

XSS

Mitigation

Contents

What is XSS ...?	02
-------------------------	-----------

XSS Mitigation	08
Escape	09
Filtering	11

Filtering Check	13
------------------------	-----------

Q & A	17
------------------	-----------

What is XSS ...?

XSS

Mitigation

Check

Q & A

Cross-site Scripting(XSS)

- 사이트 간 스크립팅은 웹 어플리케이션에서 많이 나타나는 취약점의 하나로 웹사이트 관리자가 아닌 이가 웹 페이지에 악성 스크립트를 삽입할 수 있는 취약점이다.
- XSS 종류
 - Reflected XSS
 - Stored XSS
 - DOM based XSS

What is XSS ...?

XSS

Mitigation

Check

Q & A



악의적인 스크립트가 포함된 게시물 생성



과제 해결해 드립니다~

```
<script>alert`XSS`</script> ㅋㅋ 그걸 속네
```

Submit

What is XSS ...?

[XSS](#)[Mitigation](#)[Check](#)[Q & A](#)

[main](#)[board](#)[update](#)[delete](#)

과제 해결해 드립니다~

ㅋㅋ 그걸 속네

prev

```
<!DOCTYPE html>
<html>
  <head>...</head>
  <body>
    <div class="header">...</div>
    <div class="post-form">
      <div class="title-field">과제 해결해 드립니다~</div>
      <div class="contents-field">
        ... <script>alert`XSS`</script> == $0
        "ㅋㅋ 그걸 속네"
      </div>
      <a href="/view.php?no=26">...</a>
    </div>
  </body>
</html>
```

What is XSS ...?

XSS

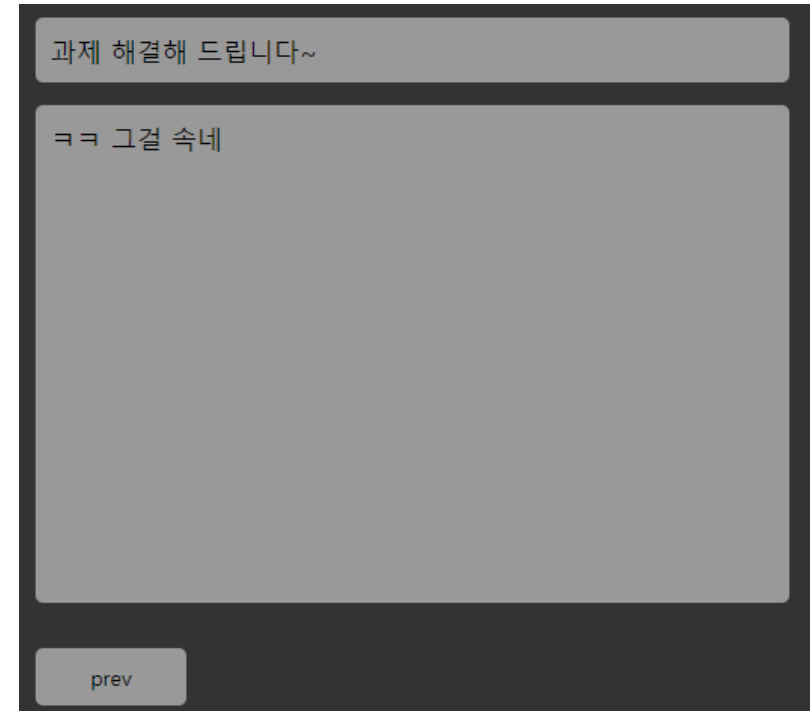
Mitigation

Check

Q & A



게시글을 읽으면서 삽입된 스크립트 실행



What is XSS ...?

