



[PHP + MySQL] 게시판 구현 2

2020/08/03 이유경

목차

1. php 코드

1) view.php

2) update.php

3) update_check.php

4) delete.php

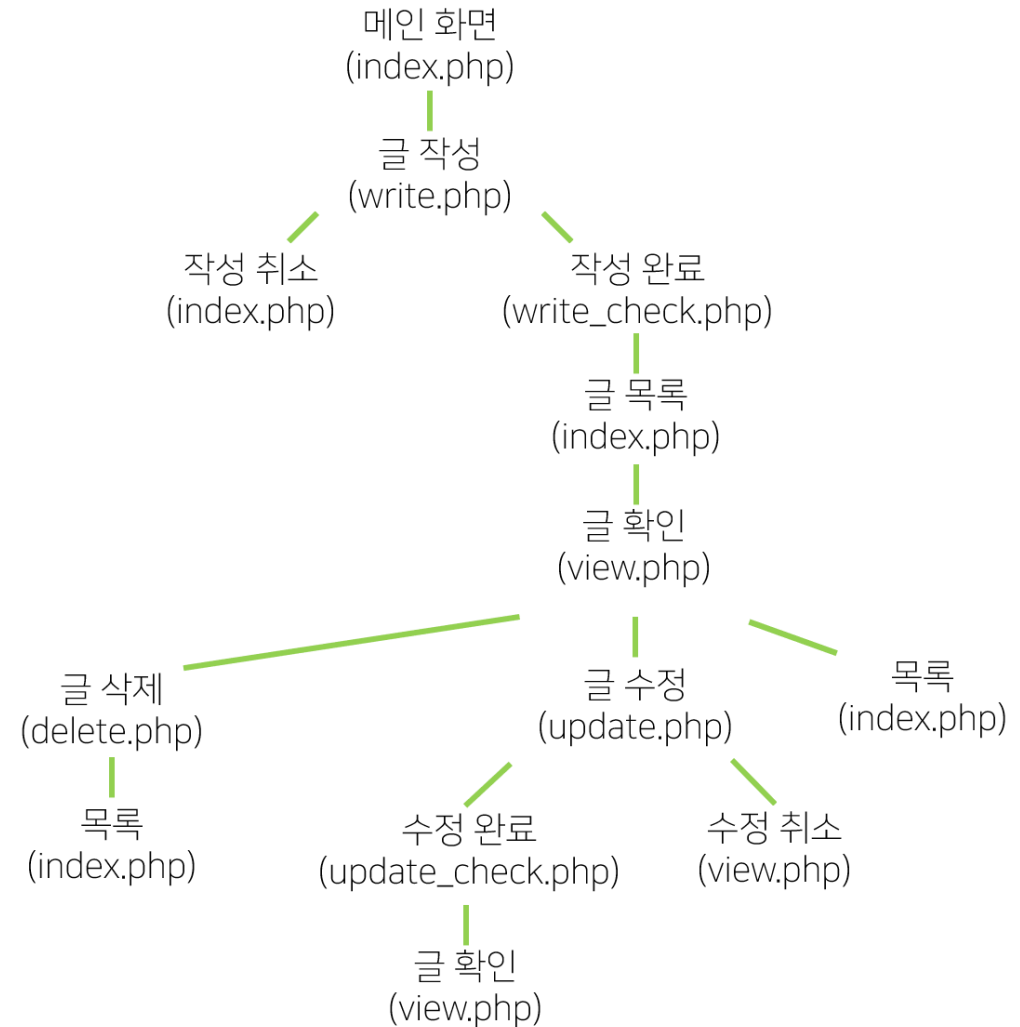
2. XSS 실습

1. php 코드

게시판 구성 / 구조

- index.php
- write.php
- write_check.php

- view.php
- update.php
- update_check.php
- delete.php



1. php 코드

1) view.php

PDO(PHP Data Object)란?

다양한 종류의 데이터베이스를
같은 방식으로 다룰 수 있게 해준다.

```

1  <?php
2  $db = new PDO("mysql:host=127.0.0.1;dbname=training;charset=utf8","root","1234");
3
4  $sql = "SELECT * FROM board WHERE idx = '{$_GET['idx']}'";
5  $row = $db->query($sql)->fetch();
6
7  ?>
8  <!DOCTYPE html>
9  <html lang="en">
10 <head>
11   <meta charset="UTF-8">
12   <title>게시물 조회</title>
13 </head>
14 <body>
15   <ul>
16     <li>글번호: <?php echo $row['idx'] ?></li>
17     <li>작성자: <?php echo $row['writer'] ?></li>
18     <li>제목: <?php echo $row['subject'] ?></li>
19     <li>작성 시간: <?php echo $row['reg_date'] ?></li>
20     <li>내용: <?php echo $row['content'] ?></li>
21   </ul>
22   <p>
23     <a href="./update.php?idx=<?php echo $row['idx'] ?>">수정</a>
24     <a href="./delete.php?idx=<?php echo $row['idx'] ?>">삭제</a>
25     <a href="./index.php">목록</a>
26   </p>
27 </body>
28 </html>

