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

```php
<?php
    $db = mysqli_connect('127.0.0.1', 'root', '', '210322');
    session_start();

    $sql = "
        INSERT INTO board SET
        subject = '{$_POST['subject']}',
        writer = '{$_POST['writer']}',
        content = '{$_POST['content']}',
        reg_date = now();
    ";
    if ($db->query($sql)) {
        header('Location:./main.php');
    } else {
        print_r($db->errorInfo());
    }
?>
```

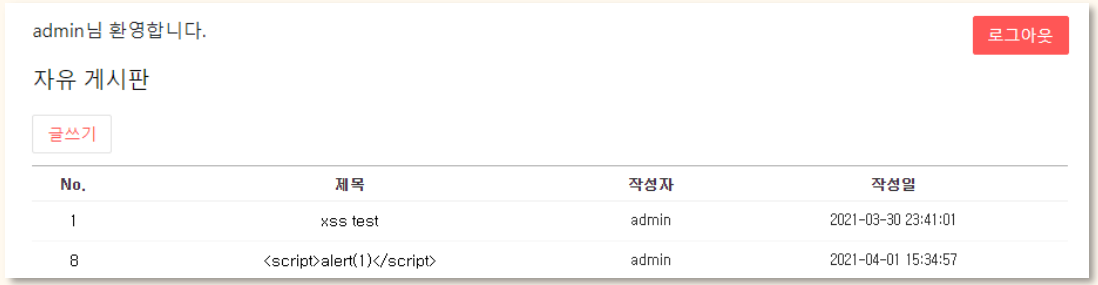
함수 적용 코드

```php
<?php
    $db = mysqli_connect('127.0.0.1', 'root', '', '210322');
    session_start();

    $ensubject = htmlspecialchars($_POST['subject']);

    $sql = "
        INSERT INTO board SET
        subject = '{$ensubject}',
        writer = '{$_POST['writer']}',
        content = '{$_POST['content']}',
        reg_date = now();
    ";
    if ($db->query($sql)) {
        header('Location:./main.php');
    } else {
        print_r($db->errorInfo());
    }
?>
```

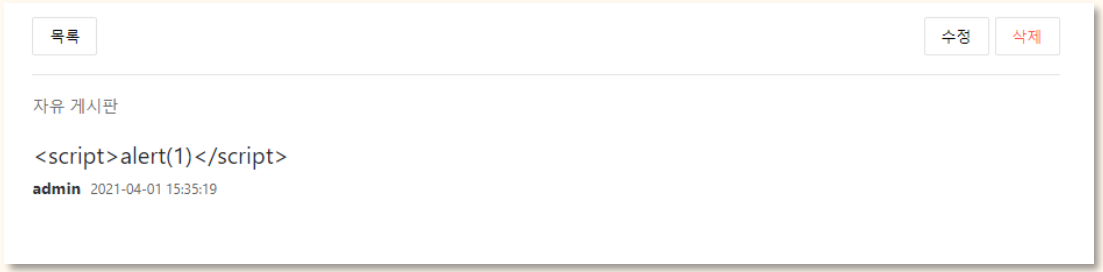
1-1. htmlspecialchars()

