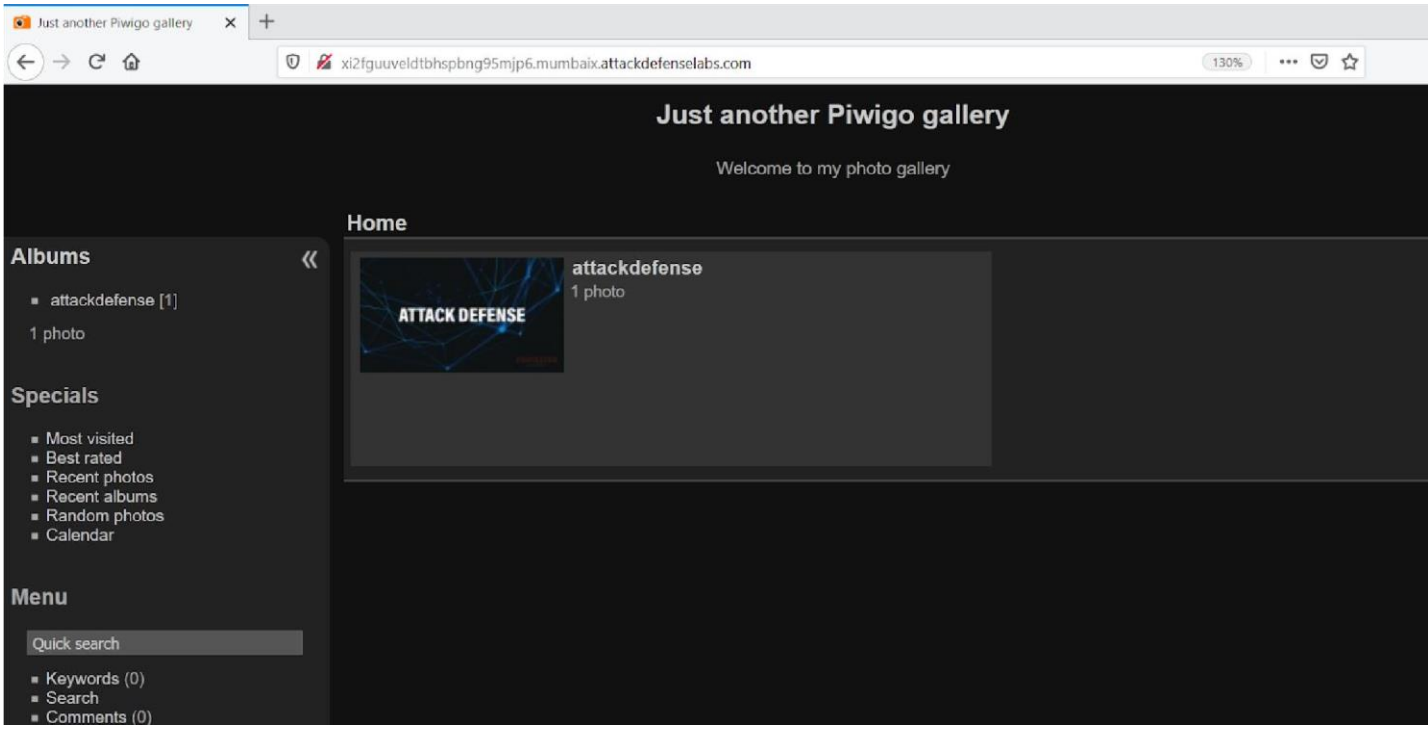
Stored xss solved

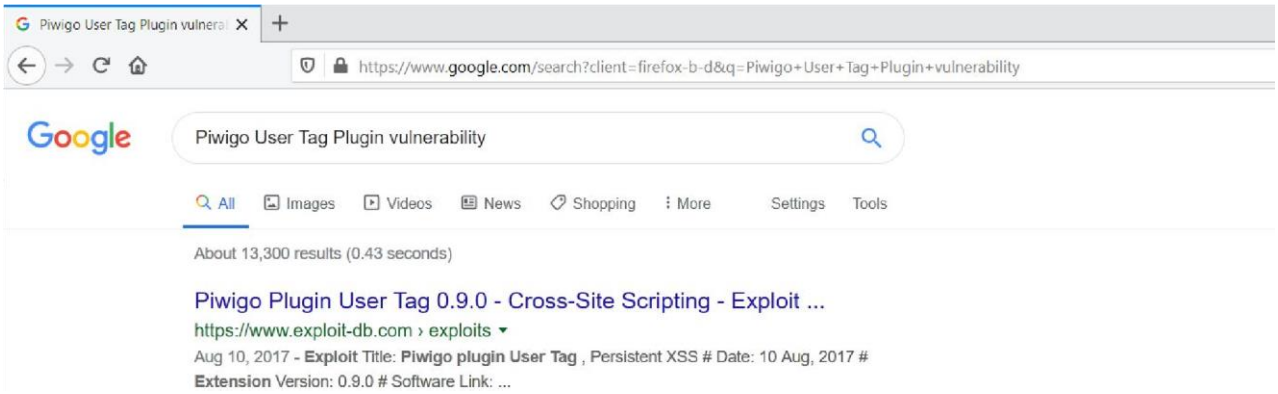
Name	Piwigo User Tag Plugin
URL	https://www.attackdefense.com/challengedetails?cid=329
Type	Real World Webapps : Stored XSS

