어플리케이션 진단 및 검색도구

앱스파커(AppSparker)

2014.01.01

DAWIN ICT
information & communication

제품 및 서비스 소개 – 앱스파커(AppSparker)

소스코드 연관검색 및 취약점 진단 솔루션

- 앱스파커 (AppSparker : Application Security & Vulnerability Scanner)는 어플리케이션 소스코드의 연관 검색 및 취약점 진단, 표준 가이드 제공하는 Security Assessment tool 입니다.
- 구성 및 용도 : SecureScan (개인정보 노출 취약 소스 진단 및 연관 검색
  SecureCoding (시큐어코딩 취약 소스 진단 및 검색, 표준 가이드 제공)

기 능	내용
개인정보 노출 취약 소스 진단 및 검색 (SecureScan)	▪ 개인정보 항목에 대한 영향도 분석 ▪ 대상 현황 및 항목별 어플리케이션 현황 ▪ 테이블/칼럼 항목별 상세 연관 검색(프로그램 라인 , 소스코드, 연관검색값)
시큐어코딩 취약 소스 진단 및 검색 (SecureCoding)	▪ 보안취약 목록 조회 (Redirect, SQL-Injection, XSS 등) ▪ 해당 프로그램 Directory, 파일명 조회 ▪ 해당 취약 대상 프로그램 해당 라인 조회 및 소스코드 연계 ▪ 해당 취약점 준수 가이드 조회

앱스파커 시큐어스캔(SecureScan) 개요

시큐어스캔은 다양한 운영환경의 Application 영향분석 사업의 경험과 노하우를 결집하여 개발한 소스코드 연관 검색 도구로서 다양한 환경(OS, 소스종류, Framework:Spring, iBatis, Struts, AnyFrame 등) 환경에서 간편하고 빠른 속도로 유연하게 원하는 조건의 소스를 End-to-End 연관 검색하여 레포트를 제공함으로써 비용과 작업 공수의 절감에 획기적인 효과를 가져다 주는 솔루션입니다.

SecureScan 구조도

Target System

검색 조건
- Table, Column
- 복합검색조건

대상 소스
- JSP, Java, XML
- C, Pro*c
- Report PG

단순 검색
- ASP, sql, mxml 등 쿼리가 있는 모든 소스

AppSparker SecureScan **Framework Functional Architecture**

Parser (Syntax/Rule)

Meta Data 생성
- Query ID
- Class, Method

Search Engine (Search Rule)

Meta Data & Rule Set에 따른 Source Code Scan

Fhnd (File Handler)

대상 파일의 관리
검색조건 대비 PG/Class/Method

RPT & Logger (Report)

Search 결과 및 검증결과 보고서 작업상세로그

Source Parsing/ Validation Check/ Code Handling/ Code Mapping

Meta Data Repository / Common Running Search Engine

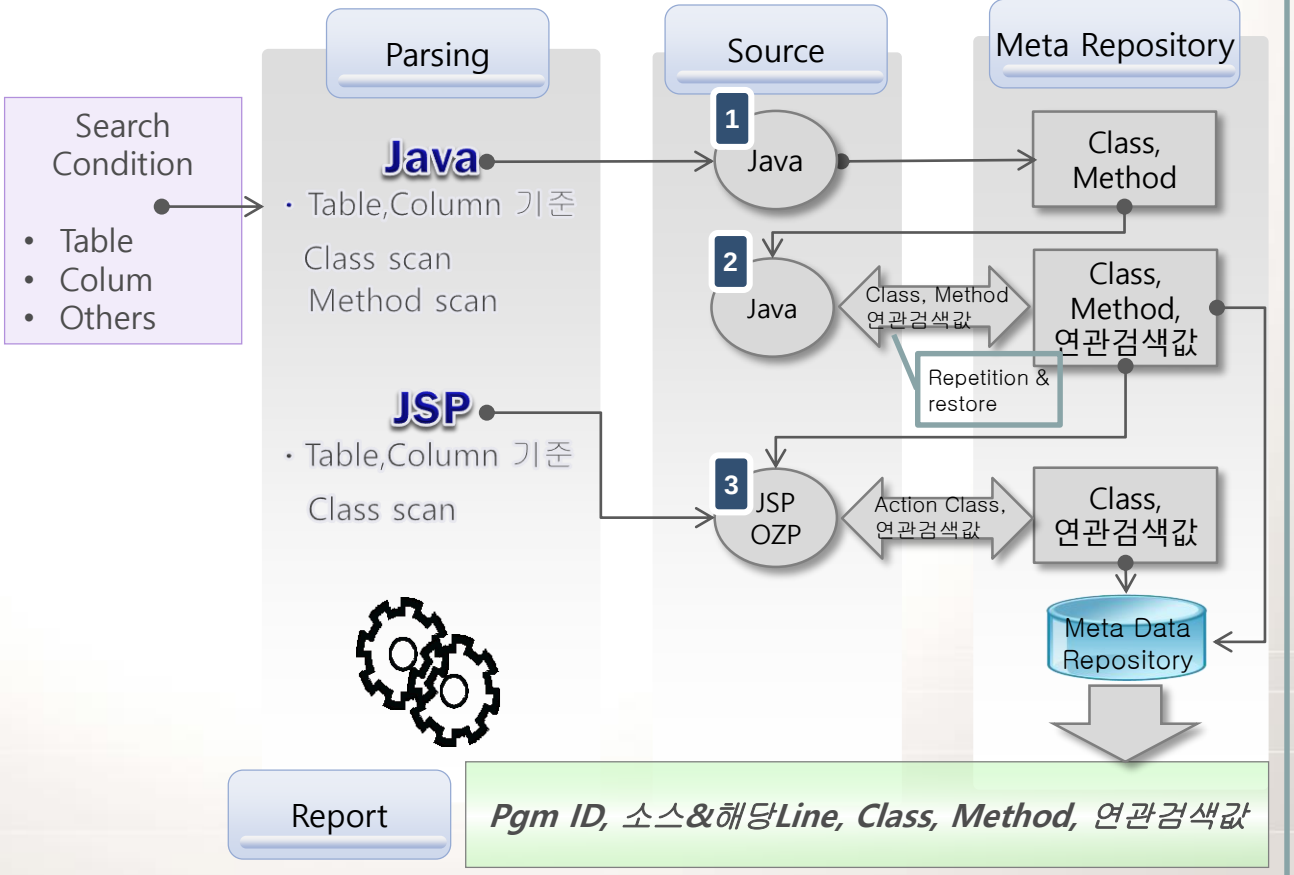
Application Source Code Migration System

