

10장 프로그래밍 언어 활용

용어	설명
헝가리안 표기법	변수명 작성 시 변수의 자료형을 알 수 있도록 자료형을 의미하는 문자를 포함하여 작성하는 방법
%o	8진수
%x	16진수
Int j = 011	8진수로 11인 값이 저장 됨
Int j = 0x11	16진수로 11인 값이 저장 됨
스크립트 언어	Html 안에 프로그래밍 언어를 삽입하여 사용하는 언어
서버용 스크립트	서버에서 해석됨. ASP, JSP, PHP, Python
클라이언트용 스크립트	클라이언트에서 해석됨. JavaScript, VB 스크립트 (Visual Basic)
자바 스크립트	클래스가 존재하지 않으며 변수 선언도 필요 없음
VB 스크립트	마이크로소프트 사에서 자바 스크립트에 대응하기 위해 제작한 언어. Active X를 사용하여 마이크로 소프트 사의 애플리케이션들을 컨트롤 가능
ASP (Active Server Page)	서버 측에서 동적으로 수행하는 페이지를 만들기 위한 언어. 마이크로소프트 사에서 제작.
JSP (Java Server Page)	JAVA로 만들어진 서버용 스크립트 언어
PHP (Professional Hypertext Preprocessor)	리눅스, 유닉스, 윈도우 os에서 사용 가능. C, java와 문법 유사
파이썬	객체지향 기능을 지원하는 인터프리터 언어. 플랫폼 독립적, 문법이 간단하여 배우기 쉬움
셸 스크립트	유닉스/리눅스 계열의 셸에서 사용되는 명령어들의 조합으로 구성된 스크립트 언어
Basic	절차지향 기능을 지원하는 대화형 인터프리터 언어
선언형 언어	프로그램이 수행해야 할 문제를 기술하는 언어. 목표 명시, 알고리즘은 명시하지 않음 (ex. Html, xml, prolog, xml, haskell)
- 함수형 언어	수학적 함수를 조합하여 문제를 해결하는 언어. LISP
- 논리형 언어	기호 논리학에 기반을 둔 언어. PROLOG

용어	설명
명령형 언어	<ol style="list-style-type: none"> 1. 문제를 해결하기 위한 방법을 기술하는 언어. 2. 일반적으로 알고 있는 프로그래밍 언어라고 생각하면 된다. 3. 순차 명령 수행을 기본으로 하며 폰노이만 구조를 기념적인 기초로 두고 있다. 4. 절차지향 언어와 객체지향 언어로 나뉜다. 5. ex. COBOL, FORTRAN, C, JAVA ...
객체지향 프로그래밍	현실 세계의 개체를 하나의 객체로 만들어 객체들을 조립하듯이 개발하는 것
라이브러리	<p>자주 사용하는 함수나 데이터들을 미리 만들어 모아 놓은 집합체</p> <ul style="list-style-type: none"> - 표준 라이브러리 : 기본적으로 포함되어 있는 라이브러리 - 외부 라이브러리 : 개발자들이 인터넷에 공유해 놓은 라이브러리
XOR 계산법	$1 \text{ XOR } 0 = 1$ $0 \text{ XOR } 1 = 1$ $1 \text{ XOR } 1 = 0$ $0 \text{ XOR } 0 = 0$
Byte a = 15; Byte b = ~a;	<p>1 byte = 8bit => 8bit로 표기해야 한다.</p> <p>15 => 0000 1111 ~15 => 1111 0000</p> <p>첫번째 비트는 부호 비트이므로 10진수 값을 알으려면 2의보수 값을 구해야 함. 2의 보수는 1의보수 + 1이다. 1의 보수는 전체 비트를 반전하는 것이므로 0000 1111이 되며 여기에 +1을 하면 0001 0000이 됨.</p> <p>~15의 부호는 음수(1)이므로 0001 0000에 음수를 붙여주면 된다. 그러므로 b = -16</p>

