|  |
| --- |
| WEB 보안 취약점 점검 프로그램 개발 |
| 프로젝트 완료보고 |
| EVA Project |

|  |
| --- |
| 2019-8-9  JSL인재개발원 36기 정상훈 |

<문서 변경 내역 기록표>

|  |  |  |  |
| --- | --- | --- | --- |
| 문서버전 | 작성일 | 작성자 | 내용 |
| 1.0 | 2019-08-09 | 정상훈 | 최초 작성 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

목차

[1. 시스템 개요 4](#_Toc16262002)

[1-1 시스템 명칭 : EVA Project (Expandable Vulnerability Assessment) 4](#_Toc16262003)

[1-2 개발 목적 4](#_Toc16262004)

[1-3 개발 환경 4](#_Toc16262005)

[1.4 시스템 기능 4](#_Toc16262006)

[2. 시스템 구성 5](#_Toc16262007)

[3. 시스템 구성도 6](#_Toc16262008)

[3-1 개요 6](#_Toc16262009)

[3-2 클래스 설명 6](#_Toc16262010)

[3-2-1 패키지 : application 6](#_Toc16262011)

[3-2-2 패키지 : core 7](#_Toc16262012)

[3-2-3 패키지 : database 8](#_Toc16262013)

[3-2-4 패키지 : evalution 8](#_Toc16262014)

[3-2-5 패키지 : project 9](#_Toc16262015)

[3-2-6 패키지 : policy 9](#_Toc16262016)

[3-2-7 패키지 : util 9](#_Toc16262017)

[4. UI 및 기능 설명 10](#_Toc16262018)

[4-1 메인 화면 10](#_Toc16262019)

[4-1-1 StartComposite 10](#_Toc16262020)

[4-1-2 SpiderComposite 11](#_Toc16262021)

[4-1-3 SiteTreeViewer 12](#_Toc16262022)

[4-1-4 ReqRespComposite 13](#_Toc16262023)

[4-2 Dialog 14](#_Toc16262024)

[4-2-1 ProjectCreateDialog 14](#_Toc16262025)

[4-2-2 ProjectOpenDialog 14](#_Toc16262026)

[4-2-3 PolicyManagerDialog 15](#_Toc16262027)

[4-2-4 Help / Contact Dialog 15](#_Toc16262028)

[4-2-5 ReferenceDialog 16](#_Toc16262029)

[4-2-6 ConfigDialog 16](#_Toc16262030)

[5. 탐지 기준 정의 18](#_Toc16262031)

[5-1 카테고리 18](#_Toc16262032)

[5-2 공격명 상세 19](#_Toc16262033)

[6. 데이터베이스 설정 20](#_Toc16262034)

[6.1 접속 정보 20](#_Toc16262035)

[6-2 테이블 구성 20](#_Toc16262036)

[7. 탐지 패턴 추가 적용 방법 22](#_Toc16262037)

[7-1 클래스 생성 방법 22](#_Toc16262038)

[7-2 작성 예 23](#_Toc16262039)

[8. 배포 23](#_Toc16262040)

[8-1 형상관리 23](#_Toc16262041)

[[별첨] 참고 문서 24](#_Toc16262042)

# 1. 시스템 개요

## 1-1 시스템 명칭 : EVA Project (Expandable Vulnerability Assessment)

## 1-2 개발 목적

- 안전한 웹 서비스를 위하여 해킹위협이 될 수 있는 보안 취약점의 존재 여부를 점검할 수   
있도록 프로그램을 제작하고자 함

- 어플리케이션에서 개발 후 WEB이나 IDE 등 다양한 플랫폼에서 사용할 수 있도록 라이브러리화

- 독립형 어플리케이션 개발 후 Web-Base 로 업그레이드

- 공격 패턴의 지속적인 연구 및 테스트를 통해 확장할 수 있는 환경 제공

## 1-3 개발 환경

|  |  |  |  |
| --- | --- | --- | --- |
| **구분** | **내용** | **버전** | **비고** |
| 개발 도구 | Eclipse IDE | 4.12.0 |  |
| 개발 언어 | Java | 1.8.0\_211 |  |
| 데이터베이스 | Oracle XE | 18c |  |
| 사용 라이브러리 | SWT/JFace |  | UI |
| jsoup | 1.12 | HTML Parse |
| apache http client | 4.5 | http util |
| maven | 3.8.0 | Library version online management |