Report

앱스파커 시큐어스캔(SecureScan) 구조

시큐어스캔은 처리 속도와 작업의 유연성을 위해 자체 개발 Parser를 이용하여 PC, UNIX, Linux 등 다양한 서버 환경에서 구동 가능하며 각 종 소스코드 및 다양한 검색 패턴 처리가 가능한 구조로 구성되어 있습니다.

AppSpaker SecureScan Framework



AppSparker 처리 Process

Rule 생성
- 검색 조건별 대상 소스별 검색 Rule 선택
- Java 소스 Class, Method
- JSP 소스 Action Class 등 Meta data 생성

검색
- Class, Method 대 Java 소스 검색
- 연관검색값 추출 및 검색
- Java 소스 검색 반복 및 저장
- Class, Method 대 JSP 및 OZP소스 검색

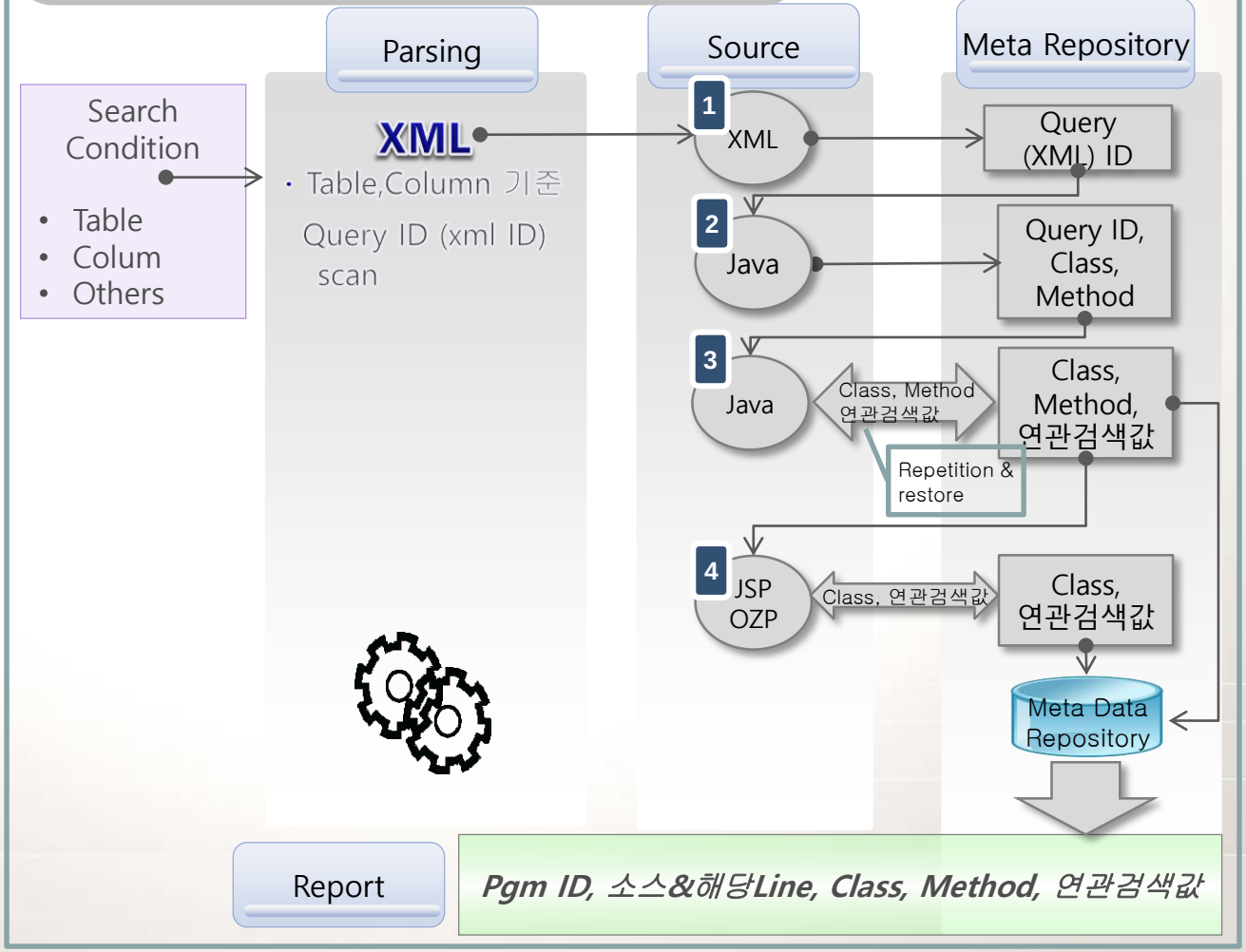
Report
- 작업 현황
- Rule별 소스파일, 해당소스 Line, Class, Method 연관검색값 출력

