Отчет по HTML Injection 14.2 - 14

Tester: Stanley Ford

Lab 14.2:

• General information:

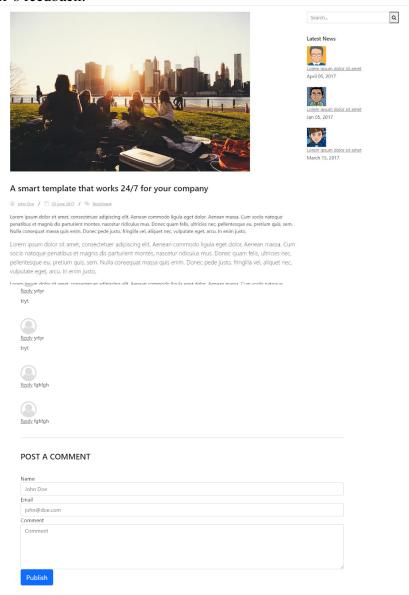
• Testing period: 22/01/2023

• Test object: http://51.250.73.193:8082/

Description of actions:

So, I received a request to check this resource with a clear emphasis on the possibility of leaving feedback by users.

After a quick glance at the page, I counted four fields with the ability to enter, where you can enter user's feedback:



- 1. Search field
- 2. Name field
- 3. E-mail field
- 4. Comment field

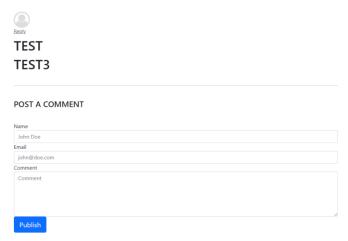
I checked each of them for vulnerability to the HTML Injection attack type. I tried to add arbitrary header text to each of the available fields by entering the HTML code <h1>Test</h1>:

- 1. The test of the Search field didn't add my "Test" string to the end of the page, so the code didn't pass and that's fine.
- 2. There is a check in the Email field that does not allow you to enter an HTML tag into it. It is good that such a check exists. This is to be praised.

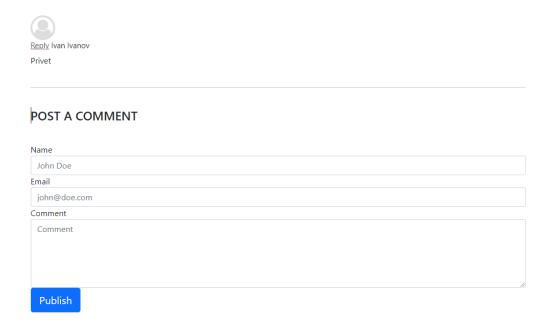
POST A COMMENT



3. However, the problems started right after that. The HTML injection in the fields with the name and content of the comment went smoothly and the test headers were added to the new comment.



For example, here's what a valid comment looks like:



This result indicates a vulnerability in the Name and Comment fields.

Since there is a technical task regarding the creation of forms, I then tried to create an HTML form using the <form" tag>

POST A COMMENT

Name			
123213			
Email			
john@dum.com			
Comment			
<form>HACKED HA</form>	HA		
Publish			

After clicking the "Publish" button, I was taken to a page with the flag: flag{Htm1_1nj3ct10n_\$0lut10n_fl@g}

Lab passed:)

Self-Assessment Questions:

• List the tools (programs and utilities) that you used to solve this lab:

Web Browser

• List the vulnerabilities you've discovered:

HTML Injection

• Give advice on how to improve security:

Add a check for characters like <, >, / and in general HTML tags to the POST request for the Name and Comment fields.