**Lab: CSRF vulnerability with no defenses**

Graphical user interface, application

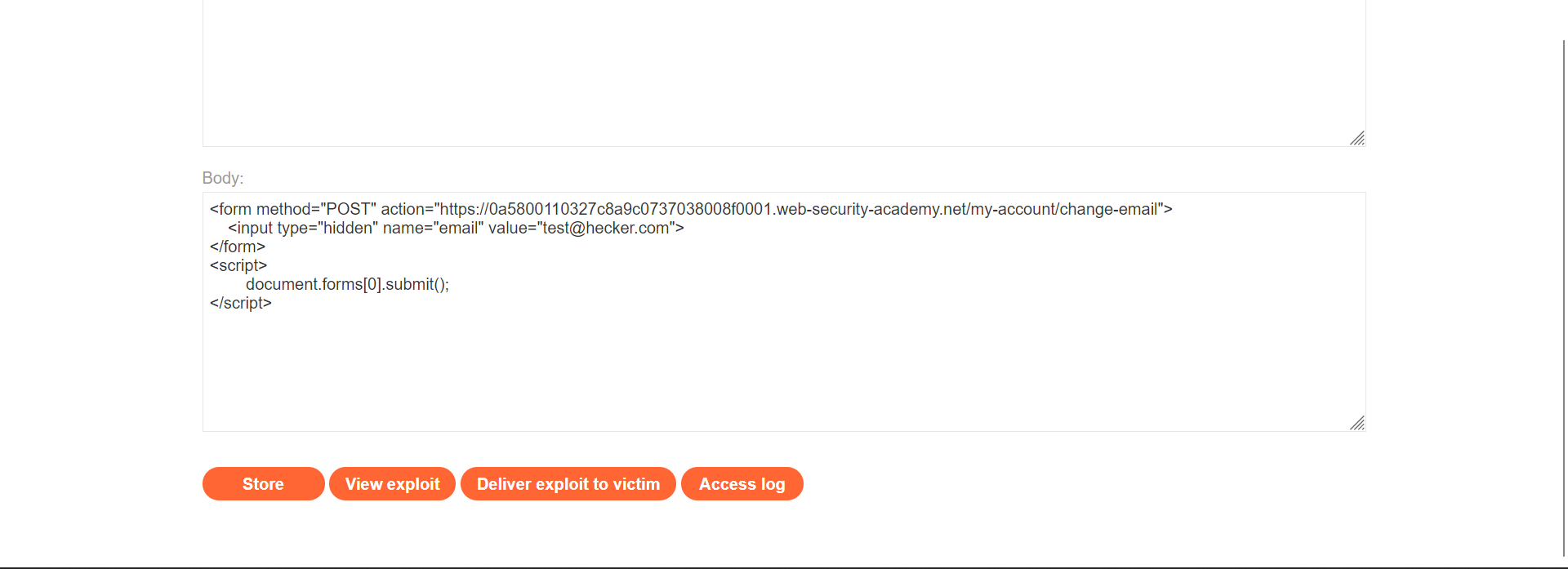
Description automatically generatedGiven lab’s update email function is vulnerable to CSRF attacks. We need use some html code which use to done CSRF attacks and upload it to the victim’s browser to exploit the vulnerability. We can use the exploit server given by the portswigger. First, we need to log the given account using the mentioned username and password.

The following part is the vulnerable section in this application.

