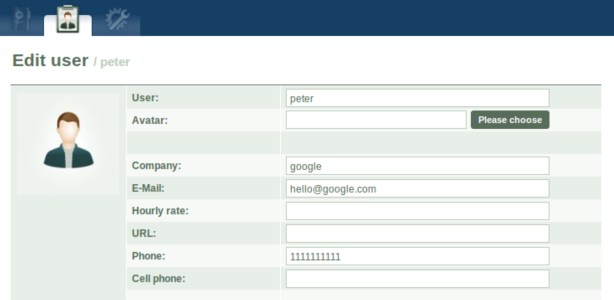
Lab 8 : Cross-Site Request Forgery (CSRF) Attack Lab

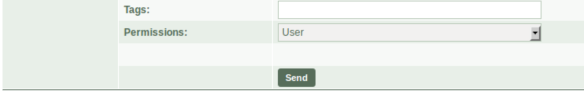
Yukui Ye

SUID: 439644268

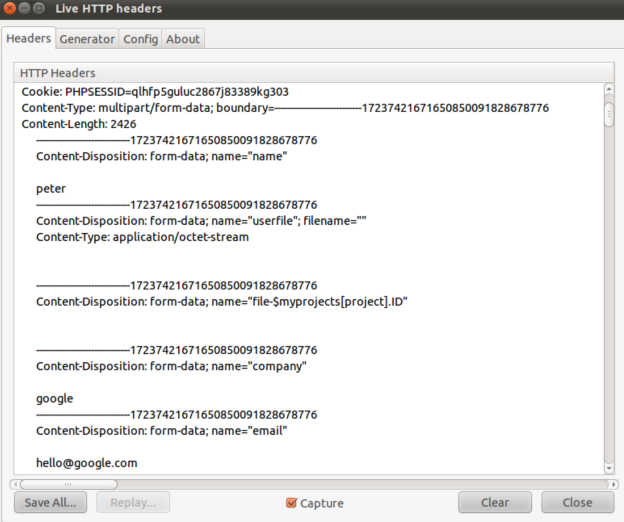
Task1 : Modifying the Victim’s Profile



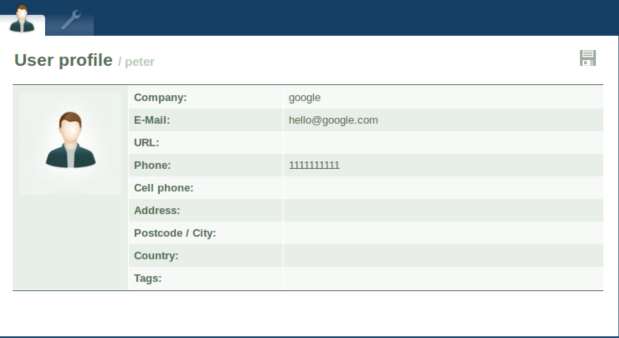
POST a request form: The web application will submit all information we leave inside the form at the time we submit a form from a page by POST request.



After we click submit. From the LiveHTTP headers, we can see all the data we send through this page.



The server update the user profile based on the data.

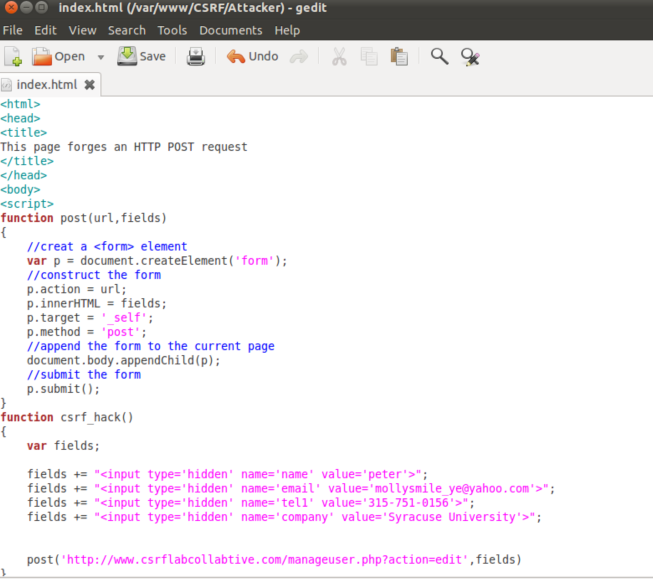


CSRF attacks:

Modify the attack page ,first change the file permission for enabling being modified.

