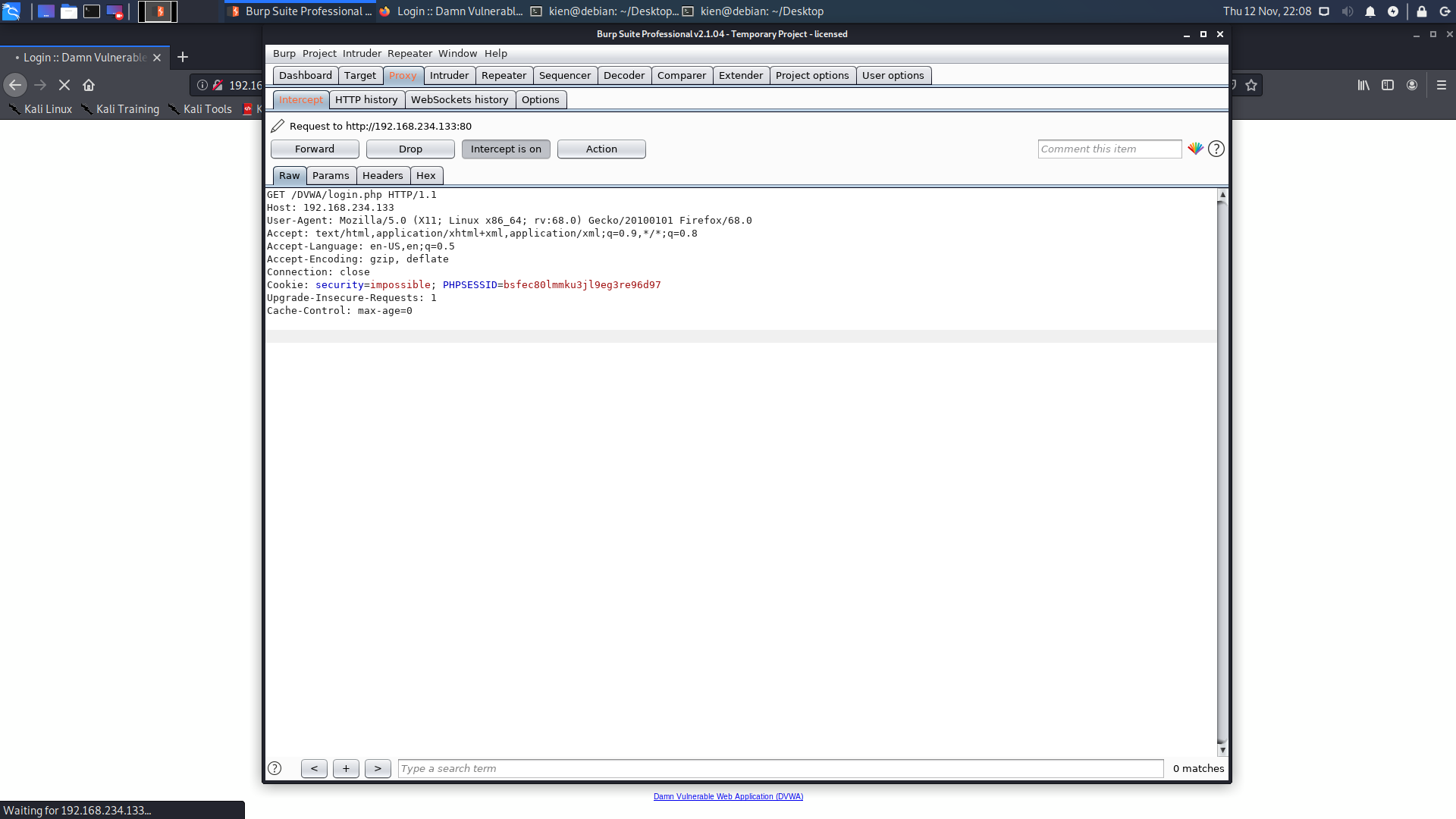
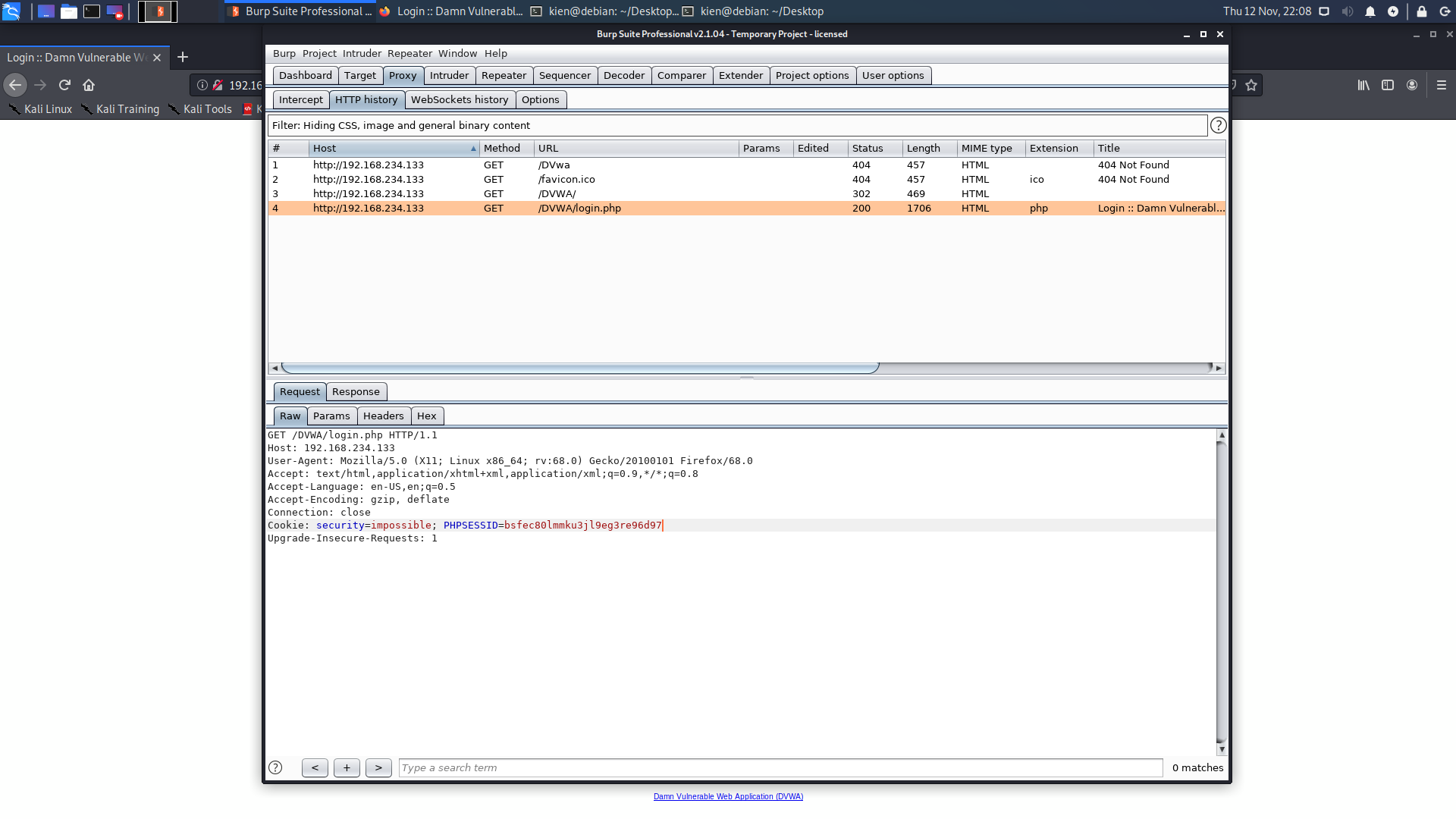
|  |  |
| --- | --- |
| Class & Module | IAW301 |
| Name | Nguyễn Đức Kiên |
| IC No. | HE141763 |
| Date & Time | November 12, 2020 |