XSS

Mitigation

Check

Q & A

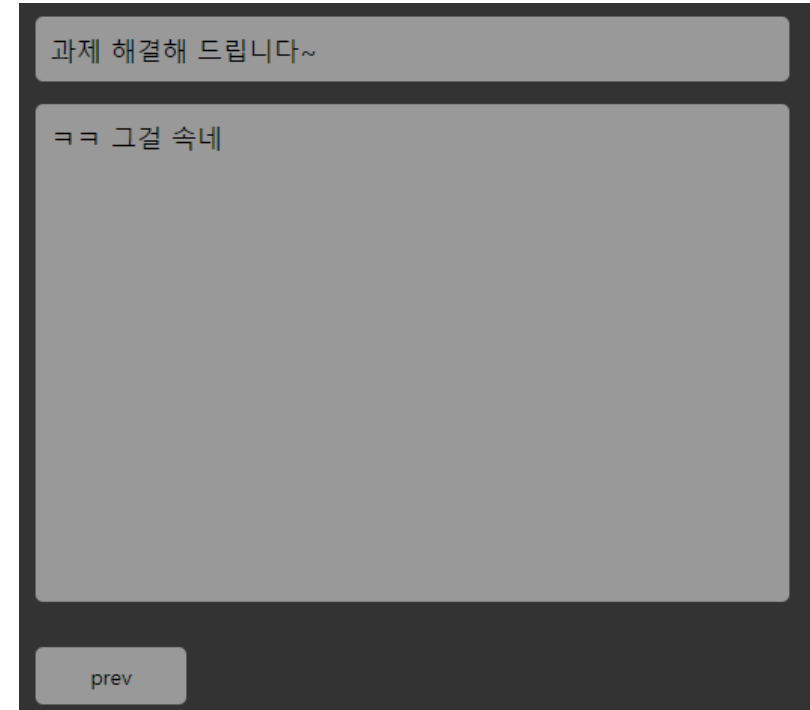


게시글을 읽으면서 삽입된 스크립트 실행



XSS 공격으로 인한 피해

- 쿠키 / 세션 탈취
- 악성코드 다운로드
- 시스템 관리자 권한 획득



Escape

- 사용자가 입력한 값 중 '<', '>' 와 같은 특수문자가 HTML 태그로 인식하는 것이 아닌 단순한 문자로 인식하기 위해 HTML Entity로 변환하는 것

Filtering

- 사용자가 입력한 값 중 '<script>', 'alert()', 'onerror=' 와 같이 악의적인 행동을 위해 사용하는 태그, 함수, 이벤트 등을 필터링 하여 입력할 수 없도록 하는 것

XSS Mitigation - Escape

XSS

Mitigation

Check

Q & A

`htmlspecialchars($string, $flags, $encoding, $double_encode)`

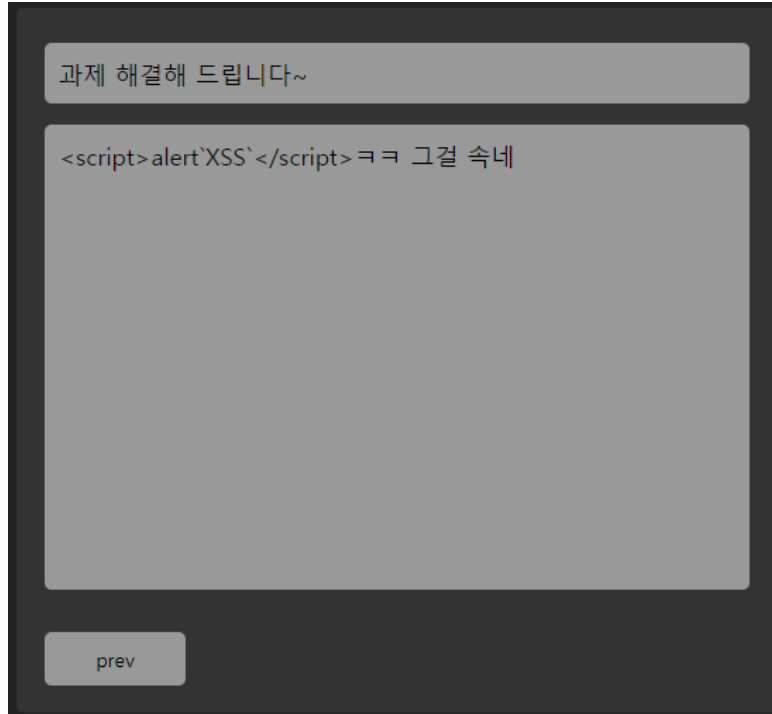
- `&`(ampersand), `"`(double quote), `'`(quote), `<`(less than), `>`(greater than)와 같은 특정 문자를 HTML Entite로 변환한다.
- 해당 함수와 달리 `htmlentities` 함수는 해당하는 모든 문자를 HTML Entitie로 변환한다.

`strip_tags($string, $allowed_tags)`

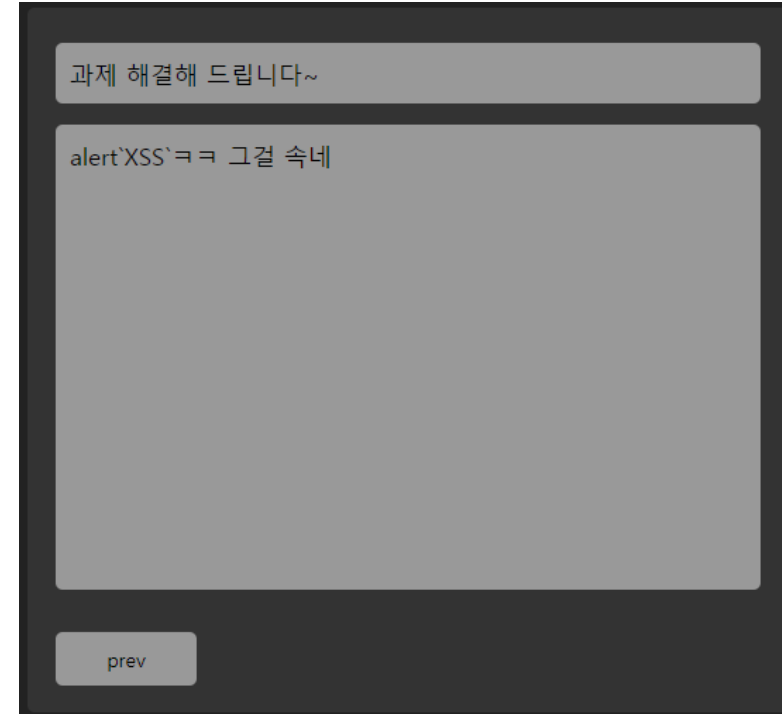
- 문자열에 포함된 HTML, PHP 태그를 제거한다.
- `allowed_tags`에 특정 태그를 지정하면 해당 태그는 제외할 수 있다.

```
<div class="post-form">
  <div class="title-field"><?php echo htmlspecialchars($row['title']);?></div>
  <div class="contents-field"><?php echo htmlspecialchars($row['contents']);?></div>
</div>
```

