Syedmudassiruddinalvi Follow
Nov 5 · 3 min read · Listen

CVE-2022–43146: RCE via Arbitrary File Upload

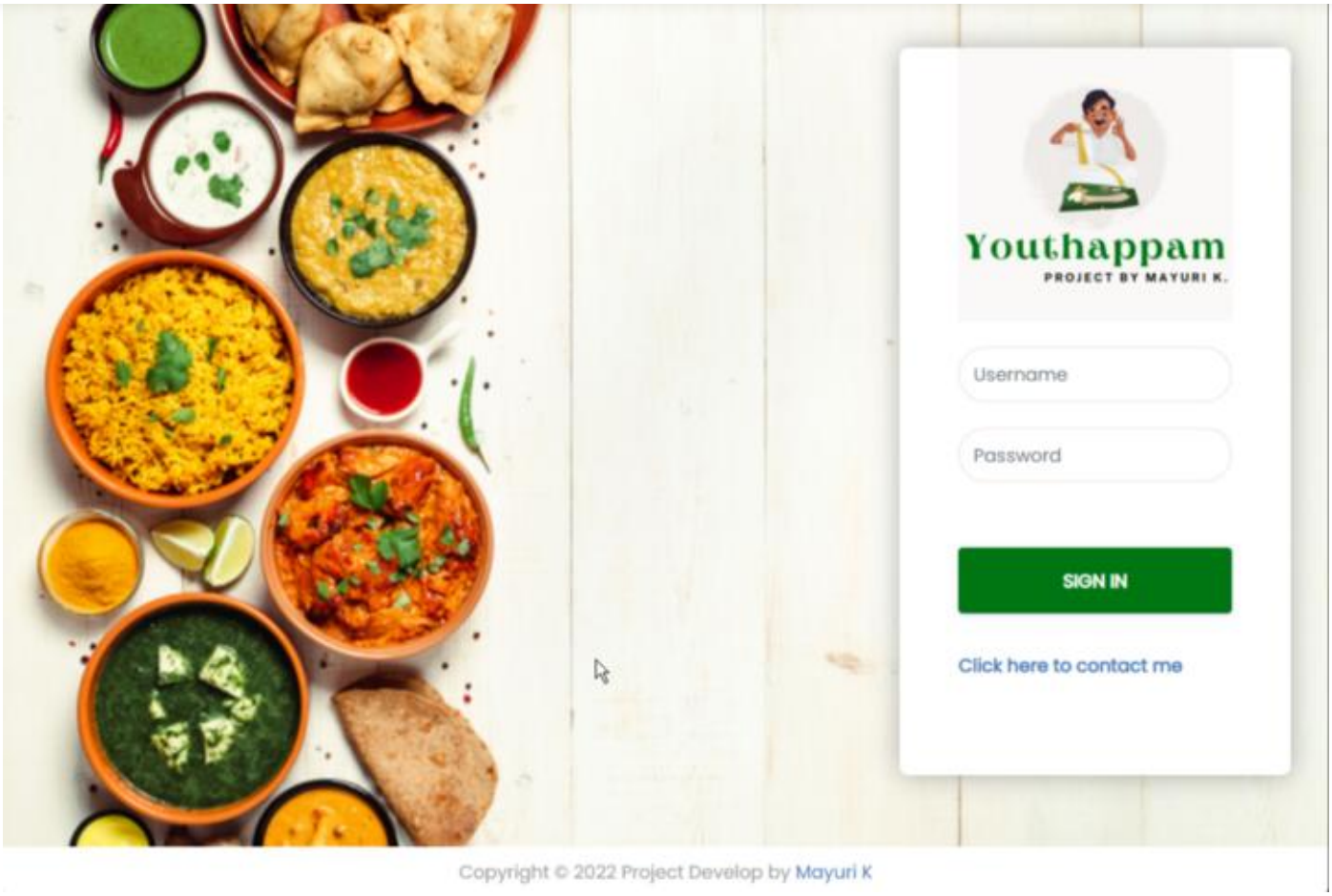
Introduction :

The purpose of this article is to describe CVE-2022–43146 in detail. This CVE is related to remote code execution vulnerability via Arbitrary File Upload which was recently discovered on an open-source Canteen Management System. The motive of this application is to manage orders/invoices and generate reports.