Solution:

Step 1: Inspect the web application.

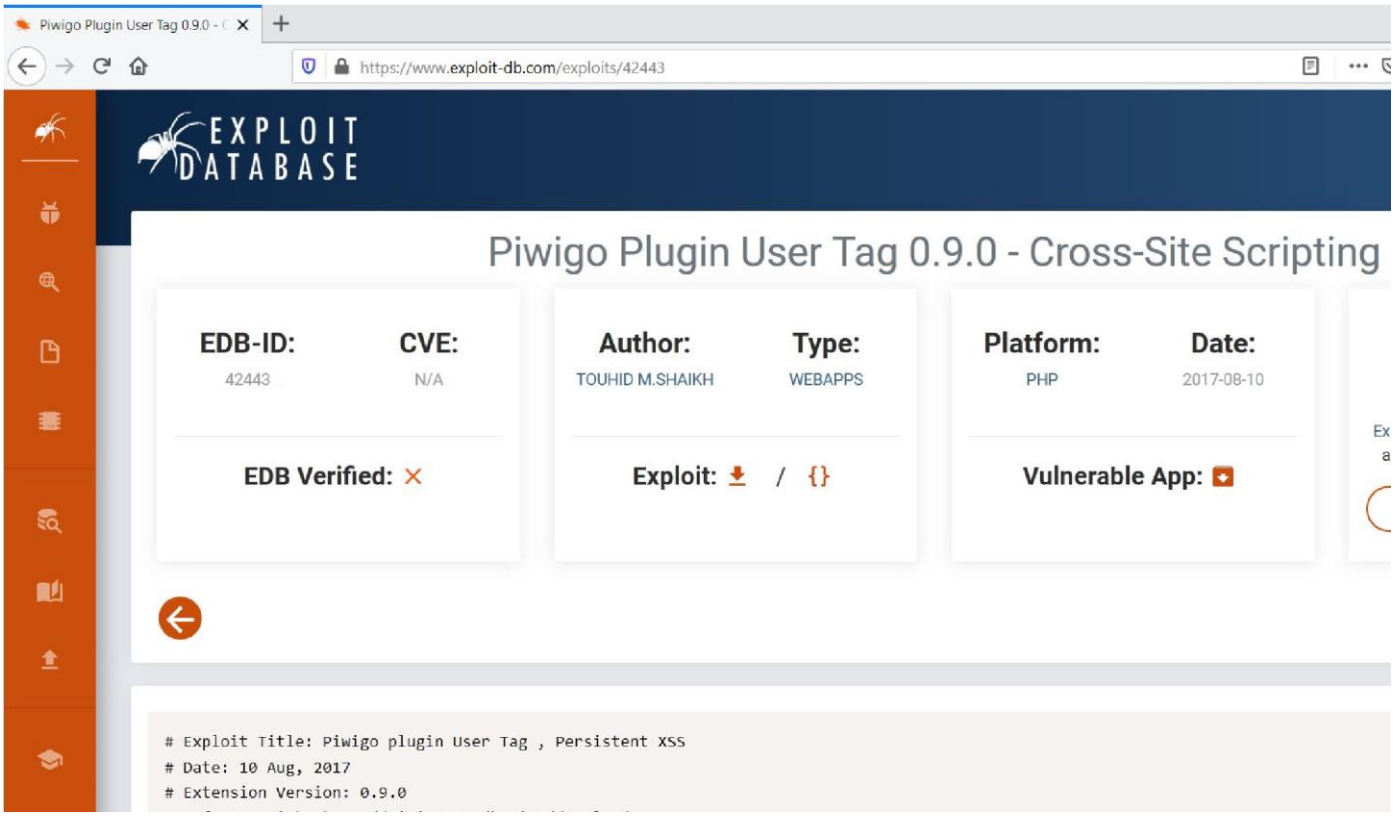


Step 2: Search on google “Piwigo User Tag Plugin vulnerability” and look for publicly available exploits.



