발 간 등 록 번 호
11-1311000-000395-14

전자정부 SW 개발보안 진단원을 위한

소프트웨어 보안약점 진단가이드

2013. 11.



안전행정부

Contents

04 제1장 개요

04 제1절 배경

04 제2절 가이드 목적 및 구성

08 제2장 소프트웨어 보안약점 진단방법

08 제1절 입력데이터 검증 및 표현

1. 경로 조작 및 자원 삽입 / 08
2. 메모리 버퍼 오버플로우 / 11
3. 포맷스트링 삽입 / 15

17 제2절 보안기능

1. 반복된 인증시도 제한 기능 부재 / 17
2. 중요정보 평문저장 / 19
3. 중요정보 평문전송/ 22

25 제3절 코드 오류

1. 해제된 자원 사용 / 25
2. 초기화되지 않은 변수 사용 / 27

29 제4절 취약한 API 사용

1. 취약한 API 사용 / 29

32

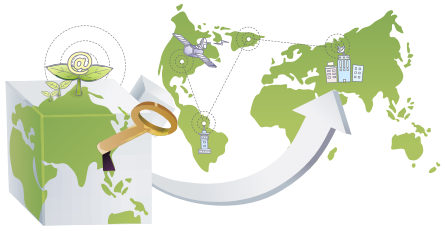
부 록

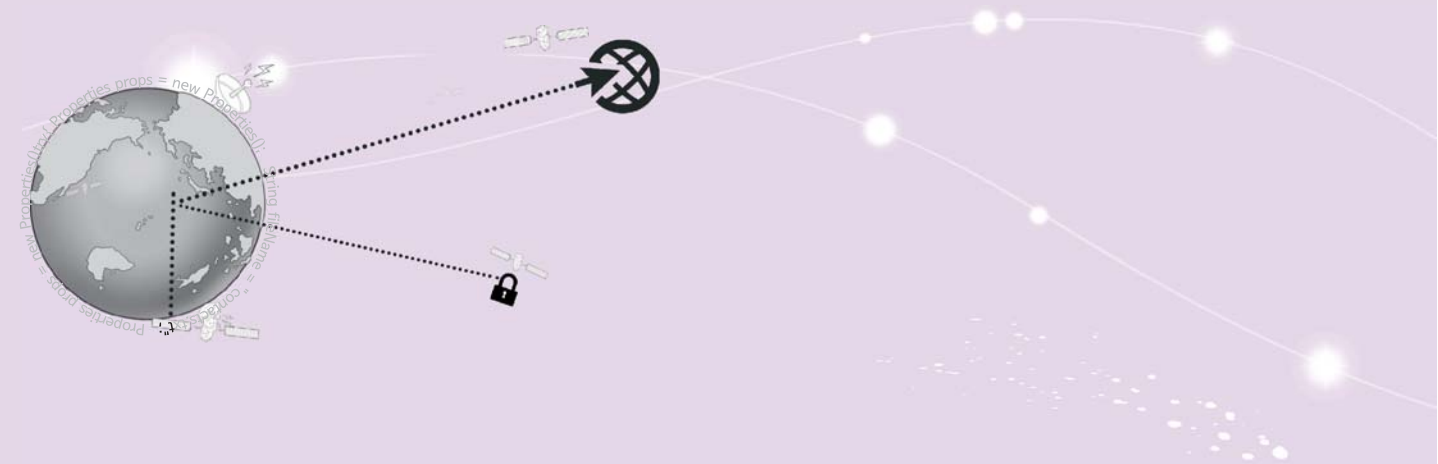
32 제1절 신규 소프트웨어 보안약점 항목

34 제2절 소프트웨어 보안약점 항목 신구 대비표

37 제3절 취약한 API 목록(MS SDL)

39 제4절 참고자료





제 1 장
개요

제1절 배경
제2절 가이드 목적 및 구성

01 개요



제1절 배경

개정 고시된 '행정기관 및 공공기관 정보시스템 구축 · 운영 지침(안행부고시 제2013-36호, 2013. 8. 27)' 별표3의 보안약점 기준의 변경사항(43개→47개로 변경)에 대한 보안약점 진단방법을 SW 보안약점 진단가이드 개정발간 전에 별책으로 먼저 발간하여 SW 보안약점 진단원의 SW 개발보안 적용여부 확인 업무를 지원하고자 한다.

제2절 가이드 목적 및 구성

목적	• '행정기관 및 공공기관 정보시스템 구축 · 운영 지침(**안행부고시, 2013. 8**)'에 따라 정보화사업 수행시 시큐어코딩을 준수하여 SW를 개발했는지 여부를 확인하기 위한 SW 보안약점 진단기법 제시 • SW 개발 전 과정에서의 진단 프로세스를 제시하고, 진단원 관점에서 보다 근본적인 보안약점 진단 방법론을 제시하고 효과적인 진단 업무 지원 • 진단도구 사용여부와 무관하게 보안약점에 대해서 검증할 수 있는 방안 제시
대상	• 전자정부 SW 보안약점 진단원
범위	• 신규로 개발되거나 유지보수로 변경되는 전체 소스코드에 대한 시큐어코딩 적용의 적절성 여부 진단시 참조 ※ 행정기관등[1]이 추진하는 정보화사업 단계 중 구현단계에 초점

1) 행정기관등 : 전자정부법 제2조에서 정의하는 행정기관, 공공기관

구성	• **(2장)** SW 보안약점에 대한 설명 및 보안대책과 진단예시 소개 • **(부록)** 신규 SW 보안약점, SW 보안약점 신구 대비표, 참고자료
활용	• **(발주자)** SW 보안약점 진단 · 제거 요구사항 도출시 활용 • **(사업자)** 자체적으로 SW 보안약점 진단 · 제거시 활용 • **(진단원)** 사업자가 수행한 SW 보안약점 제거 결과 진단시 활용 • **(기 타)** SW 개발보안체계 및 보안약점 진단· 제거 방법에 대한 이해




the world