## 1.4 시스템 기능

- 웹 페이지 크롤링 : 점검 대상 사이트에 존재하는 링크들을 찾아내어 취약점 스캐닝을 수행할

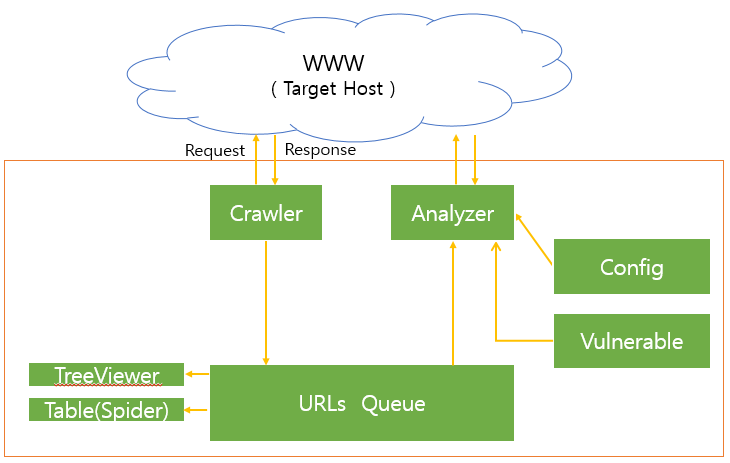
웹 페이들을 찾아서 리스트업 한다.

- 웹 취약점 스캐닝 : 어떠한 웹 취약점을 점검할 것인지 선택하여 Policy 를 지정 한 후

크롤링 결과 페이지들에 대해 스캐닝을 하여 취약점 여부를 판단한다

# 3. 시스템 구성도

## 3-1 개요



크롤링한 결과가 URL Queue 에 저장되고 Analyzer 는 스레드로 대기중 상태에서

URL Queue 에 정보가 들어오게 되면 기본설정을 Config 로, 세부 공격은 Vulnerable 인터페이스의

구현체로 HTTP 통신 및 스캐닝을 수행한다. 결과는 Table 에 표시한다.

## 3-1 패키지 구성

|  |  |
| --- | --- |
| **패키지** | **설명** |
| berry.eva.application | 화면에 보여지는 Viewr, UI |
| berry.eva.core | 메인이 되는 검색 엔진 기능 |
| berry.eva.database | 데이터 베이스를 접근하는 클래스 및 DAO 로 구성 |
| berry.eva.evalution | 취약점 정의 및 분석을 위한 클래스로 구성 |
| berry.eva.project | 점검대상 site 를 관리하기 위한 Project 로 구별하기 위함 |
| berry.eva.policy | 해당 Project 별 점검 정책 관리를 위함 |
| berry.eva.util | 그 외 텍스트 변환 등의 Util 클래스로 구성 |

## 3-2 클래스 설명

### 3-2-1 패키지 : application

|  |  |
| --- | --- |
| **클래스** | **설명** |
| MainApplication | JFace 의 ApplicationWindow 을 상속하여 구현한 클래스이다.  프로그램의 메인 클래스스이다 메뉴, Table, Composite 등을 멤버로 가지고 있다. |
| ApplicationLauncher | MainApplication 을 구동하기 위한 Launcher 클래스 이다.  MainApplication 이 메모리에 올라가는 동안 SplashWindow 가  5초간 화면에 보여지게 되어 있다 |
| ConfigDialog | JFace 의 TitleAreaDialog 를 상속받아 구현한 클래스이다.  HTTP Request Header 값을 설정할 수 있다. |
| HelpDialog | JFace 의 TitleAreaDialog 를 상속받아 구현한 클래스이다.  프로그램의 버전, 개발자 연락처 정보를 팝업으로 보여준다 |
| PolicyManagerDialog | JFace 의 TitleAreaDialog 를 상속받아 구현한 클래스이다.  취약점 검사를 위한 규칙을 관리하기 위한 클래스이다. |
| ProjectCreateDialog | JFace 의 TitleAreaDialog 를 상속받아 구현한 클래스이다.  사이트 Project 를 생성하기 위한 Dialog 이다 |
| ProjectOpenDialog | JFace 의 TitleAreaDialog 를 상속받아 구현한 클래스이다.  이전에 생성된 Project 를 선택 및 열기 위한 Dialog 이다. |
| ReferenceDialog | 보안 취약점 관련 각종 레퍼런스 링크를 보여주기 위한 Dialog 이다 |
| R | 리소스 관리를 위한 클래스이며 프로그램의 상수를 정의 한다. |
| ReqRespComposite | SWT 의 Composite 를 상속받아 구현한 클래시이다.  취약점 검사 이후 HTTP Response 및 Request 정보를 보여주기 위한  Composite (컨테이너) 이다 |
| SpiderComposite | 검사 대상 웹 페이지의 a 링크를 찾은 결과를 Table 로 보여주기 위한 컨테이너 이다 |
| SiteNode | JFace 의 TableViewer 를 구현하기 위한 클래스 이다  경로가 도메인인지, 디렉토리인지, 파일인지 구별한다 |
| SiteNodeManager | SiteNode 를 관리하기 위한 클래스 이다. |
| SiteTreeContentProvider | JFace 의 TableViewer 를 구현하기 위한 클래스 이다  ITreeContentProvider 를 구현하였다 |
| SiteTreeLabelProvider | SiteNode 의 종류(도메인,디렉토리,파일) 에 따라 각각 별도의 이미지를 리턴한다 |
| ScanComposite | 상기한 SpiderComposite 에서 찾은 사이트 링크들을 각각  점검한 결과를 Table 로 보여주기 위한 컨테이너 이다 |
| StartComposite | 최초 검사 대상이 되는 사이트 주소를 입력받기 위한 컨테이너 이다 |
| SplashWindow | MainApplication 이 구동되기 전에 임시로 보여주기 위한  SplashWindow 이다 |

