

XSS 대응 방안

2021.04.01 이유경

XSS 종류

- Reflected XSS

- 반사형 / 파라미터를 통해 발생 /
브라우저에 응답할 때 파라미터에 삽입된 스크립트를 클라이언트에게 전달

- Stored XSS

- 저장형 / 게시판 등에서 발생 /
웹서버에 스크립트를 저장하여 데이터베이스에 기록

- Dom based XSS

- 서버로 전달되지 않고, 클라이언트 측에서 브라우저를 통해 발생

1. HTML character entity

- HTML 엔티티: 마크업과 충돌을 막기 위해 만들어진 특수 코드 (ex. `<` → `<`)
<https://dev.w3.org/html5/html-author/charref>

- XSS는 입력한 문자가 HTML 코드로 인식되어 발생

`<script>alert(1)</script>` → `<script>alert(1)</script>`

- `htmlspecialchars()`

1-1. htmlspecialchars()

기존 코드

```
1 <?php
2 $db = mysqli_connect('127.0.0.1', 'root', '', '210322');
3 session_start();
4
5 $sql = "
6     INSERT INTO board SET
7     subject = '{$_POST['subject']}',
8     writer = '{$_POST['writer']}',
9     content = '{$_POST['content']}',
10    reg_date = now();
11 ";
12 if ($db->query($sql)) {
13     header('Location:./main.php');
14 } else {
15     print_r($db->errorInfo());
16 }
17 ?>
```

함수 적용 코드

```
1 <?php
2 $db = mysqli_connect('127.0.0.1', 'root', '', '210322');
3 session_start();
4
5 $ensubject = htmlspecialchars($_POST['subject']);
6
7 $sql = "
8     INSERT INTO board SET
9     subject = '{$ensubject}',
10    writer = '{$_POST['writer']}',
11    content = '{$_POST['content']}',
12    reg_date = now();
13 ";
14 if ($db->query($sql)) {
15     header('Location:./main.php');
16 } else {
17     print_r($db->errorInfo());
18 }
19 ?>
```

1-1. htmlspecialchars()

- 동일 스크립트 코드를 각각 subject와 content에 넣었을 때

subject

admin님 환영합니다. 로그아웃

자유 게시판

글쓰기

No.	제목	작성자	작성일
1	xss test	admin	2021-03-30 23:41:01
8	<script>alert(1)</script>	admin	2021-04-01 15:34:57

content

localhost 내용:

1

확인

목록 수정 삭제

자유 게시판

<script>alert(1)</script>

admin 2021-04-01 15:35:19

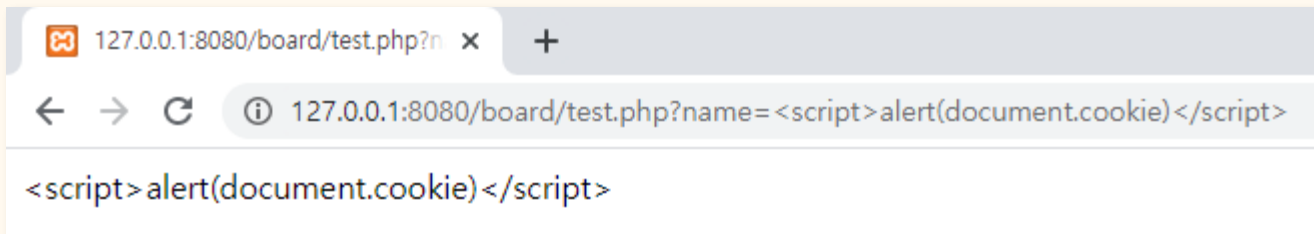
개발자 모드

```
<p style="font-size:20px;"><script>alert(1)</script></p>
▶<div style="margin-top:-15px">...</div>
▼<p style="font-size:15px;padding-top:28px;width:100%;">
  <script>alert(1)</script>
```

