

시큐어코딩과 정적분석 툴

에스이랩 박연구

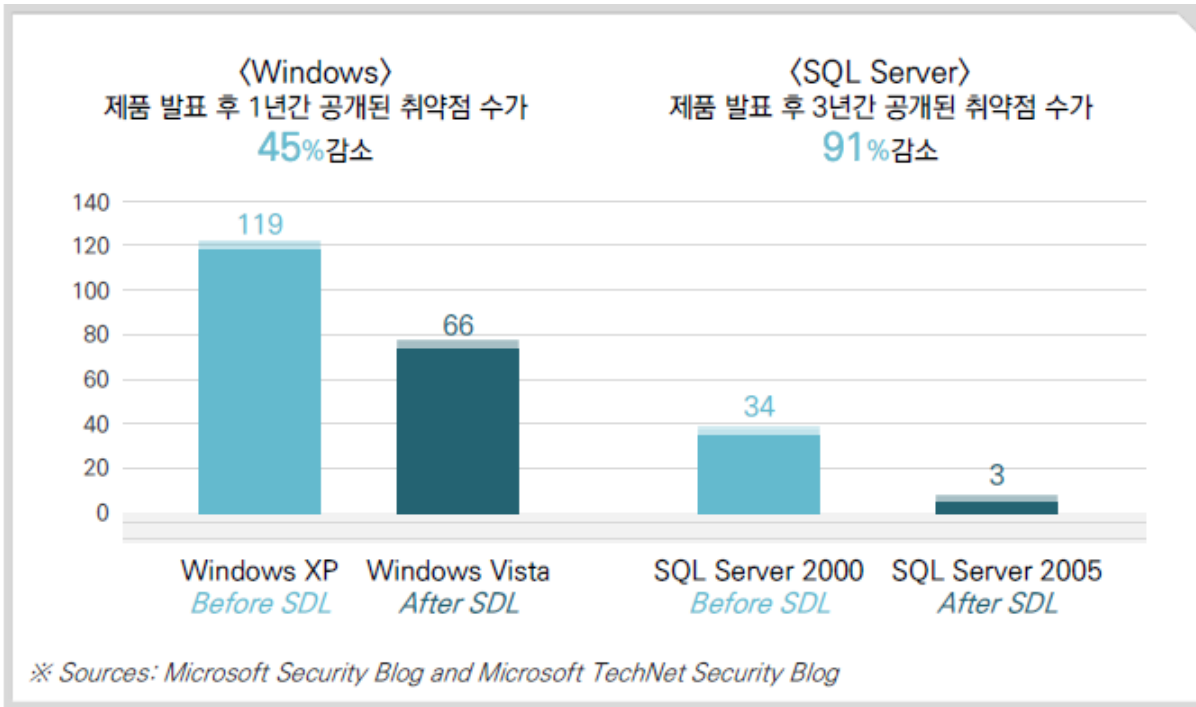
2023-08-02

시큐어코딩 (소프트웨어 개발 보안)

안전한 소프트웨어 개발을 위해 소스 코드 등에 존재할 수 있는
잠재적인 보안 취약점을 제거하고, 보안을 고려하여
기능을 설계 및 구현하는 등 보안 활동

- 미국
 - 2002년 연방정보보안관리법(FISMA)를 제정해 시큐어 코딩 의무화
 - MS Windows Vista 개발할 때 도입
- 한국
 - 2012년 12월 sw 개발 보안 의무제 시행