관리
- 백업(로그,원본,대상소스)
- 변경 이력에 대한 지속 관리
- 유사 변환작업에 대한 노하우 및 Rule 축적

앱스파커 시큐어스캔(SecureScan) 구조

시큐어스캔은 처리 속도와 작업의 유연성을 위해 자체 개발 Parser를 이용하여 PC, UNIX, Linux 등 다양한 서버 환경에서 구동 가능하며 각 종 소스코드 및 다양한 검색 패턴 처리가 가능한 구조로 구성되어 있습니다.

AppSpaker SecureScan Framework



AppSparker 처리 Process

Rule 생성
- 검색 조건별 대상 소스별 검색 Rule 선택
- XML 소스 XML ID 검색

검색
- XML ID 대 Java 소스 검색
- Class, Method 대 Java 소스 검색
- 연관검색값 추출 및 검색
- Java 소스 검색 반복 및 저장
- Class, Method 대 JSP 및 OZP소스 검색

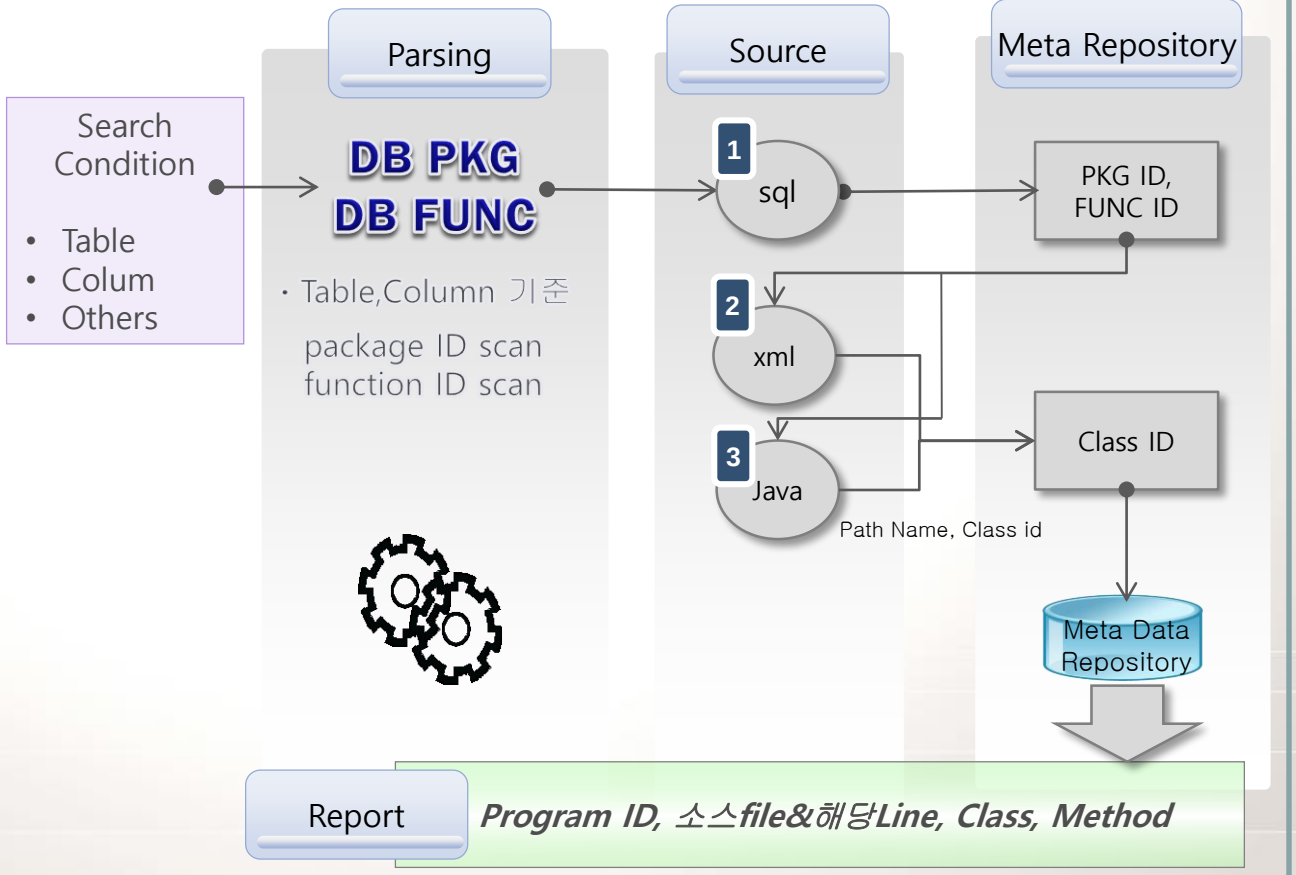
Report
- 작업 현황
- Rule별 소스파일, 해당소스 Line, Class, Method 연관검색값 출력

관리
- 백업(로그,원본,대상소스)
- 변경 이력에 대한 지속 관리
- 유사 변환작업에 대한 노하우 및 Rule 축적

앱스파커 시큐어스캔(SecureScan) 구조

시큐어스캔은 처리 속도와 작업의 유연성을 위해 자체 개발 Parser를 이용하여 PC, UNIX, Linux 등 다양한 서버 환경에서 구동 가능하며 각 종 소스코드 및 다양한 검색 패턴 처리가 가능한 구조로 구성되어 있습니다.