1-1. htmlspecialchars()

```
1  <?php
2      $db = mysqli_connect('127.0.0.1', 'root', '', '20210318');
3  ?>
4  <html>
5  <head>
6      <title></title>
7  </head>
8  <body>
9      <?php
10         echo htmlspecialchars($_GET['name']);
11     ?>
12 </body>
13 </html>
```

◀ test.php



1-1. htmlspecialchars()

- 특정 상황의 조건이 부합되면 우회 가능

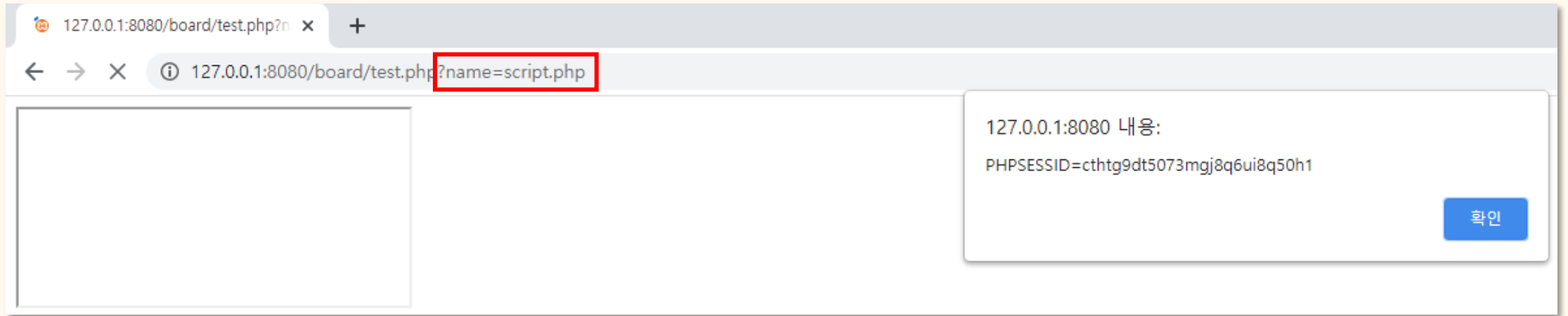
```
1  <?php
2      $db = mysqli_connect('127.0.0.1', 'root', '', '20210318');
3      session_start();
4  ?>
5  <html>
6  <head>
7      <title></title>
8  </head>
9  <body>
10     <?php
11         echo '<iframe src="" . htmlspecialchars($_GET['name']) .'"></iframe>';
12     ?>
13 </body>
14 </html>
```

◀ test.php

```
1  <?php
2      echo '<script>alert(document.cookie)</script>';
3  ?>
```

◀ script.php

1-1. htmlspecialchars()



- <iframe>
- <embed>
- <object>
-
- 등

2. strip_tags()

- 문자열에서 HTML 태그와 PHP 태그를 제거

기존 코드

```
1 <?php
2 $db = mysqli_connect('127.0.0.1', 'root', '', '210322');
3 session_start();
4
5 $sql = "
6     INSERT INTO board SET
7     subject = '{$_POST['subject']}',
8     writer = '{$_POST['writer']}',
9     content = '{$_POST['content']}',
10    reg_date = now();
11 ";
12
13 if ($db->query($sql)) {
14     header('Location:./main.php');
15 } else {
16     print_r($db->errorInfo());
17 }
18 ?>
```

함수 적용 코드

```
1 <?php
2 $db = mysqli_connect('127.0.0.1', 'root', '', '210322');
3 session_start();
4
5 $encontent = strip_tags($_POST['content']);
6
7 $sql = "
8     INSERT INTO board SET
9     subject = '{$_POST['subject']}',
10    writer = '{$_POST['writer']}',
11    content = '{$encontent}',
12    reg_date = now();
13 ";
14
15 if ($db->query($sql)) {
16     header('Location:./main.php');
17 } else {
18     print_r($db->errorInfo());
19 }
20 ?>
```

2. strip_tags()

자유 게시판

test

admin

`<script>alert(1)</script>`

◀ 글 작성

목록

수정 삭제

자유 게시판

test

admin 2021-04-01 19:31:25

alert(1)

◀ 글 확인

감사합니다.