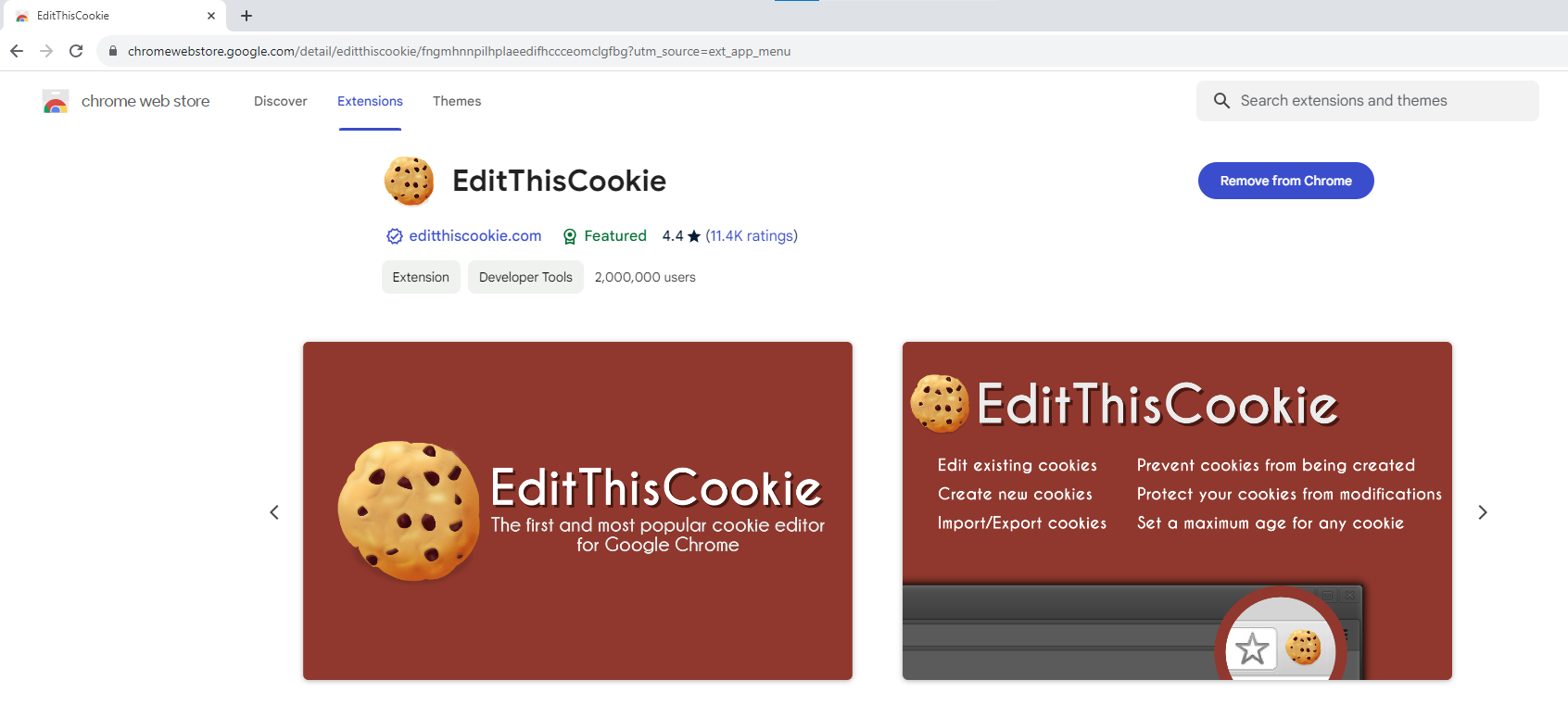
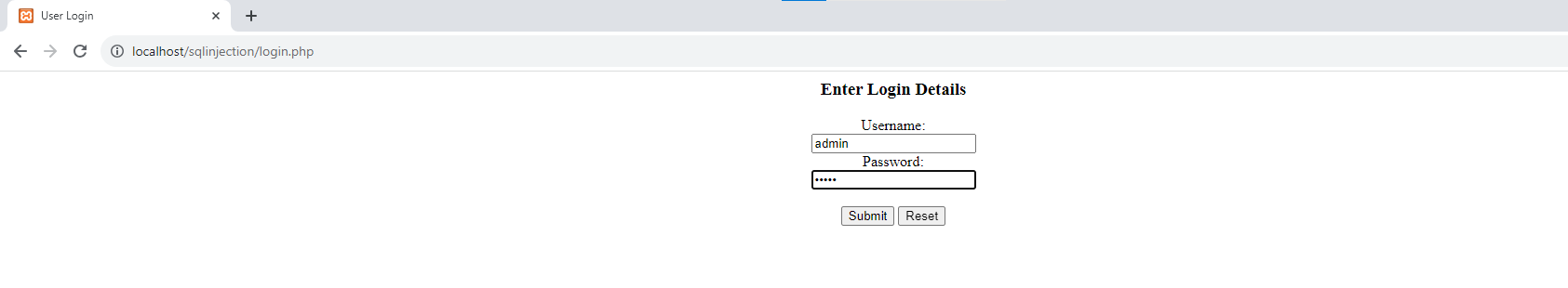
Practical 6

