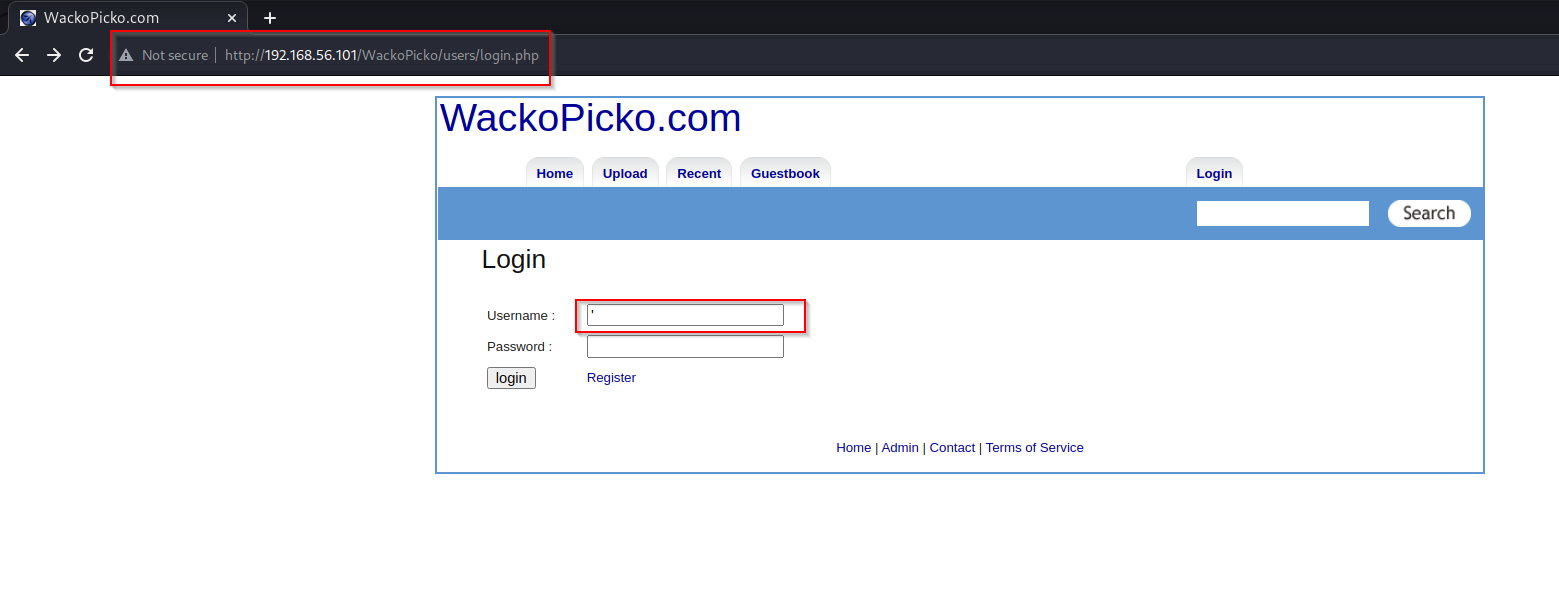
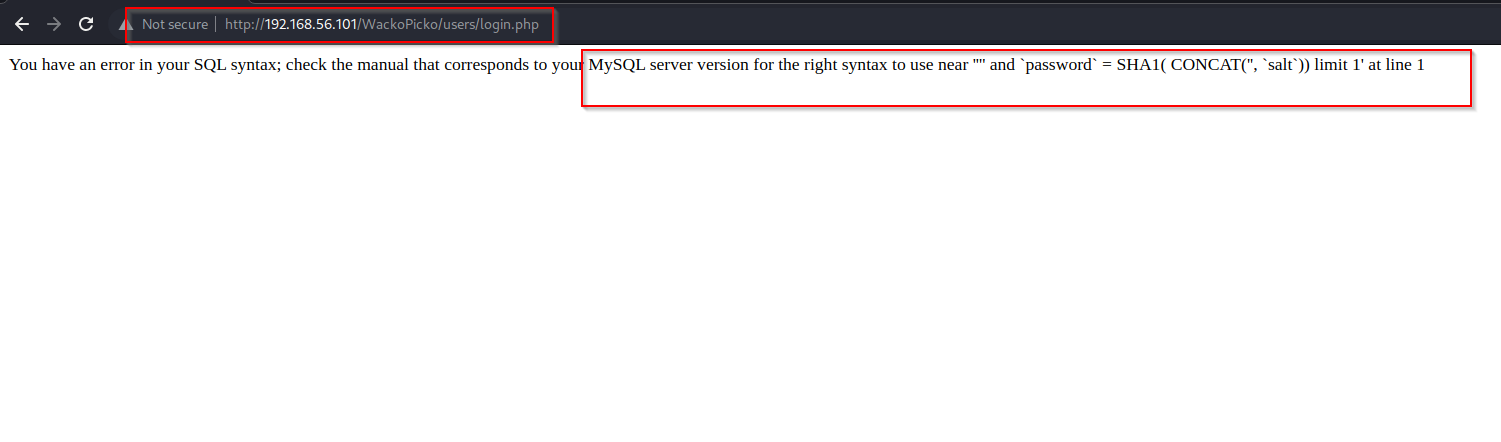
**WackoPicko**

**1 Injection**

* 1. **SQL injection**

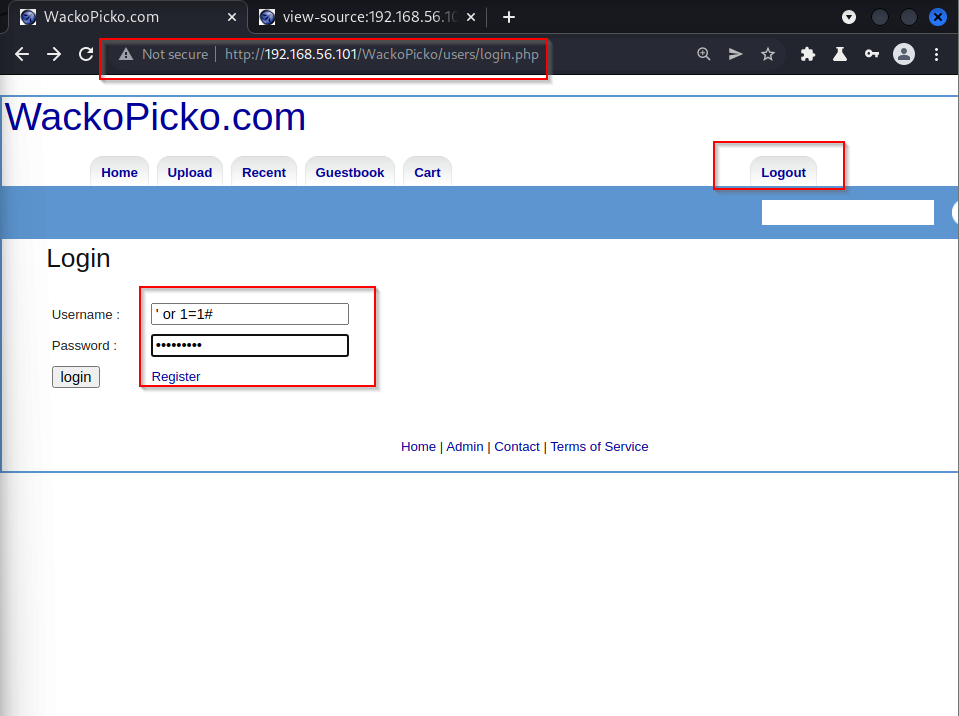
We put value “ ‘ “ inside username field to check whether application is vulnerable to Injection