### 3-2-2 패키지 : core

|  |  |
| --- | --- |
| **클래스** | **설명** |
| Config | HTTP Request 시 필요한 데이터를 담을 수 있다.  멤버필드로 userAgent, pragma, cache-control, cookie 가 있다 |
| Context | 검사 결과 정보를 담을 수 있는 클래스이다.  ID, URL, http method, 시간, cwe\_id 등을 담을 수 있으며  Table 을 통해서 보여줄 때 사용 된다 |
| ContextManager | Context 클래스를 관리하기 위한 클래스이다  SingleTone 으로 되어 있으며 HashMap 클래스를 Wrap 하는 형태로  구현되어 있다 |
| Crawler | java.lang.Runnable 인터페이스의 구현체이다.  주요 메소드로 getPageLinks 를 통하여 재귀적으로 HTML 의 a  태그를 찾는다. |
| SearchEngine | StartComposite 에서 입력받은 사이트 주소를 대상으로 삼으며  Cralwer 스레드를 실행시킬 수 있다 |
| Status | 검사 스레드 종료를 위한 상태값을 저장한다.  Searching 값에 ON 또는 OFF 를 설정해 놓는다. |
| URLQueue | Crawler 에서 새로운 웹페이지 발견시 URLQueue 으로 저장 시킨다  SigleTon 이며 LinkedList 클래스의 Wrap 구조로 되어있다. |
| Validator | isinScope 함수를 통해서 검사대상의 Scope 가 관련 없는 사이트로  접근하지 않도록 한다. |

### 3-2-3 패키지 : database

|  |  |
| --- | --- |
| **클래스** | **설명** |
| CrudManager | 데이터 베이스에 접근, 조회 및 저장하기 위한 클래스 이다 |
| DAO\_policy | Policy 객체의 DAO 클래스이다 |
| DAO\_project | Project 객체의 DAO 클래스이다 |
| DAO\_vulns\_insert | Vulns 정보의 DAO 클래스 이다 |

### 3-2-4 패키지 : evalution

|  |  |
| --- | --- |
| **클래스** | **설명** |
| Analyzer | java.lang.Runnable 인터페이스의 구현체이다.  주요 메소드로 startScan 이 있다.  URLQueue 에서 URL 을 빼면서 Vulnerable 한지를 분석하며  그 결과를 Table 에 보여준다 |
| Category | 웹 공격 종류 10가지를 정의한 enum 이다. |
| Result | 취약 여부를 판단한 결과값을 저장할 수 있는 클래스이다  기본값으로 CWE\_ID 에 “NotFound” 를 가지며 취약하다고 판단될 시 고유의 CWE\_ID 를 지정한다 |
| Vulnerable (인터페이스) | 이 인터페이스는 execute 메소드를 실행하고 Context 를 반환한다  관련 클래스로는 AbstractScan 추상화 클래스가 있다. |
| Weakness | 취약점 개별에 대한 Category 와 CWE\_ID, 공격이름, 공격에 대한 세부 정보를 담을 수 있는 클래스 이다. |
| WeaknessEnumeration | 상기의 Weakness 클래스를 HashMap 으로 담아서 관리하기 위한 클래스 이다. |

### 3-2-5 패키지 : project

|  |  |
| --- | --- |
| **클래스** | **설명** |
| Project | 프로젝트, 생성시간, Policy 리스트를 멤버로 가지는 클래스이다 |
| ProjectManager | Project 클래스를 리스트로 관리하기 위한 클래스이다.  CRUD 클래스를 통하여 데이터 베이스에 저장할 수 있다 |

### 3-2-6 패키지 : policy

|  |  |
| --- | --- |
| **클래스** | **설명** |
| Policy | 어느 취약점을 이번 대상에 포함시킬 것인지를 정하고 이름을 정의한다. Vulnerable 인터페이스를 리스트로 관리한다. |
| PolicyManager | Policy 클래스를 관리하기 위한 클래스이며  CRUD 클래스를 통하여 데이터베이스에 저장할 수 있다 |

