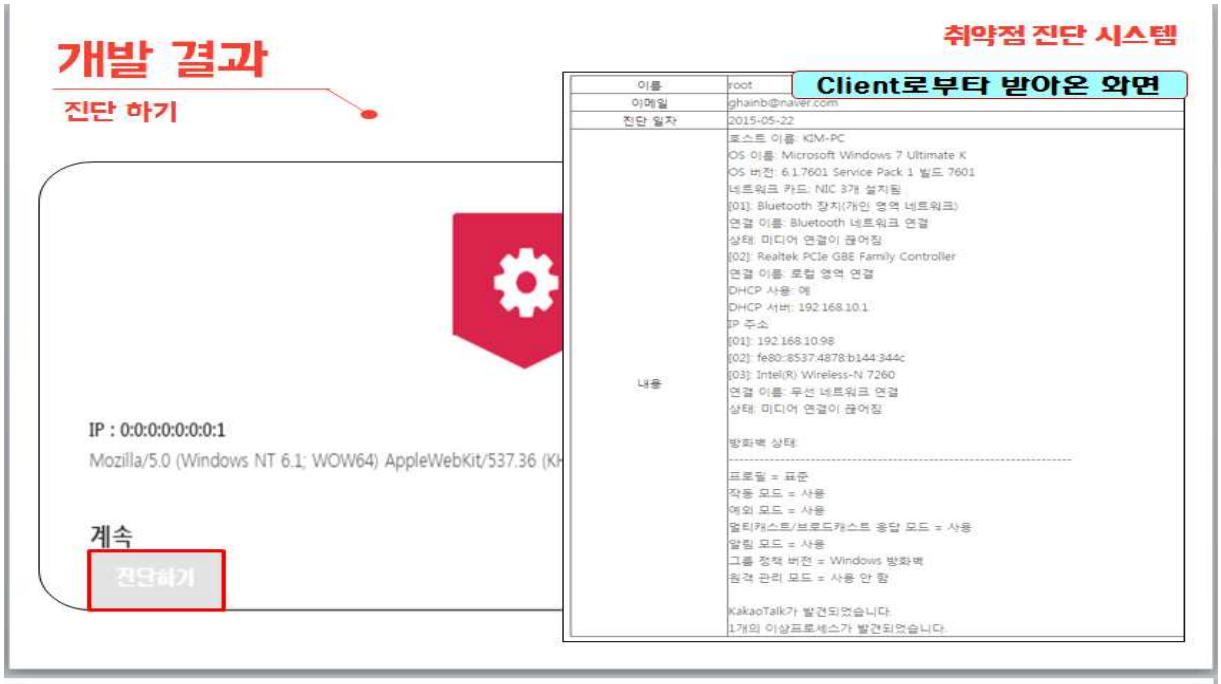
```
public class test_windump {
    Connection conn = DBConnect.Connect();
    PreparedStatement pstmt = null;
    HashMap<String, String> map = new HashMap<String, String>();

    public static void main(String[] args) {
        new test_windump();
    }

    public test_windump() {
        // 실행 커맨드
        String[] cmd = { "cmd", "/
        Process process = null;

        try {
            // 프로세스빌더 실행
            process = new ProcessB
```

