CIS 643 Computer Security

Lab 8 Cross-Site Request Forgery (CSRF) Attack Lab

**Instructor: Wenliang (Kevin) Du**

Contents

Task 1: Modifying the Victim’s Profile 2

POST request form 2

CSRF attacks 3

Visit the attacker page 4

Task 2: Implementing a countermeasure for Collabtive 4

Step One: Add secret-token in the body of the request. 4

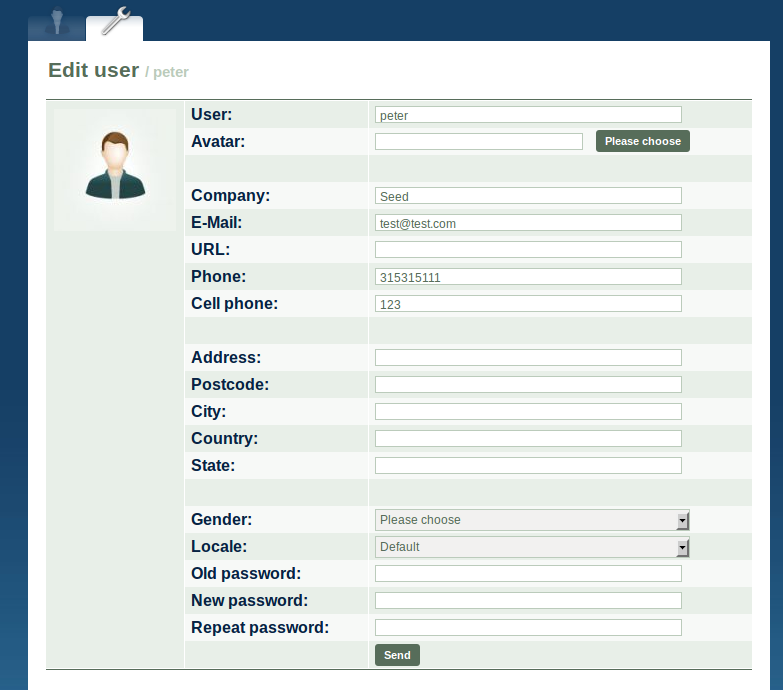
Step Two: Validate the secret-token. 4

Step Three: Validate countermeasure. 5

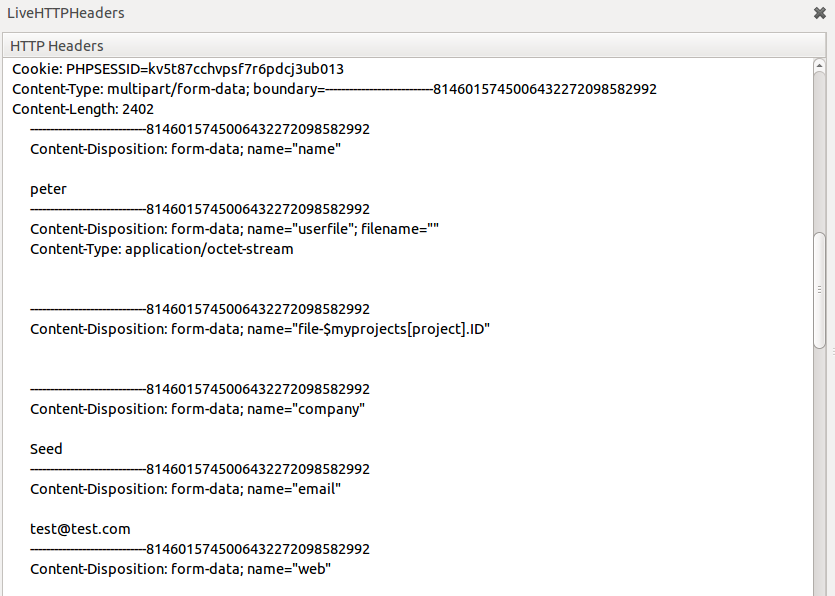
## Task 1: Modifying the Victim’s Profile