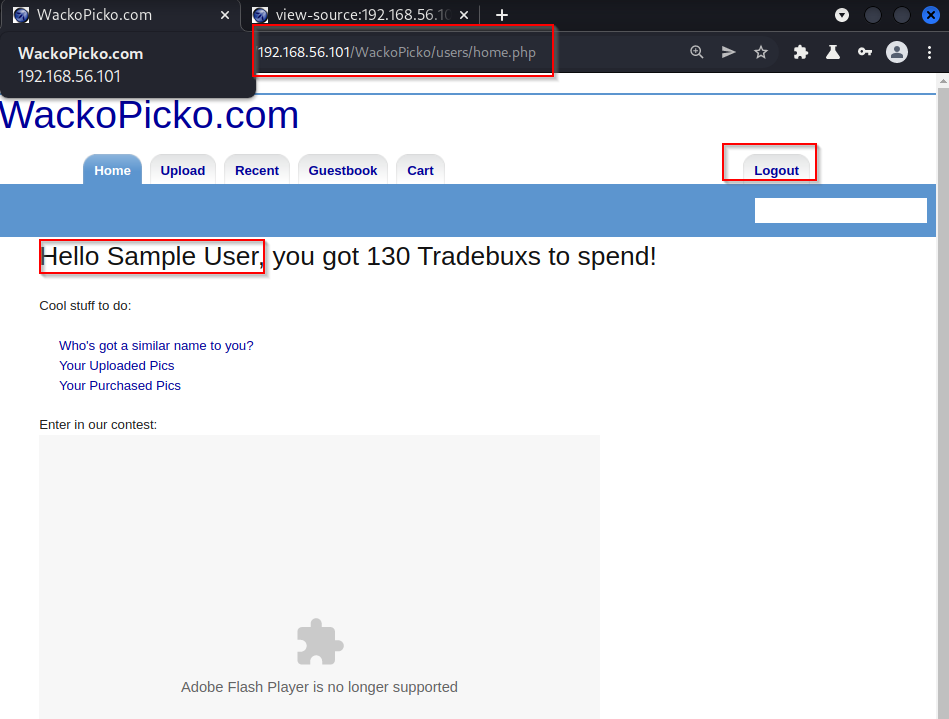


By this output error we got to know this application is vulnerable to SQL Injection

* 1. **SQl injection**

Command used to get user access “ ‘ or 1=1# “

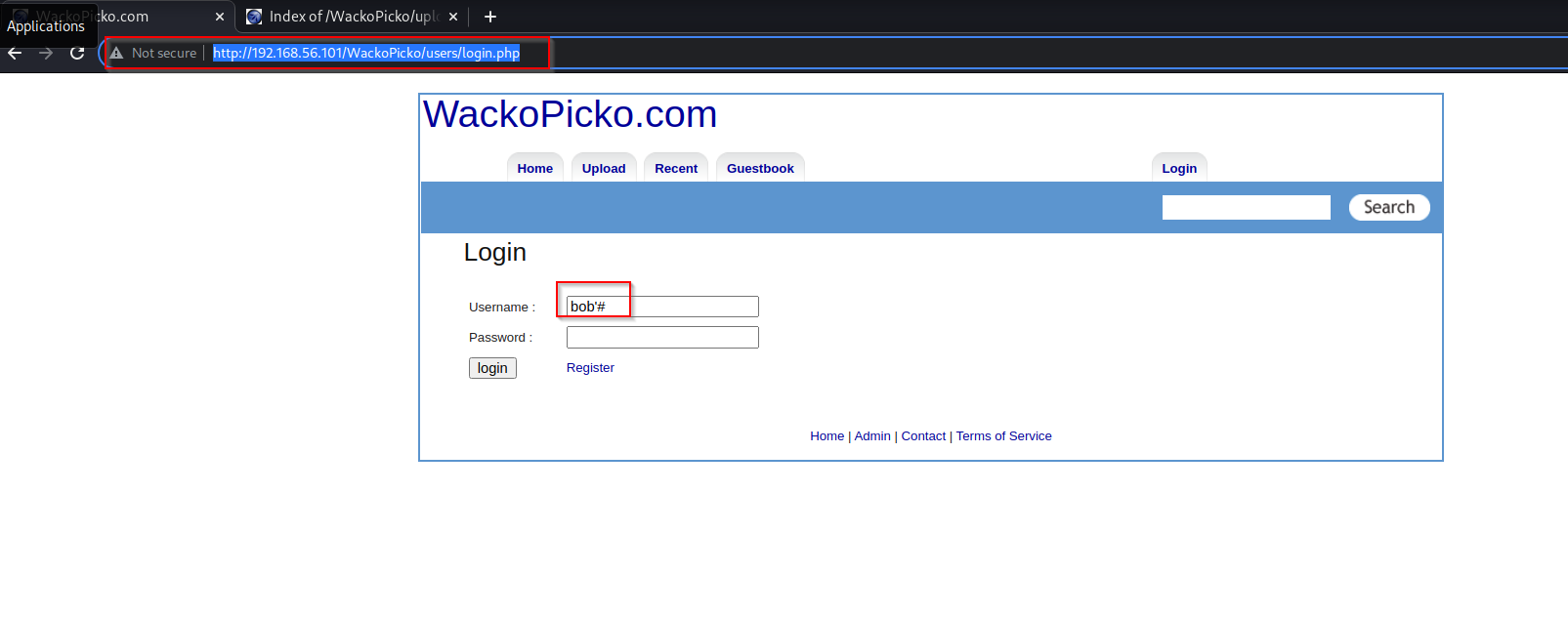
url: <http://192.168.56.101/WackoPicko/users/login.php>

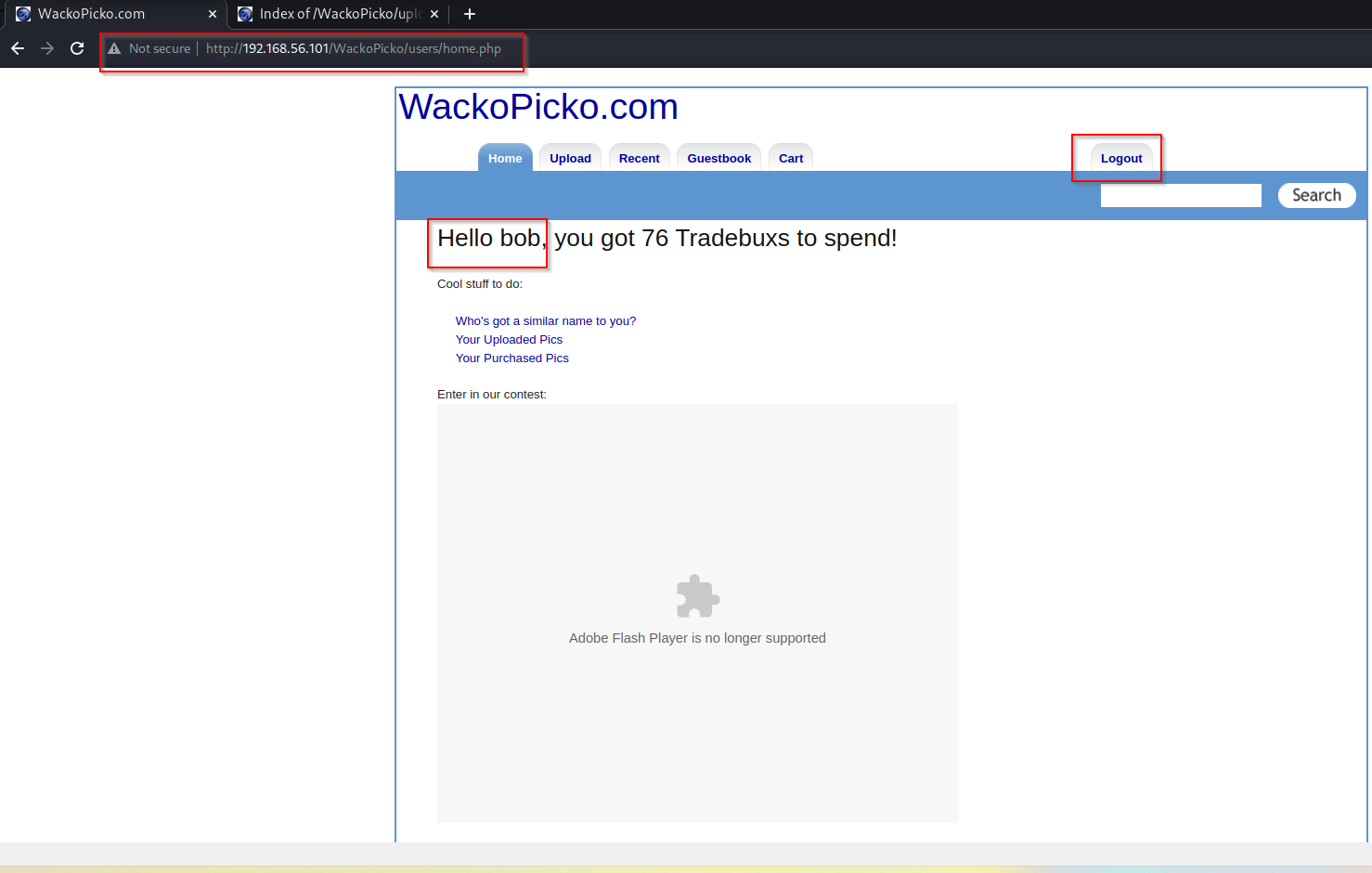


we successfully got access to “**Sample User**”

