

Лабораторная работа 8. Часть 1.
Предотвращение атак, связанных с XSS

Индивидуальность отчетов:

Как минимум, в имени пользователя ОС

Обязательно скриншотить каждый этап и пояснять

Обязательно выводы должны быть

1. Откроем ранее созданную виртуальную машину Ubuntu

2. Создадим таблицу comments в базе edu

С полями:

id int primary A_I

name varchar 100

text varchar 255

The screenshot shows the phpMyAdmin web interface. The browser address bar indicates the URL is `edu.local/phpmyadmin/tbl_create.php?server=1&db=edu`. The interface is for a server at `localhost:3306` and a database named `edu`. The 'Table name' field is set to `comments`, and the 'Add' button is visible. The table structure is being defined with the following columns:

Name	Type	Length/Values	Default	Collation	Attributes	Null	Index	A_I	Co
id	INT		None			<input type="checkbox"/>	PRIMARY	<input checked="" type="checkbox"/>	
name	VARCHAR	100	None			<input type="checkbox"/>	---	<input type="checkbox"/>	
text	VARCHAR	255	None			<input type="checkbox"/>	---	<input type="checkbox"/>	
	INT		None			<input type="checkbox"/>	---	<input type="checkbox"/>	

At the bottom, the 'Table comments:' field is empty, and the 'Storage Engine:' is set to InnoDB.

3. Создадим папку /var/www/edu/comments

4. Создадим файл style.css

```
1  ▾ .form {
2      width: 300px;
3      margin-top: 50px;
4      margin-left: auto;
5      margin-right: auto;
6  }
7
8  ▾ .form div {
9      margin-bottom: 10px;
10 }
11
12 ▾ .form input {
13     width: 100%;
14 }
15
16 ▾ .form textarea {
17     width: 100%;
18     height: 150px;
19 }
20
21 ▾ .comments {
22     width: 300px;
23     margin-top: 100px;
24     margin-left: auto;
25     margin-right: auto;
26 }
27
28 ▾ .comments__item {
29     margin-top: 30px;
30 }
31
32 ▾ .comments__name {
33     color: ■ #969696;
34 }
35
```

5. Создадим файл index.php

```
1  <?php
2  $dbh = new PDO('mysql:host=localhost;dbname=edu', 'newuser', '123');
3  $name = $_POST["name"];
4  $comment = $_POST["comment"];
5  if (!empty($name) && !empty($comment)) {
6      $sql = "INSERT INTO `comments` (`name`, `text`) VALUES (:name, :text)";
7      $stmt = $dbh->prepare($sql);
8      $stmt->bindParam(":name", $name, PDO::PARAM_STR);
9      $stmt->bindParam(":text", $comment, PDO::PARAM_STR);
10
11     if (!$stmt->execute()) {
12         echo "ERROR";
13     }
14 }
15
16 $sql = "SELECT `name`, `text` FROM `comments`";
17 $comments = $dbh->prepare($sql);
18 $comments->execute();
19
20 ?>
21 <html>
22
23 <head>
24     <title>Комментарии</title>
25     <link rel="stylesheet" href="./style.css" />
26 </head>
27
28 <body>
29     <section class="form">
30         <form action="" method="POST">
31             <div>Имя:</div>
32             <div><input name="name" type="text"></div>
33             <div>Комментарии:</div>
34             <div><textarea name="comment"></textarea></div>
35             <div><input type="submit"></div>
36         </form>
37     </section>
38
39     <section class="comments">
40         <h1>Комментарии</h1>
41         <div>
42
43 <?php
44 foreach ($comments->fetchAll() as $row) {
45     echo '<div class="comments__item">';
46     echo '<div class="comments__name">' . $row['name'] . '</div>';
47     echo '<div>' . $row['text'] . '</div>';
48     echo '</div>';
49 }
50 ?>
51
52     </div>
53 </section>
54
55 </body>
56
57 </html>
58
```

6. Создадим файл reflected.php

```
1  <?php
2  $category_name = $_GET["category"];
3
4  echo "<p>Category: " . $category_name . "</p>";
5
```

7. Создадим файл dom.html

```
1  <script>
2      let hash = window.location.hash.substring(1);
3      eval(hash);
4  </script>
```

8. /var/www/edu/comments должна иметь такой вид

```
a@a:/var/www/edu/comments$ ls -l -a
total 24
drwxr-xr-x 2 www-data www-data 4096 окт 6 03:39 .
drwxrwxr-x 3 www-data www-data 4096 окт 6 02:39 ..
-rwxr-xr-x 1 www-data www-data 81 окт 6 03:39 dom.html
-rwxr-xr-x 1 www-data www-data 1325 окт 6 03:09 index.php
-rwxr-xr-x 1 www-data www-data 91 окт 6 03:13 reflected.php
-rwxr-xr-x 1 www-data www-data 386 окт 6 02:41 style.css
```

9. Использовать XSS

Использовать в качестве вредоносного кода:

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

Либо:

alert(1);

На страницах поэксплуатировать уязвимость в учебных целях:

<http://edu.local/comments>

<http://edu.local/comments/reflected.php>

<http://edu.local/comments/dom.html>

В отчет добавить скриншоты и пояснения для каждого случая