사례



Microsoft 사
례

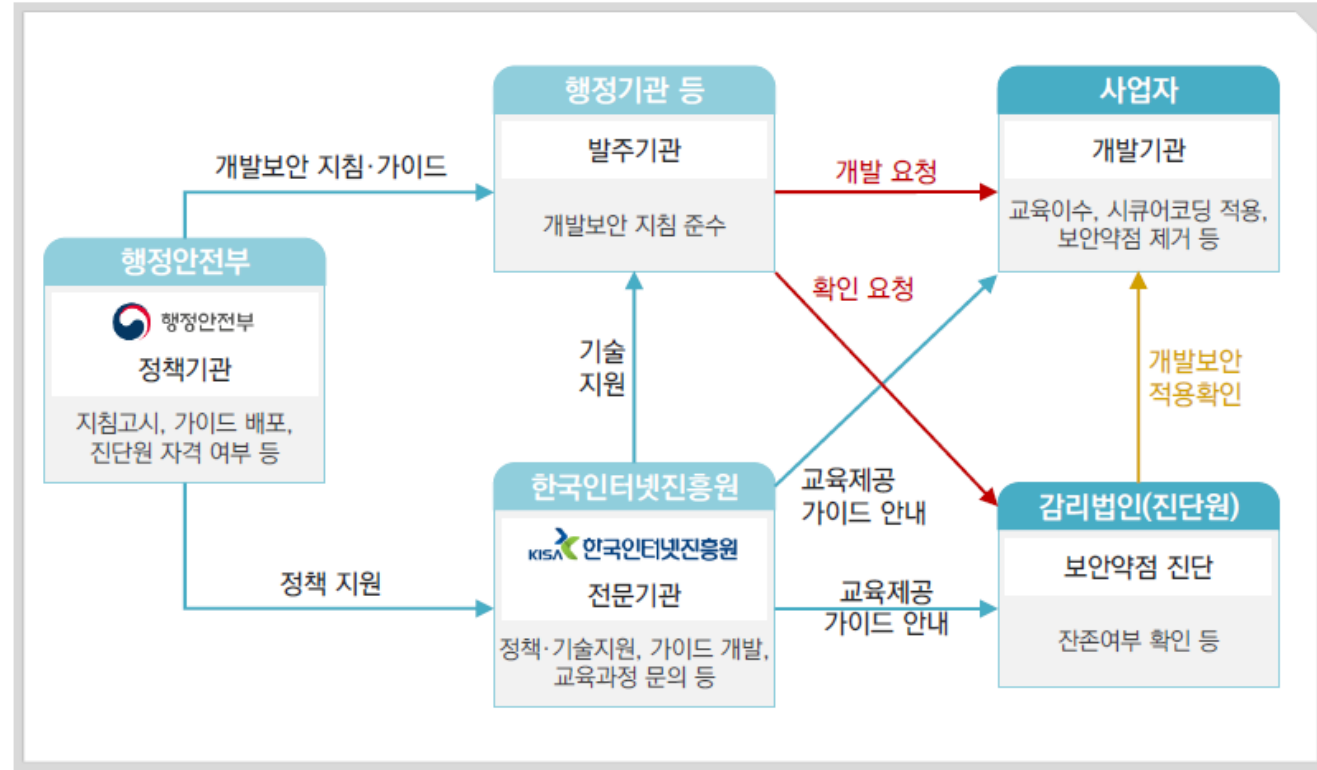
구분	설계단계	코딩단계	통합단계	베타제품	제품출시
설계과정 결함	1배	5배	10배	15배	30배
코딩과정 결함		1배	10배	20배	30배
통합과정 결함			1배	10배	20배

제품출시단계에 발견되는 결함을 제거하
기 위해
30배의 비용이 요구됨

전자정부SW 보안 기준 및 절차

구분	내 용	비고
대 상	<ul style="list-style-type: none"> 정보시스템 감리대상 정보화사업 	'전자정부법 시행령 제71조제1항' 참조
범 위	<ul style="list-style-type: none"> 분석·설계단계 산출물 소스코드(신규개발 전체, 유지보수로 변경된 부분) 	상용 SW 제외
기 준	<ul style="list-style-type: none"> 분석·설계단계 설계항목(총 20개 항목) 구현단계 SW 보안약점 기준(총 47개 항목) ※ 행정기관 및 공공기관 정보시스템 구축·운영 지침 '별표3' ※ 정보시스템 감리기준(제10조 제1항 세부검사항목)에 포함 	진단기준
기 타	<ul style="list-style-type: none"> 감리법인이 진단도구 사용시, 국정원장이 인증한 도구 사용 ※ 정보보호시스템 평가·인증 지침 	'14.1월부터 적용
	<ul style="list-style-type: none"> 감리법인은 SW 보안약점 진단 시, 진단원을 우선적으로 배치 ※ 감리대상외 사업은 자체적으로 SW 보안약점 진단·제거결과 확인 ※ 행정기관 및 공공기관 정보시스템 구축·운영 지침 '별표4' 	진단원 활용

SW개발보안 기준 및 절차



활동 주체별 개발보안 활동

보안 취약점 항목

입력 데이터 검증 및 표현	SQL 삽입	경로 조작 및 자원 삽입	크로스사이트 스크립트	운영체제 명령어 삽입	위험한 형식 파일 업로드	신뢰되지 않은 URL 주소로 자동 접속 연결
	XQuery 삽입	XPath 삽입	LDAP 삽입	크로스사이트 요청 위조	HTTP 응답 분할	정수형 오버플로우
	보안기능 결정에 사용되는 부적절한 입력값	메모리 버퍼 오버플로우	포맷 스트링 삽입			
보안 기능	적절한 인증 없는 중요 기능 허용	부적절한 인가	중요한 자원에 대한 잘못된 권한 설정	취약한 암호화 알고리즘 사용	중요정보 평문 저장	중요정보 평문전송
	하드코드된 비밀번호	충분하지 않은 키 길이 사용	적절하지 않은 난수값 사용	하드코드된 암호화 키	취약한 비밀번호 허용	사용자 하드디스크에 저장되는 쿠키를 통한 정보 노출
	주석만 안에 포함된 시스템 주요정보	솔트 없이 일방향 해쉬 함수 사용	무결성 검사 없는 코드 다운로드	반복된 인증시도 제한 기능 부재		