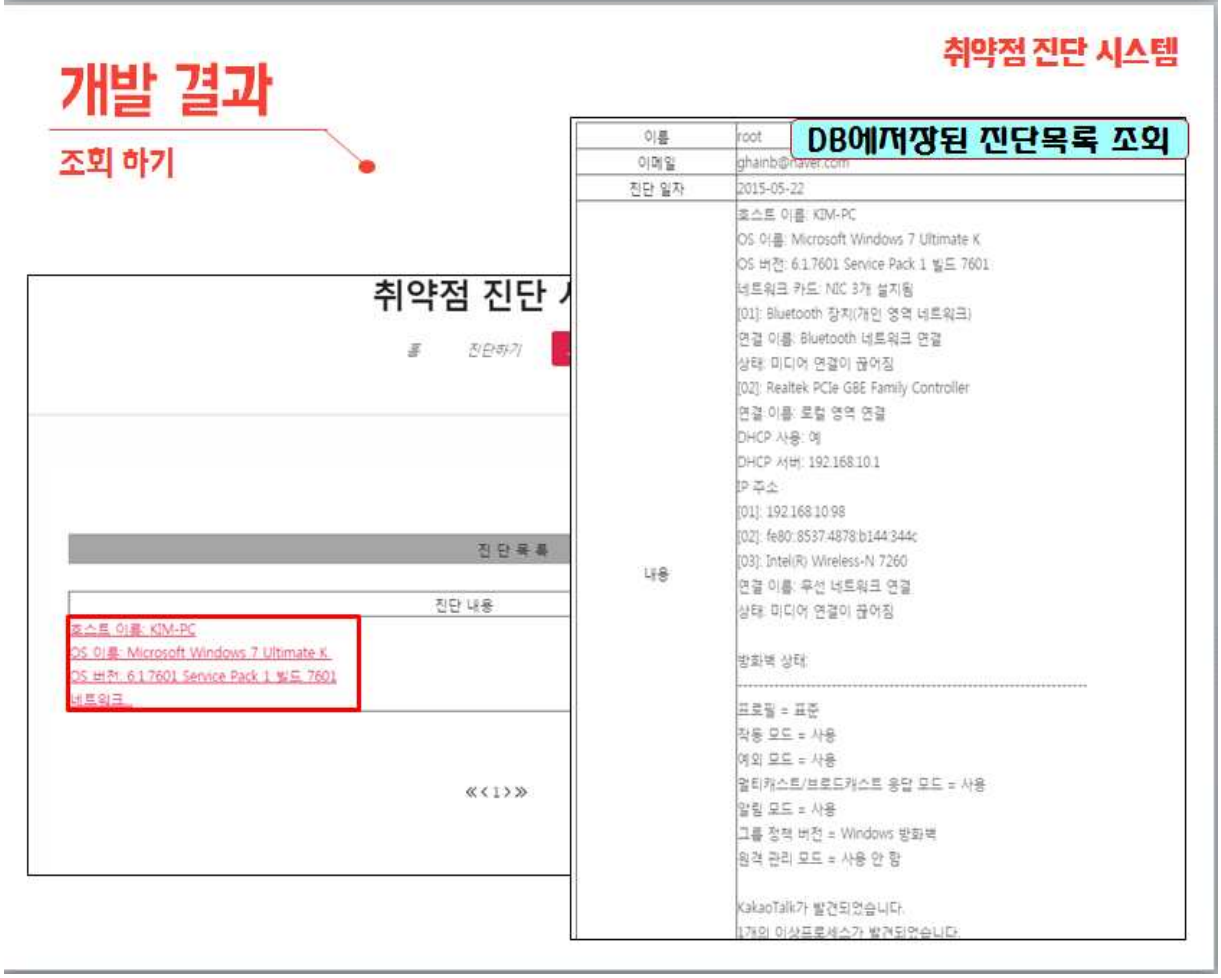
WinDump 캡쳐화면

```
21:02:25.421630 IP (tos 0x0, ttl 128, id 19522, offset 1480, flags [+], proto: ICMP (
21:02:25.421652 IP (tos 0x0, ttl 128, id 19522, offset 2960, flags [+], proto: ICMP (
21:02:25.421674 IP (tos 0x0, ttl 128, id 19522, offset 4440, flags [+], proto: ICMP (1), length: 1500) kim-PC > 192.168.219.102: icmp
21:02:25.421696 IP (tos 0x0, ttl 128, id 19522, offset 5920, flags [+], proto: ICMP (1), length: 1500) kim-PC > 192.168.219.102: icmp
21:02:25.421719 IP (tos 0x0, ttl 128, id 19522, offset 7400, flags [+], proto: ICMP (1), length: 1500) kim-PC > 192.168.219.102: icmp
21:02:25.421741 IP (tos 0x0, ttl 128, id 19522, offset 8880, flags [+], proto: ICMP (1), length: 1500) kim-PC > 192.168.219.102: icmp
21:02:25.421763 IP (tos 0x0, ttl 128, id 19522, offset 10360, flags [+], proto: ICMP (1), length: 1500) kim-PC > 192.168.219.102: icmp
21:02:25.421784 IP (tos 0x0, ttl 128, id 19522, offset 11840, flags [+], proto: ICMP (1), length: 1500) kim-PC > 192.168.219.102: icmp
21:02:25.421807 IP (tos 0x0, ttl 128, id 19522, offset 13320, flags [+], proto: ICMP (1), length: 1500) kim-PC > 192.168.219.102: icmp
21:02:25.421828 IP (tos 0x0, ttl 128, id 19522, offset 14800, flags [+], proto: ICMP (1), length: 1500) kim-PC > 192.168.219.102: icmp
21:02:25.421851 IP (tos 0x0, ttl 128, id 19522, offset 16280, flags [+], proto: ICMP (1), length: 1500) kim-PC > 192.168.219.102: icmp
21:02:25.421873 IP (tos 0x0, ttl 128, id 19522, offset 17760, flags [+], proto: ICMP (1), length: 1500) kim-PC > 192.168.219.102: icmp
21:02:25.421895 IP (tos 0x0, ttl 128, id 19522, offset 19240, flags [+], proto: ICMP (1), length: 1500) kim-PC > 192.168.219.102: icmp
21:02:25.421917 IP (tos 0x0, ttl 128, id 19522, offset 20720, flags [+], proto: ICMP (1), length: 1500) kim-PC > 192.168.219.102: icmp
21:02:25.421938 IP (tos 0x0, ttl 128, id 19522, offset 22200, flags [+], proto: ICMP (1), length: 1500) kim-PC > 192.168.219.102: icmp
```