The exploit db link contains the payload required to exploit the vulnerability.

Exploit DB Link: https://www.exploit-db.com/exploits/42443



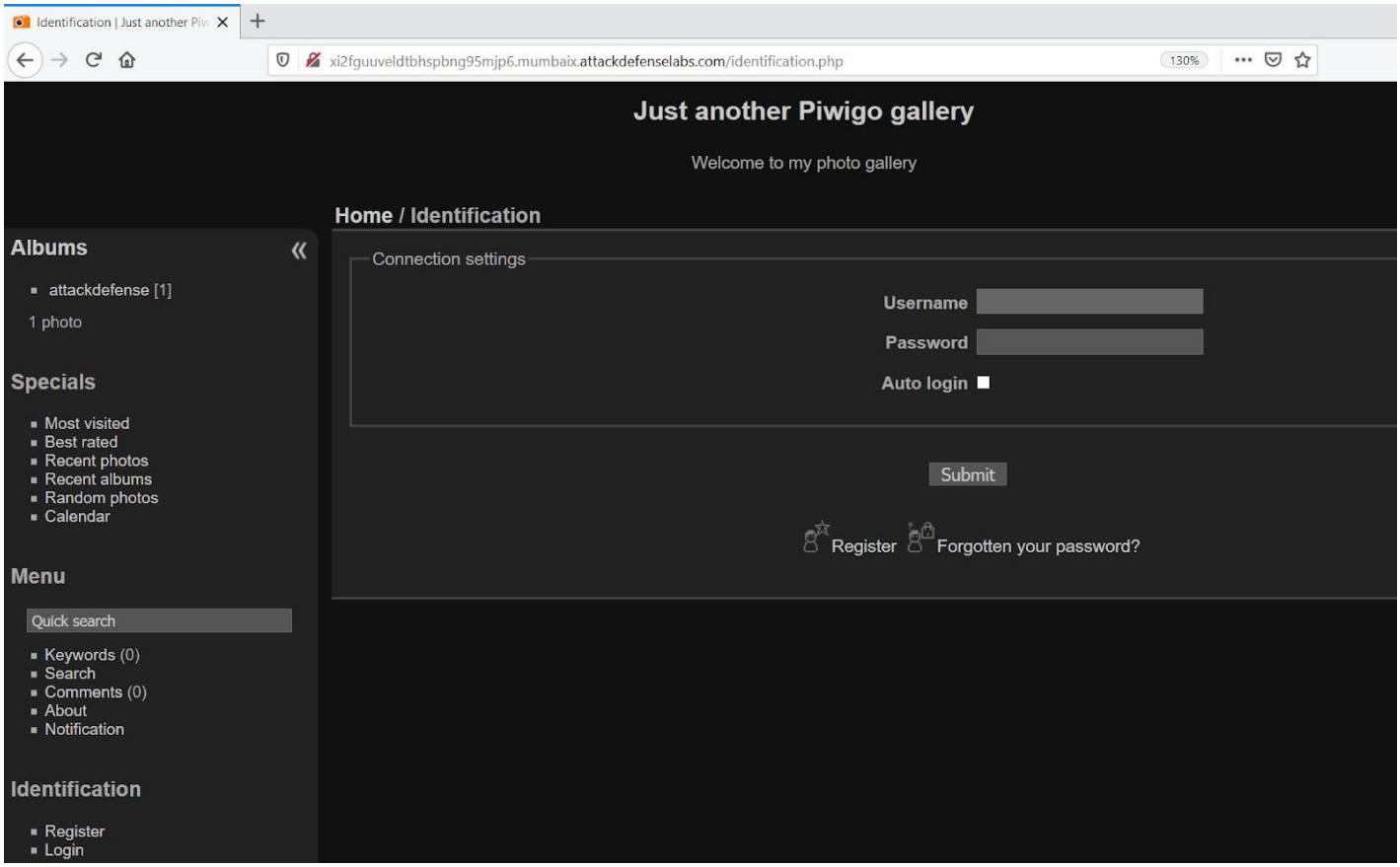
Step 3: The user has to authenticate in order to exploit the vulnerability. The login credentials are provided in the challenge description.