On the first computer, before login to dvwa, turn on burp suite, then go back and log in to dvwa. A burp suite window pop up:

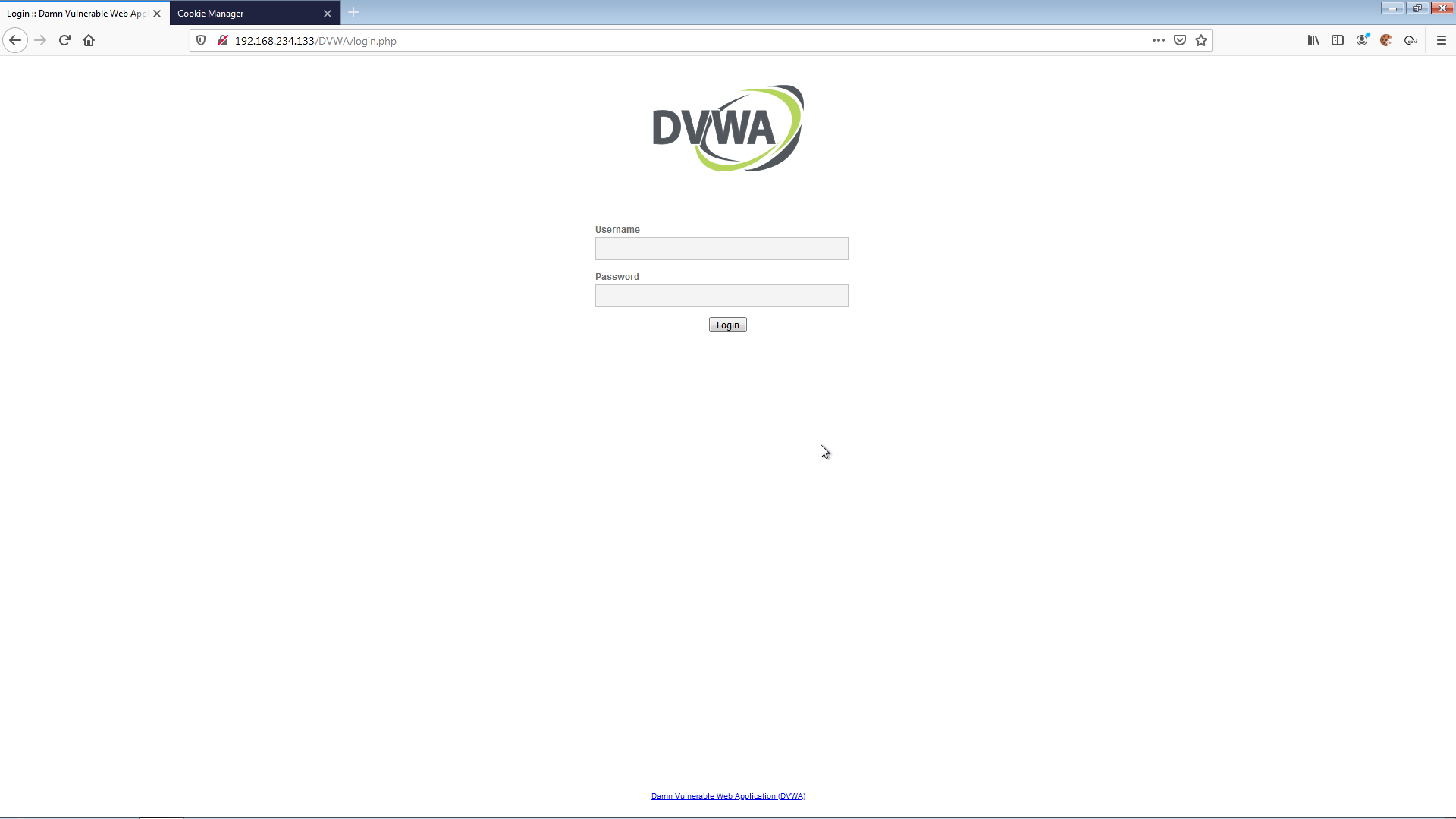


Click Forward until request is sent completely, go to HTTP history tab, find the line that have method Post and url /dvwa/login.php:

We have the Cookie : security=impossible; PHPSESSID=bsfec80lmmku3jl9eg3re96d97

Save this to notepad or somewhere else to use later.