AppSpaker SecureScan Framework



AppSparker 처리 Process

Rule 생성
- 검색 조건별 대상 소스별 검색 Rule 선택
- DataBase Package 및 Function sql 소스 ID 검색

검색
- PKG ID 및 FUNC ID대 Java /xml 소스 ID 검색

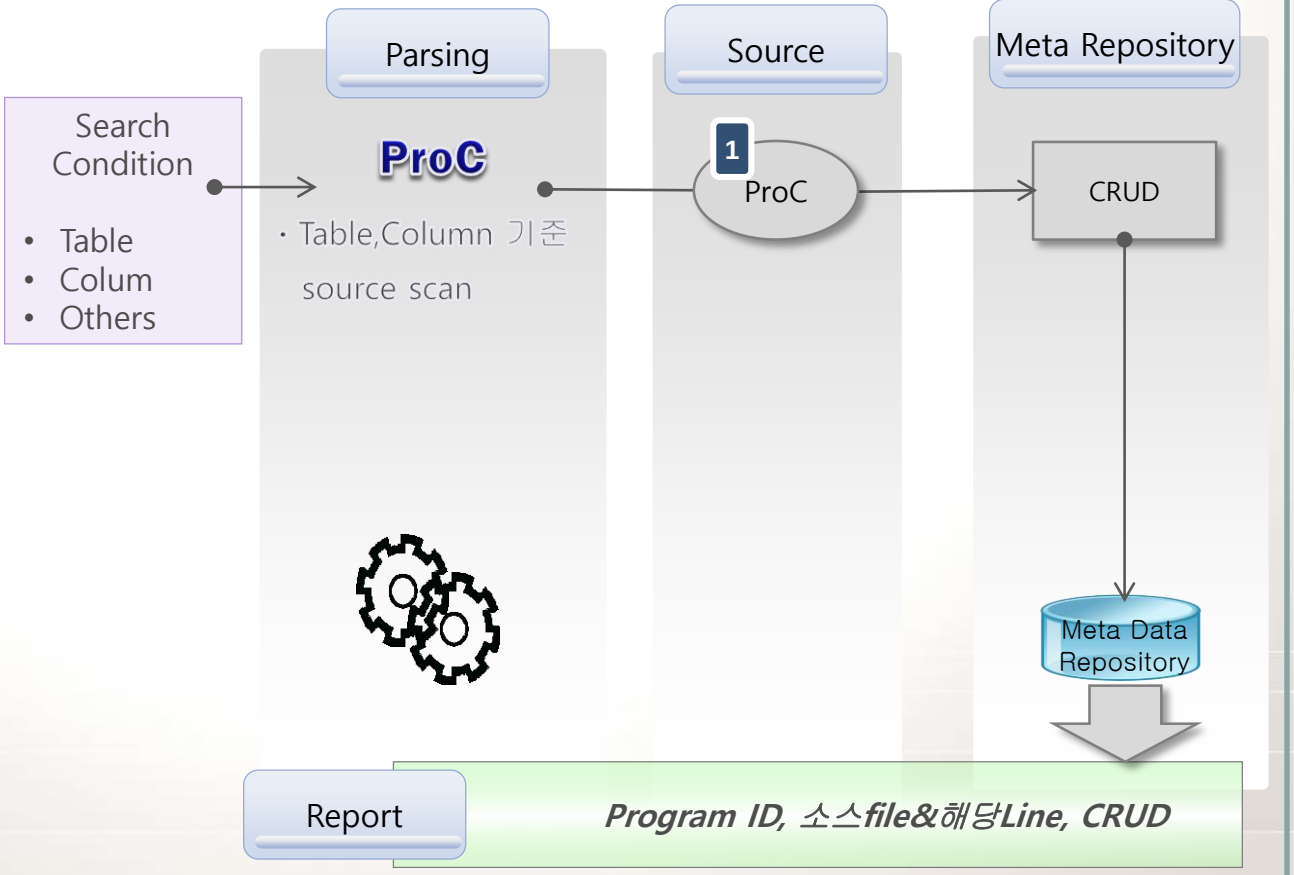
Report
- 작업 현황
- Rule별 소스파일, 해당소스 Line, Class, Method 연관정보 출력

관리
- 백업(로그,원본,대상소스)
- 변경 이력에 대한 지속 관리
- 유사 변환작업에 대한 노하우 및 Rule 축적

앱스파커 시큐어스캔(SecureScan) 구조

시큐어스캔은 처리 속도와 작업의 유연성을 위해 자체 개발 Parser를 이용하여 PC, UNIX, Linux 등 다양한 서버 환경에서 구동 가능하며 각 종 소스코드 및 다양한 검색 패턴 처리가 가능한 구조로 구성되어 있습니다.

