[정보보호] 사이버 보안 정보의 배포 및 교환을 위한 CYBEX 표준화 추진 현황

최근 들어, 사이버 위협이 점차 증가되고 있는 바, 사이버 보안에 관련된 기술적 세부 정보를 활용해야만 그 위험 평가가 가능하다. 이에, 연관된 세부 정보들을 유관 기관들 간에 서로 교환하기 위한 지식 기반 표준인 CYBEX가 필요하며, 이에 대한 표준화가 ITU-T SG 17에서 진행되고 있다. (*주, CYBEX : CYBersecurity information dissemination and Exchange)

1. CYBEX 표준화 추진 현황

CYBEX의 주요 표준화 대상 분야 및 추진 내용은 다음과 같다.

1) 공통 취약성 목록(CVE : Common Vulnerability Enumeration) 표준화

이는 사이버 보안 취약성 및 노출 관련 정보를 교환하는 구조적 수단으로 공개적으로 알려진 문제점들에 대한 공통 식별자를 제공하며, ITU-T X.1520 권고안으로 표준화 되었다. 이에 관련하여 미국 및 일본에서 구축된 데이터 베이스로는 미국의 NIST NVD, 일본의 JVN이 있다.

데이터 보호를 위해 널리 사용되는 소프트웨어에 대한 취약성의 예는 다음과 같다.

- MySQL에 대한 CVE 기재 항목 :

Search Results

There are **437** CVE entries that match your search.

Name	Description
CVE-2014-5104	Multiple SQL injection vulnerabilities in ol-commerce 2.1.1 allow remote attackers to execute arbitrary SQL commands via the (1) a_country parameter in a process action to affiliate_signup.php, (2) affiliate_banner_id parameter to affiliate_show_banner.php, (3) country parameter in a process action to create_account.php, or (4) entry_country_id parameter in an edit action to admin/create_account.php.
CVE-2014-4987	server_user_groups.php in phpMyAdmin 4.1.x before 4.1.14.2 and 4.2.x before 4.2.6 allows remote authenticated users to bypass intended access restrictions and read the MySQL user list via a viewUsers request.
CVE-2014-4260	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.37 and earlier, and 5.6.17 and earlier, allows remote authenticated users to affect integrity and availability via vectors related to SRCHAR.

2) 공통 약점 목록(CWE : Common Weakness Enumeration) 표준화

동일한 종류의 취약성 그룹을 약점이라 하고, 이에 번호를 부여한다. 상용 및 공개 소프트웨어 내의 공개적으로 알려진 문제점들에 대해 공통 명칭을 부여하며, 이는 소스 코드 및 운용 시스템내의 취약성을 찾는 보안 도구 및 서비스를 위한 것이다. 이는 또한 구조 및 설계와 연관된 소프트웨어 취약성을 이해하고 관리하는 데 도움을 주며, ITU-T X.1524 권고안으로 표준화 되었다.

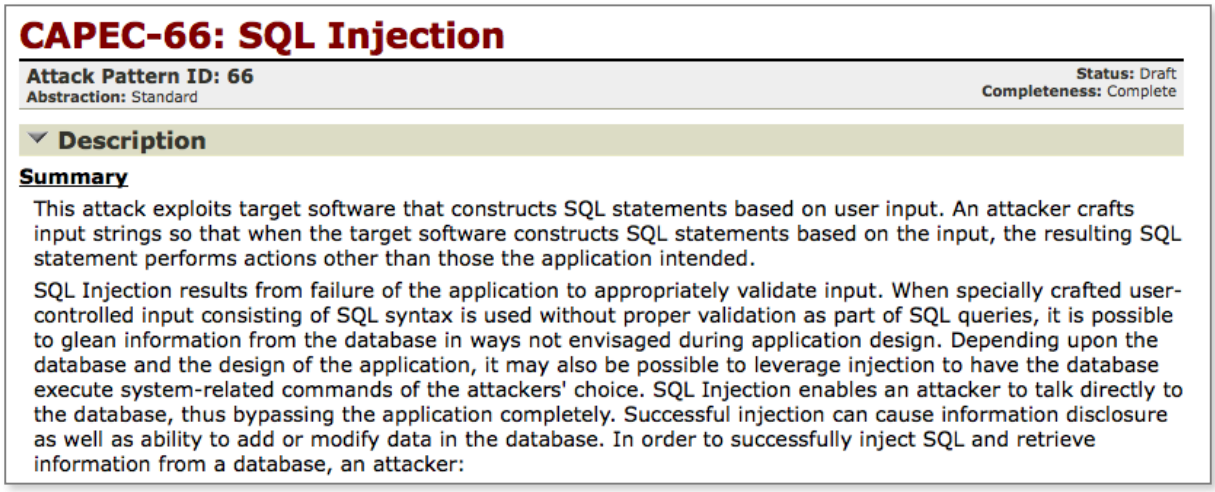
3) 공통 취약성 점수 시스템(CVSS : Common Vulnerability Scoring System) 표준화