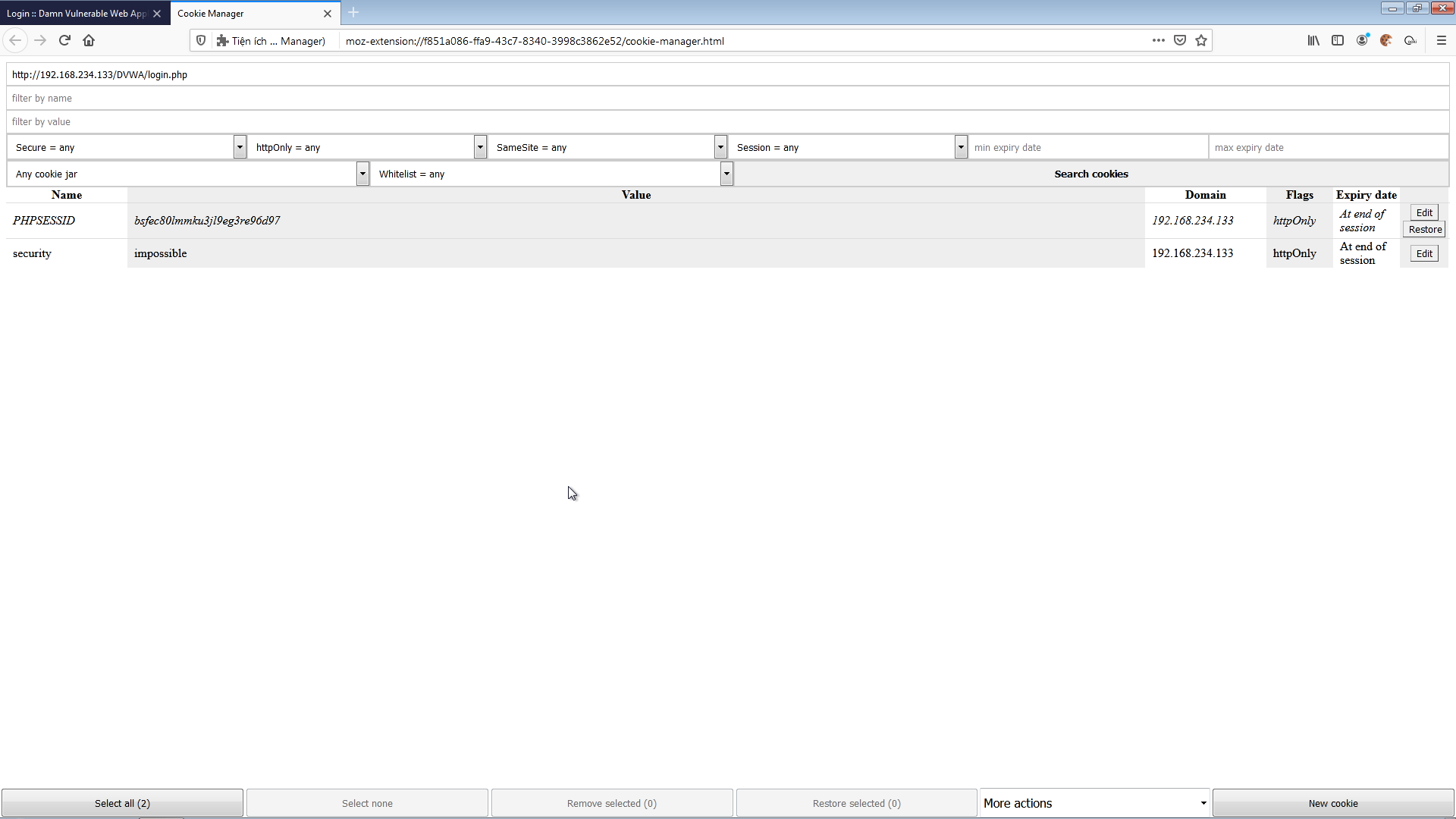
On the second computer, access to dvwa according to IP of the first computer. Enter this url:

http://192.168.234.133/DVWA/ 

Add cookie manager add-ons to Firefox, from this link :