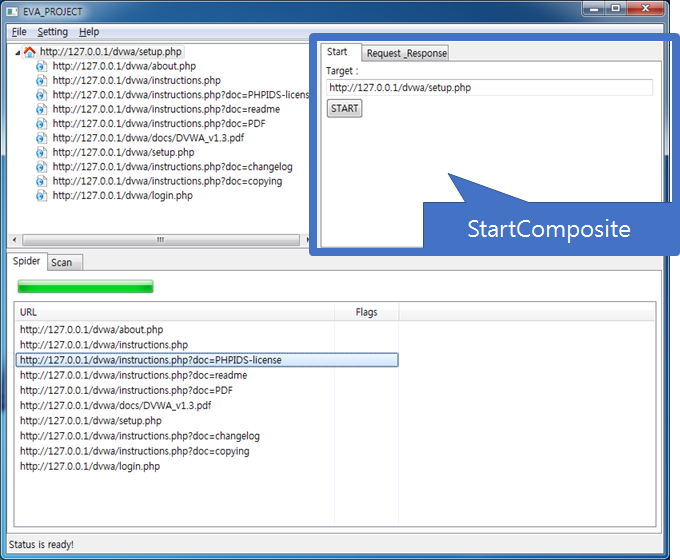
### 3-2-7 패키지 : util

|  |  |
| --- | --- |
| **클래스** | **설명** |
| TextConverter | boolean type 를 UI 에 보여주기 용이하게끔 변환해 주는 클래스이다 |