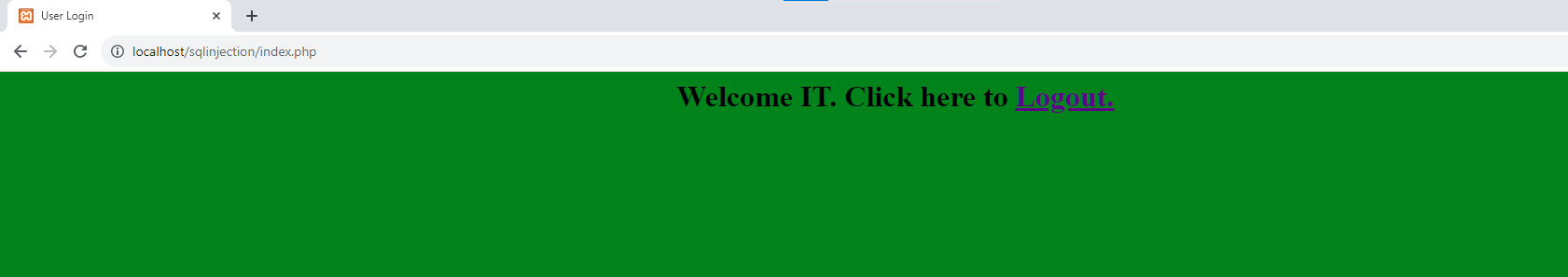
**Session Hijacking**

EditThisCookie extension:



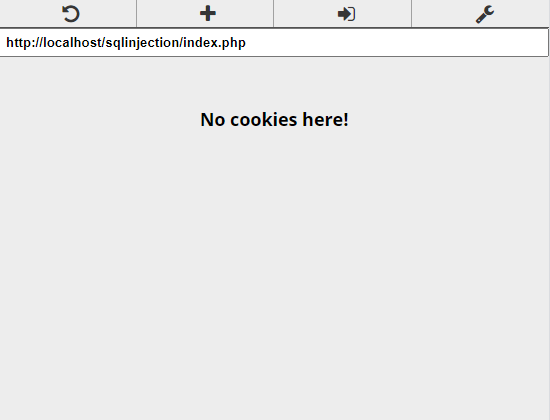
Clear all cookies

****

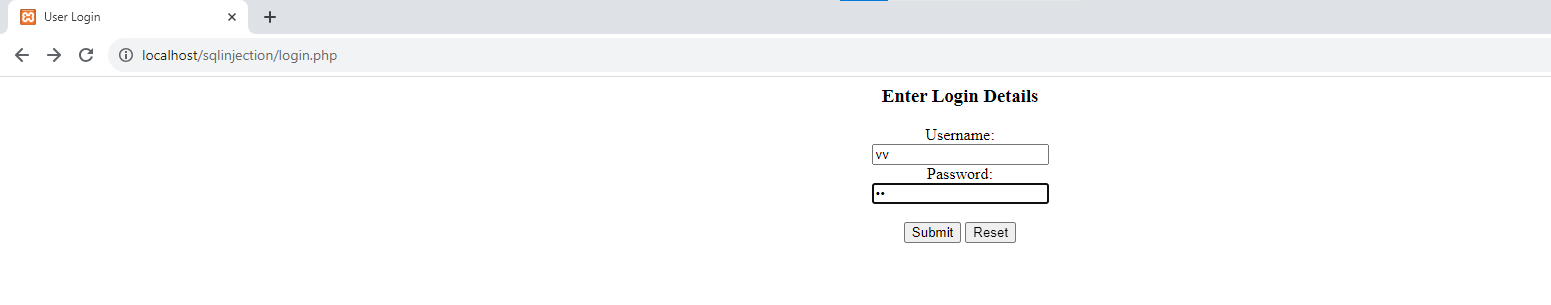
****

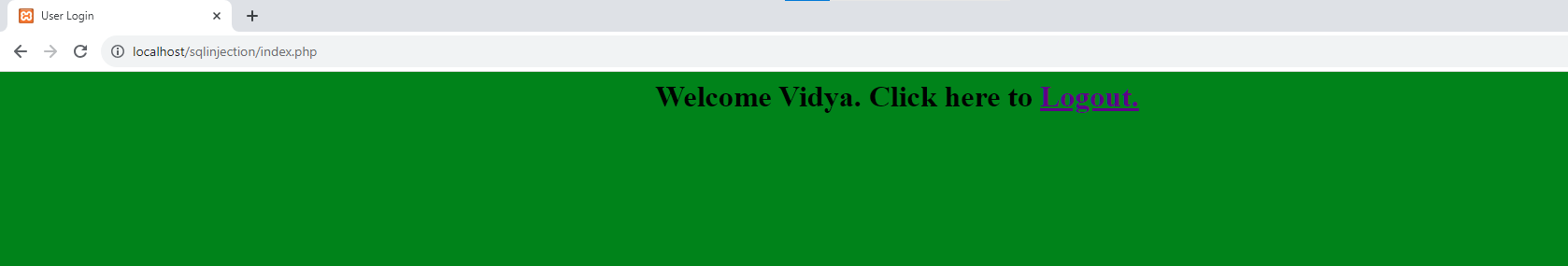
Now PHPSESSID for Admin **= ndrfddk7h1cn5ocr801n1sioef**

Next,delete the above session after it is recorded above.