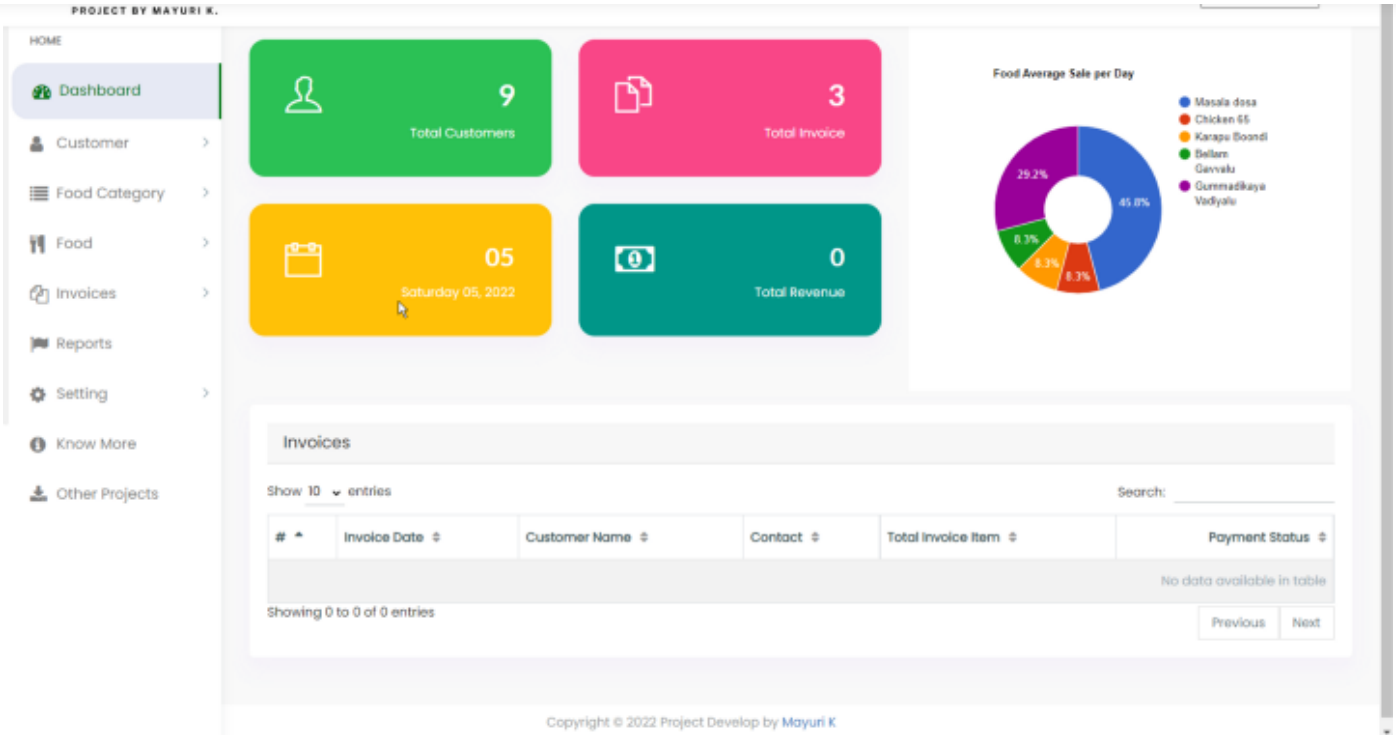
Details:

Effected Application can be downloaded here. We used XAMPP to host the application locally.