# 4. UI 및 기능 설명

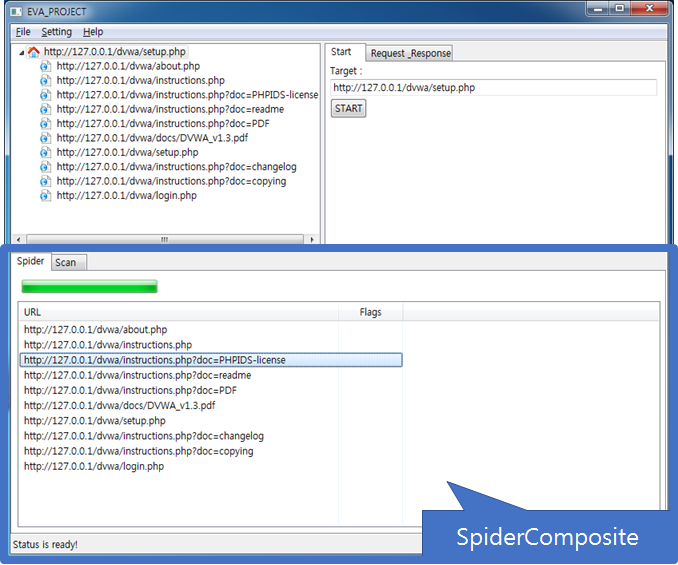
## 4-1 메인 화면

### 4-1-1 StartComposite



점검 대상 사이트 웹페이지주소를 입력하고 Start 버튼을 클릭한다

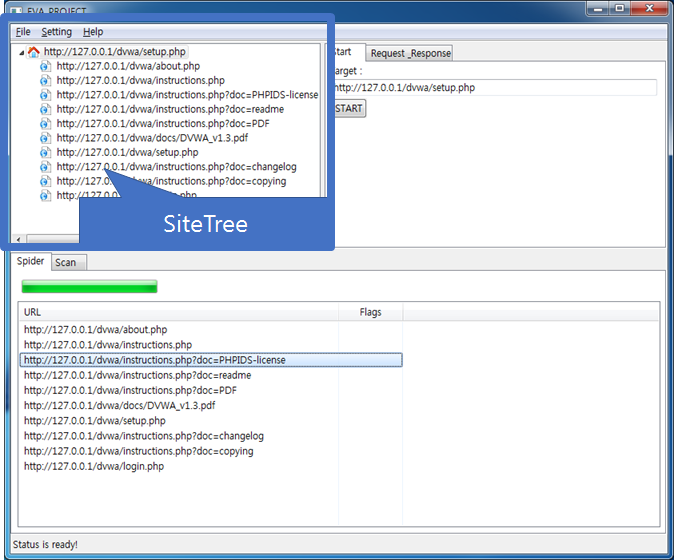
### 4-1-2 SpiderComposite



SearchEngine 이 크롤링한 결과를 SpiderComposite 내의 Table 에 표시해 주면서

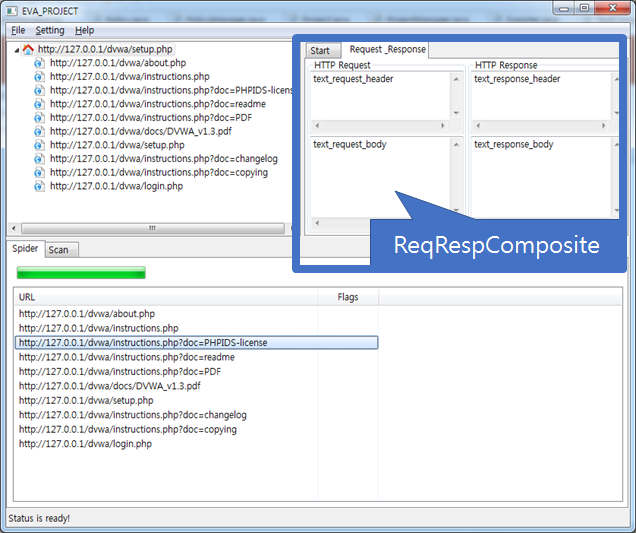
TreeViewer 에도 같이 표시해 준다

### 4-1-3 SiteTreeViewer



크롤링 결과를 Tree 에 표시해 준다.

### 4-1-4 ReqRespComposite

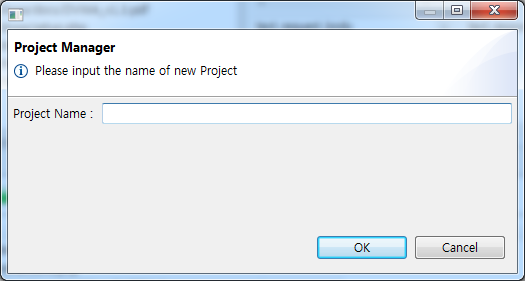


각 HTTP Request 와 Response 를 표시해 주는 부분이다.

이벤트는 하단의 Table 의 Item 을 클릭 할 때 마다 ReqRespComposite 에 변경하여 표시해 준다

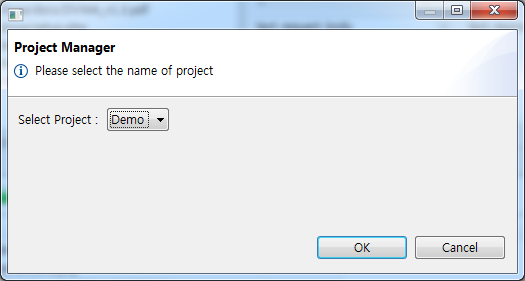
## 4-2 Dialog

### 4-2-1 ProjectCreateDialog



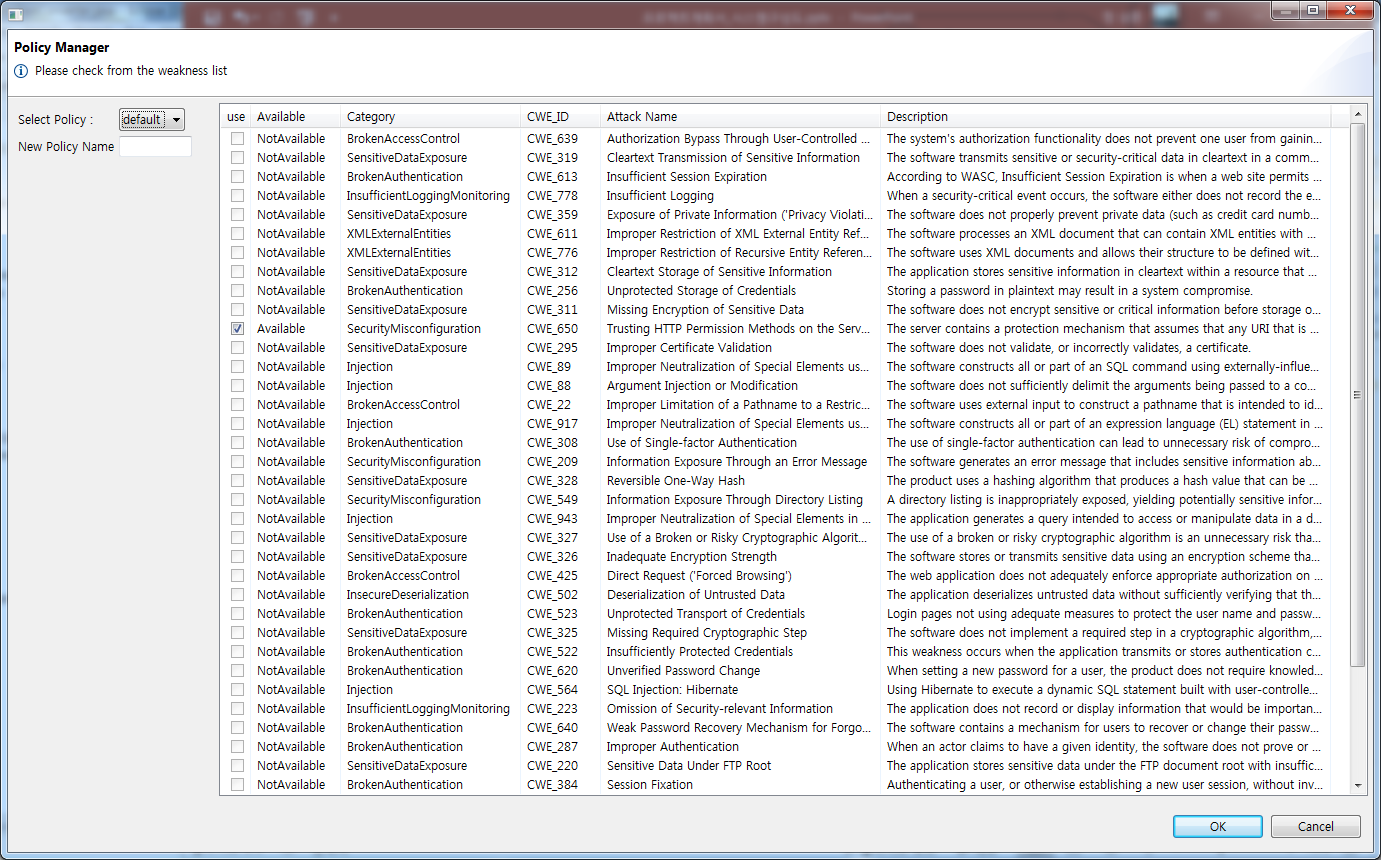
새로 생성하고 싶은 프로젝트 이름을 입력받는 다이얼로그 이다.

