

## Level 02

Bishal Khadka

**Step 1:** First examine carefully the information provided in motd.txt in level 01. It says to point on <http://localhost:8002> and also go to /levels/level02/ to find some relevant information.

**Step 2:** Using curl to point on to the browser to <http://localhost:8002/>. First, we need to find the ip-address of our localhost. For that, type **ifconfig** and copy the ip-address of eth0. After that process is done: Type **curl http://192.168.1.13(ip address of localhost):8002(port number)**.

```
level01@box:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:9F:47:FC
          inet addr:192.168.1.13  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:807 errors:0 dropped:0 overruns:0 frame:0
          TX packets:249 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:112999 (110.3 KiB)  TX bytes:25255 (24.6 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:48 errors:0 dropped:0 overruns:0 frame:0
          TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4207 (4.1 KiB)  TX bytes:4207 (4.1 KiB)

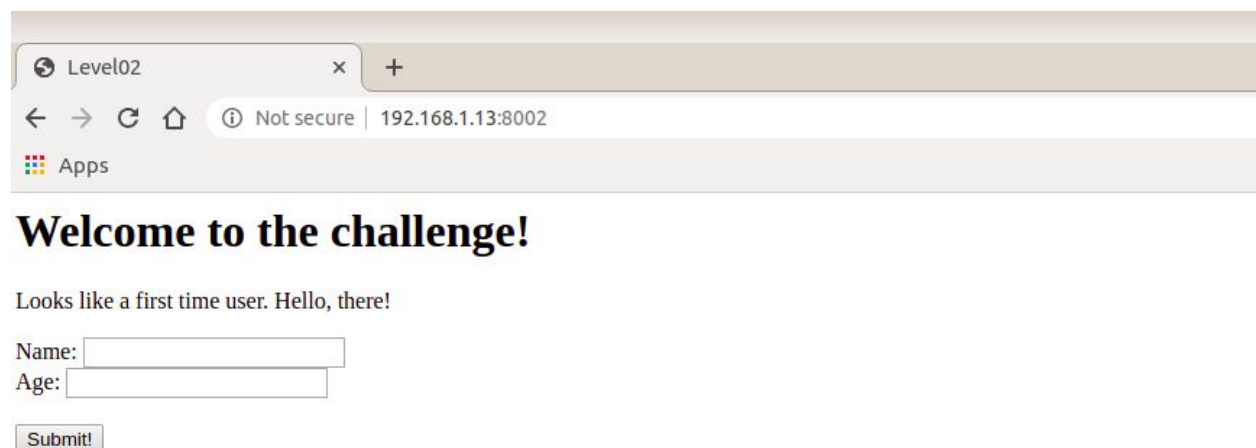
level01@box:~$
```

```
level01@box:~$ curl http://192.168.1.13:8002
<html>
  <head>
    <title>Level02</title>
  </head>
  <body>
    <h1>Welcome to the challenge!</h1>
    <div class="main">
      <p>Looks like a first time user. Hello, there!</p>

      <form action="#" method="post">
        Name: <input name="name" type="text" length="40" /><br />
        Age: <input name="age" type="text" length="2" /><br /><br />
        <input type="submit" value="Submit!" />
      </form>

    </div>
  </body>
</html>level01@box:~$
```