- 동일 스크립트 코드를 각각 subject와 content에 넣었을 때

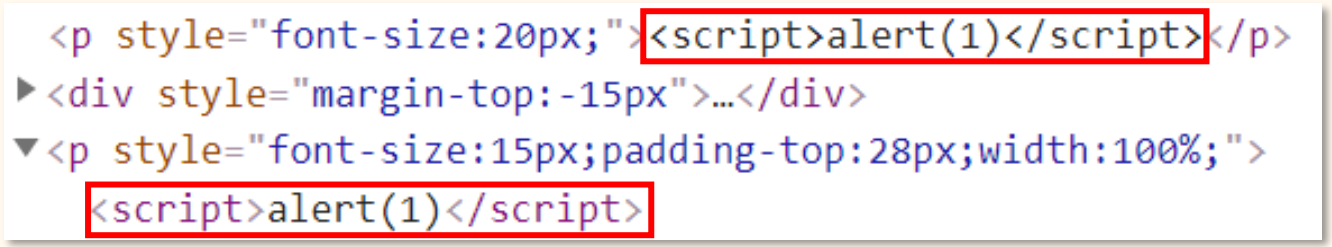
subject



content



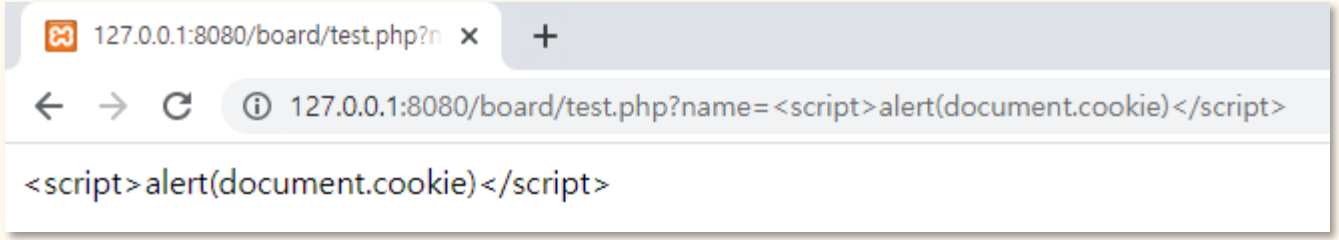
개발자 모드



1-1. htmlspecialchars()

```php
<?php
    $db = mysqli_connect('127.0.0.1', 'root', '', '20210318');
?>
<html>
<head>
    <title></title>
</head>
<body>
    <?php
        echo htmlspecialchars($_GET['name']);
    ?>
</body>
</html>
```

◀ test.php



1-1. htmlspecialchars()

- 특정 상황의 조건이 부합되면 우회 가능

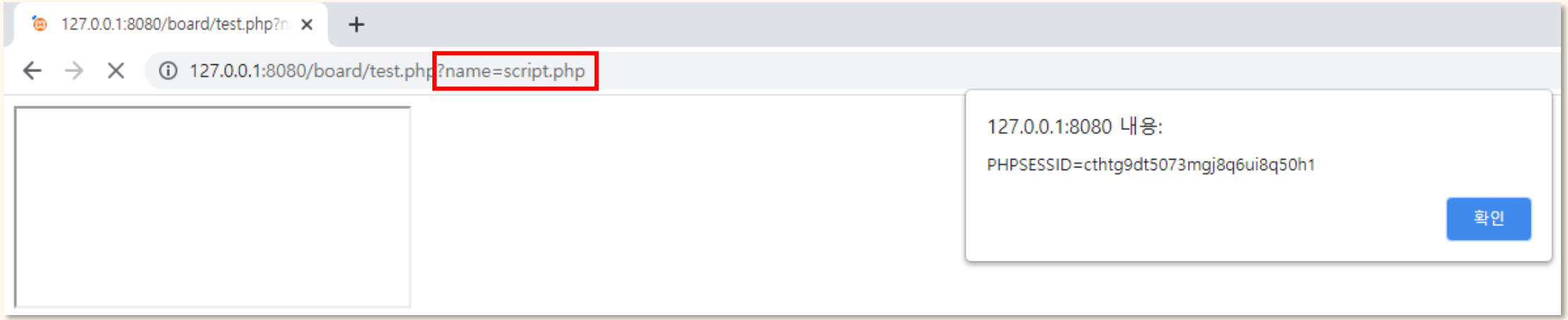
```php
<?php
    $db = mysqli_connect('127.0.0.1', 'root', '', '20210318');
    session_start();
?>
<html>
<head>
    <title></title>
</head>
<body>
    <?php
        echo '<iframe src="' . htmlspecialchars($_GET['name']) .'"></iframe>';
    ?>
</body>
</html>
```

◀ test.php

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

◀ script.php

1-1. htmlspecialchars()



- <iframe>
- <embed>
- <object>
- <img>
- 등

2. strip_tags()