AppSpaker SecureScan Framework

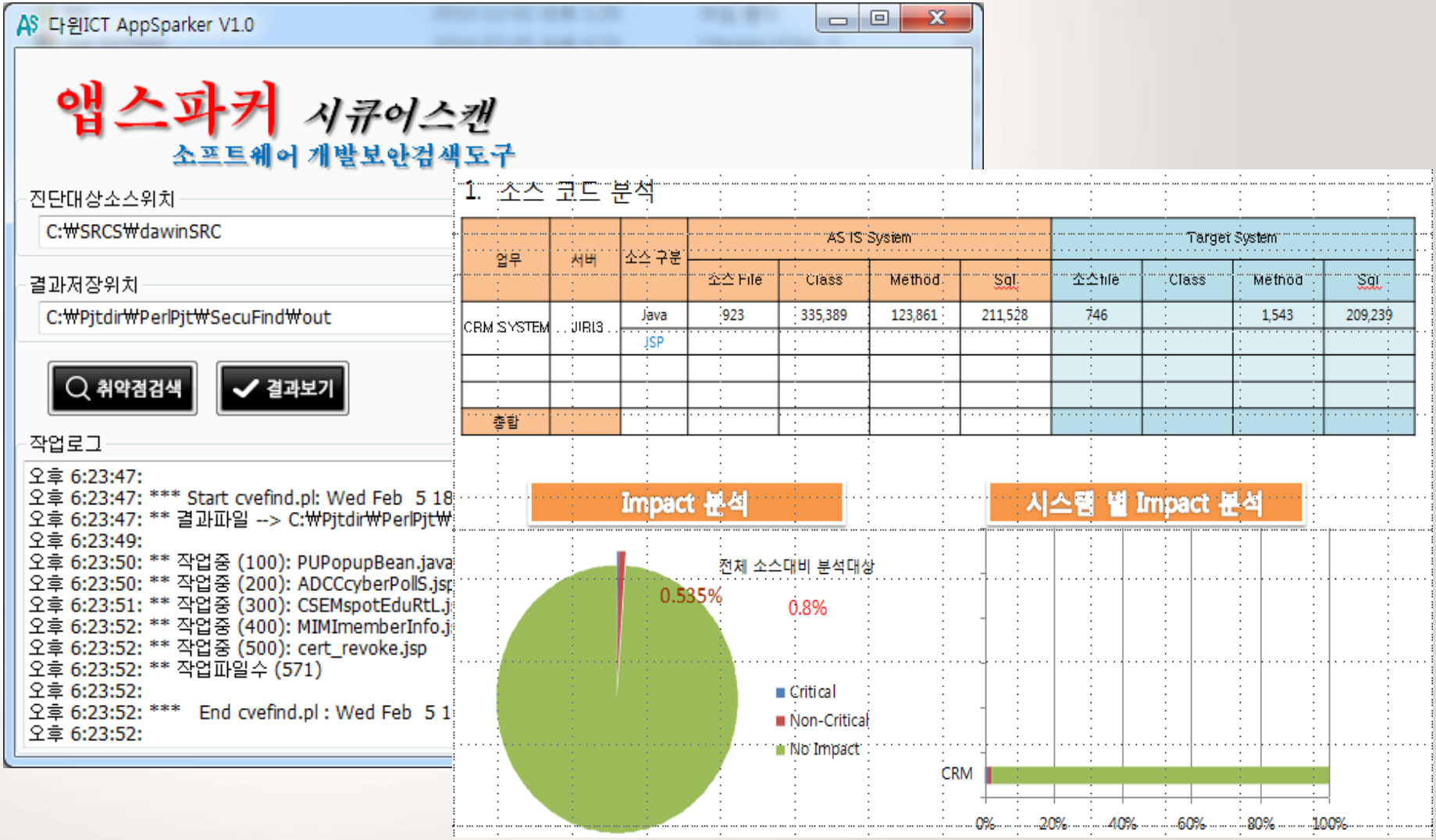


AppSparker 처리 Process

- **Rule 생성**
  - 검색 조건별 대상 소스별 검색 Rule 선택
  - DataBase Package 및 Function sql 소스 ID 검색
- **검색**
  - PKG ID 및 FUNC ID대 Java /xml 소스 ID 검색
- **Report**
  - 작업 현황
  - Rule별 소스파일, 해당소스 Line, Class, Method 연관정보 출력
- **관리**
  - 백업(로그,원본,대상소스)
  - 변경 이력에 대한 지속 관리
  - 유사 변환작업에 대한 노하우 및 Rule 축적

주요 기능

- 작업 수행 화면 및 보고서 샘플



주요 기능

검색 결과 샘플 (사용자 개인정보 노출 취약소스 진단 및 검색)

TBL	Column	Directory	프로그램ID	line	검색내용	QueryID or Class	Method	seq	CRUD	연관검색값
DS_PDF_INFO	TEMP_02		DSDBUtil.java	55	TEMP_02")); } } catch (Exception e) { e.printStackTrace(); } finally {	DSDBUtil	selectOnePdfData		SELECT	
DS_PDF_INFO	TEMP_02		DSDBUtil.java	82	TEMP_02 "; strStatus = strStatus + " FROM DS_TIFF_INFO, DS_PDF_INFO WHERE "; strStatus = strSt	DSDBUtil	selectOneTiffData		SELECT	
DS_PDF_INFO	TEMP_02		DSDBUtil.java	95	TEMP_02")); } } catch (Exception e) { e.printStackTrace(); } finally { } }	DSDBUtil	selectOneTiffData		SELECT	
DS_PDF_INFO	TEMP_02		EDMSReprocess.java	86	this.mHashTiffData = this.mdbUtil.selectOneTiffData(strSulgyeNumber, strWordCode, nPageNumber);	EDMSReprocess	startTiffProcess	1		selectOneTiffData
DS_PDF_INFO	TEMP_02		EDMSReprocess.java	47	this.mHashPdfData = this.mdbUtil.selectOnePdfData(strSulgyeNumber, strWordCode);	EDMSReprocess	startLMSProcess	1		selectOnePdfData