**1.3 SQl Injection**

url: <http://192.168.56.101/WackoPicko/users/login.php>

we tried to get user account access with injecting only user name with “ **#** “

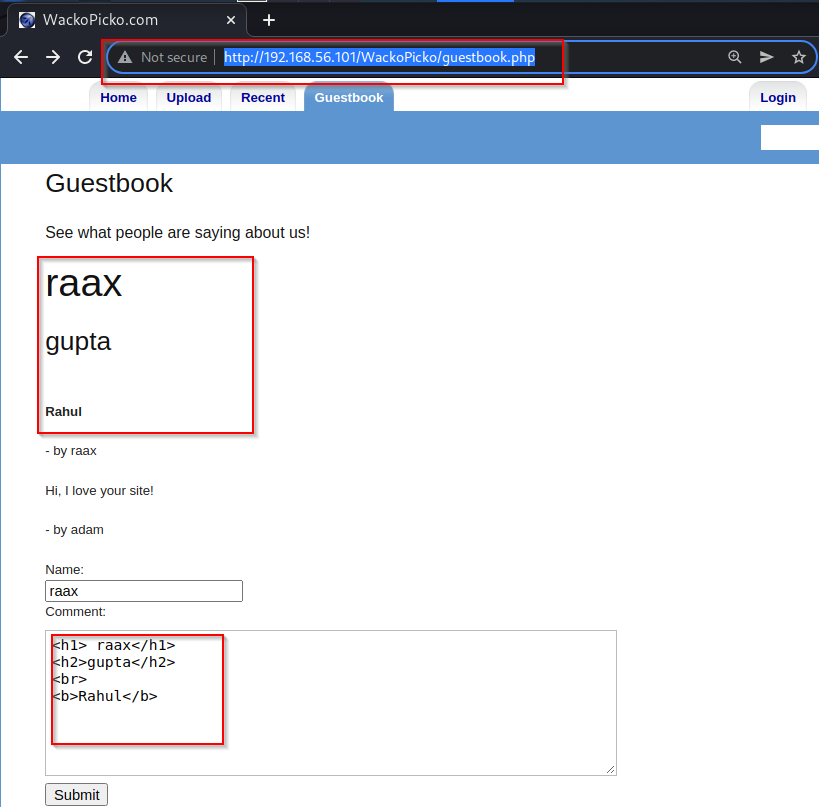


we were successful to get access

**1.4 HTML Injection**

Url: <http://192.168.56.101/WackoPicko/guestbook.php>

Application infected to HTML Injections

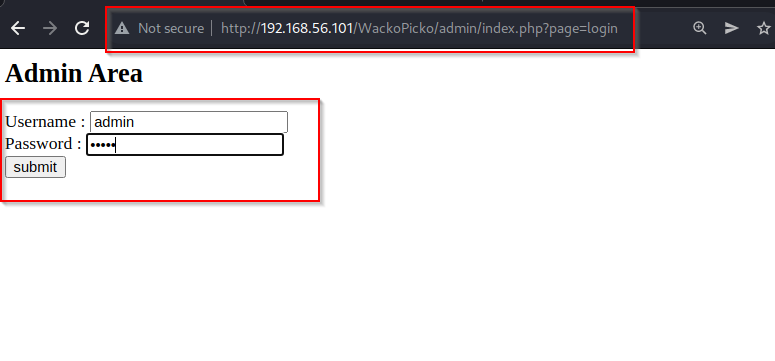
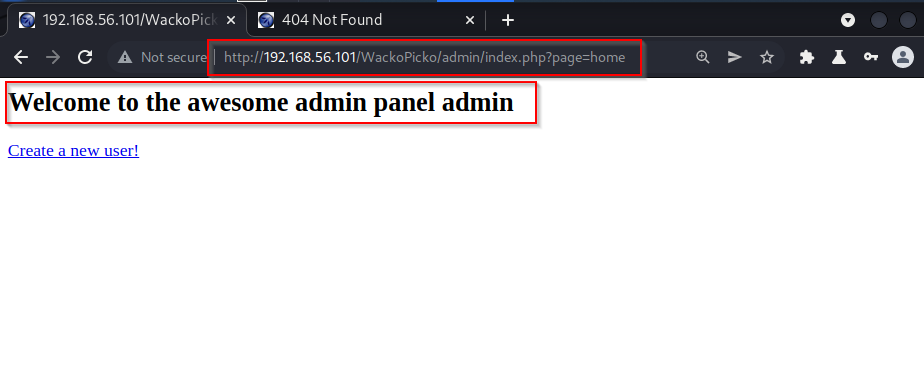


**2 Security Misconfiguration**

**2.1 Default password**

We used default username and password to login as admin

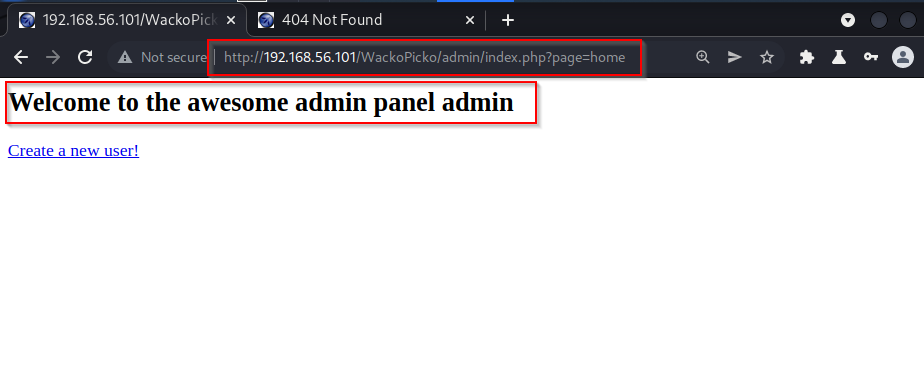
**Username**: admin **password**: admin

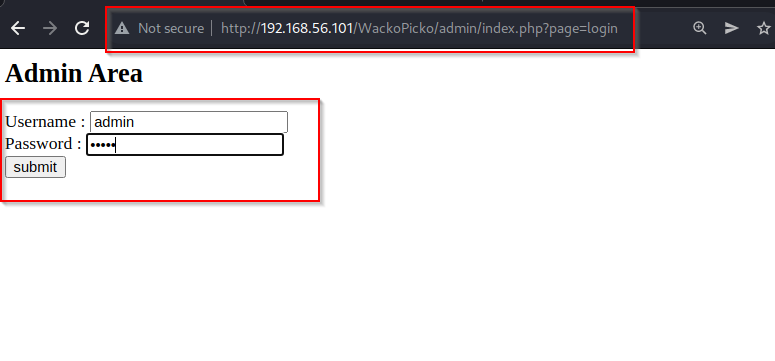
url: <http://192.168.56.101/WackoPicko/admin/index.php?page=login>

we got admin access with default credential

**3.Back button Browsing**

url: <http://192.168.56.101/WackoPicko/admin/index.php?page=home>

Application is vulnerable to back button Browsing , after successful login we presss back button and we were with same credential