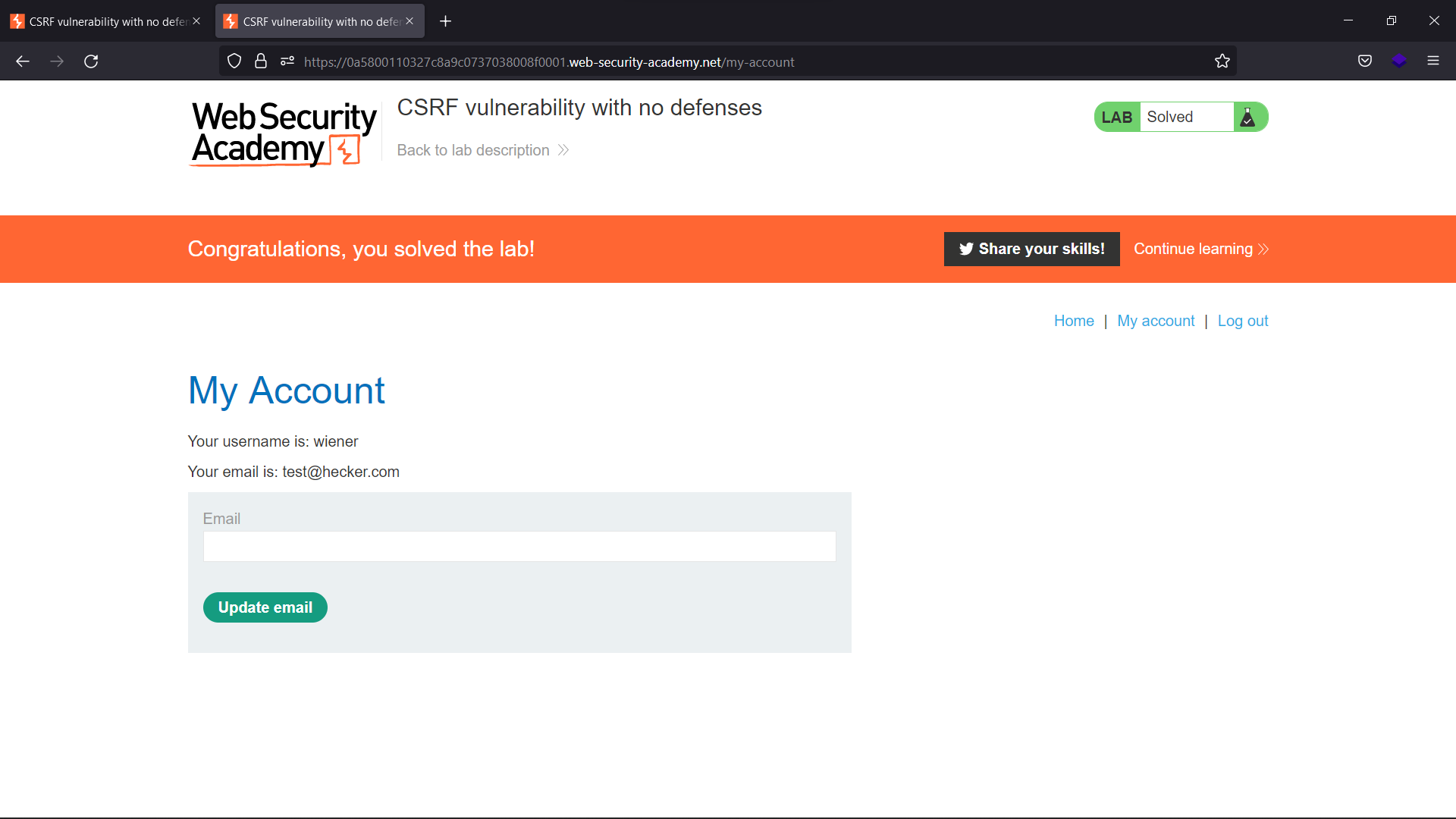
Graphical user interface, application

Description automatically generated

Then click the “Go to exploit server” and create the CSRF Poc code with burp suite professional edition, otherwise you can use the code given by portswigger itself. Then we need to fill the several parameters as method as post , URL to as following figure, email as name, and your created email as valid temporary email.



Then press the button Deliver to exploit to the victim. For confirmation of this attack press view exploit and see whether email as you enter in the code.



# Lab: CSRF where token validation depends on request method

This lab’s update email function is vulnerable for several request types. It defenses against the CSRF attacks, but not covered all the types of requests. To compromise this lab, we need to use given exploit server and HTML language script.

First, we need to login using given credentials as previous labs.Graphical user interface, application

Description automatically generated

After login to your account, if you have burp suite professional version you can use it create CSRF poc file. If haven’t that no need to worry, portswigger is given a template and you can use it to solve the lab. Script is given in the lab starting page and modify the content as following.

Graphical user interface, text, application, email

Description automatically generated

As previous labs, after modifying the code you must store it on the server and deliver exploit to the victim. Now the lab is solved. If you want to confirm the exploitation you go view exploit.

Graphical user interface

Description automatically generated

# Lab: CSRF where token validation depends on token being present

This lab is also vulnerable to csrf. If there is a csrf token, it will be validated or not, but if there isn’t a csrf token, it won’t execute the validation process. After login to the account, we need to go to the exploit server.

Text

Description automatically generated

As previous labs, edit the given html template as above figure and store it on the server and deliver the exploit to victim. If the request is analyzing with the burp suite, we can see the csrf token is there. If we change token and try to submit, result gives us as a bad request error and show invalid csrf token message. So, we can remove the csrf parameter and the token, then generate the html code.

Graphical user interface, text, website

Description automatically generated