AP 영향도 분석

Application 영향도 분석 (단위:본수)

Part	시스템명	Application 전체현황						Application 암호화 대상 분석					
		전체	.PC	XML	JSP	Java	기타	대상	.PC	XML	JSP	Java	기타
공통	계정계	640	354				286	219	26				193
예금	에금	4,434	3,808				626	1,238	739				499
	환수탁	2,091	1,667				424	594	211				383
보험	계정계	4,483	3,086				1,397	1,529	750				779
	상품	1,977	492	6	745	732		20	12			3	
전자금융	WEB	13,679		963	9,126	3,590	1,265			154	249	862	
	스마트금융	15,454		1,086	317	14,051		369		127	13	229	

주요 산출물

AP 영향도 분석

Application 항목별 대상 목록 (단위:본수)

Part	시스템명	DIR	파일명	CUD			실명번호		여권번호		외국인번호		면허번호		성명		이메일		전화번호		주소	
				여부	CUD	R	CU	R	CU	R	CU	R	CU	R	CU	R	CU	R	CU	R	CU	R
예금	계정계	Sp_aa/src	AAB8033.PC			1														1		
			AAB8099.PC	1	D																	
			AAC8199.PC	1	CU										1							
			AAJOINT.PC			1										1				1		1
			AAKUKOH.PC	1	CU		1								1							
			AAEBPH.PC	1	CU										1							

주요 산출물

AP 영향도 분석

Application 항목별 상세 목록 (J2EE) (단위:본수)

TBL	Column	항목명	DIR	프그램ID	Line	검색내용	QueryID or Class	연관 검색값	SEQ
INICDMIT	DEOR_MCLS_NM	성명	Src/org/kpic/eus/app/ing/slq	Ing020301.xml	173	,DEOR_MCLS_NM, SICK_NM,DTLS_SICK_NM,TO_CHAR(CRT_DTTM) CRT_DTTM From	selectListcdm		
					208	INICDMIT(APLY_DATE, SICK_CSDT_CIDE, DEOR_MCLS, DEOR_SCLS	Insertcdm		
INUSERMT	PSWD	패스워드	Src/org/kpic/eus/app/inz/slq	INZ010101.xml	43	.PSWD, A_USER_NM, A_DEPT_CODE, A_ROLE_MGNT	selectUser		
	MOBL_NO				43	.MOBL_NO, A_UTLZ_YN,A_CRTR_NO	selectUser		
	HOME_TLNO				43	HOME_TLNO, A_COMP_TLNO	selectUser		
INCUSTMT	CUST_KRNM	성명	Src/org/kpic/eus/app/ina/controller	INA010101OAd.java	157	resultObj=(INA010101OEv)defaultDao.queryForObject("INA010101.selectClientInfo3",map)	INA010101OAd	selectClientInfo3	1
	RNNO	실명번호	Src/org/kpic/eus/app/ina/controller	INA010101OAd.java	165	resultObj=(INA010101OEv)defaultDao.queryForObject("INA010101.selectClientInfo2",map)	INA010101OAd	selectClientInfo2	1
INKDSDHT	ISRT_RNO	실명번호	Src/org/kpic/eus/app/ina/controller	INA010102OAd.java	306	onfoTotalCount=queryForInt("INA010108.selectInfoTotalCount",INA010108)	INA010101OAd	selectInfoTotalCount	1
MUMS280	M25_6	실명번호	Src/org/kpic/eus/app/ina/controller	INA010102OAd.java	317	quList=(List<INA010107OEv>)defaultDao.queryForList("INA010107.selectListQa",INA010107);	INA010102OAd	selectListQa	1
	M20_1	실명번호	Src/org/kpic/eus/app/ina/controller	INA010102OAd.java	318	emmList=(List<INA010107OEv>)defaultDao.queryForList("INA010107.selectListemm",INA010107);	INA010102OAd	selectListEmm	1

주요 산출물

AP 영향도 분석

Application 항목별 상세 목록 (Pro*C) (단위:본수)

TBL	Column	항목명	DIR	프그램ID	Line	검색내용	DML	CUD
AAJOINT	OPTR_NM	성명	Sp_aa/src	AAA899902T.PC	281	,optr_nm, rcmn_no, inf	SELECT	0
					535	,optr_dvsn, optr_nm,rcmn_no	INSERT	1
					574	SET optr_nm = :gtAajoint.v_optr-nm, info_chg_sqnu	UPDATE	1
BCPFINCT	MAIN_TLNO	전화번호	Sp_aa/src	AAB803300R.PC	567	"substr(D.amin_tlno,4,12) main_tlno	SELECT	0
					710	"substr(D.amin_tlno,4,12) main_tlno	SELECT	0
					1232	"OUT.main_tlno	SELECT	0
					1149	"D.main_tlno	SELECT	0
AAJOINT	OPTR_NM	성명	Sp_aa/src	AAB809903W.pc	394	,A.optr_nm, A.txt_temn_no, A.eod_yn_jeodyn, A	SELCT	0
AAOPGOMT	OPTR_NM	성명	Sp_aa/src	AAB809903W.pc	394	,A.optr_nm, A.txt_temn_no, A.eod_yn_jeodyn, A	SELCT	0
AAJOINT	OPTR_NM	성명	Sp_aa/src	AAB809904W.pc	408	,A.optr_nm, A.txt_temn_no, A.eod_yn_jeodyn, A	SELCT	0
AAOPGOMT	OPTR_NM	성명	Sp_aa/src	AAB809904W.pc	408	,A.optr_nm, A.txt_temn_no, A.eod_yn_jeodyn, A	SELCT	0
BCPFINCT	MAIN_TLNO	전화번호	Sp_aa/src	AABRNMITjoin.pc	1328	OUT.main_tlno INTO :gtAabrnmit50.v_brn_code,	SELECT	0