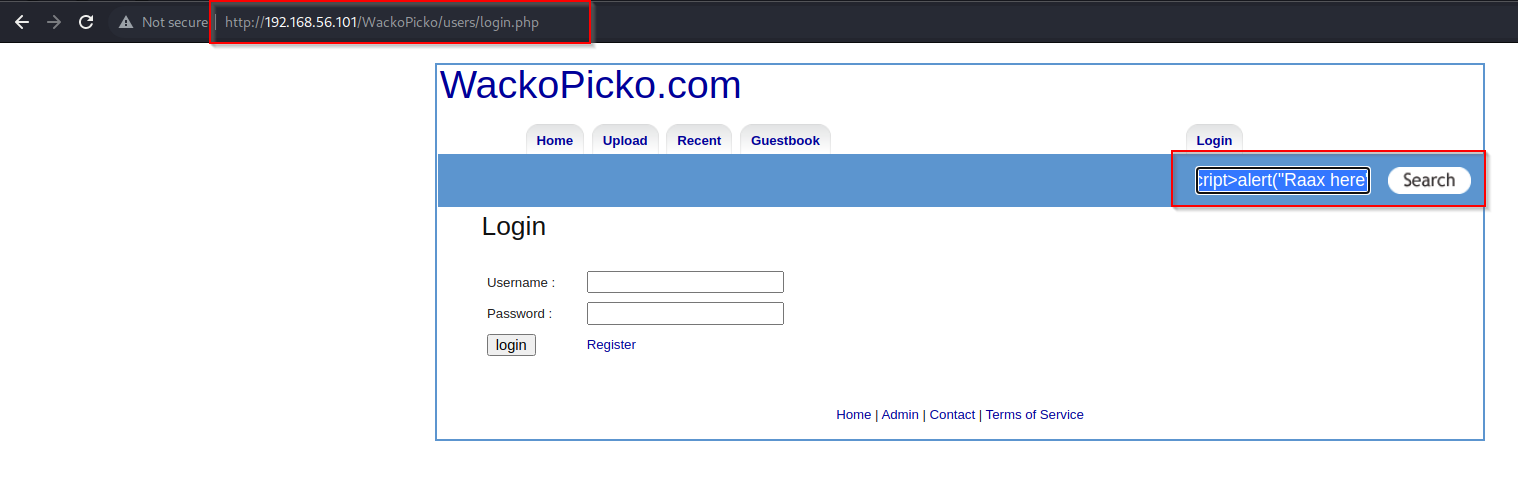


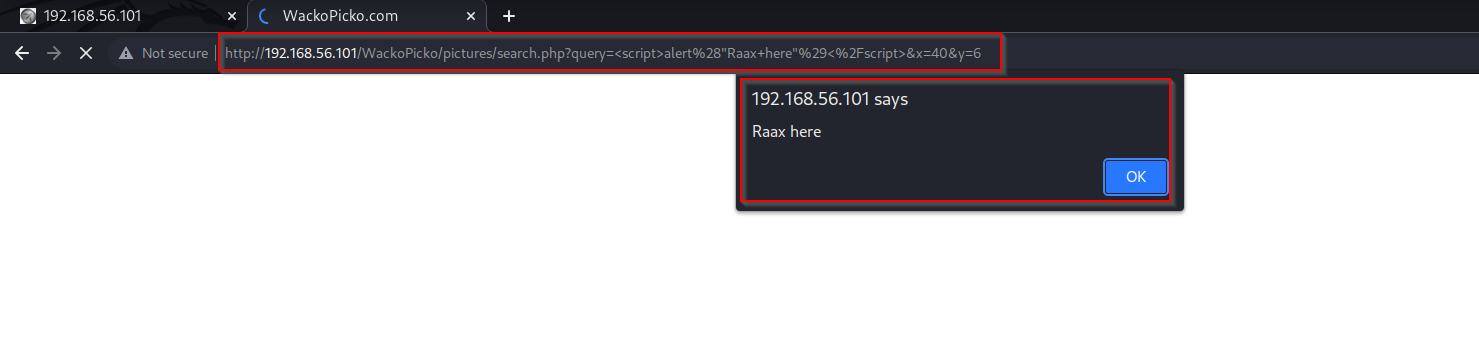
**4. Cross Site Scripting**

**4.1 Xss (reflected)**

url: <http://192.168.56.101/WackoPicko/users/login.php>

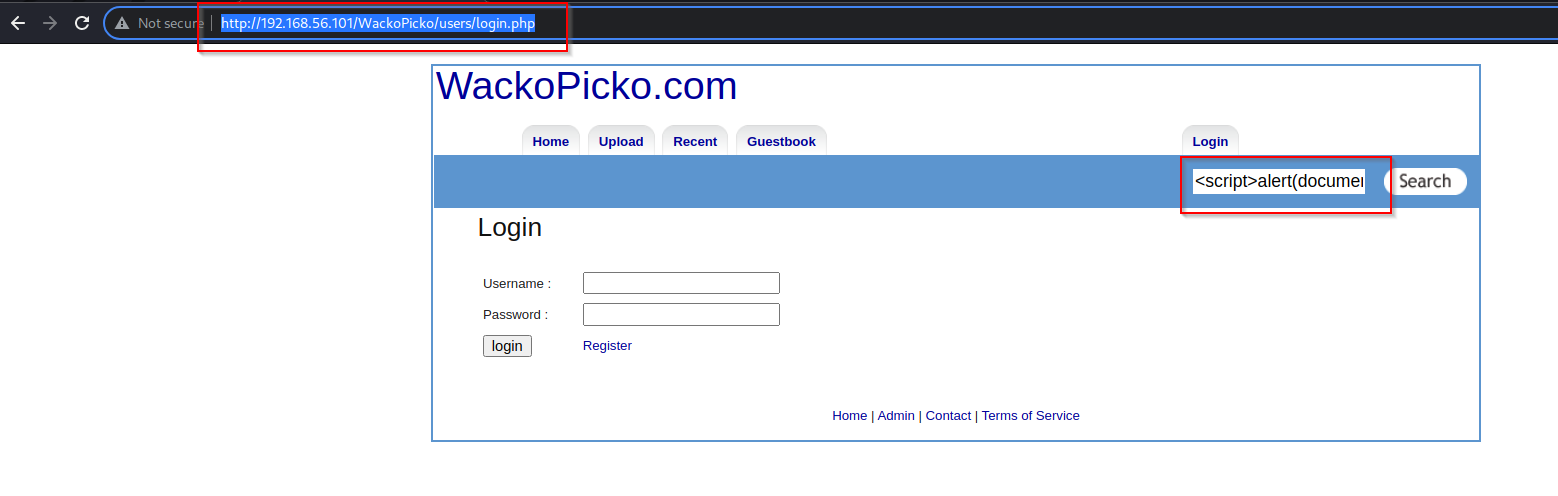
**we used script**: <script>alert(“Raax here”)</script>