취약점 진단 시스템
개발 결과
워드 파일 다운로드
Word File
<%@ page language="java" contentType="application/vnd.word;charset=UTF-8
<%@ page import="java.sql.*"
import = "java.text.SimpleDateFormat"
import = "java.util.Date"
import = "java.io.*"
%>
String list_content = (String) session.getAttribute("msg");
String date = (String) session.getAttribute("day");
response.setHeader("Content-Disposition", "attachment;filename=member.doc");
response.setHeader("Content-Description", "JSP Generated Data");
int member_RcdNo = 0;
String name = null;
String mail = null;
Connection conn = null;
PreparedStatement pstmt = null;
Statement stmt = null;
ResultSet rs1 = null;
ResultSet rs2 = null;
String Query1 = "";
String Query2 = "";
String Query3 = "";
String jdbcUrl = "jdbc:mysql://localhost:3306/web_db";
String jdbcId = "root";
String jdbcPw = "1234";
Class.forName("com.mysql.jdbc.Driver");
conn = DriverManager.getConnection(jdbcUrl,jdbcId,jdbcPw);
String member_pwd="";
워드파일 다운로드 화면
파일 다운로드
이 파일을 열거나 저장하시겠습니까?
이름: member.doc
유형: Microsoft Word 97 - 2003 문서
시작: localhost
열기(O)
저장(S)
취소
일부 파일은 사용자의 컴퓨터에 피해를 줄 수 있습니다. 파일 정보가 의심스럽거나 원본을 신뢰할 수 없으면 이 파일을 열거나 저장하지 마세요. 위험성


취약점 진단 시스템
개발 결과
웹 MAIN 화면
취약점 진단 시스템
홈
진단하기
조회하기
관리자 페이지
아이디
비밀번호
진단
보고서 출력
조회


취약점 진단 시스템
개발 결과
진단 하기
Client로부터 받아온 화면
이름 root
이메일 ghainb@naver.com
진단 일자 2015-05-22
내용
호스트 이름: KIM-PC
OS 이름: Microsoft Windows 7 Ultimate K
OS 버전: 6.1.7601 Service Pack 1 빌드 7601
네트워크 카드: NIC 3개 설치됨
[01]: Bluetooth 장치(개인 영역 네트워크)
연결 이름: Bluetooth 네트워크 연결
상태: 미디어 연결이 끊어짐
[02]: Realtek PCIe GBE Family Controller
연결 이름: 로컬 영역 연결
DHCP 사용: 예
DHCP 서버: 192.168.10.1
IP 주소
[01]: 192.168.10.98
[02]: fe80::8537:4878:b144:344c
[03]: Intel(R) Wireless-N 7260
연결 이름: 무선 네트워크 연결
상태: 미디어 연결이 끊어짐
방화벽 상태:
프로필 = 표준
작동 모드 = 사용
예외 모드 = 사용
멀티캐스트/브로드캐스트 응답 모드 = 사용
알림 모드 = 사용
그룹 정책 버전 = Windows 방화벽
원격 관리 모드 = 사용 안 함
KakaoTalk가 발견되었습니다.
1개의 이상프로세스가 발견되었습니다.
IP : 0:0:0:0:0:0:0:1
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KH
계속
진단하기