URL: http://xi2fguuveldtbhspbng95mjp6.mumbaix.attackdefenselabs.com/identification.php

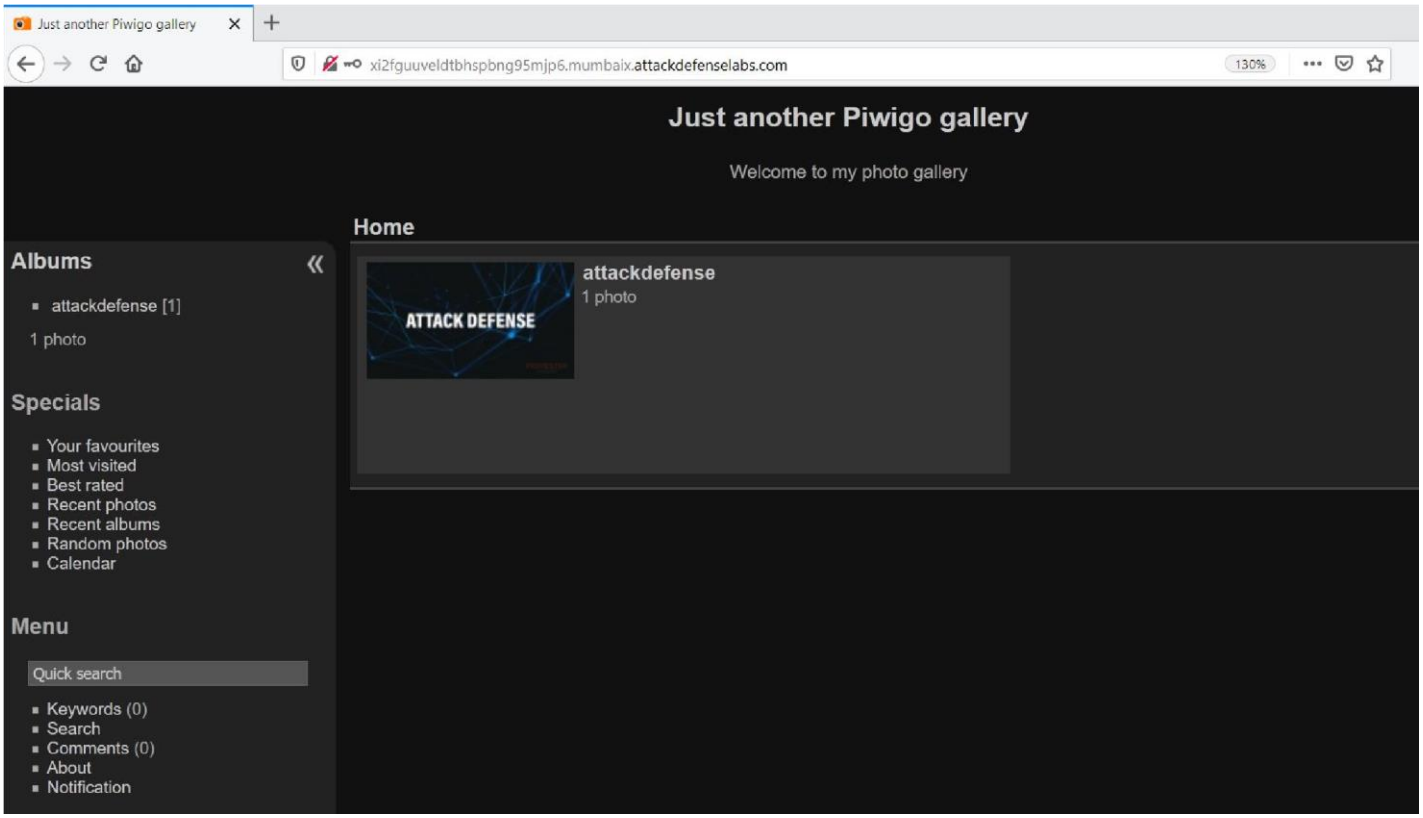
Credentials:

- **Username:** admin
- **Password:** password

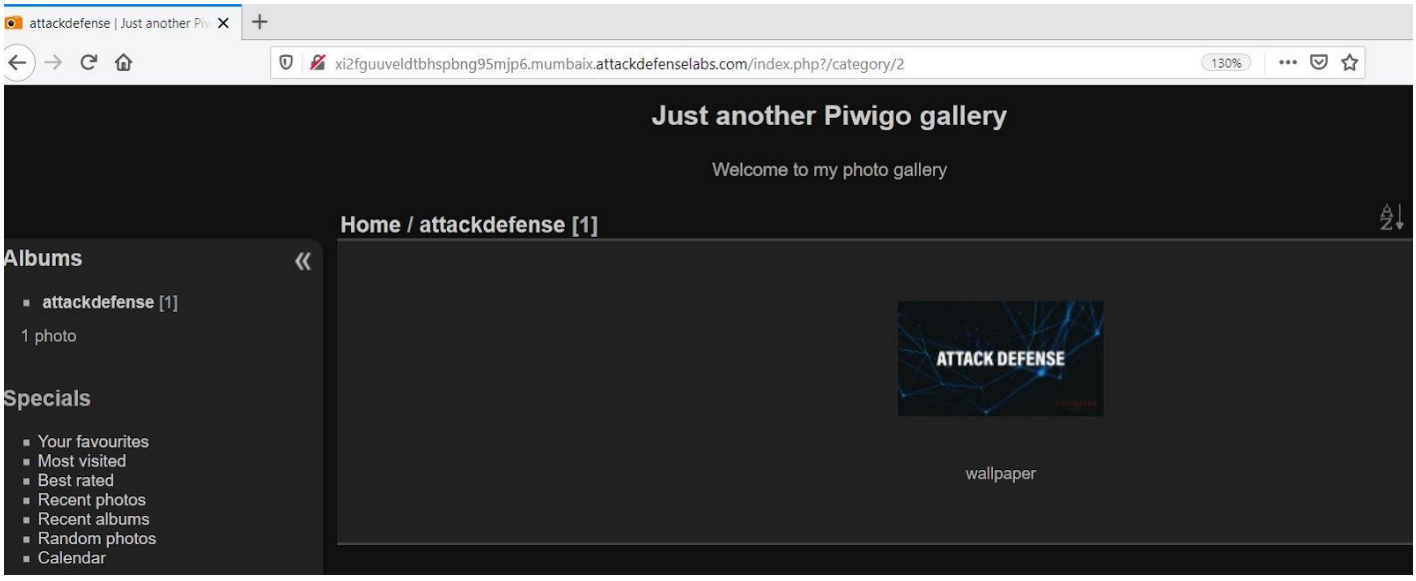
Admin Login



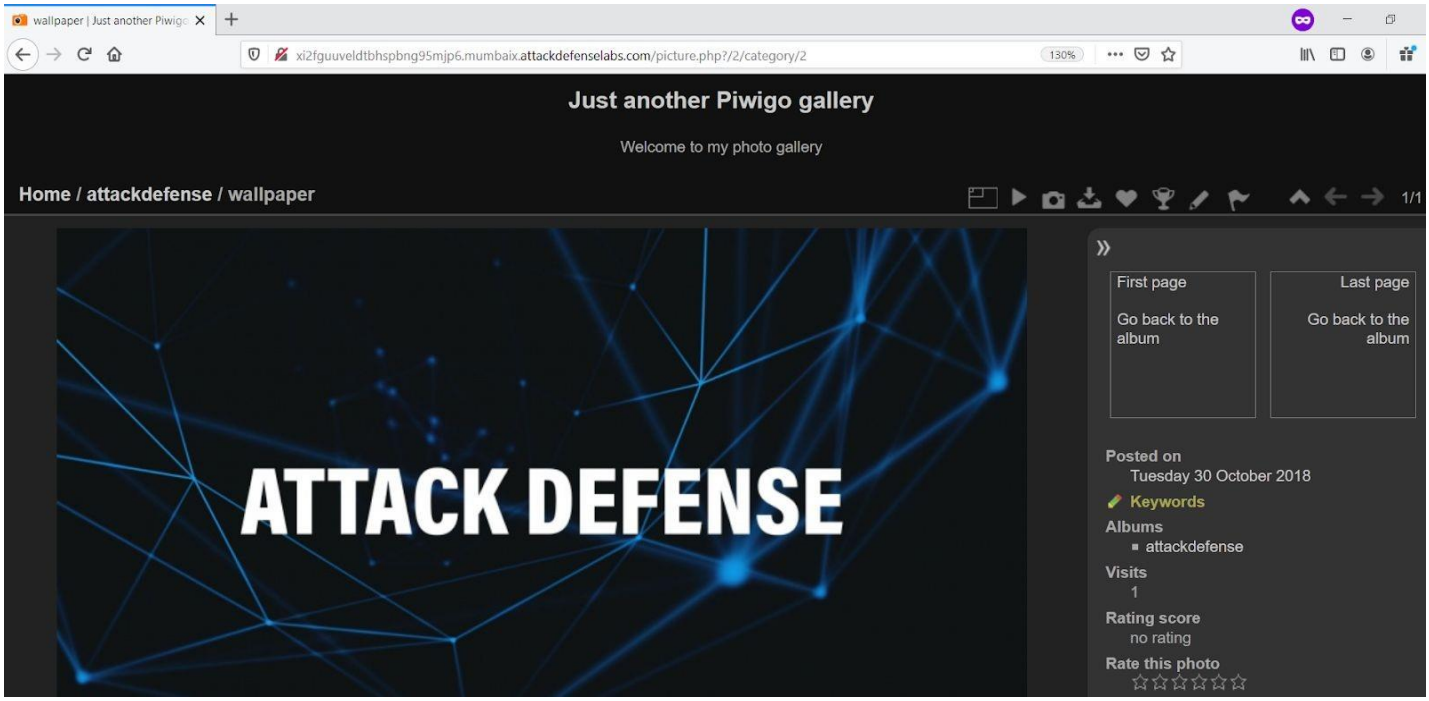