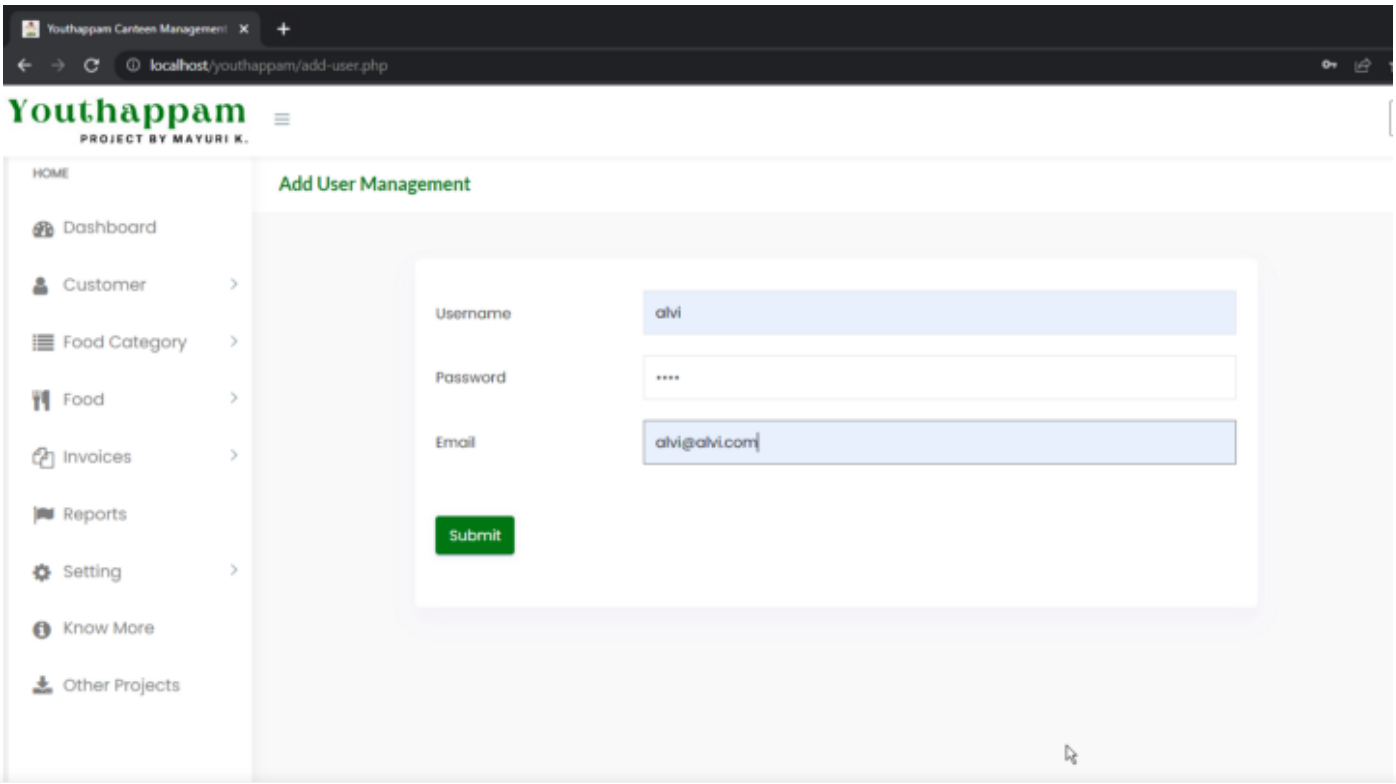
Once the application is up and running we can visit the login page.

