Barbarossa XSS Challenge 5

1. First, when I'm reviewing the PHP source code, I found that the user input reflects into two places. The first place in value attribute in input tag, and the second place in src attribute in img tag but all of them were sanitized with htmlspecialchars() function.

2. I try to inject special characters to see how the website interacts with it, so I entered (test'"<>) and I was surprised. In input tag he deal with special characters as string, but in img tag, he consider (') as a normal special character (does not filter it) and encrypt all the others.

```
<input type="text" id="imgSrc" name="imgSrc" value="test'"<>">
```

```
<img src="test" &quot;&lt;&gt;'>
```

3. I try this payload (test' onerror='alert()) and it quickly got to work.

```
<img src="test" onerror="alert()">
```