

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:




Latest News



Lorem ipsum dolor sit amet
April 05, 2017



Lorem ipsum dolor sit amet
Jan 05, 2017



Lorem ipsum dolor sit amet
March 15, 2017


A smart template that works 24/7 for your company

John Doe / 29 June 2017 / Bootstrap


Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean commodo ligula eget dolor. Aenean massa. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Donec quam felis, ultricies nec, pellentesque eu, pretium quis, sem. Nulla consequat massa quis enim. Donec pede justo, fringilla vel, aliquet nec, vulputate eget, arcu. In enim justo,

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean commodo ligula eget dolor. Aenean massa. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Donec quam felis, ultricies nec, pellentesque eu, pretium quis, sem. Nulla consequat massa quis enim. Donec pede justo, fringilla vel, aliquet nec, vulputate eget, arcu. In enim justo,


Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean commodo ligula eget dolor. Aenean massa. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Donec quam felis, ultricies nec, pellentesque eu, pretium quis, sem. Nulla consequat massa quis enim. Donec pede justo, fringilla vel, aliquet nec, vulputate eget, arcu. In enim justo,



Reply yrtyr
tryt



Reply fghfgh
tryt



Reply fghfgh

POST A COMMENT

Name

John Doe

Email

john@doe.com

Comment

Comment

Publish

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


Name

Email

Comment

 A part followed by '@' should not contain the symbol '<'.

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.

 Reply

TEST
TEST3


POST A COMMENT

Name

Email

Comment

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



[Reply](#) Ivan Ivanov
Privet

POST A COMMENT

Name

Email

Comment

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

Email

Comment

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.