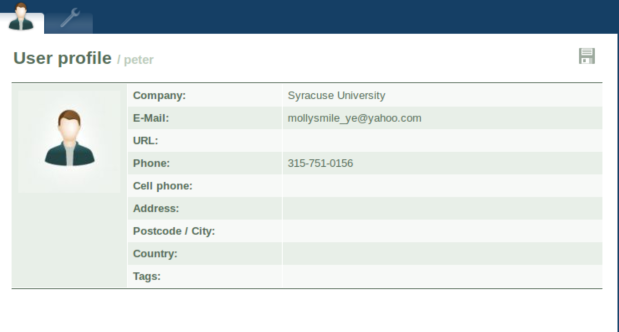
Macintosh HD:Users:yukuiye:Desktop:1.png

modify the file by using gedit: Use JavaScript to implement post request & The forge form data





Then visit the [www.csrflabattacker.com](http://www.csrflabattacker.com), it will link to the login page, use peter to login, we can see from the following screenshot, we successfully modified the user’s information by using the forge data.

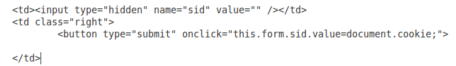


Task2: Implementing a countermeasure for Collabtive

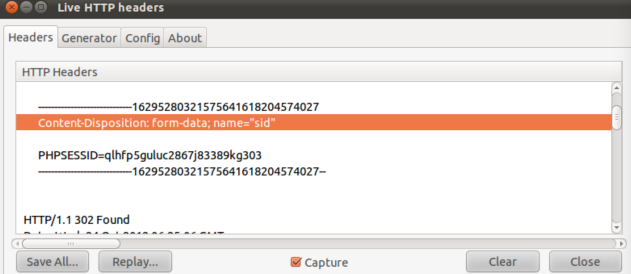
Step One: Add secret-token in the body of the request by using gedit to open edituserform.tpl with root permission.

Macintosh HD:Users:yukuiye:Library:Application Support:QQ:Users:394852457:QQ:Temp.db:DB34DB72-4507-4B6C-BBAD-EA17DAB2D784.png

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

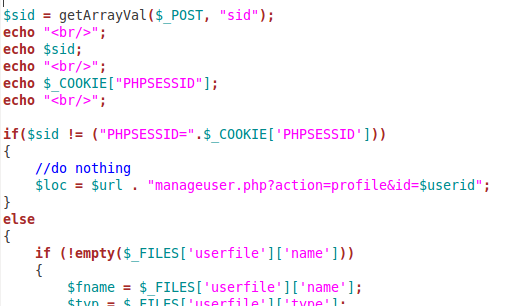


we can tell from the result from the following picture.

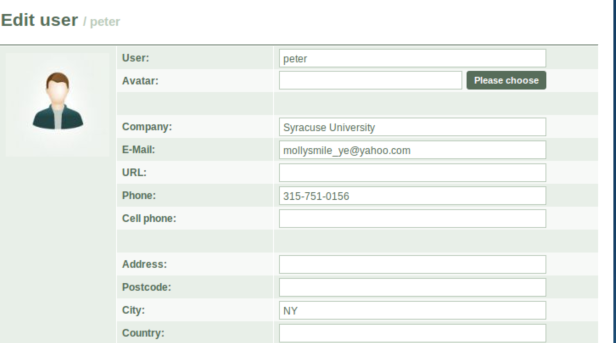


Step two: Validate the secret-token by using gedit to open manageruser.php with root permission.

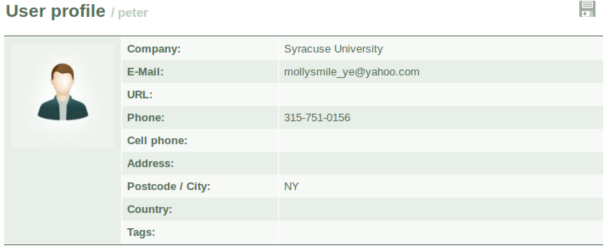




Step Three: Validate countermeasure : Modify user profile by using real page.



we can successfully update the user information



But when we are trying to attack the page, it cannot reach the page, due to cookies does not match.

sid:

cookie:

Macintosh HD:Users:yukuiye:Library:Application Support:QQ:Users:394852457:QQ:Temp.db:97C61FB8-486B-4C08-B6B5-CB5A1E695569.png

Therefore the countermeasure does work well.