### 4-2-2 ProjectOpenDialog



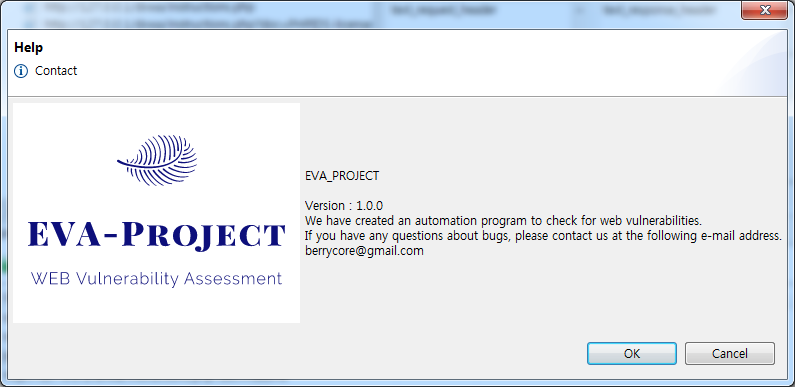
이전에 생성 되었던 프로젝트 이름을 표시해주며 콤보박스를 통해서 프로젝트를 선택할 수 있다

### 4-2-3 PolicyManagerDialog



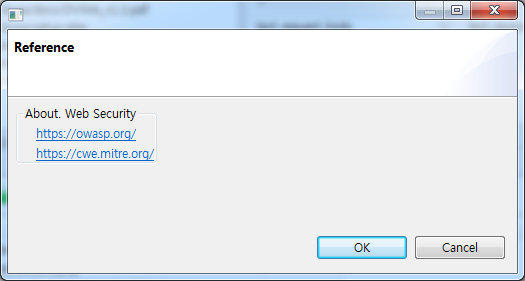
Project 에 각각 생성한 Policy 별로 탐지 여부를 체크하여 저장하는 다이얼 로그 이다.

### 4-2-4 Help / Contact Dialog



프로그램의 버전정보와 개발자 연락처를 표시하는 Dialog 이다

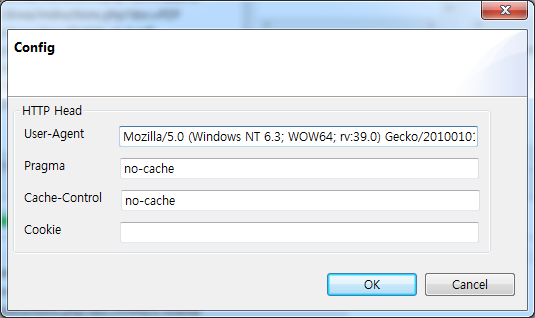
### 4-2-5 ReferenceDialog



보안 취약점에 대한 외부 링크정보 이다. 항목을 클릭하게 되면 웹브라우저가 실행되며

링크로 연결된다.