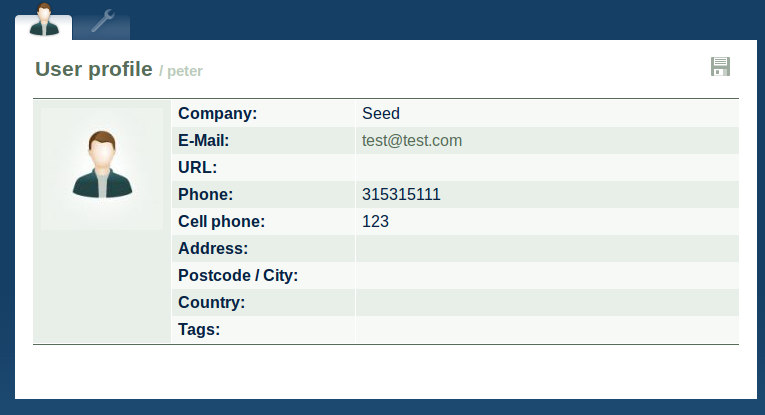
### POST request form

When we submit a form from page by post request, the web application will submit all information we leave in the inputs inside the form



From the HttpHeader, we could see the data that send to the form



Base on the sent information, the server will update the profile of user:

### CSRF attacks

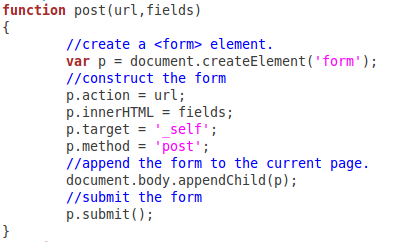
Use gedit with root permission to modify the attack page

Macintosh HD:Users:Ider:Desktop:Screen Shot 2011-11-07 at 6.37.59 PM.png

The forge form data

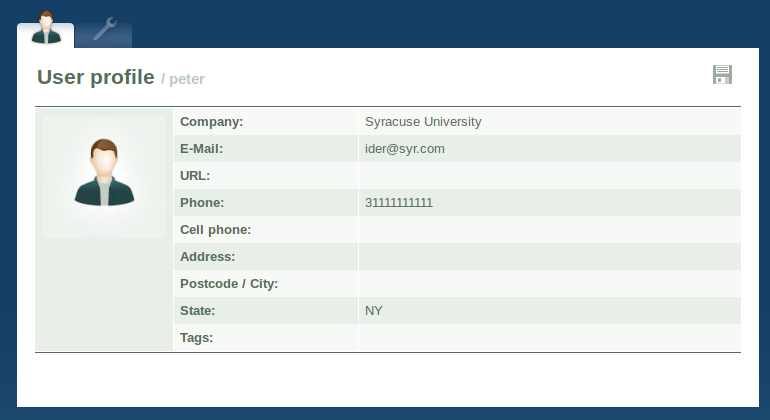


Use JavaScript to implement post request:



### Visit the attacker page

Visit the <http://www.crsflabattacker.com>. It we redirect us to the user profile, but we could find that the profile has been already modified with the forge data

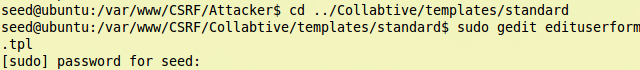


We have done the CRSF successfully.

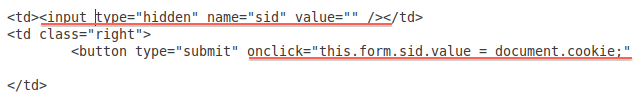
## Task 2: Implementing a countermeasure for Collabtive