시간 및 상태	검사시점과 사용시점	종료되지 않은 반복문 재귀함수				
에러 처리	오류메시지를 통한 정보 노출	오류 상황 대응 부재	부적절한 예외 처리			
코드 오류	Null Pointer 역참조	부적절한 자원해제	해제된 자원 사용	초기화되지 않은 변수 사용		
캡슐화	잘못된 세션에 의한 데이터 정보노출	제거되지 않고 남은 디버그 코드	시스템 데이터 정보 노출	Public 메소드 부터 반환된 Private 배열	private 배열에 public 데이터 할당	
API 오용	DNS Lookup에 의존한 보안 결정	취약한 API 사용				

입력값 검증
보안기능
에러처리
세션통제

OWASP TOP 10

OWASP Top 10 - 2013			OWASP Top 10 - 2017		
No	취약점	비고	No	취약점	비고
1	인젝션		1	인젝션	
2	취약한 인증과 세션 관리		2	취약한 인증	
3	크로스 사이트 스크립팅		3	민감한 데이터 노출	
4	안전하지 않은 직접 객체 참조	2017:A5	4	XML 외부 개체(XXE)	신규
5	잘못된 보안 구성		5	취약한 접근 통제	합침
6	민감한 데이터 노출		6	잘못된 보안 구성	
7	기능 수준의 접근 통제 누락	2017:A5	7	크로스 사이트 스크립팅(XSS)	
8	크로스 사이트 요청변조(CSRF)	삭제	8	안전하지 않은 역직렬화	신규
9	알려진 취약점이 있는 구성요소 사용		9	알려진 취약점이 있는 구성요소 사용	
10	검증되지 않은 리다이렉트 및 포워드	삭제	10	불충분한 로깅 및 모니터링	신규

OWASP (The Open Web Application Security Project)

- 오픈소스 웹 애플리케이션 보안 프로젝트

OWASP TOP 10

- 보안상 영향을 크게 줄 수 있는 것들 10가지 선정
- 4년 마다 기준 발표

정적 분석 vs 동적 분석


BASIS FOR COMPARISON	STATIC TESTING	DYNAMIC TESTING
Basic	Does not execute the software.	Execution of the software is necessary.
Cost	Low	High
Statement coverage	100%	50%
Time consumption	Less	More
Uncovers	Large variety of bugs	Limited types of bugs
Performed	Before compilation	Only when executables are available

정적 분석 도구

- SpotBugs (구 FindBugs)
 - 코드에서 발생할 수 있는 버그 취약 코드 탐지
 - 컴파일된 바이트코드로 작동
 - 룰셋 커스터마이징 가능
 - FindSecurityBugs
 - SpotBugs용 보안 전용 플러그인
 - OWASP TOP 10 & CWE 적용
 - PMD
 - 개발에서 실수 할 수 있는 패턴 탐지
 - try, catch, finally, switch의 빈 블록, 불필요한 Object 생성 등
 - Jenkins CI/CD, SonarQube
 - Jenkins는 CI 내에 정적분석이 있는 반면, SonarQube는 정적분석에만 특화되어 있음
- * CVE (Common Vulnerabilities and Exposures) 취약점 리스트
* CWE (Common Weakness Enumeration) 보안약점 리스트

정적 분석 도구


- SpotBugs (구 FindBugs)
 - IntelliJ, Eclipse
- FindSecurityBugs
 - IntelliJ, Eclipse
- PMD
 - IntelliJ, Eclipse
 - VSCode (Apex PMD Extension)
- SonarLint
 - VSCode, IntelliJ, Eclipse
- Microsoft DevSkim
 - VSCode



EMP 비즈를
업그레이드해주러 왔어



뭘, 지금도 완벽한데

A woman with dark skin and her hair styled in two large, intricate braided buns. She is wearing a light-colored top and a choker necklace made of white, shell-like beads. She is looking towards a man whose back is partially visible on the left side of the frame. The background is a blurred outdoor setting with some architectural elements.

잘 작동해도
얼마든지 개선의 여지가 있거든?

참고 링크

- 공개 SW를 활용한 소프트웨어 개발보안 점검가이드(2019.6.)
- 소프트웨어 개발보안 가이드(2019.11.)
- 소프트웨어 보안약점 진단가이드(2019.6.)

- 정적 코드 분석, Static Code Analysis
<https://camelsource.tistory.com/58>

- 우아한형제들 조민재, 2018, 오픈소스로 만나보는 DevSecOps
https://www.sosconhistory.net/soscon2018/pdf/day2_1100_1.pdf

- SpotBugs
<https://spotbugs.github.io/>

- Find Security Bugs
<https://find-sec-bugs.github.io/>

끝