한국컴퓨터정보학회 동계학술대회 논문집 제24권 제1호 (2016. 1)

설계 단계의 보안 코딩 지침-입력 데이터 검증 및 표현

신성윤[*O], 이현창[**] 안우영[***]
[*O]군산대학교 컴퓨타정통신공학부
[**]원광대학교 정보전자상거래학부
[***]대전보건대학교 바이오정보과
e-mail: s3397220@kunsan.ac.kr[*O], hclgloty@wku.ac.kr[**], wyahn@hit.ac.kr[***]

Secure Coding Guide of Design Step-Verification and Expression of Input Data

SSeong-Yoon Shin[*O], Hyun-Chang Lee[**], Woo-Young Ahn[***]
[*O]School. of Computer Inf. & Comm. Eng., Kunsan National University
[**]Div. of Inf. and E. Com., (Ins. of Conv. & Cre.), Wonkwang University
[***]Dept. of Bio Information, Daejeon Health Institute Technology

● 요 약 ●

본 논문에서는 S/W 개발 보안 지침에서 설계 단계의 보안 코딩 지침을 알려준다. 크로스 사이트 스크립트 공격 취약점(XSS)에서부터 자원 삽입 까지 S/W 보안 취약점의 주요 내용을 입력 데이터의 검증 및 표현에 맞추어 지침을 전달하도록 한다.

키워드: 보안 지침(security guide), 취약점(vulnerability), 검증 및 표현(Verification and Expression)

I. Introduction

S/W의 설계란 유저의 요구사항을 개발하는 시스템에서 어떻게 만족시킬 것인가의 해결책을 찾고 이를 구체화하는 단계로 유저의 요구사항에 대한 분석 결과와 실제 PL로 구현하는 단계를 연결해주는 역할을 담당한다[1].

행안부의 전자정부 소프트웨어 개발 운영자를 위하여 2012년에 발표한 소프트웨어 개발보안 가이드를 개선하기 위한 방안을 제안한 논문[2]도 있었다.

본 논문에서는 이 같은 S/W 설계 단계에 포함 되어야할 크로스 사이트 스크립트 공격 취약점(XSS)에서부터 자원 삽입 까지 S/W 보안 취약점의 주요 내용을 제시한다.

II. Secure Guide of S/W

행정기관 등이 안전한 소프트웨어를 개발하여 각종 사이버위협으로부터 예방 · 대응코자 하여 만든 것이다. SW 개발단계부터 보안약점을 제거하는 'SW 개발보안' 의무제가 시행되며 이에 따른 관련 가이드를 보급한 것이다. 가이드 주된 내역서는 개발할 때 참고하는 소프트웨어 개발보안 가이드인 언어별 시큐어코딩 가이드가 있다. 이는 JAVA, C, Android-JAVA등을 포함한다. 그리고 점검할 때 참고하는 소프트웨어 보안약점 진단가이드가 있다.

III. Sort of S/W Security Vulnerability

구분	SW 보안 취약점 주요 내용(입력 데이터 검증 및 표현)
크로스 사이트 스크립트 공격 취약점(XSS)	•외부로 부터 입력된 문자열을 사용하여 동적 웹페이지를 생성할 경우 공격자에 의한 부적절한 스크립트 삽입이 가능하며, 그에 따른 보안 취약성 발생
SQL 삽입	•외부입력이나 변수로부터 받은 값이 SQL 함수에 직접 전달됨에 따라 외부에서 내부 정보에 접근허용이 가능 •ex) „xx" or 1=1 삽입
HTTP 응답 분할	•외부에서 입력된 인자값이 HTTP 응답헤더(Set Cookie 등)에 포함될 경우 공격자가 해당 응답헤더에 악성코드 삽입이 가능 •ex) CR, LF 등을 입력하여 HTTP 응답을 2개 이상으로 분리 후 코드 삽입
버퍼오버플로우	•프로그램이 버퍼에 오버플로우가 발생 가능한 데이터를 입력하는 것으로, 임의의 코드가 다른 영역의 메모리의 떨어지는 등의 오작동 발생 가능 •ex) strcpy() 등의 사용

디렉토리 경로조작	•외부의입력이직접파일이름을생성할경우접근이제한된디렉토리또는파일에접근이가능해짐 •ex) ../../rootfile.txt
운영체제 명령어 삽입	•외부에서 전달되는 값으로 시스템 내부 명령어를 사용할 경우 외부에서 운영체제 제어가 가능
LDAP 삽입	•외부입력이 LDAP 필터 문자열로 사용될 경우, 공격자에 의한 LDAP 명령문의 구성이 변동 가능
버퍼 범위 한칸 벗어난 부 분 읽기	•버퍼 크기를 넘어서는 인덱스 사용 또는 버퍼 범위를 넘어서는 영역을 참조할 경우 공격자의 의도에 따라 민감한 정보에 접근하거나, 예상치 못한 동작이 수행
자원 삽입	•외부 입력을 자원 식별자로 사용할 경우 의도한 통제 범위 밖의 자원에 접근이 가능해짐 •ex) 소켓 번호 또는 포트 번호를 외부로부터 입력 받아 사용

IV. Conclusions

본 논문에서는 S/W 개발 보안 지침에서 설계 단계의 보안 코딩 지침을 전달해 주었다. 특히, S/W 설계 단계에 포함 되어야할 크로스 사이트 스크립트 공격 취약점(XSS) 에서부터 자원 삽입 까지 S/W 보안 취약점의 주요 내용을 제시한다. 이는 S/W 보안 취약점의 주요 내용을 입력 데이터의 검증 및 표현에 맞추어 지침을 전달하는 것이다.

References

[1] http://www.happycampus.co.kr/doc/3614795/

[2] Kyung Sook Han,Taehwan Kim, Ki Young Han, Jae Myung Lim,Changwoo Pyo, "An Improvement of the Guideline of Secure Software Development for Korea E-Government," Journal of the Korea Institute of Information Security and Cryptology, Vol. 22, No. 5, pp.1179-1189, 2012