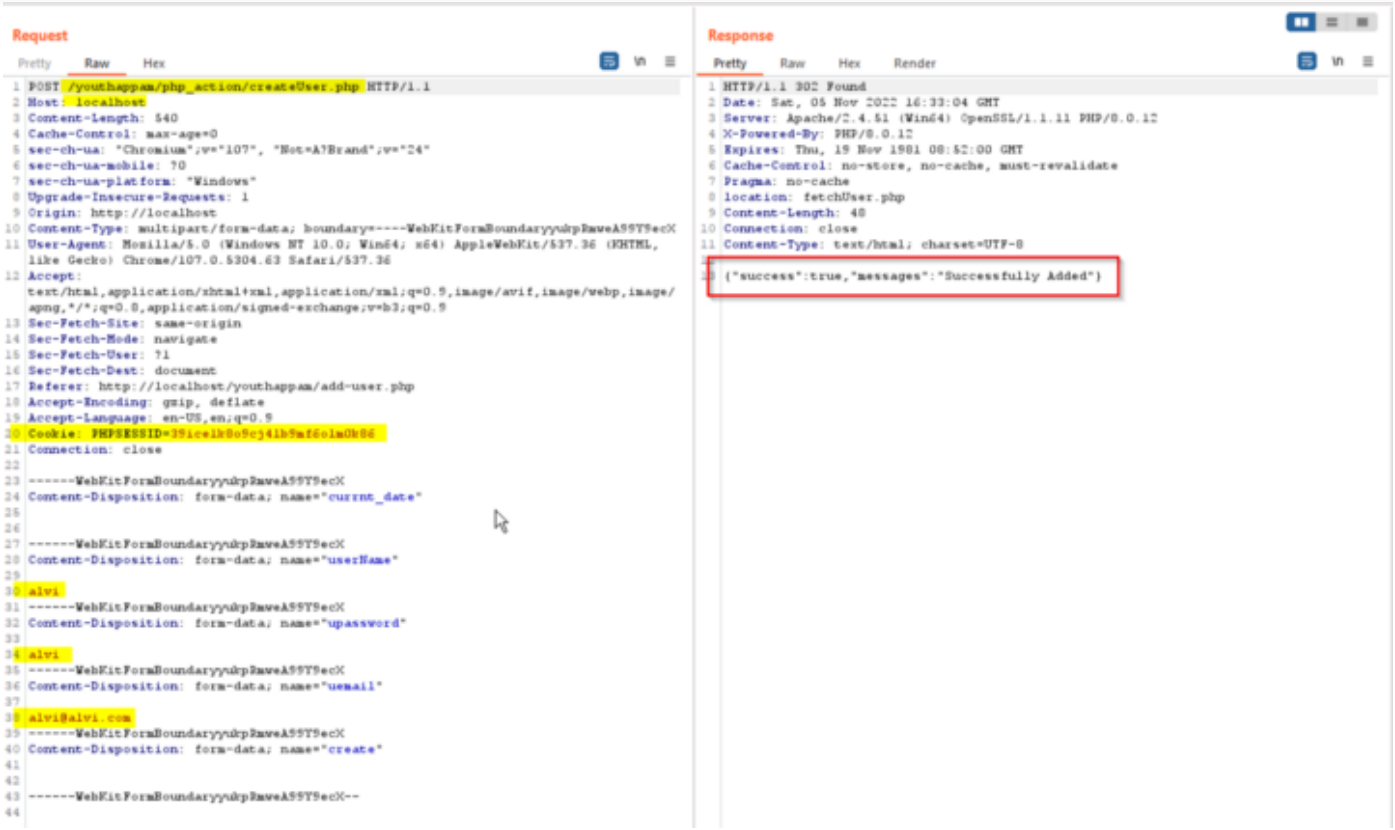


Let us login using a highly privileged account.