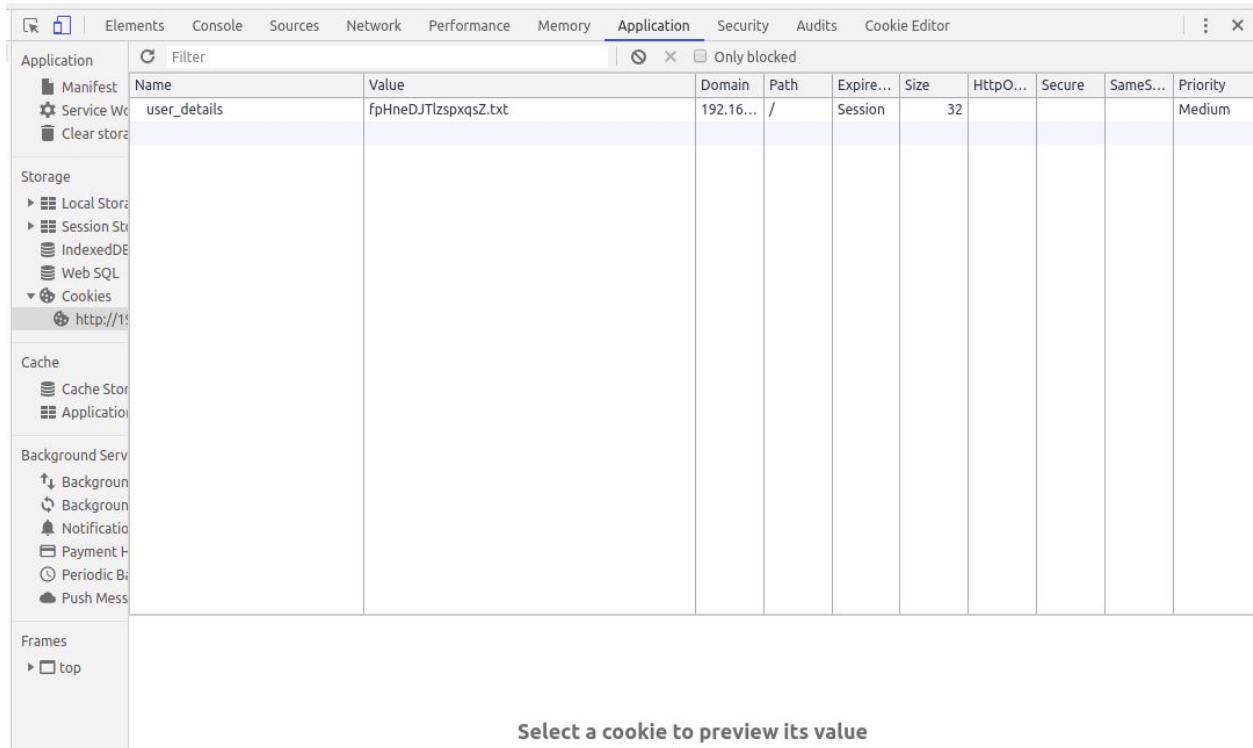
**Step 3:** Open up your favourite browser in your host machine or other virtual machine. Type the ip-address followed by port number, for instance, **192.168.1.13:8002** and the following window should pop up.



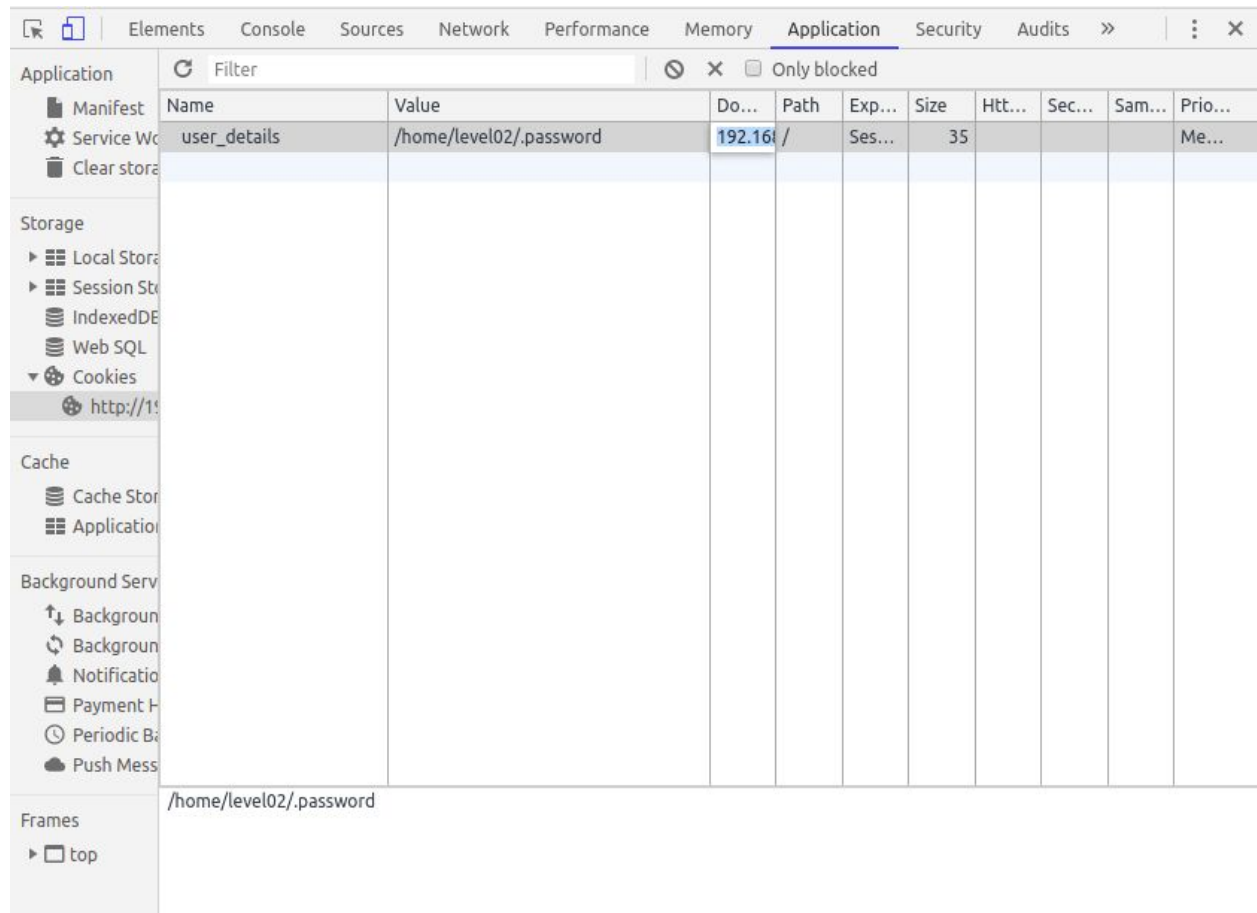
The screenshot shows a web browser window with the title "Level02". The address bar displays "Not secure | 192.168.1.13:8002". The page content includes a heading "Welcome to the challenge!", a message "Looks like a first time user. Hello, there!", and a form with two input fields labeled "Name:" and "Age:", and a "Submit!" button.