### 4-2-6 ConfigDialog



HTTP 요청 헤더의 정보를 저장하거나 불러올 수 있는 Dialog 이다

# 5. 탐지 기준 정의

## 5-1 카테고리

|  |  |
| --- | --- |
| **Category** | |
| A1 | Injection  *인젝션* |
| A2 | Broken Authentication  *취약한 인증* |
| A3 | Sensitive Data Exposure  *민감한 데이터 노출* |
| A4 | XML External Entities(XXE)  *XML 외부 개체 참조* |
| A5 | Broken Access Control  *취약한 접근 통제* |
| A6 | Security Misconfiguration  *잘못된 보안 구성* |
| A7 | Cross-Site Scripting(XSS)  *크로스 사이트 스크립팅* |
| A8 | Insecure Deserialization  *안전하지 않은 역직렬화* |
| A9 | Using Components with Known Vulnerabilities  *알려진 취약점이 있는 구성요소 사용* |
| A10 | Insufficient Logging & Monitoring  *불충분한 로깅 및 모니터링* |

- 다양한 웹 공격 유형 중 OWASP TOP-10[[1]](#footnote-2) (버전:2017년)를 기준으로 하여 공격 패턴 작성

## 5-2 공격명 상세

|  |  |
| --- | --- |
| CWE-ID | Name |
| 22 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') |
| 77 | Improper Neutralization of Special Elements used in a Command ('Command Injection') |
| 78 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') |
| 79 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') |
| 88 | Argument Injection or Modification |
| 89 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') |
| 90 | Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') |
| 91 | XML Injection (aka Blind XPath Injection) |
| 209 | Information Exposure Through an Error Message |
| 220 | Sensitive Data Under FTP Root |
| 223 | Omission of Security-relevant Information |
| 256 | Unprotected Storage of Credentials |
| 284 | Improper Access Control |
| 285 | Improper Authorization |
| 287 | Improper Authentication |
| 295 | Improper Certificate Validation |
| 308 | Use of Single-factor Authentication |
| 311 | Missing Encryption of Sensitive Data |
| 312 | Cleartext Storage of Sensitive Information |
| 319 | Cleartext Transmission of Sensitive Information |
| 325 | Missing Required Cryptographic Step |
| 326 | Inadequate Encryption Strength |
| 327 | Use of a Broken or Risky Cryptographic Algorithm |
| 328 | Reversible One-Way Hash |
| 359 | Exposure of Private Information ('Privacy Violation') |
| 384 | Session Fixation |
| 425 | Direct Request ('Forced Browsing') |
| 502 | Deserialization of Untrusted Data |
| 522 | Insufficiently Protected Credentials |
| 523 | Unprotected Transport of Credentials |
| 548 | Information Exposure Through Directory Listing |
| 564 | SQL Injection: Hibernate |
| 611 | Improper Restriction of XML External Entity Reference |
| 613 | Insufficient Session Expiration |
| 620 | Unverified Password Change |
| 639 | Authorization Bypass Through User-Controlled Key |
| 640 | Weak Password Recovery Mechanism for Forgotten Password |
| 776 | Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion') |
| 778 | Insufficient Logging |
| 917 | Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') |
| 943 | Improper Neutralization of Special Elements in Data Query Logic |

# 6. 데이터베이스 설정

## 6.1 접속 정보

- 데이터베이스 접근가능한 서비스 계정명은 evaproject 로 한다,

- 테이블의 권한은 select, update, insert, delete 로 제한한다

## 6-2 테이블 구성

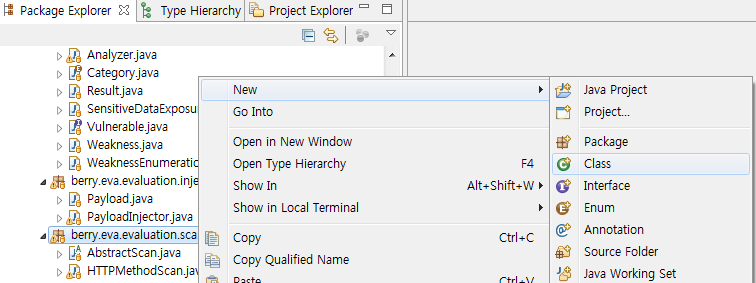
|  |  |  |
| --- | --- | --- |
| 테이블 : **EVA\_PROJECT** | | |
| PROJECTNAME | VARCHAR(50) | **PRIMARY\_KEY** |
| CREATEDTIME | VARCHAR(50) |  |

|  |  |  |
| --- | --- | --- |
| 테이블 : **EVA\_POLICY**S | | |
| PROJECTNAME | VARCHAR(50) | **FOREIGN\_KEY** |
| POLICYNAME | VARCHAR(50) |  |
| CREATEDTIME | VARCHAR(50) |  |