Admin Dashboard



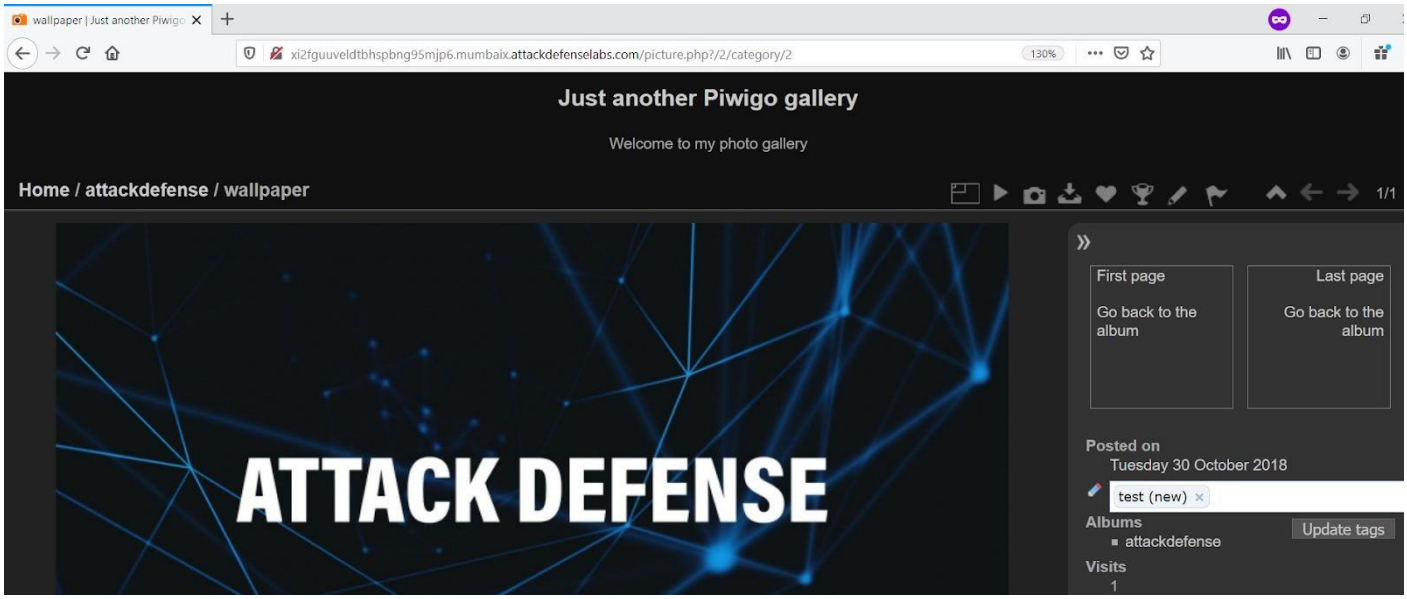
Step 4: Click on the album attackdefense.