주요 기능

- 검색 결과 샘플(시큐어코딩 취약 소스 진단 및 검색)

보안취약목록

- SQL-INJECTION
- XSS

프로그램목록(SQL-INJECTION)

No	Directory	파일명	줄번호	검색내용
1	오픈시스템_다윈시스템_JAVA_/com/kbdawin/ab	[redacted]	99	whereQuery = " where EMP_NO = '" + emp_no + "'";

2	오픈시스템_다윈시스템_JAVA_/com/kbdawin/ad/ag	[redacted]	177	query.append(") m \n");
				query.append(" where rnum between ").append(helper.getCurpage()*(int)helper.getPagesize()-(int)helper.getPagesize()+1);
				query.append(" and ").append(helper.getCurpage()*(int)helper.getPagesize());

3	오픈시스템_다윈시스템_JAVA_/com/kbdawin/ad/ag	[redacted]	269	query.append(" DELETE TDA_HOLIDAY ");
				query.append(" WHERE idx in (" + idx + ")");
				result = mdao.executeQuery(query.toString());

4	오픈시스템_다윈시스템_JAVA_/com/kbdawin/ad	[redacted]	160	queryS.append(" ,TDA_EDU_MAIN B \n");
				queryS.append(" WHERE MNG_FP_NO = '"+empNo+"' \n");
				queryS.append(" AND A.REU_NO = B.REU_NO \n");

5	오픈시스템_다윈시스템_JAVA_/com/kbdawin/ad	[redacted]	519	query2.append(" FROM TDA_EMPL \n");
				query2.append(" WHERE ORG_SUB_BRNC = (SELECT ORG_SUB_BRNC FROM TDA_EMPL WHERE EMP_NO = '"+empNo+"') \n");
				query2.append(" AND (CHIEF_GB = '1' or NOW_PSTN='901')) A \n"
				);

6	오픈시스템_다윈시스템_JAVA_/com/kbdawin/ad	[redacted]	528	query2.append(" FROM TDA_ORG A \n");
				query2.append(" ,(SELECT * FROM TDA_EMPL WHERE EMP_NO = '"
				+empNo+"') B \n");
				query2.append(" WHERE A.ORG_CD = B.ORG_SUB_BRNC) B \n");

7	오픈시스템_다윈시스템_JAVA_/com/kbdawin/ad	[redacted]	549	query3.append(" FROM TDA_EMPL \n");
				query3.append(" WHERE ORG_SUB_BRNC = '"+orgCdI+"' \n");
				query3.append(" AND EMP_GB = '1' \n");

8	오픈시스템_다윈시스템_JAVA_/com/kbdawin/ad	[redacted]	765	query.append(" ,EMAIL_DOMN, CRE_USR_ID, CRE_DTM, HQ_YN, GUBUN) \n");
				query.append(" VALUES ('"+corpNo+"',(SELECT NVL(REPLACE(TO_CHAR(MAX(CORP_SEQ)+1,'000'),' ','0'),'001') AS CORP_SEQ FROM TDA_CUST_CO WHERE CORP_NO = '"+corpNo+"'),'"+corpNm+"','"+mngBrnc+"','"+busnType1+"' \n");
				query.append(" ,'"+busnType2+"','"+busnType3+"','"+zipCd+"','"+addr+"','"+addrDtil+"' \n");

