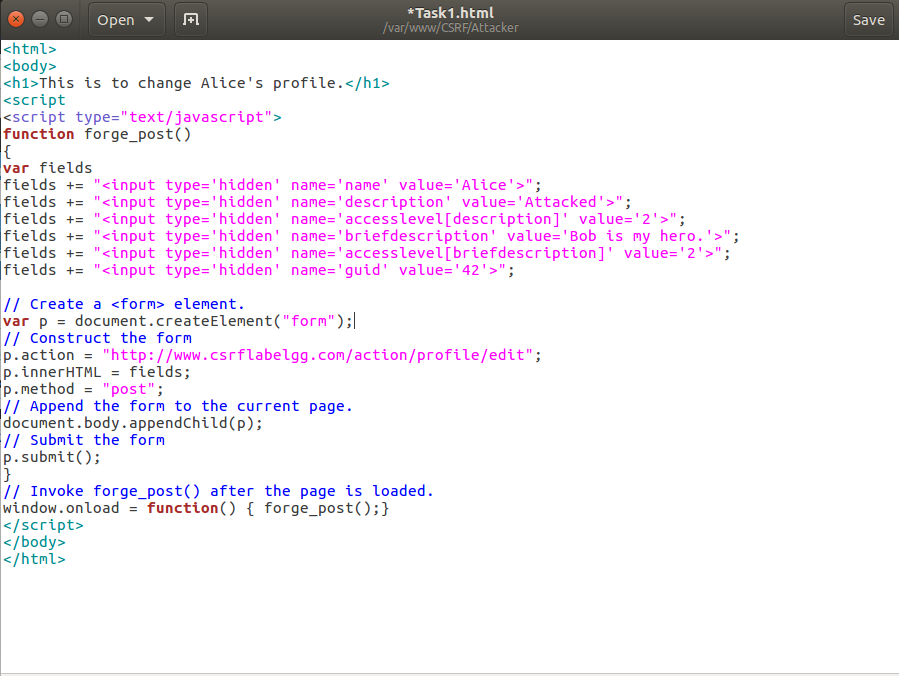
SY1939111-张思嘉

Task 1：CSRF Attack- Change Alice’s Profile with spoofed Post request

1. **The Attacker website’s source code:**

The html file can be found here.



1. **Screenshot of the CSRF Attack:**

|  |  |
| --- | --- |
| Before Hacked | After Hacked |

1. **Explain the logic as to how the attack works, mention the key aspect of your code.**

CSRF Attack uses the feature of Browser automatically attach cookie when sending message to web server with same origin.

The performed attack tricks Alice to click a malicious link. The malicious webpage contains a form pointing to Alice’s edit profile API. When loading the malicious web page, Alice’s browser sends a change profile request to Elgg server, and automatically attach Alice’s authentication info (Cookie).

Therefore, the attacker can change Alice’s profile by tricking Alice to click a malicious link and forge a POST request. To construct the POST request, a form tag is created.

The tag points to

The request method is set to be POST:

The request body is constructed with variance field:

Within the request body, 3 kinds of parameters are required, name, profile information and guid. The three kinds of parameters are set subsequently.