Select the wallpaper and click on keywords button

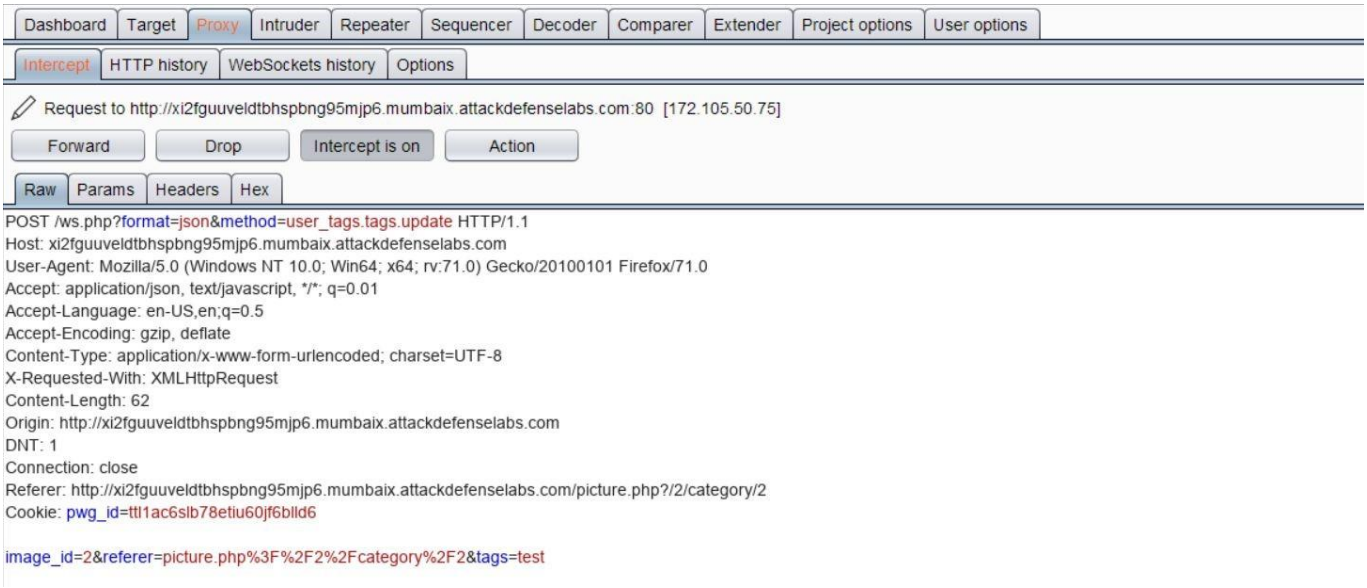


Step 5: Enter anything in keywords.