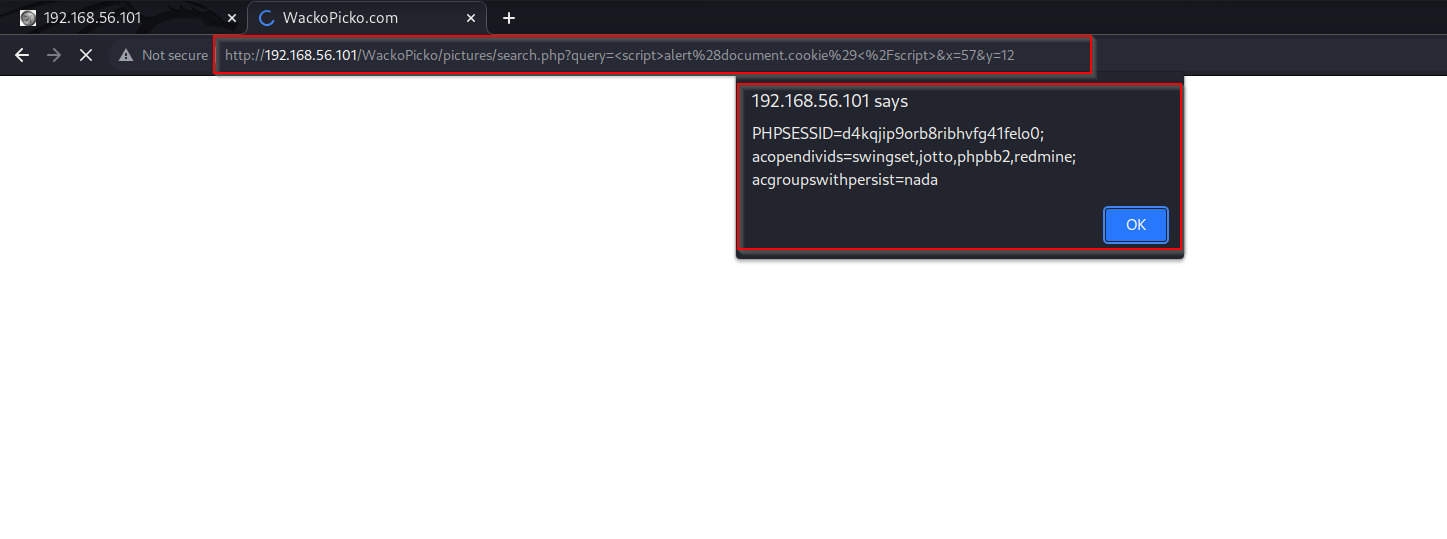




**4.2 XSS to get Cookie**

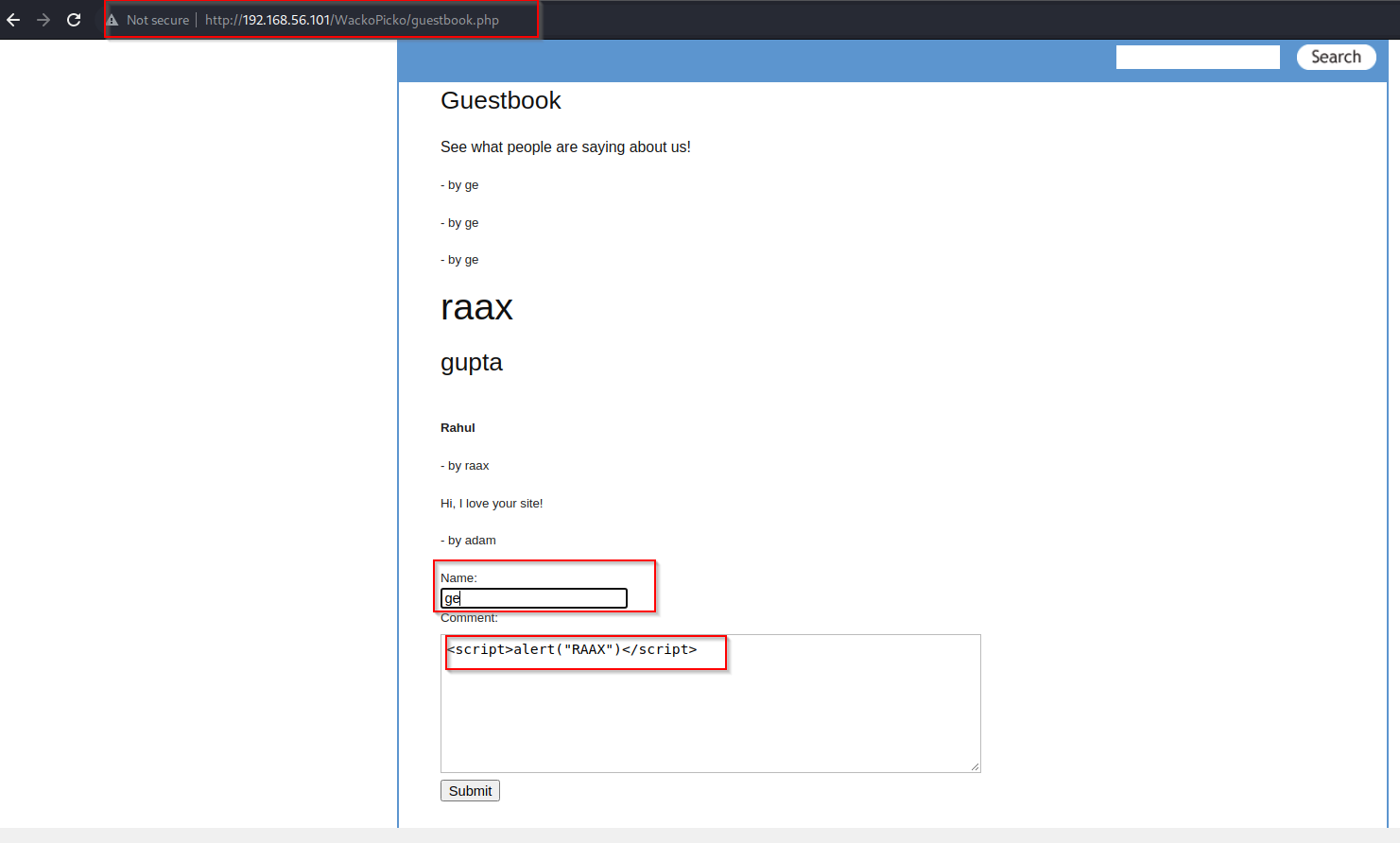
url: <http://192.168.56.101/WackoPicko/users/login.php>

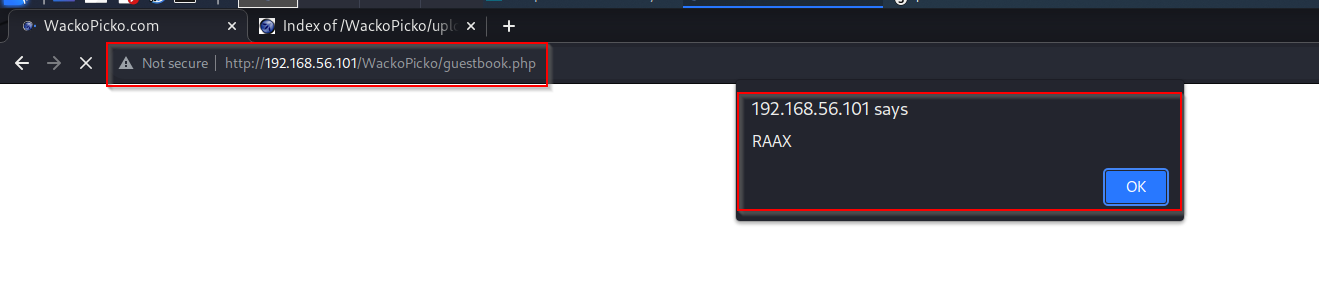
we used script : <script>alert(document.cookie)</script>