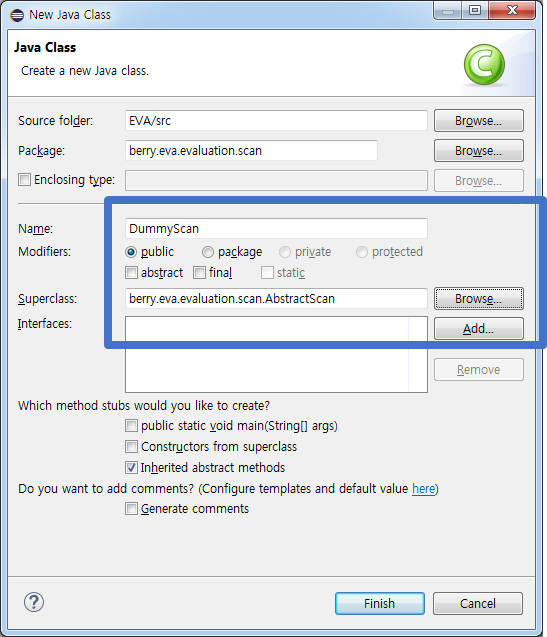
|  |  |  |
| --- | --- | --- |
| 테이블 : **EVA\_VULNS** | | |
| projectname | VARCHAR2(50) | **POREIGN\_KEY** |
| policyname | VARCHAR2(50) |  |
| cwe\_id | VARCHAR2(50) |  |
| cwe\_enable | NUMBER(1) |  |

# 7. 탐지 패턴 추가 적용 방법

## 7-1 클래스 생성 방법

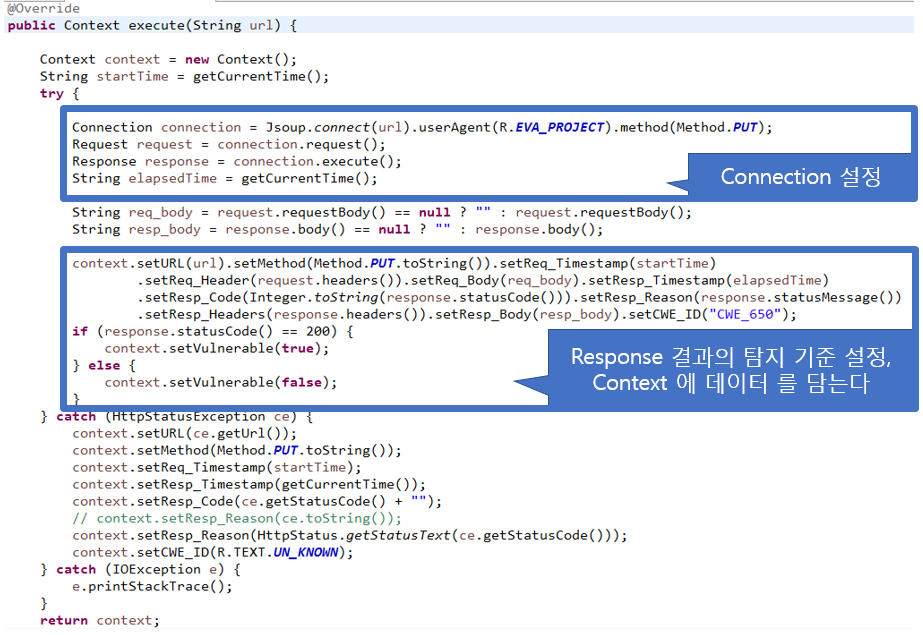


위치 : berry.eva.evalution.scan 패키지에서 새 클래스 생성하기



부모클래스로 AbstractScan 추상클래스를 지정한다

## 7-2 작성 예

****

# 8. 배포

## 8-1 형상관리

<https://github.com/berrycore/EVA-Project>

권한은 현재 public 으로 되어있으며 어플리케이션 개발 및 패턴 연구가 가능하다.

라이선스 여부 : EPL (Eclipse Public License) 오픈 소스 소프트웨어

# [별첨] 참고 문서

- RFC 2616 (HTTP/1.1) : <https://www.w3.org/Protocols/rfc2616/rfc2616.html>

- OWASP : <https://www.owasp.org/index.php/Main_Page>

- exploit-db : <https://www.exploit-db.com/>

- Web crawler : <https://en.wikipedia.org/wiki/Web_crawler>

- SWT : <https://www.eclipse.org/swt/>

- XML Parsing : <https://docs.oracle.com/javase/7/docs/api/javax/xml/crypto/dsig/Reference.html>

-시큐어코딩가이드 :

<https://mois.go.kr/frt/bbs/type001/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000015&nttId=39994>

1. OWASP : The Open Web Application Security Project 는 오픈소스 웹 어플리케이션 보안 프로젝트이다. 주로 웹에 관한 정보노출, 악성파일 및 스크립트, 보안 취약점 등을 연구하며 3~4년에 1회씩 10대 웹 어플리케이션의 취약점 (OWASP TOP 10) 을 발표한다 [↑](#footnote-ref-2)