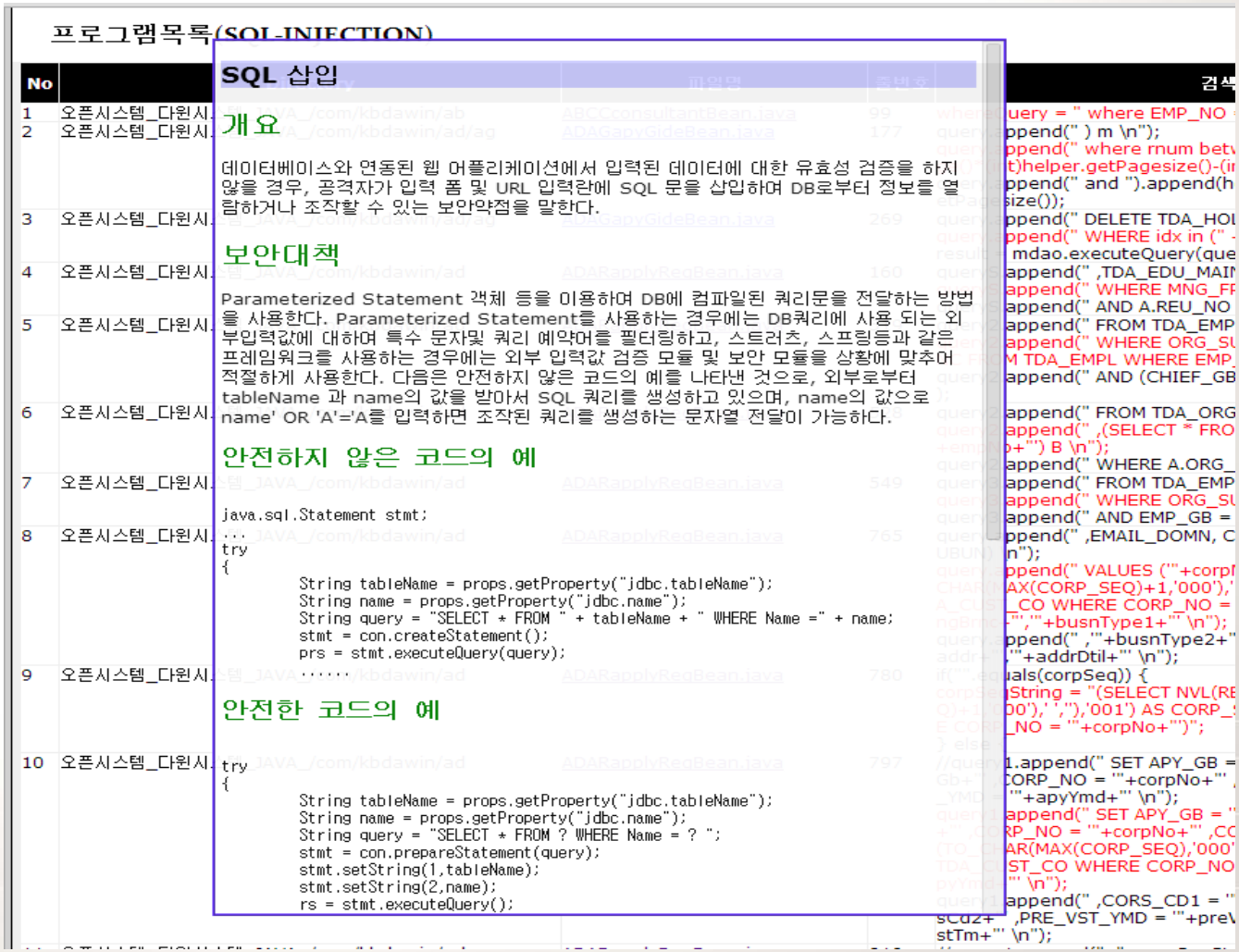
9	오픈시스템_다윈시스템_JAVA_/com/kbdawin/ad	[redacted]	780	if("".equals(corpSeq)) {
				corpSeqString = "(SELECT NVL(REPLACE(TO_CHAR(MAX(CORP_SEQ)+1,'000'),' ','0'),'001') AS CORP_SEQ FROM TDA_EDU_MAIN WHERE CORP_NO = '"+corpNo+"')";
				} else {

10	오픈시스템_다윈시스템_JAVA_/com/kbdawin/ad	[redacted]	797	//query1.append(" SET APY_GB = '"+apyGb+"' ,STAT_GB = '"+statGb+"' ,CORP_NO = '"+corpNo+"' ,CORP_SEQ = '"+corpSeq+"' ,APY_YMD = '"+apyYmd+"' \n");
				query1.append(" SET APY_GB = '"+apyGb+"' ,STAT_GB = '"+statGb+"' ,CORP_NO = '"+corpNo+"' ,CORP_SEQ = (SELECT NVL(REPLACE(TO_CHAR(MAX(CORP_SEQ),'000'),' ','0'),'001') AS CORP_SEQ FROM TDA_CUST_CO WHERE CORP_NO = '"+corpNo+"') ,APY_YMD = '"+apyYmd+"' \n");
				query1.append(" ,CORS_CD1 = '"+corsCd1+"' ,CORS_CD2 = '"+corsCd2+"' ,PRE_VST_YMD = '"+preVstYmd+"' ,PRE_VST_TM = '"+preVstTm+"' \n");

11	오픈시스템_다윈시스템_JAVA_/com/kbdawin/ad	[redacted].java	810	//query1.append(" ,"+corpSeqString+",'"+usrId+"','"+apyUsrNm+"','"+apyYmd+"','"+apyUsrTel+"' \n"); query1.append(" ,(SELECT NVL(REPLACE(TO_CHAR(MAX(CORP_SEQ),'000'),' ','0'),'001') AS CORP_SEQ FROM TDA_CUST_CO WHERE C

주요 기능

- 검색 결과 샘플(시큐어코딩 취약 소스 진단 및 검색)



● 프로그램목록 부분을 클릭하였을때 나타나는 취약점에 대한 설명과 조치방법이다.

회사소개

DawinICT (Dawin Information & Communication Technology)는 IT분야의 각종 시스템 진단 및 컨설팅, 플랫폼 마이그레이션, SI를 주 사업 영역으로 하고 있으며, 특히 플랫폼 마이그레이션 부분의 새로운 솔루션과 서비스의 경쟁력을 제고 시키기 위해 전력을 다하고 있습니다.

회 사 명	㈜다윈아이씨티	대표이사	김 성덕
주 소	135-860 서울시 강남구 대치동 889-5 샹제리제센터 A동 904호		
전화번호	070-4259-8117	e-Mail	sdkim@dawinict.com
종업원수	10명	설립연도	2010년 2월

Thank You