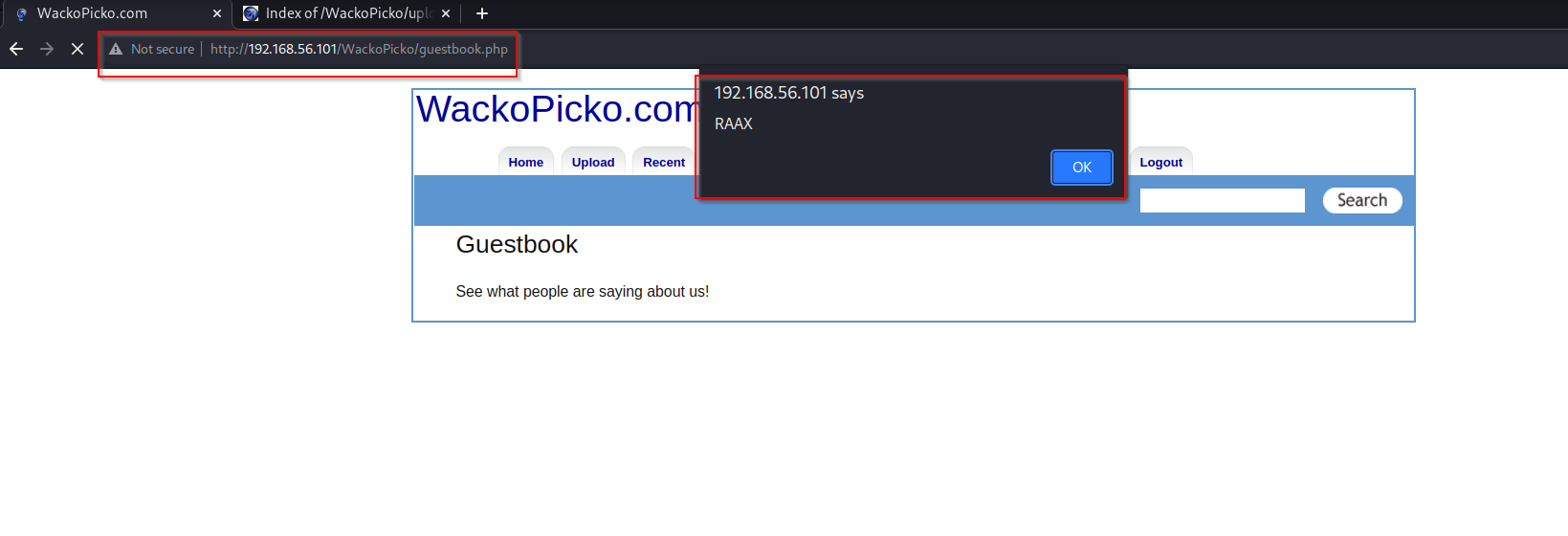


**4.3 XSS Stored**

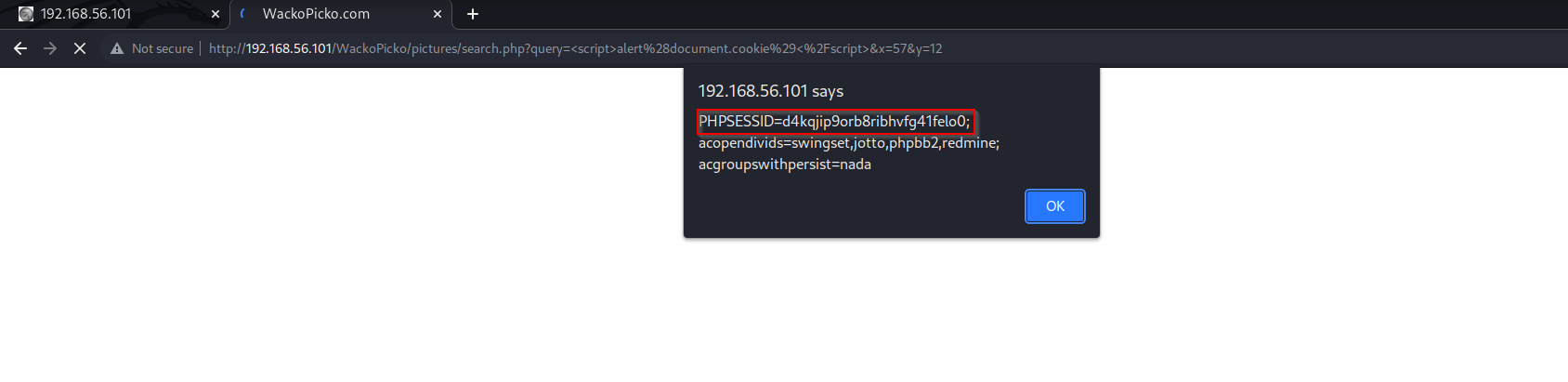
<http://192.168.56.101/WackoPicko/guestbook.php>

we used script : <script>alert(“RAAX”)</script>



After refreshing page , again we got alert message

**Session Id**

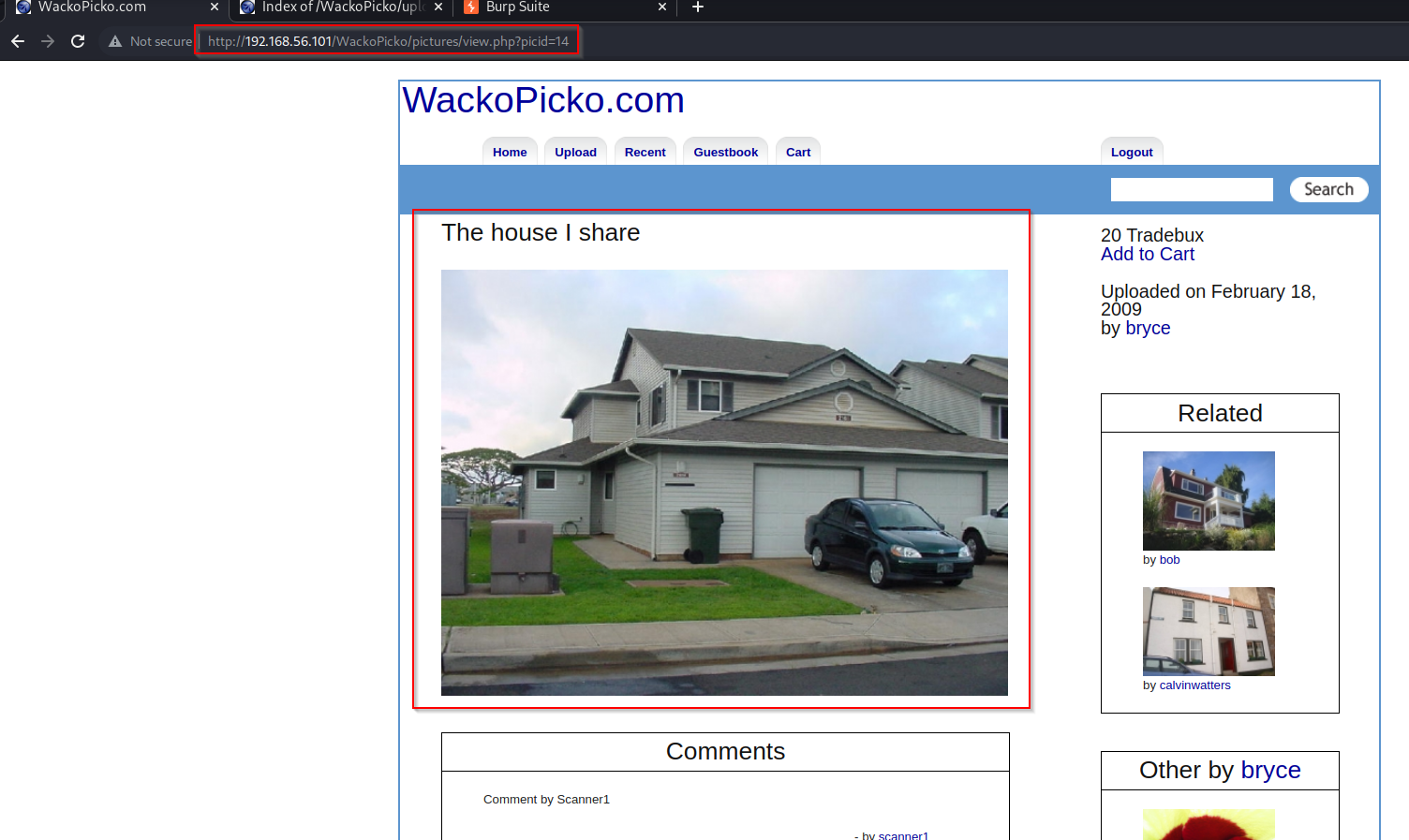
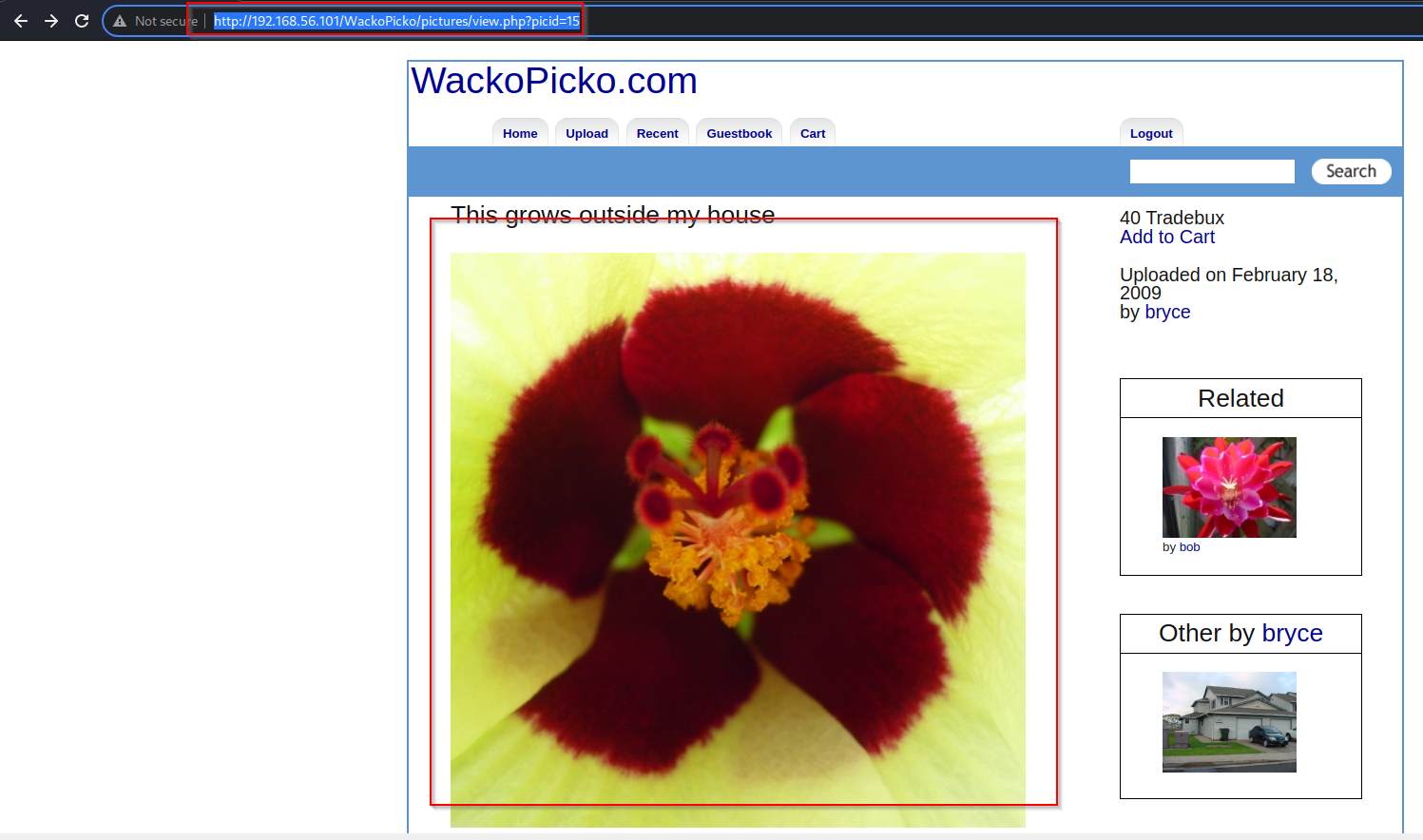