- 문자열에서 HTML 태그와 PHP 태그를 제거

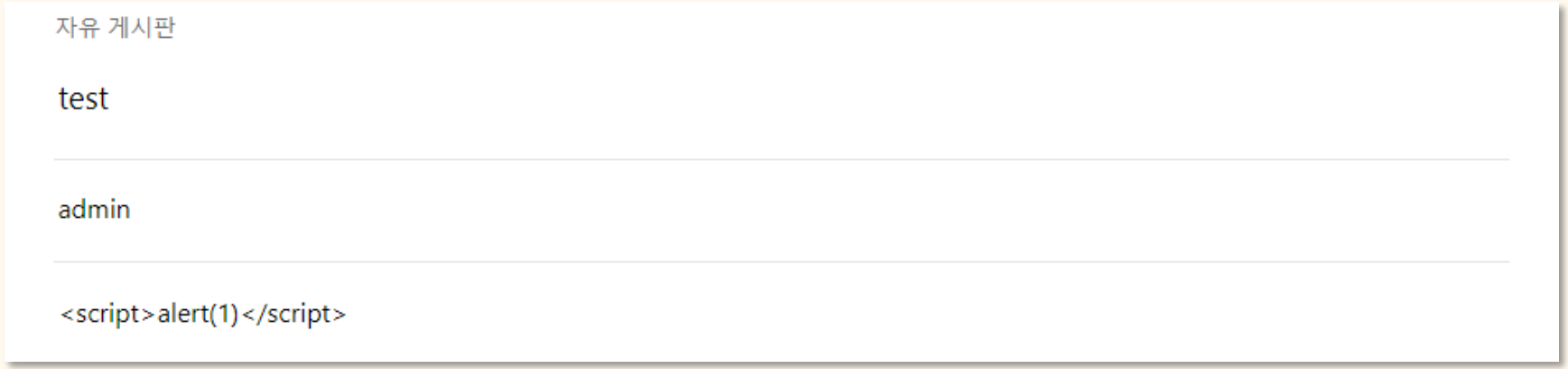
기존 코드

```php
<?php
    $db = mysqli_connect('127.0.0.1', 'root', '', '210322');
    session_start();

    $sql = "
        INSERT INTO board SET
        subject = '{$_POST['subject']}',
        writer = '{$_POST['writer']}',
        content = '{$_POST['content']}',
        reg_date = now();
    ";

    if ($db->query($sql)) {
        header('Location:./main.php');
    } else {
        print_r($db->errorInfo());
    }
?>
```

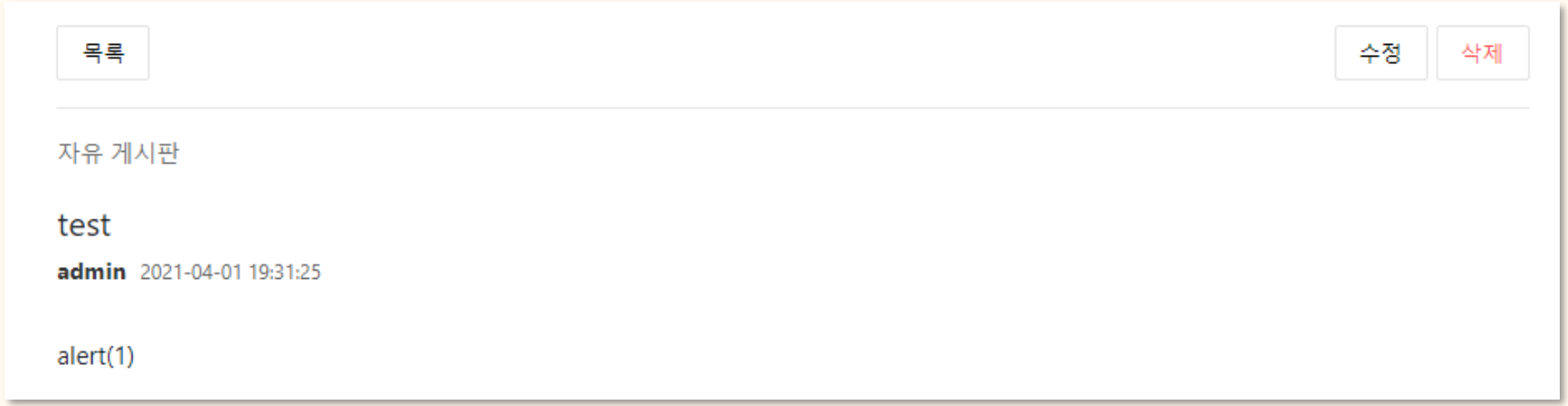
함수 적용 코드

```php
<?php
    $db = mysqli_connect('127.0.0.1', 'root', '', '210322');
    session_start();

    $encontent = strip_tags($_POST['content']);

    $sql = "
        INSERT INTO board SET
        subject = '{$_POST['subject']}',
        writer = '{$_POST['writer']}',
        content = '{$encontent}',
        reg_date = now();
    ";

    if ($db->query($sql)) {
        header('Location:./main.php');
    } else {
        print_r($db->errorInfo());
    }
?>
```

2. strip_tags()



◀ 글 작성



◀ 글 확인

감사합니다.