XSS Mitigation - Escape

[XSS](#)[Mitigation](#)[Check](#)[Q & A](#)

`htmlspecialchars()`



`strip_tags()`

XSS Mitigation - Filtering

XSS

Mitigation

Check

Q & A

`str_replace($search, $replace, $subject, $count)`

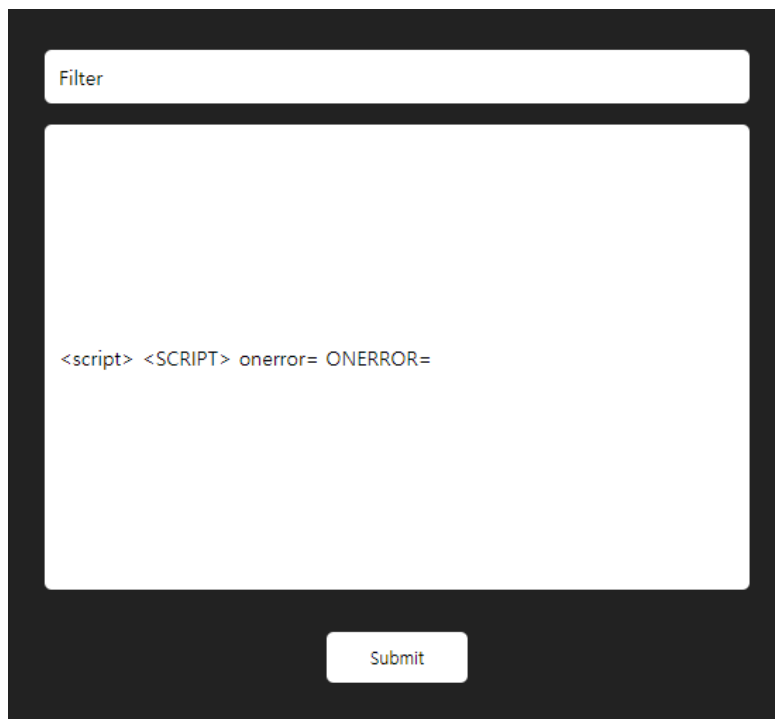
- 대상 문자열에서 특정 문자열 검색 후 검색된 문자열을 다른 문자열로 교체한다.
- 대/소문자 구분 0 -> `str_ireplace`를 사용하면 이를 해결할 수 있다.

`preg_replace($pattern, $replacement, $subject, $limit, $count)`

- 대상 문자열에서 정규표현식을 사용한 문자열 검색후 검색된 문자열을 다른 문자열로 교체한다.
- 잘못된 정규표현식을 구현하면 실 사용자에게 피해를 줄 수 있다.

```
$contents = str_replace("<script>", "_", $contents);  
$contents = preg_replace("/onerror\s*=/i", "_", $contents);  
$contents = preg_replace("/onload\s*=/i", "_", $contents);  
$contents = preg_replace("/onclick\s*=/i", "_", $contents);  
$contents = preg_replace("/onwheel\s*=/i", "_", $contents);
```

XSS Mitigation - Filtering

[XSS](#)[Mitigation](#)[Check](#)[Q & A](#)

Filter

<script> <SCRIPT> onerror= ONERROR=

Submit

입력전



Filter

_ <SCRIPT> _ _

prev next

입력후



Selenium

- 웹 브라우저의 자동화를 가능하게 하고 지원하는 다양한 도구와 라이브러리를 포함한 프로젝트
- 지원 언어
 - Java, Python, C#, Ruby, JavaScript, Kotlin

find_element_by_XXX()

- 특정 요소를 찾기 위해 사용하는 함수
- 다음과 같은 속성을 이용하여 찾을 수 있다.
 - class, css selector, id, name, tag_name, xpath, link_text, partial_link_text

XPath(XML Path Language)

- XML 문서의 특정 요소나 속성에 접근하기 위한 경로를 지정하는 언어
- XPath Helper를 사용하면 경로를 짜거나 검증할 때 도움을 주어 훨씬 편하게 사용할 수 있다.
 - XPath Helper는 크롬 웹 스토어에서 다운로드 받을 수 있다.

간 단 시 연

XSS

Mitigation

Check

Q & A

Q & A