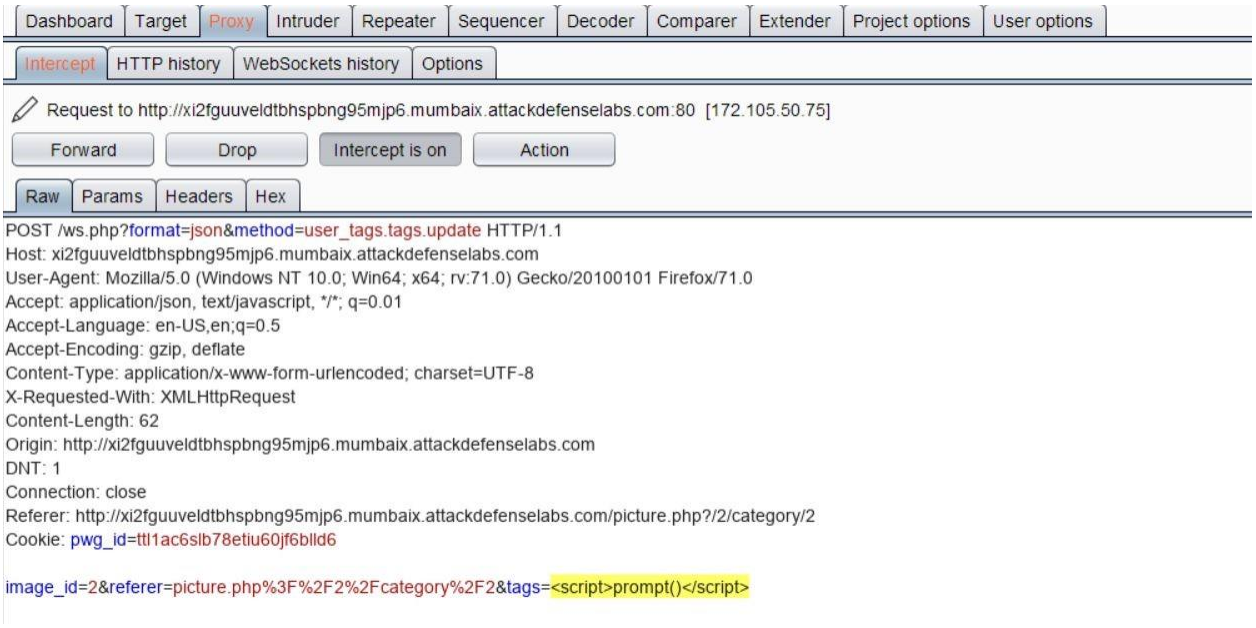
Step 6: Click on Update tags and Intercept the request with burp suite.

To configure Burp Suite check the Appendix.

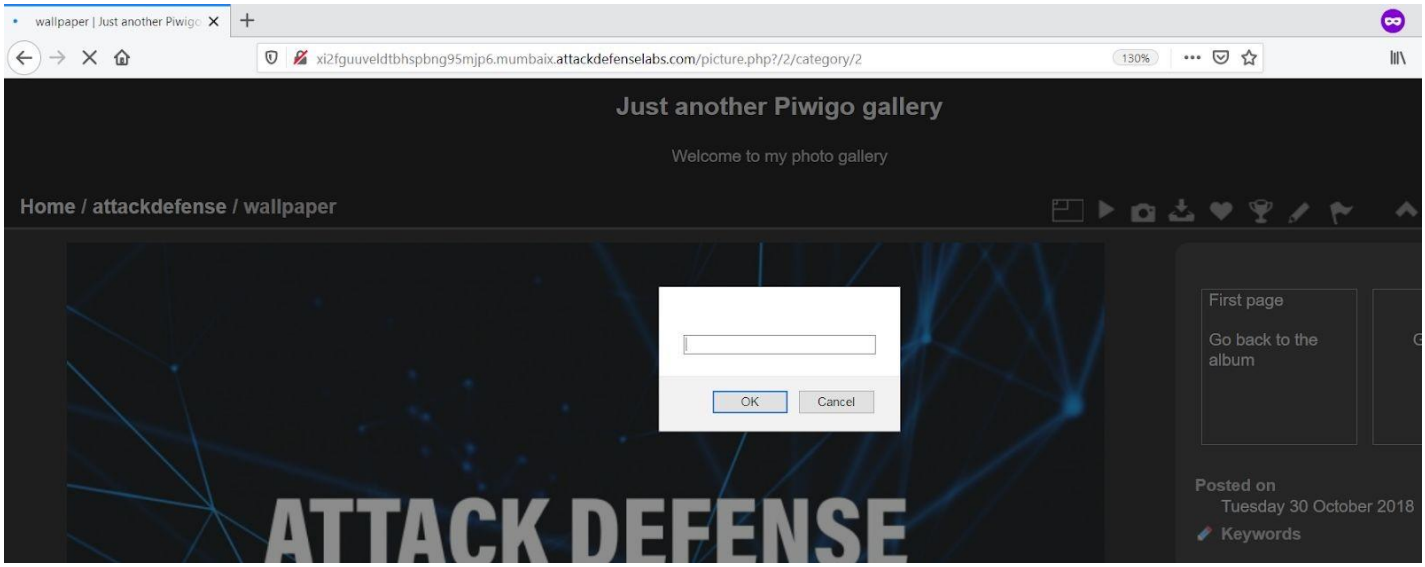


Step 7: Inject the payload in tags field and click on Forward.

Payload: < script>prompt()</script>



Reload the webpage.



The XSS payload triggered successfully.