8장 SQL응용

용어	설명
	2

용어	설명
묵시적 커서	DBMS에 의해 내부에서 자동으로 생성되어 사용하는 커서. 속성 : SQL%FOUND, SQL%NOTFOUND, SQL%ROWCOUNT, SQL%ISOPEN
명시적 커서	사용자가 직접 정의해서 사용하는 커서. Open -> Fetch -> Close 순으로 이뤄짐
웹 응용 시스템	웹서버와 웹 애플리케이션 서버로 구성됨, 웹서버와 웹 애플리케이션 서버를 합쳐도 됨, dbms로 부터 데이터를 얻기 위해선 이것을 거쳐야 함
JDBC	Java 언어로 다양한 종류의 db에 접속할 때 사용하는 표준 API
ODBC	개발 언어에 관계 없이 데이터베이스에 접근하기 위한 표준 개방형 API
MyBatis	JDBC 코드를 단순화하여 사용할 수 있는 SQL Mapping 기반 오픈 소스 접속 프레임워크
RANK	중복값 동일 순위, 다음 순서는 중복값 개수 만큼 건너뛰고 순위 매김
DENSE_RANK	중복값 동일 순위, 다음 순서는 순차 순위 매김
ROW_NUMBER	중복 관계 없이 순차 순위 매김
동적 SQL	다양한 조건에 따라 SQL 구문을 동적으로 변경하여 처리할 수 있는 SQL 처리 방식
단문 SQL 테스트	DDL : DESCRIBE(DESC) 명령어 이용, DML : SELECT 명령어 이용, DCL : 권한 정보가 저장된 테이블 조회
절차형 SQL 테스트	디버깅을 통해 적합성 여부 검증, SHOW ERRORS; 명령어를 통해 에러 내용 확인 가능
ORM	객체와 관계형 데이터베이스의 데이터를 연결하는 기술
- JAVA	JPA, Hibernate, EclipseLink, DataNucleus, EBean
- C++	ODB, QxOrm
- Python	Django, SQLAlchemy, Storm
- .NET	NHibernate, DatabaseObjects, Dapper
- PHP	Doctrine, Propel, RedBean
옵티마이저	작성된 SQL이 가장 효율적으로 수행되도록 최적의 경로를 찾아주는 모듈
- RBO	Rule Based Optimizer, 데이터베이스 관리자가 사전에 정의해둔 규칙에 의거하여 경로를 찾는 규칙 기반 옵티마이저
- CBO	Cost Based Optimizer, CPU 사용량/블록 개수/튜플 개수 등을 종합하여 산출되는 비용으로 최적의 경로를 찾는 옵티마이저

9장 소프트웨어 개발 보안 구축

용어	설명
Secure SDLC	SDLC (소프트웨어 개발 과정을 단계별로 나눈 것)에 보안 강화를 위한 프로세스를 포함한 것
- CLASP	SDLC의 초기 단계에서 보안을 강화하기 위해 개발된 방법론
- SDL	마이크로소프트 사에서 안전한 소프트웨어 개발을 위해 기존의 SDLC를 개선한 것
- Seven Touchpoints	소프트웨어 보안의 모범사례를 SDLC에 통합한 방법론
소프트웨어 개발 보안 요소	
- 기밀성	시스템 자원은 인가된 사용자만 접근 할 수 있음
- 무결성	시스템 자원은 인가된 사용자만 수정 할 수 있음
- 가용성	인가된 사용자는 언제든지 시스템 자원에 접근할 수 있어야 함
- 인증	시스템 정보를 사용하려는 사용자가 인가된 사용자인지를 확인하는 행위
- 부인 방지	데이터를 송/수신한 사용자가 송/수신한 사실을 부인할 수 없도록 증거를 제공함
세션 통제	세션 연결, 연결로 인해 발생하는 정보를 통제하는 것
- 불충분한 세션 관리	세션 id가 너무 규칙적이거나, time out이 너무 길면 발생하는 세션 통제의 보안 약점
- 잘못된 세션에 의한 정보 노출	다중 스레드 환경에서 멤버 변수에 정보를 저장할 때 발생하는 보안 약점
입력 데이터 검증 및 표현	

