XS (상)	크로스사이트 스크립팅
취약점 개요	
점검목적	■ 웹 사이트 내 크로스사이트 스크립팅 취약점을 제거하여 악성 스크립트의 실행을 차단
보안위협	■ 웹 애플리케이션에서 사용자 입력 값에 대한 필터링이 제대로 이루어지지 않을 경우, 공격자는 사용자 입력 값을 받는 게시판, URL 등에 악의적인 스크립트(Javascript, VBScript, ActiveX, Flash 등)를 삽입하여 게시글이나 이메일을 읽는 사용자의 쿠키(세션)를 탈취하여 도용하거나 악성코드 유포 사이트로 Redirect 할 수 있음
참고	**※ 크로스 사이트 스크립팅 :** 악의적인 사용자가 공격하려는 사이트에 스크립트를 넣는 기법으로 공격 방식은 크게 stored 공격 방식과 reflected 공격 방식으로 나누어 짐 ※ OWASP - XSS 필터링 관련 참고사항 https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet ※ 소스코드 및 취약점 점검 필요
조치방법	웹 사이트의 게시판, 1:1 문의, URL 등에서 사용자 입력 값에 대해 검증 로직을 추가하거나 입력되더라도 실행되지 않게 하고, 부득이하게 웹페이지에서 HTML을 사용하는 경우 HTML 코드 중 필요한 코드에 대해서만 입력되게 설정

보안설정 방법

* 웹 사이트에 사용자 입력 값이 저장되는 페이지는 공격자가 웹 브라우저를 통해 실행되는| 스크립트 언어(HTML, Javascript, VBScript 등)를 사용하여 공격하므로 해당되는 태그 사용을 사전에 제한하고, 사용자 입력 값에 대한 필터링 작업이 필요함
* 게시물의 본문뿐만 아니라 제목, 댓글, 검색어 입력 창, 그 외 사용자 측에서 넘어오는 값을 신뢰하는 모든 form과 파라미터 값에 대해서 필터링을 수행함
* 입력 값에 대한 필터링 로직 구현 시 공백 문자를 제거하는 trim, replace 함수를 사용하여 반드시 서버 측에서 구현되어야 함
* URLDecoder 클래스에 존재하는 decode 메소드를 통해 URL 인코딩이 적용된 사용자 입력 값을 디코딩함으로써 우회 공격 차단
* 웹 방화벽에 모든 사용자 입력 폼(회원정보 변경, 게시판, 댓글, 자료실, 검색, URL 등)을 대상으로 특수문자, 특수 구문 필터링하도록 룰셋 적용

※ 필터링 조치 대상 입력 값

- 스크립트 정의어 : <SCRIPT>, <OBJECT>, <APPLET>, <EMBED>, <FORM>, <IFRAME> 등
- 특수문자 : <, >, ", ', &, %, %00(null) 등

※ 웹 애플리케이션 별 상세 설정

■ ASP

```
<%
  … 중략 …
  If use_HTML Then
  content = Server.HTMLEncode(content)
  … 중략 …
  Sub ReplaceStr(content, byref str)
  content = replace(content, "'", " ₩'")
  content = replace(content, "&", "&amp;")
  content = replace(content, " ₩'", "&quot")
  content = replace(content, "<", "&lt")
  content = replace(content, ">", "&gt")
  str = content
  End Sub
  … 중략 …
%>
```

■ PHP

```
… 중략 …
if($use_html == 1) // HTML tag를 사용해야 하는 경우 부분 허용
$memo = str_replace("<", "&lt", $memo);// HTML TAG 모두 제거
$tag = explode(",", $use_tag);
for($i=0; $i<count($tag); $i++) { // 허용할 TAG만 사용할 수 있도록 변경
$memo = eregi_replace("&lt".$tag[$i]." ", "<".$tag[$i]." ", $memo);
$memo = eregi_replace("&lt".$tag[$i].">", "<".$tag[$i].">", $memo);
$memo = eregi_replace("&lt/".$tag[$i], "</".$tag[$i], $memo); }
else // HTML tag를 사용하지 못하게 할 경우
$memo = str_replace("<", "&lt", $memo);
$memo = str_replace(">", "&gt", $memo);
… 중략 …
```

■ **JSP**

```
<%
   … 중략 …
   string subject = request.getParameter("subject_BOX");
   subject = subject.replaceAll("<", "&lt");
   subject = subject.replaceAll(">", "&gt");
   … 중략 …
%>
```

※ 참고: 필터링 대상

<	>	<	>	innerHTML
javascript	eval	onmousewheel	onactive	onfocusout
expression	charset	ondataavailable	oncut	onkeyup
applet	document	onafteripudate	onclick	onkeypress
meta	string	onmousedown	onchange	onload
xml	create	onbeforeactivate	onbeforecut	onbounce
blink	append	onbeforecopy	ondbclick	onmouseenter
link	binding	onbeforedeactivate	ondeactivate	onmouseout
style	alert	ondatasetchaged	ondrag	onmouseover
script	msgbox	cnbeforeprint	ondragend	onsubmit
embed	refresh	cnbeforepaste	ondragenter	onmouseend
object	void	onbeforeeditfocus	ondragleave	onresizestart
iframe	cookie	onbeforeuload	ondragover	onuload
frame	href	onbeforeupdate	ondragstart	onselectstart
frameset	onpaste	onpropertychange	ondrop	onreset
ilayer	onresize	ondatasetcomplete	onerror	onmove