

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

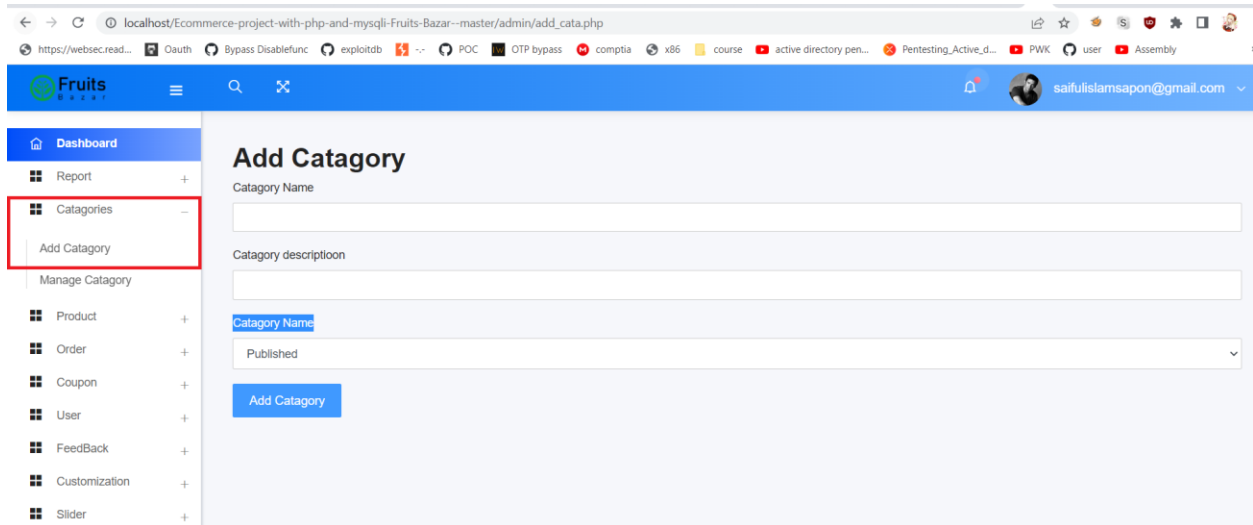
Contact : <https://github.com/APTX-4879>

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

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

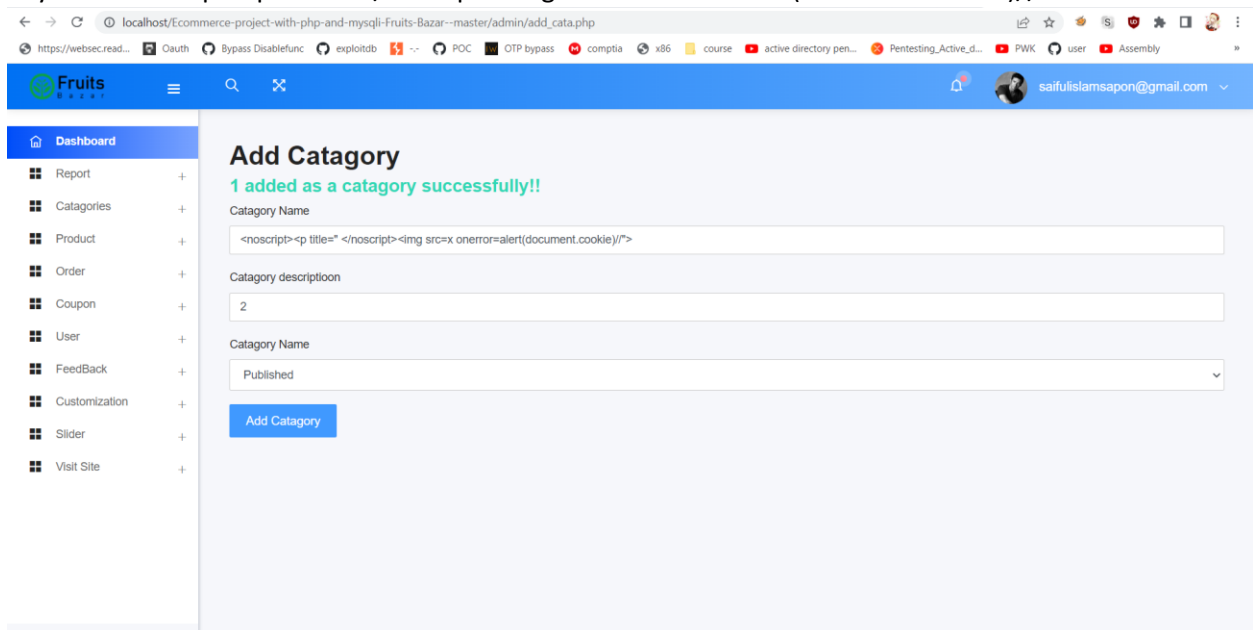
Description: XSS stored exist in Category Name field allow attacker excute arbitrary web script

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

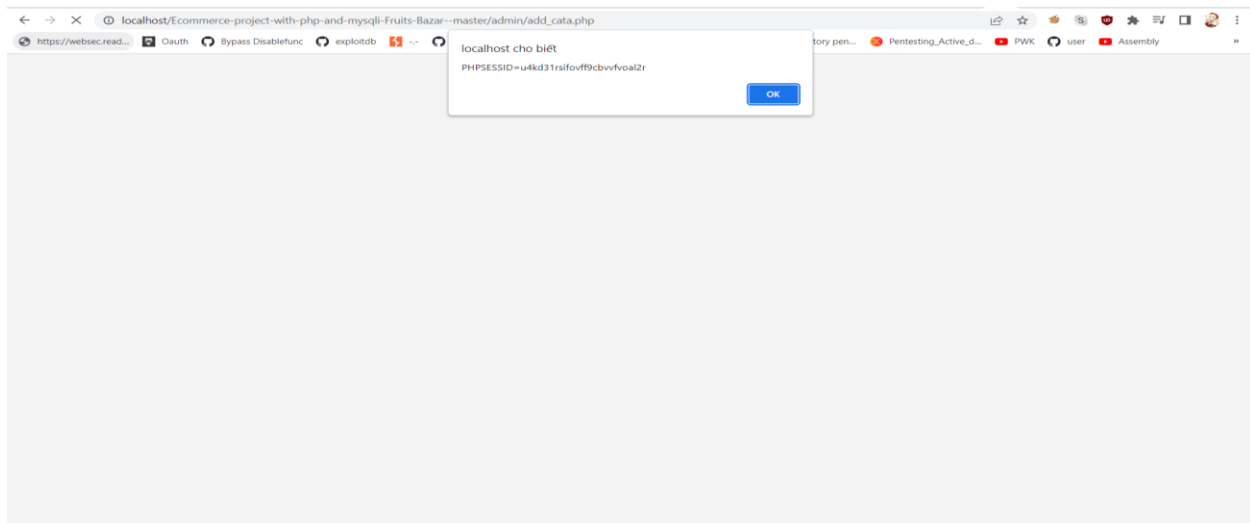


In Category Name field inject payload and click Add Category

Payload: `<noscript><p title=" </noscript>`



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



Vulnerable Code:

add_cata_view.php - Notepad

File Edit Format View Help

<?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";
```

```
    }
```

```
}
```