**Broken access control**

**5.1 INSURE DIRECT OBJECT REFERENCE(IDOR)**

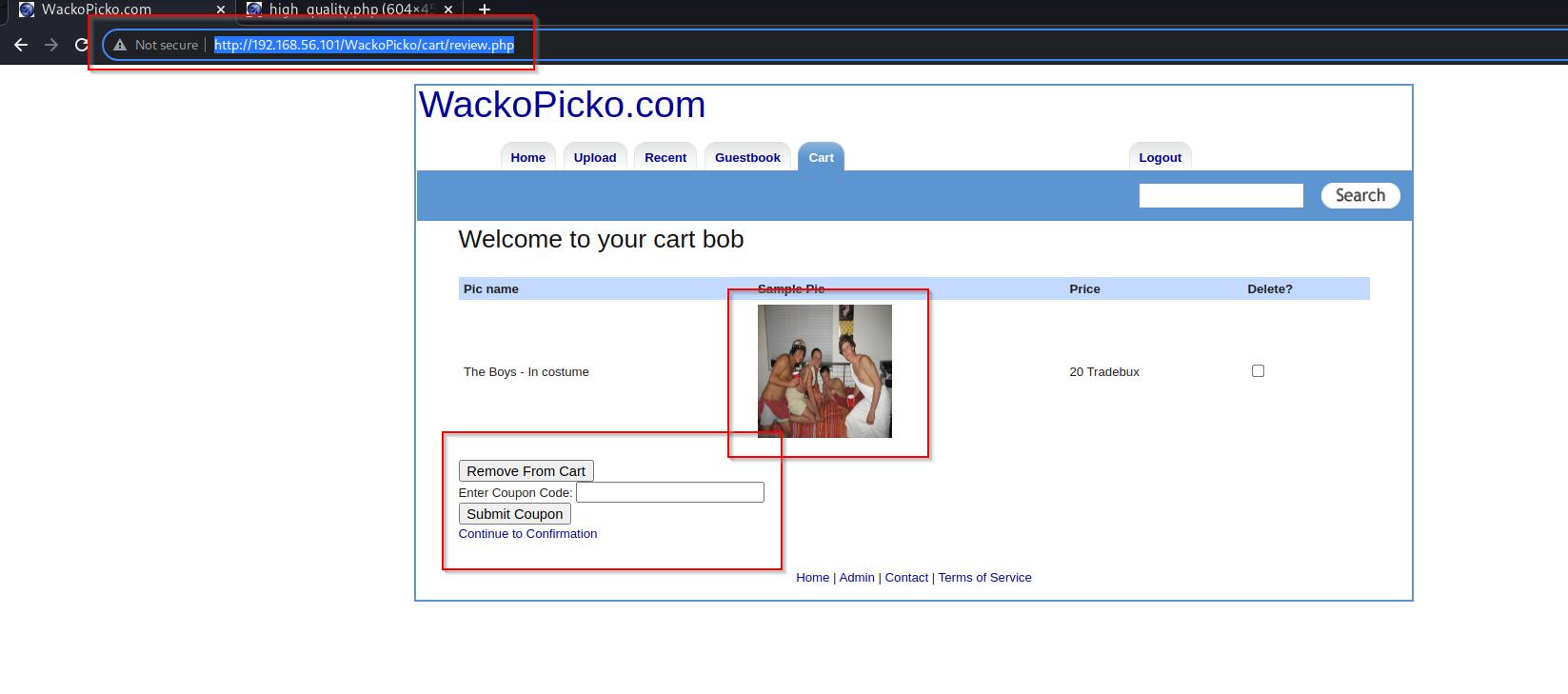
Altering picid number in URL we get different pages

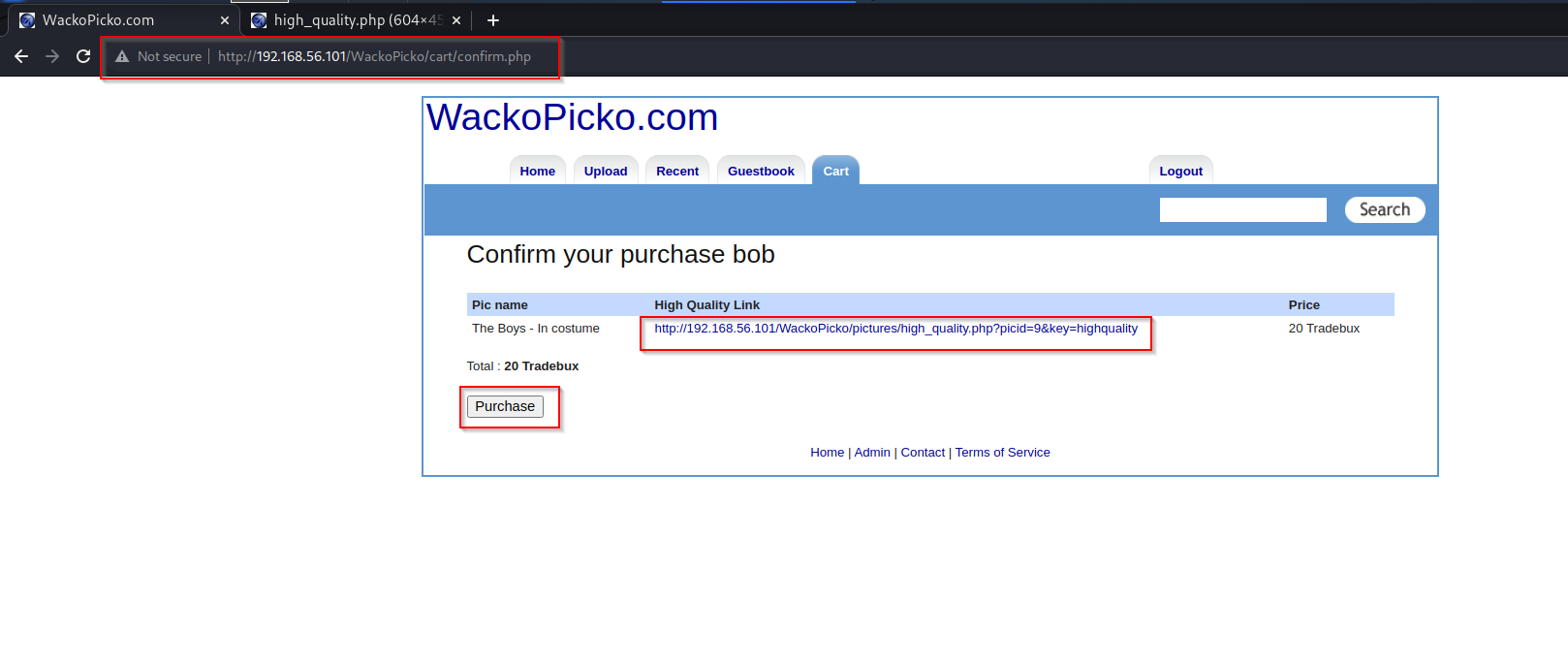
<http://192.168.56.101/WackoPicko/pictures/view.php?picid=15>