### Step One: Add secret-token in the body of the request.

Using gedit to open edituserform.tpl with root permission



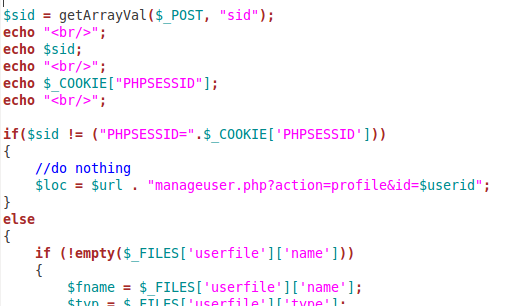
Add secret token, and assigned a value to the token when the submit button clicked:



### Step Two: Validate the secret-token.

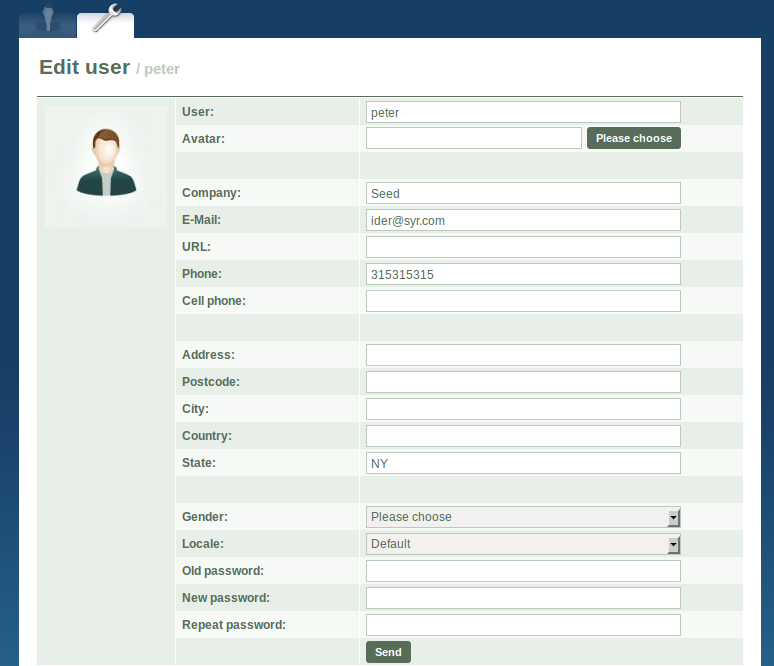
Using gedit to open manageruser.php with root permission

Macintosh HD:Users:Ider:Desktop:Screen Shot 2011-11-07 at 6.59.48 PM.png

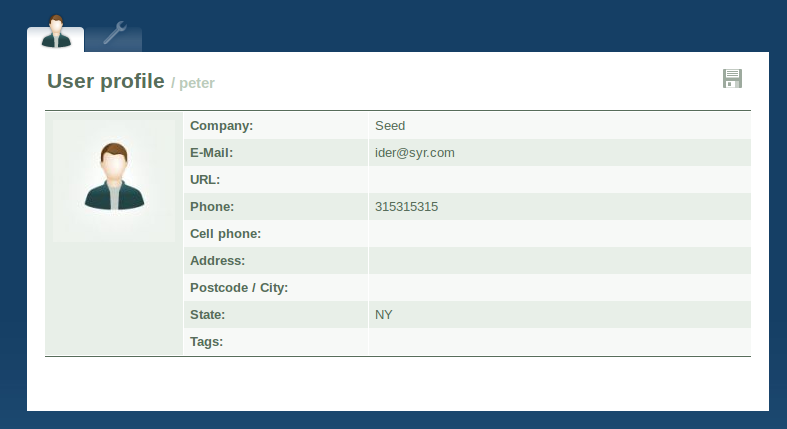
Get the secrete value using getArrayVal(), compare it with the COOKIER value on the server side, if they does not match, do nothing.

### Step Three: Validate countermeasure.

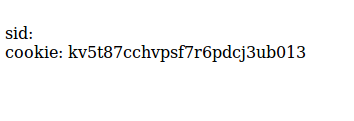
Use the real page to modify the user profile



We could update the user information successfully



But if we want to attack the page, we would not reach the page, as the cookies do not match.



So the countermeasure works fine.