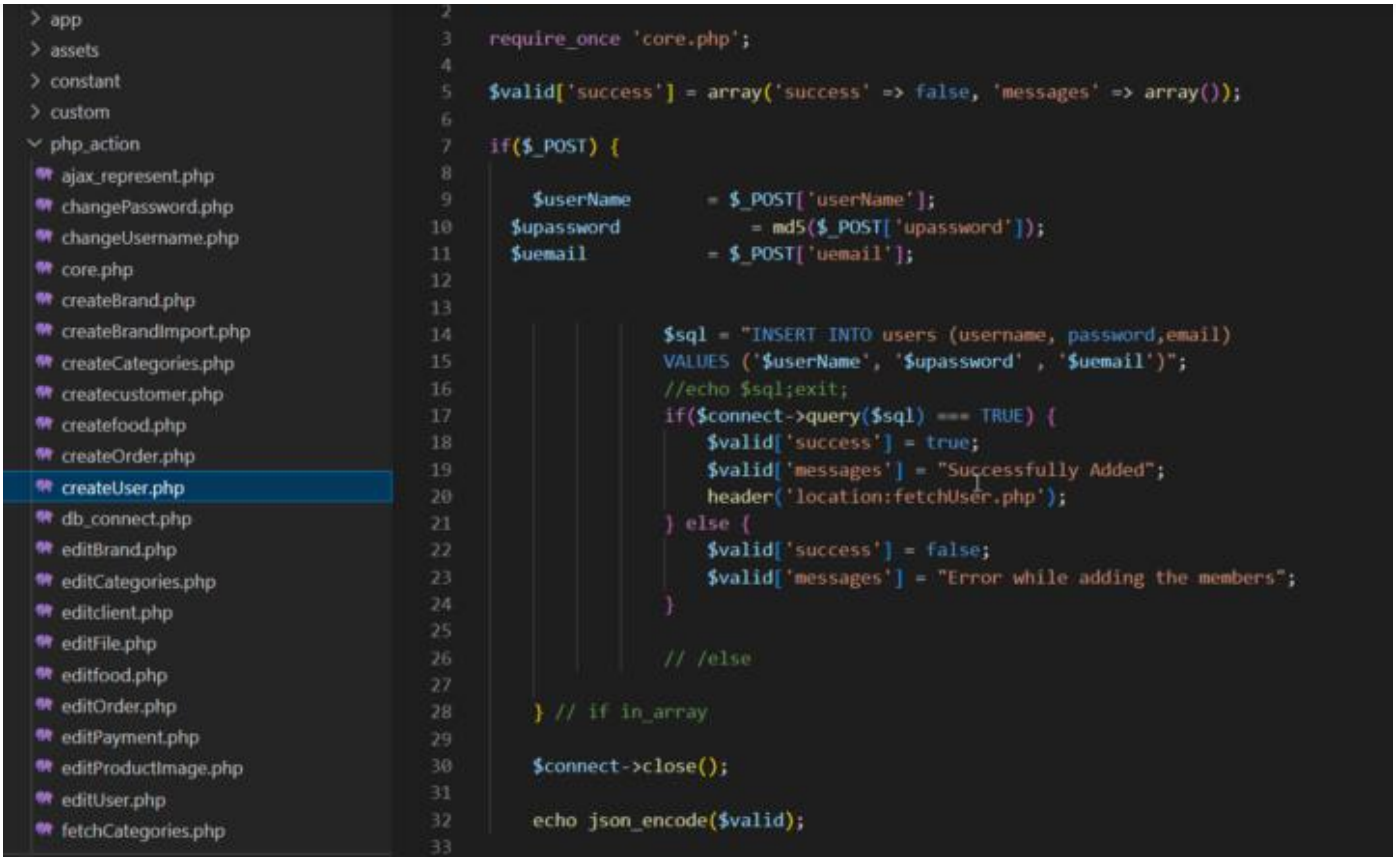
After going through the source code we discovered “add-user.php” which allows a user to add another user.





On adding a user, the application sends a request to the path “/youthappam/php_action/createUser.php”.

lets analysis the createUser.php source code.



From the above code, it is clear that **any user (unauthenticated)can create a user** as the application does not implement logic to check if a user is authenticated or not. let's validate by creating a user without a valid session token.

Let’s check the database if the user was added successfully.

user was successfully added to the database, Trying to log in using a newly created user.


The above-created user is low privileges use. which has limited features on its dashboard. The application does not implement an access control logic, hence this user can be used to perform actions to which a high-privilege user has access. One such feature is the website management feature. We can visit “manage_website.php”

Now We have access to upload image functionality. let’s analyze the source code.


The application does not perform any kind of validation on the file being uploaded and stores the file on “/assets/uploadImage/Logo/*”. enabling users to upload an arbitrary file. Users may upload the below-crafted PHP and perform remote code execution.

```
<?PHP
echo shell_exec($_GET['cmd']);
?>
```

Uploading the above PHP file.


Performing RCE

place a PHP back door to run commands remotely.