**Step 4:** Open up the inspection window (*For ex: in chrome, it is by pressing **Ctrl + Shift + I** or right click and inspect element*). Click on **Application** and then click on **cookies** option. You will find the information

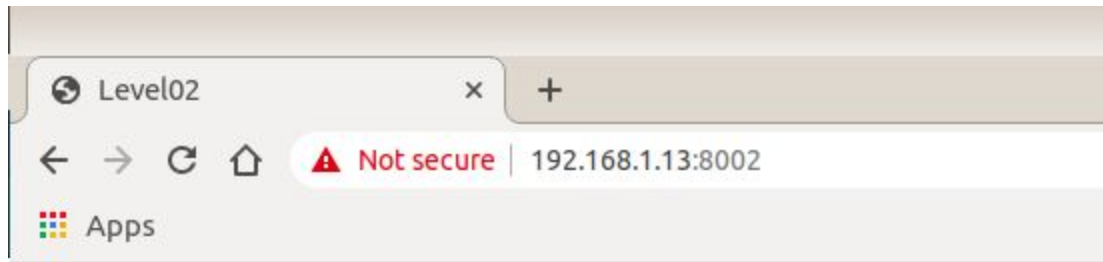
on the cookies for that website and you should be able to edit the values of the cookies right there in that window.



Now it is time to edit the value of the cookies and print the password for level 2. For that, click on the **value** option under cookies and change the value to ***/home/level02/.password***.



**Step 5:** Now, close the inspection window, type in the information in the box, and hit submit.



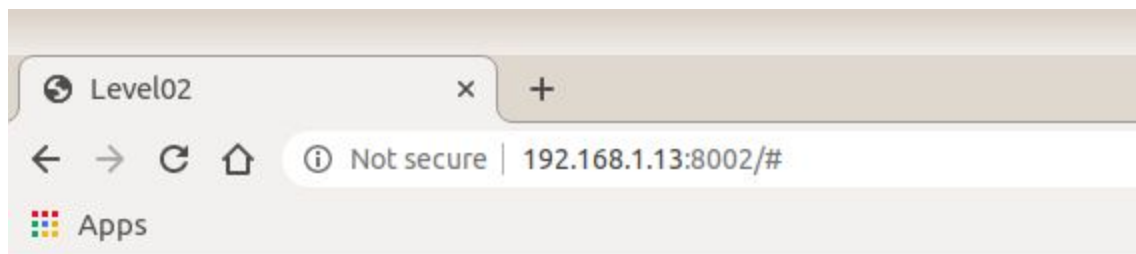
## Welcome to the challenge!

Looks like a first time user. Hello, there!

Name:

Age:

**Step 6:** Walla, you password is printed right below **Welcome to the challenge!** Text.



## Welcome to the challenge!

quemaosh

You're Bishal Khadka, and your age is 21.

The password is: ***quemaosh***

**Step 7:** Type ***su level02*** in tiny core and type in the password. It should take you to ***level02***.



```
level01@box:~$ su level02
```

```
Password:
```

```
level02@box:~$ ls
```

```
flask/      jinja2/     motd.txt    start.sh    werkzeug/
```

```
level02@box:~$ _
```