SOFTBase

xFrame5
보안 가이드

VERSION 22.12.28.1

xFrame5

서울특별시 구로구 디지털로 272, 1110 (구로동, 한신 IT 타워)
Phone 02-2108-8030 • Fax 02-2108-8031
www.softbase.co.kr

목차

1 장: XSS 보안

이 장에서는 XFrame5 솔루션에서 제공하는 보안 관련 기능중 XSS 보안에 대해서 기술합니다. 이 장에서 기술하는 내용은 아래와 같습니다.

- ✓ XSS(Cross-site Scripting) 보안
- ✓ XDataSet5 이용한 XSS 적용 방식
- ✓ UI 동작 방식
- ✓ XDataSet5.jar 동작 방식

XSS(Cross-site Scripting) 보안

SQL injection 과 함께 웹 상에서 가장 기초적인 취약점 공격 방법의 일종으로, 악의적인 사용자가 공격하려는 사이트에 스크립트를 넣는 기법을 말한다. 공격에 성공하면 사이트에 접속한 사용자는 삽입된 코드를 실행하게 되며, 보통 의도치 않은 행동을 수행시키거나 쿠키나 세션 토큰 등의 민감한 정보를 탈취한다.

- 관련 정보 https://namu.wiki/w/XSS

XDataSet5 이용한 XSS 적용 방식

UI 실행 파라미터

XTRAN_XSSENCODING 실행 파라미터 값을 true 로 설정시 동작한다.

UI 동작 방식

UI -> 서버로 데이터 송신시 아래의 작업이 수행된다.

구분	설명
1	▪ XDataSet5 HEADER부 xssencoding 값을 '1'로 설정.
2	송신 데이터를 아래의 단계로 인코딩하여 서버로 송신한다. (데이터 Encoding 시 한글/유니코드 문자로 인해, 무조건 encodeURIComponent 을 수행하고, BASE64 인코딩해야함) ▪ encodeURIComponent 인코딩 ▪ BASE64로 인코딩 ▪ encodeURIComponent 인코딩

XDataSet5.jar 동작 방식

UI 로부터 수신한 데이터 처리 방식은 아래와 같다.

구분	설명
1	▪ XDataSet5 HEADER부 xssencoding 값이 '1'인지 비교하여 수신 데이터 디코딩 처리
2	getData API 호출시 헤더부의 xssencoding 값이 '1'인 경우, 문자열을 HTML TAG FILTER 를 적용한 문자열로 리턴한다. [HTML TAG FILTER 대상] ▪ '<' -> "<" ▪ '>' -> ">" ▪ '&' -> "&" ▪ '"' -> """ ▪ '"' -> "'" 화면에서 설정한 데이터 : <&123> xssencoding 값이 '0'인 경우 getData 리턴값 : <&123> xssencoding 값이 '1'인 경우 getData 리턴값 : <&123>
3	getData API xssencoding 처리 여부에 대한 파라미터 지정 API 제공한다. public String getData(String dataset_name, String column_name, int record_index, Boolean htmlTagFilter) public String getData(String dataset_name, int column_index, int record_index, Boolean htmlTagFilter) XDataSet5 헤더부 xssencoding 값이 '1'이더라도, HTML TAG FILTER 를 적용하지 않고자 하는 경우에는 htmlTagFilter 파라미터 값을 false 로 지정하여 위의 함수를 호출한다.
4	getData API 로 구한 값이 HTML TAG FILTER 가 적용되어 있을 때, 원래대로 재치환을 해야 하는 경우 replaceHTMLTagFilter API 를 호출한다. (Static 함수임) public static String replaceHTMLTagFilter(String strData) 예를들어 다음과 같이 화면에서 전달된 데이터를 가져온 후 XDataSet5 xDataSet5 = new XDataSet5(request, response); String strEmpData = xDataSet5.getData("DS_REQ", "EMP_DATA", 0, true);

	다음처럼 값을 재치환 할 수 있다. System.out.println("strEmpData = " + XDataSet5.replaceHTMLTagFilter(strEmpData));

2 장: 데이터 보안

이 장에서는 XFrame5 솔루션에서 제공하는 보안 관련 기능중 데이터 보안에 대해서 기술합니다. 이 장에서 기술하는 내용은 아래와 같습니다.

- ✓ 데이터 복사 보안
- ✓ 데이터 암호화 API

데이터 복사 보안

데이터 복사 보안은 UI 에 표현된 데이터에 대해서 사용자의 복사를 방지하는 기능이다.

UI 실행 파라미터

PROTECT_COPY 실행 파라미터는 필드성 컴포넌트 및 그리드/그리드 컬럼에서 데이터의 사용자 복사 방지 관련 속성 값을 기본값으로 동작한다.

- true: Control C 키 입력을 통한 복사를 금지한다.
- false: Control C 키 입력을 통한 복사를 허용한다.

protect_copy 속성

protect_copy 속성은 필드성 컴포넌트 및 그리드/그리드 컬럼에서 데이터의 사용자 복사 방지 관련 속성이며, 아래와 같은 값을 제공한다.

- 0: default, PROTECT_COPY 실행 파라미터의 값이 적용된다.
- 1: allow, 데이터의 복사 관련 동작을 허용한다.
- 2: protect, 데이터의 복사 관련 동작을 금지한다.

데이터 암호화 API

xFrame5 솔루션에서 제공하는 암호화 관련 API 는 두가지 분류로 제공된다.

- BASE64 방식의 암호화/복호화
- Crypto.js 라이브러리 연계 방식: https://github.com/brix/crypto-js
  (xf5/ext/lib 폴더에 crypto-js-4.1.1.min.js 사용)

API	설명
encrypttext, decrypttext	▪ 데이터에 대한 암호화/복호화 처리 수행
setencryptkey	▪ 3DES, AES 방식에 적용될 KEY 값
gethashencrypt	▪ 해쉬 알고리즘을 사용하여 문자열을 암호화

쿠키 저장 보안

쿠키 저장에 대한 기능을 방지하는 기능이다.

UI 실행 파라미터

PROTECT_COOKIE 실행 파라미터는 factory. Setcookie API 를 통해서 쿠키 정보 저장 기능 허용 여부를 지정한다.

- true: 쿠키 데이터 저장을 금지한다.
- false: 쿠키 데이터 저장을 허용한다.