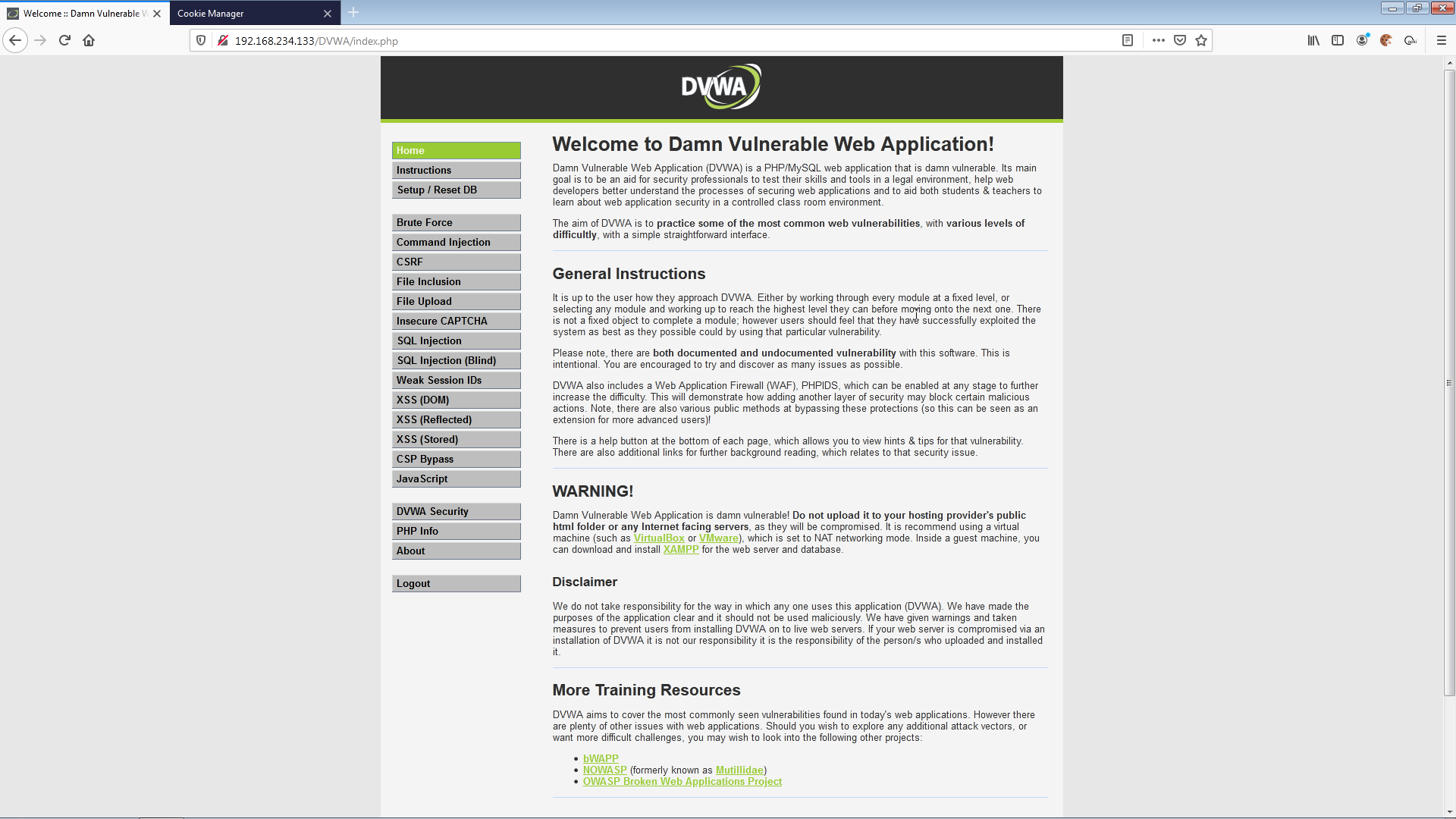
<https://addons.mozilla.org/vi/firefox/addon/a-cookie-manager/>

Enter the url : http://192.168.234.133/DVWA/login.php into the Filter by url field then click Search Cookies. Now edit the value of PHPSESSID and security to the value of cookie from the first computer we save above:



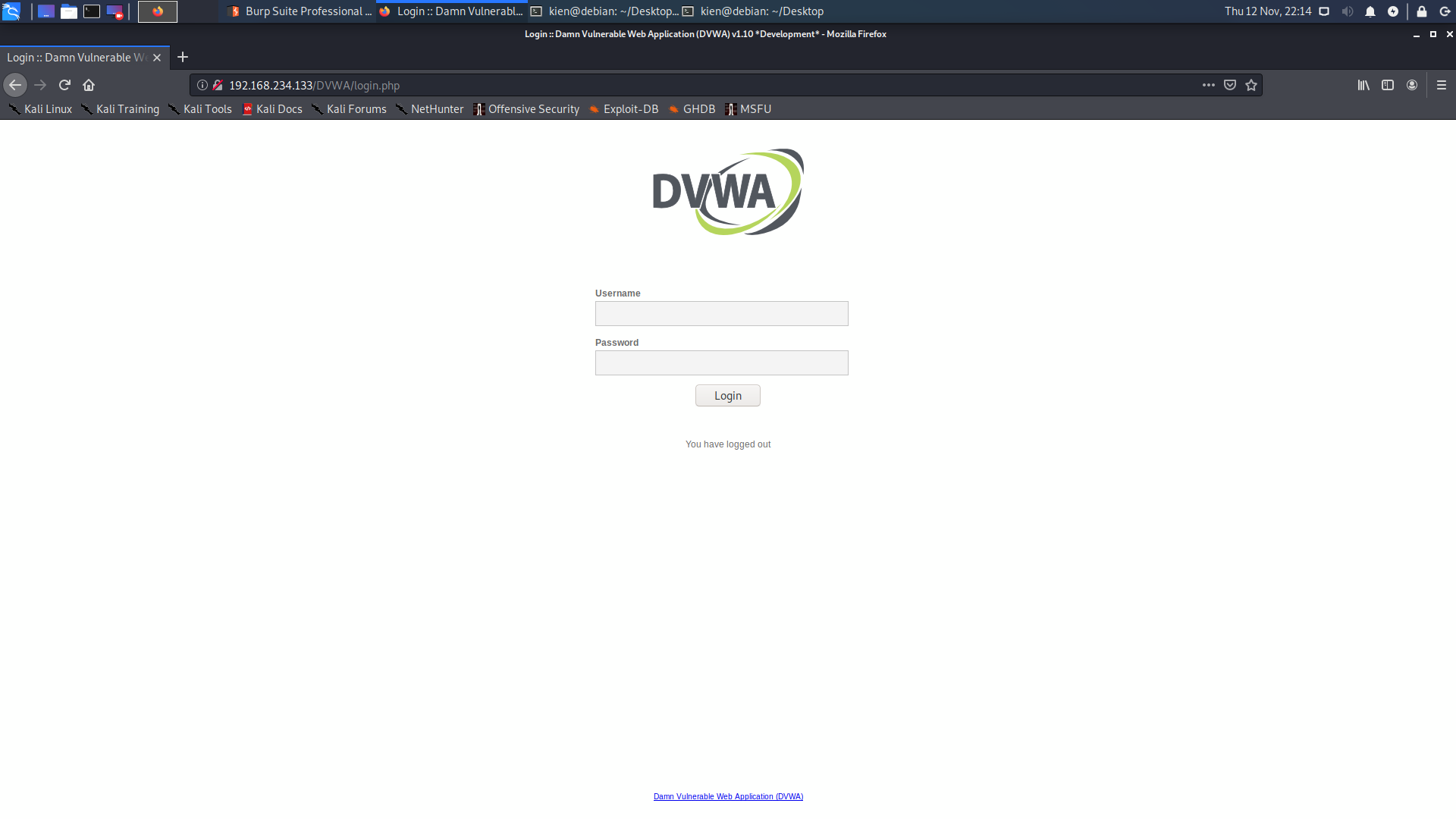
Back to the login Dvwa of the second computer page, chang the url to :

http://192.168.234.133/DVWA/index.php



Now we successfully logged in on the second computer using the session of the first computer.

Back to the first computer and log out of dvwa. Then go to dvwa page of the second computer (refresh the page) and we realized that the second computer is logged out as well. Consider our man in the middle intercept has succeeded.



First computer logged out



Second computer logged out as well