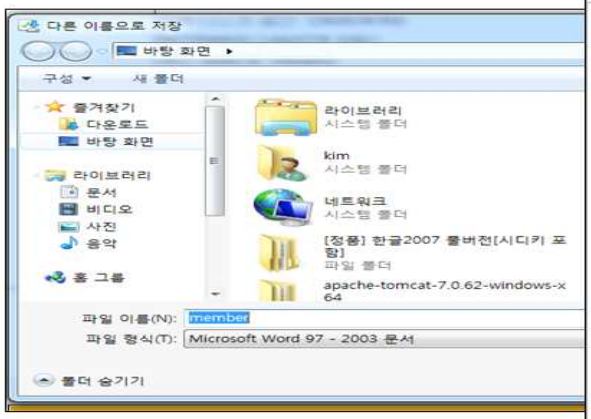

취약점 진단 시스템
개발 결과
조회 하기
DB에저장된 진단목록 조회
취약점 진단
홈
진단하기
진단 목록
진단 내용
호스트 이름: KIM-PC
OS 이름: Microsoft Windows 7 Ultimate K
OS 버전: 6.1.7601 Service Pack 1 빌드 7601
네트워크
« < 1 > »
이름 root
이메일 ghainb@naver.com
진단 일자 2015-05-22
내용
호스트 이름: KIM-PC
OS 이름: Microsoft Windows 7 Ultimate K
OS 버전: 6.1.7601 Service Pack 1 빌드 7601
네트워크 카드: NIC 3개 설치됨
[01]: Bluetooth 장치(개인 영역 네트워크)
연결 이름: Bluetooth 네트워크 연결
상태: 미디어 연결이 끊어짐
[02]: Realtek PCIe GBE Family Controller
연결 이름: 로컬 영역 연결
DHCP 사용: 예
DHCP 서버: 192.168.10.1
IP 주소
[01]: 192.168.10.98
[02]: fe80::8537:4878:b144:344c
[03]: Intel(R) Wireless-N 7260
연결 이름: 무선 네트워크 연결
상태: 미디어 연결이 끊어짐
방화벽 상태:
프로필 = 표준
작동 모드 = 사용
예외 모드 = 사용
멀티캐스트/브로드캐스트 응답 모드 = 사용
알림 모드 = 사용
그룹 정책 버전 = Windows 방화벽
원격 관리 모드 = 사용 안 함
KakaoTalk가 발견되었습니다.
1개의 이상프로세스가 발견되었습니다.

취약점 진단 시스템

개발 결과

파일로 저장

<클라이언트로부터 획득한 정보를 파일로



진단 파일의 내용

이름	손님
이메일	
진단 일자	2015-05-28
내용	호스트 이름: KIM-PC OS 이름: Microsoft Windows 7 Ultimate K OS 버전: 6.1.7601 Service Pack 1 빌드 7601 네트워크 카드: NIC 3 개 설치됨 [01]: Bluetooth 장치(개인 영역 네트워크) 연결 이름: Bluetooth 네트워크 연결 상태: 미디어 연결이 끊어짐 [02]: Realtek PCIe GBE Family Controller 연결 이름: 로컬 영역 연결 DHCP 사용: 예 DHCP 서버: 114.71.195.130 IP 주소 [01]: 10.100.124.247 [02]: fe80::8537:4878:b144:344c [03]: Intel(R) Wireless-N 7260 연결 이름: 무선 네트워크 연결 상태: 미디어 연결이 끊어짐 방화벽 상태: --- 프로필 = 표준 작동 모드 = 사용 예외 모드 = 사용 멀티캐스트/브로드캐스트 응답 모드 = 사용 알림 모드 = 사용 그룹 정책 버전 = Windows 방화벽 원격 관리 모드 = 사용 안 함

취약점 진단 시스템

개발 결과

관리자 페이지

<관리자 페이지 DOS 탐지 및

결 론

❖ 취약점 진단시스템을 틀 개념에서 웹사이트 차원으로 전환한 시스템을 개발

- 웹 접속방식으로 유해신호 등을 탐지/진단함으로써 시스템 Upgrade시 매번 재다운로드해야 하는 문제점을 해소

- 특히 PC 가동시 자동 실행방식으로 운영할 경우 최신 진단시스템을 가동, 최적의 진단체제 운영이 가능

⇨ 이러한 시스템을 직접 구현함으로써 보안 소프트웨어 개발에 필수적인 기술력을 향상