용어	설명
- SQL 삽입	웹 응용 프로그램에 sql을 삽입하여 db 서버의 데이터를 변조/유출하고 관리자 인증을 우회하는 보안 약점
- 경로 조작 및 자원 삽입	데이터 입출력 경로 조작, 서버 자원을 수정/삭제
- 크로스 사이트 스크립팅	웹페이지에 악의적인 스크립트 삽입, 방문자들 정보 탈취/비정상적인 기능 수행 유발
- 운영체제 명령어 삽입	외부 입력값을 통해 시스템 명령어 실행 유도, 권한 탈취/시스템 장애 유발
- 위험한 형식 파일 업로드	악의적인 명령어가 포함된 스크립트 파일을 업로드, 시스템에 손상을 주거나 시스템을 제어할 수 있는 보안약점
- 신뢰되지 않는 URL 주소로 자동 접속 연결	입력 값으로 사이트 주소를 받는 경우 이를 조작하여 방문자를 피싱 사이트로 유도
- 메모리 버퍼 오버플로우	할당된 메모리 범위를 넘어선 위치의 자료를 읽거나 쓰려고 할 때 발생
보안 기능	
- 적절한 인증 없이 중요 기능 허용	보안 검사를 우회하여 인증과정 없이 중요한 정보/기능에 접근 및 변경
- 부적절한 인가	접근 제어 기능이 없는 실행 경로를 통해 정보 또는 권한을 탈취할 수 있음
- 중요한 자원에 대한 잘못된 권한 설정	권한 설정이 잘못된 자원에 접근하여 해당 자원을 임의로 사용할 수 있음
- 취약한 암호화 알고리즘 사용	
- 중요 정보 평문 저장 및 전송	
- 하드코딩 된 암호화 키	
암호 알고리즘	
- 개인키 암호화 기법	대칭키 암호화 기법. 스트림 암호화 방식 : LFSR, RC4, 블록 암호화 방식 : DES, SEED, AES, ARIA
- 공개키 암호화 기법	비대칭키 암호화 기법, RSA
서비스 거부 공격(DoS)	대량의 데이터를 한 곳의 서버에 집중적으로 전송, 서버의 정상적인 기능을 방해
- 죽음의 핑(Ping of Death)	패킷 크기를 인터넷 프로토콜 허용 범위 이상으로 전송, 네트워크를 마비시키는 서비스 거부 공격. 수신한 패킷을 재조립, 응답에서 과부하 발생
- 스머핑(Smurfing)	IP, ICMP 특성 악용. 송신 주소를 공격 대상자의 ip로 변경, 해당 네트워크 라우터의 브로드캐스트 주소를 수신지로 설정. 수신한 호스트는 응답 메시지를 송신 호스트로 전송하므로써 네트워크 과부하 발생

용어	설명
- SYN Flooding	3-way handshake 을 악용. SYN 패킷을 대량으로 전송하여 서버를 대기 상태를 만들어 정상적인 서비스를 못하게 하는 것
- TearDrop	패킷의 offset을 변경하여 재조립 오류를 발생시킴
- LAND attack	송신, 수신 ip를 모두 공격 대상의 ip로 설정하여 자신에게 무한히 응답하게 하는 공격
분산 서비스 거부 공격(DDoS)	여러 곳에 분산된 공격 지점에서 한 곳의 서버에 대해 분산 서비스 공격을 수행하는 것
데몬 종류	Trin00, TFN, TFN2K, Stacheldraht
보안 솔루션	외부로 부터의 불법적인 침입을 막는 기술 및 시스템
- 방화벽	내부 네트워크와 인터넷 간에 전송되는 정보를 선별하여 수용/거부/수정 하는 기능. 내부 -> 외부는 그대로 통과, 외부 -> 내부의 경우만 엄밀히 확인
- 침입 탐지 시스템	시스템의 비정상적인 사용, 오용, 남용 등을 실시간으로 탐지하는 시스템 - 오용 탐지 : 미리 입력해둔 공격 탐지 - 이상 탐지 : 평균적인 시스템의 상태를 기준으로 비정상적인 행위나 자원의 사용이 감지되면 알려줌
- 침입 방지 시스템	방화벽 + 침입 탐지 시스템. 비정상적인 트래픽 능동적으로 차단하고 격리하는 등의 방어 조치를 취하는 보안 솔루션
- 데이터 유출 방지	내부 정보의 외부 유출을 방지하는 보안 솔루션. 사내 직원이 사용하는 pc, 네트워크 상의 모든 정보를 검색하고 사용자의 행위를 탐지하고 통제하여 외부로의 유출을 사전에 막음
- 웹 방화벽	일반 방화벽이 탐지하지 못하는 SQL injection, XSS 등의 웹 기반 공격을 방어할 목적으로 만들어짐
- VPN	공중 네트워크와 암호화 기술을 이용하여 사용자가 마치 자신의 전용 회선을 사용하는 것처럼 해주는 보안 솔루션
- NAC	네트워크에 접속하는 내부 PC의 MAC 주소를 IP 관리 시스템에 등록한 후 일관된 보안 관리 기능을 제공하는 보안 솔루션. 내부 PC의 소프트웨어 사용 현황을 관리하여 불법적인 소프트웨어 설치를 방지함
- ESM (Enterprise Security Management)	다양한 장비에서 발생하는 로그 및 보안 이벤트를 통합하여 관리하는 보안 솔루션

11장 응용 SW 기초 기술 활용

용어	설명
운영체제	컴퓨터 시스템 자원을 효율적으로 관리, 컴퓨터를 편리하고 효과적으로 사용할 수 있도록 환경을 제공하는 여러 프로그램 모임 처리 능력 향상, 반환 시간 단축, 사용 가능도 향상, 신뢰도 향상이 목적

용어	설명