소프트웨어 개발보안 기법 47

1. 입력데이터 검증 및 표현
2. SQL 삽입
3. 경로 조작 및 자원 삽입
4. 크로스사이트 스크립트
5. 운영체제 명령어 삽입
6. 위험한 형식 파일 업로드
7. 신뢰되지 않은 URL 주소로 자동접속 연결
8. XQuery 삽입
9. XPath 삽입
10. LDAP 삽입
11. 크로스사이트 요청 위조
12. HTTP 응답분할
13. 정수형 오버플로우
14. 보안기능 결정에 사용되는 부적절한 입력값
15. 메모리 버퍼 오버플로우
16. 포맷 스트링 삽입
17. 보안기능
18. 적절한 인증 없는 중요기능 허용
19. 부적절한 인가
20. 중요한 자원에 대한 잘못된 권한 설정
21. 취약한 암호화 알고리즘 사용
22. 중요정보 평문저장
23. 중요정보 평문전송
24. 하드코드된 비밀번호
25. 충분하지 않은 키 길이 사용
26. 적절하지 않은 난수값 사용
27. 하드코드된 암호화 키
28. 취약한 비밀번호 허용
29. 사용자 하드디스크에 저장되는 쿠키를 통한 정보노출
30. 주석문 안에 포함된 시스템 주요정보
31. 솔트없이 일방향 해쉬함수 사용
32. 무결성 검사 없는 코드 다운로드
33. 반복된 인증시도 제한 기능 부재
34. 시간 및 상태
35. 경쟁조건 : 검사시점과 사용시점(TOCTOU)
36. 종료되지 않는 반복문 또는 재귀함수
37. 에러처리
38. 오류메시지를 통한 정보노출
39. 오류 상황 대응 부재
40. 부절절한 예외처리
41. 코드오류
42. Null Pointer 역참조
43. 부적절한 자원 해제
44. 해제된 자원사용
45. 초기화되지 않은 변수 사용
46. 캡슐화
47. 잘못된 세션에 의한 데이터 정보노출
48. 제거되지 않고 남은 디버그 코드
49. 시스템 데이터 정보노출
50. Public 메소드로부터 반환된 private 배열
51. Private 배열에 Public 데이터 할당
52. API 오용
53. DNS lookup에 의존한 보안결정
54. 취약한 API 사용