```

DB 연결

DB에서 데이터 불러오기

Fetch : 단일 데이터
FetchAll : 다중 데이터

update.php (수정)페이지로 이동

1. php 코드

2) update.php

```
$_POST['subject']
$_POST['writer']
$_POST['content']
```

```
1 <?php
2 $db = new PDO("mysql:host=127.0.0.1;dbname=training;charset=utf8","root","1234");
3
4 $sql = "SELECT * FROM board WHERE idx = '{$_GET['idx']}'";
5 $row = $db->query($sql)->fetch();
6 ?>
7 <!DOCTYPE html>
8 <html lang="en">
9 <head>
10 <meta charset="UTF-8">
11 <title>게시물 작성</title>
12 </head>
13 <body>
14 <form action="./update_check.php?idx=<?php echo $_GET['idx']?>" method="post">
15 <fieldset>
16 <legend>글작성</legend>
17 <ul>
18 <li>
19 <label>
20 제목
21 <input type="text" name="subject" value="<?php echo $row['subject']?>">
22 </label>
23 <button type="submit">완료</button>
24 <button type="button" onclick="location.href = './view.php?idx=<?php echo $row['idx']?>'>취소</button>
25 </li>
26 </ul>
27 </fieldset>
28 </form>
29 </body>
30 </html>
```

게시물 데이터 가져오기

method="post"

Get방식: \$_GET
Post방식: \$_POST

게시물의 제목이 기본값으로 입력

1. php 코드

3) update_check.php

```
1  <?php
2  $db = new PDO("mysql:host=127.0.0.1;dbname=training;charset=utf8","root","1234");
3
4  $sql = "
5      UPDATE board SET
6      subject = '{$_POST['subject']}',
7      writer = '{$_POST['writer']}',
8      content = '{$_POST['content']}'
9      WHERE idx = '{$_GET['idx']}'
10 ";
11
12 if ($db->query($sql)) {
13     header('Location:../view.php?idx='.$_GET['idx']);
14 } else {
15     print_r($db->errorInfo());
16 }
```

DB 연결

쿼리문 작성

쿼리문 실행

1. php 코드

4) delete.php

```
1  <?php
2  $db = new PDO("mysql:host=127.0.0.1;dbname=training;charset=utf8","root","1234");
3
4  $sql = "
5      DELETE FROM board WHERE idx = '{$_GET['idx']}';
6  ";
7
8  if ($db->query($sql)) {
9      header('Location:../index.php');
10 } else {
11     print_r($db->errorInfo());
12 }
```

DB 연결

쿼리문 작성

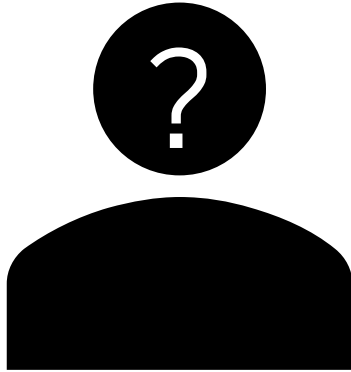
쿼리문 실행

2. XSS 실습

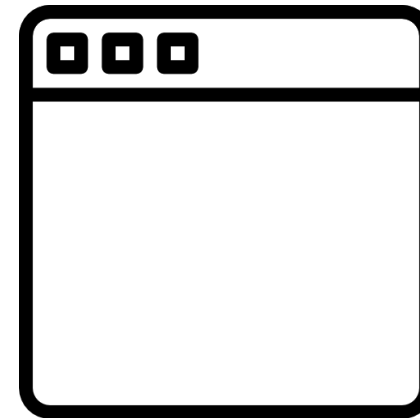
XSS : cross site scripting

웹사이트 관리자가 아닌 이가 웹 페이지에 악성 스크립트를 삽입하는 공격 기법

<script>
악성 스크립트
</script>



Hacker



Web Site

2. XSS 실습

XSS

```
<script>alert("SCP");</script>
```

글작성

- 제목
- 작성자
- 내용
-

127.0.0.1:8080 내용:

SCP

확인

```
<!DOCTYPE html>
<html lang="en">
  <script>...</script>
  <head>...</head>
  <body>
    <ul>
      <li>글번호: 57</li>
      <li>작성자: 작성자</li>
      <li>제목: xss실습</li>
      <li>작성 시간: 2020-08-03 02:18:28</li>
      <li>
        "내용: "
        <script>alert("SCP");</script> == $0
      </li>
    </ul>
    <p>...</p>
  </body>
</html>
```

QnA