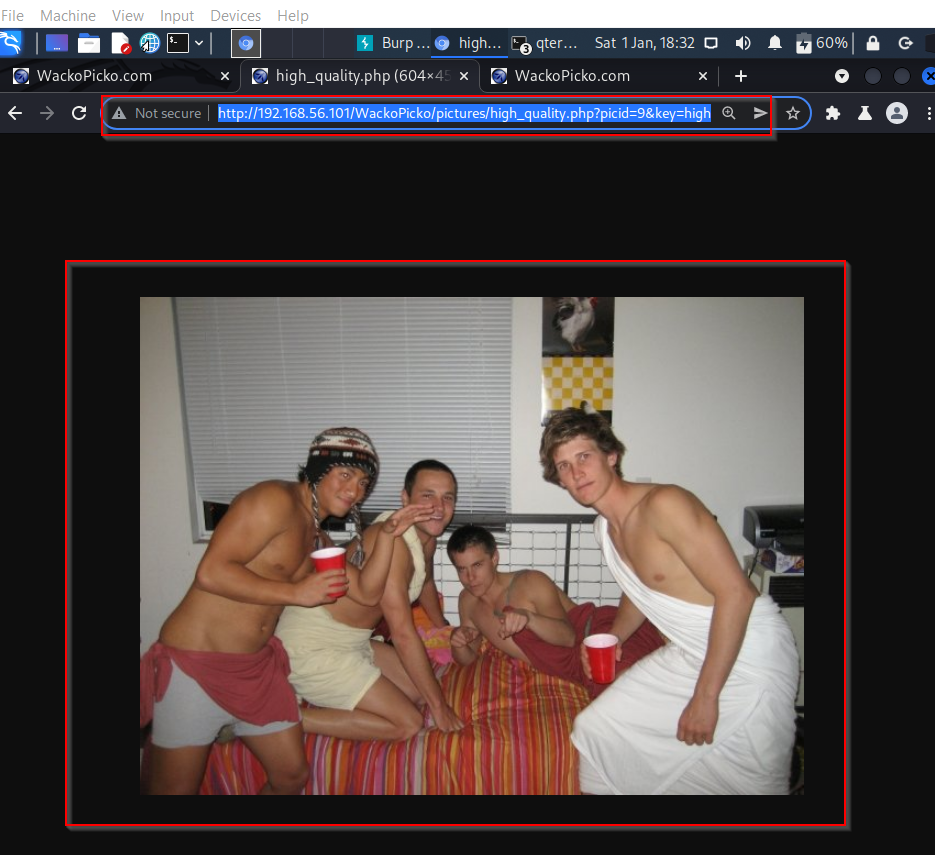
**5.2 IDOR**

url: <http://192.168.56.101/WackoPicko/cart/review.php>

After putting product in cart

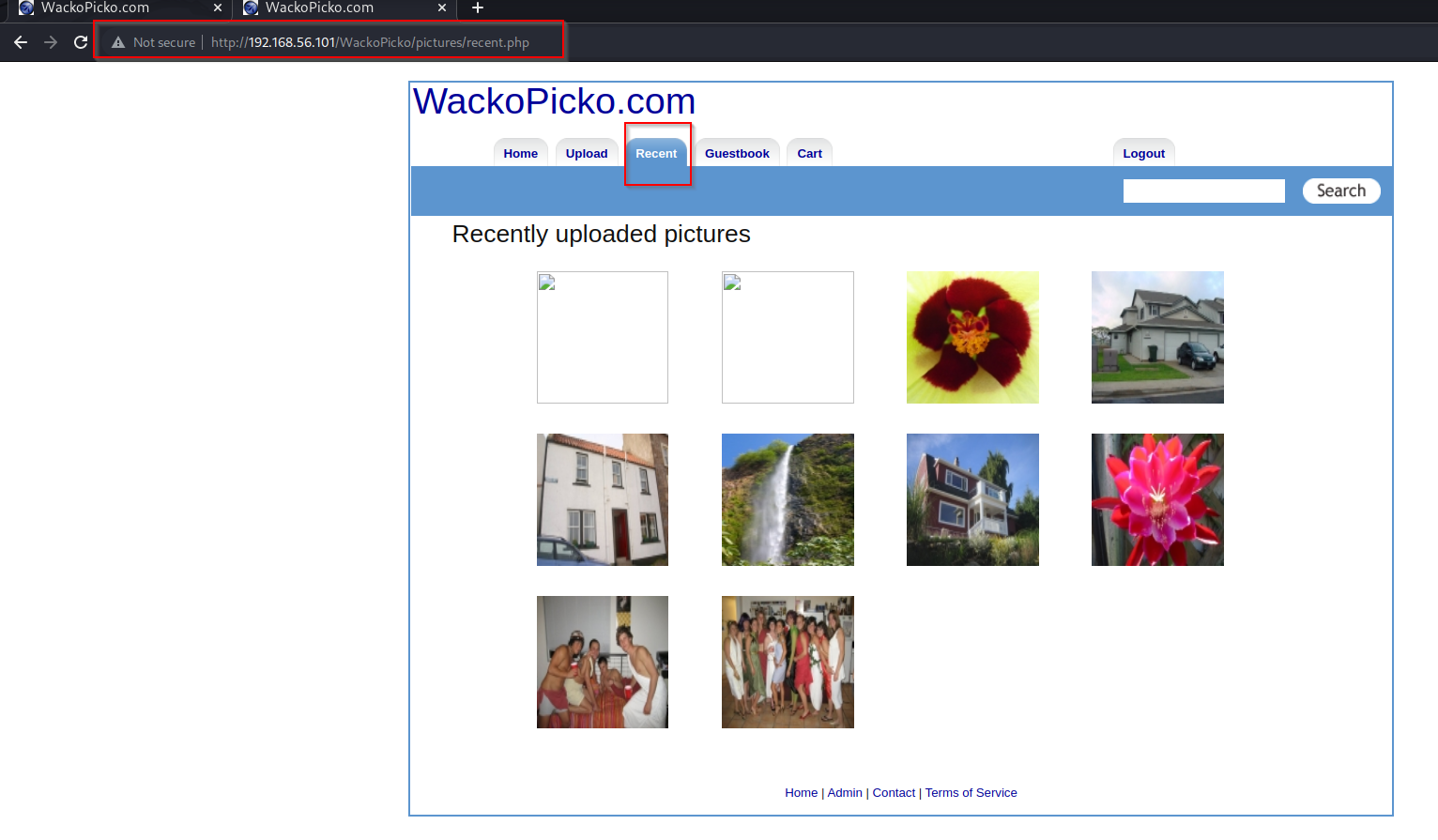
As we click in **continue to confirmation,** we get purchase page. This page contains location of image that is saved in server. as location is visible, we user can direct access that location and download that image without purchasing

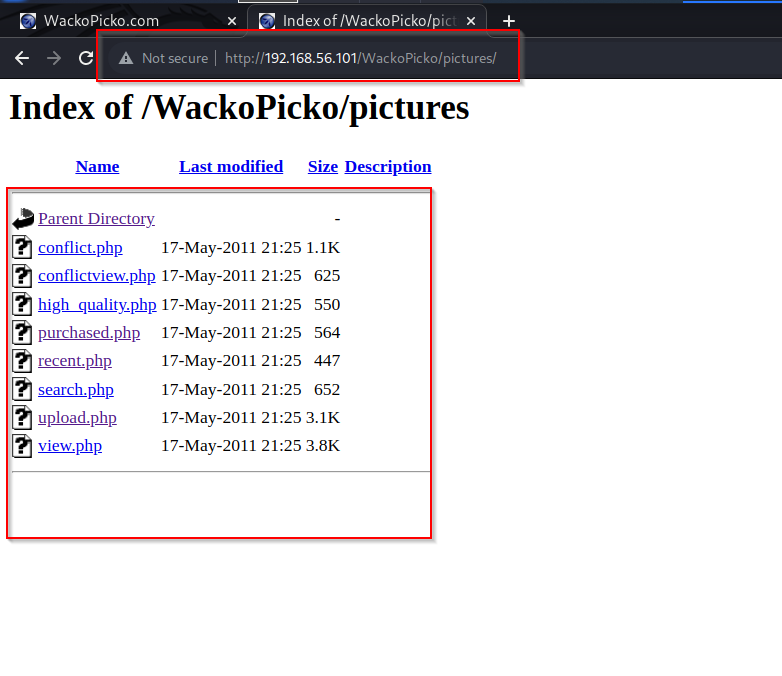
<http://192.168.56.101/WackoPicko/pictures/high_quality.php?picid=9&key=highquality>



**6.Path traversal**

url: <http://192.168.56.101/WackoPicko/pictures/recent.php>

we are in /pictures/recent.php

After removing **recent.php** from URL we got access to Pictures Directory