취약성에 대한 정량화는 취약성 관리 시점에 우선순위 매김을 용이하게 한다. CVSS는 이용자 환경에 걸친 기반적, 시간적, 환경적 측정기준으로써, ITU-T X.1521 권고안으로 표준화 되었다.

4) 공통 공격 형태 목록 및 등급(CAPEC : Common Attack Pattern Enumeration and classification) 표준화

CAPEC은 공격 패턴, 해결책 및 경감 방법들에 관련된 사전으로써, 사건 및 이슈 뿐만 아니라 검증 방법 및 경감 전략들의 교신을 용이하게 하며, ITU-T X.1544 권고안으로 표준화 되었다.

CAPEC의 예는 다음과 같다.



CAPEC-66: SQL Injection

Attack Pattern ID: 66
Abstraction: Standard

Status: Draft
Completeness: Complete

Description

Summary

This attack exploits target software that constructs SQL statements based on user input. An attacker crafts input strings so that when the target software constructs SQL statements based on the input, the resulting SQL statement performs actions other than those the application intended.

SQL Injection results from failure of the application to appropriately validate input. When specially crafted user-controlled input consisting of SQL syntax is used without proper validation as part of SQL queries, it is possible to glean information from the database in ways not envisaged during application design. Depending upon the database and the design of the application, it may also be possible to leverage injection to have the database execute system-related commands of the attackers' choice. SQL Injection enables an attacker to talk directly to the database, thus bypassing the application completely. Successful injection can cause information disclosure as well as ability to add or modify data in the database. In order to successfully inject SQL and retrieve information from a database, an attacker:

5) OVAL 관련 표준화 및 적용 예

OVAL은 취약성에 대한 공개적 정의 및 시스템 상태를 평가하기 위한 언어로써, 컴퓨터 시스템의 머신 상태를 평가/보고하는 표준이다. OVAL은 시스템 명세를 인코딩하는 언어와 어떤 집단에 대한 내용물 저장소들의 분류를 포함하며, ITU-T X.1526 권고안으로 표준화되었다.

2. CYBEX의 활용 예

CYBEX의 활용 예는 다음과 같다. 사이버 보안 관련 국가 협력 센터는 공공 경보를 위하여 취약점 정보 식별자 및 점수 표준을 활용한다. 사고 대응팀은 CYBEX에 의해 예측되는 일련의 명료한 식별자를 통해 취약성과 공격 패턴을 추적한다. 시스템 관리자는 CYBEX를 채용하는 소프트웨어 도구를 이용하여 취약성의 존재를 평가한다. 크라우드 및 네트워크 서비스 제공자는 표준화된 점수 시스템을 이용하여, 그들의 인프라에 미치는 영향에 따라 우선순위를 매긴다. 임베디드 및 IoT 장비 개발자는 CYBEX의 일부인 공공 지식베이스를 통하여 소프트웨어 취약성에 대한 대표적 패턴을 파악한다. 취약성 연구자는 공통 취약성 식별자를 통하여, 상호 연결되고 통합되는 취약성에 대한 지식 기반을 총괄적으로 유지한다.

3. 결론

ITU-T 사이버 보안 표준들은 데이터 보호에 직접 기여하며, 급격히 변하고 다변화되는 사이버 보안 환경을 다루는 중요한 도구이다. 또한, 목록 표준들은 어느 단체, 사업체 및 정부 기관에 있어 효율적 소통 수단을 제공한다. 사이버 위험은 매우 불안정하며, 각종 인자들이 예기치 못한 조합을 통해 나타나므로, 지식기반 표준을 통해 기술적 위험을 주의 깊게 관찰하고 감소시켜야 할 것이다.

진병문(순천향대학교 초빙교수, bmchin@tta.or.kr)