****

Login as username=vv and password =vv

****

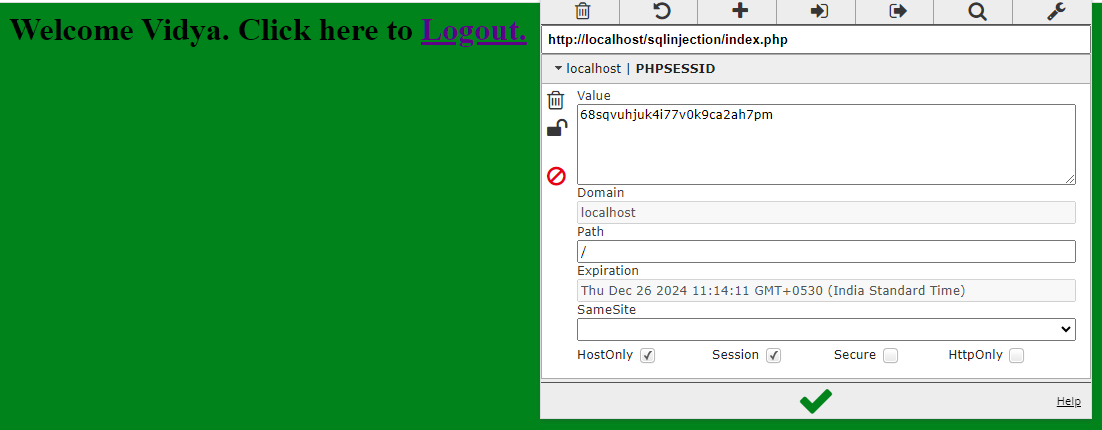
****

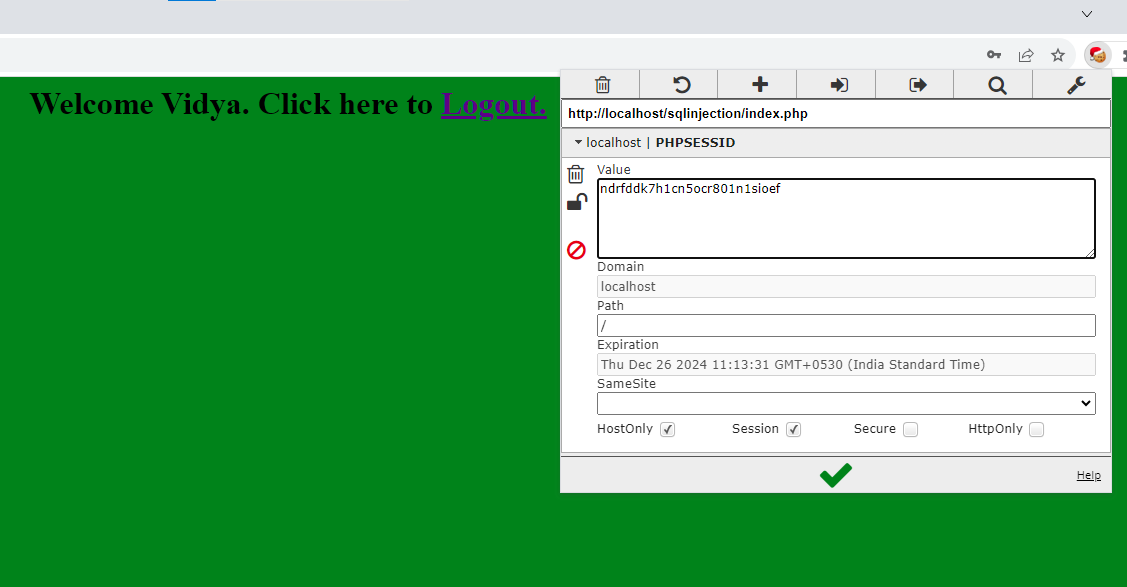
Now PHPSESSID for vv = **68sqvuhjuk4i77v0k9ca2ah7pm**

Now the admin is trying to hijack the session of username vv

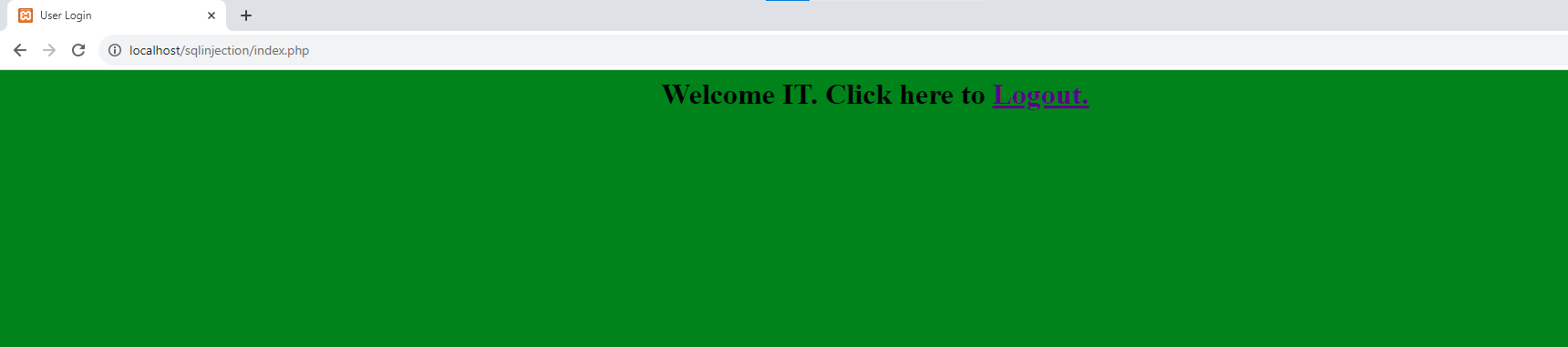
In the PHPSessID replace vv’s PHPSESSID=**68sqvuhjuk4i77v0k9ca2ah7pm**

With Admin sessionid PHPSESSID= **ndrfddk7h1cn5ocr801n1sioef**

****



Click the green tick symbol and refresh the page

****

Without logging in the notice that the name is changed to IT.

What are the ways to prevent your data hacked by packet sniffers?

* Using HTTPS, the secure version of HTTP will prevent packet sniffers from seeing the traffic on the websites you are visiting.
* To make sure you are using HTTPS, check the upper left corner of your browser.
* Tunnel your connectivity to a virtual private network, or a VPN. A VPN encrypts the traffic being sent between your computer and the destination. This includes information being used on websites, services, and applications. A packet sniffer would only see encrypted data being sent to your VPN service provider.