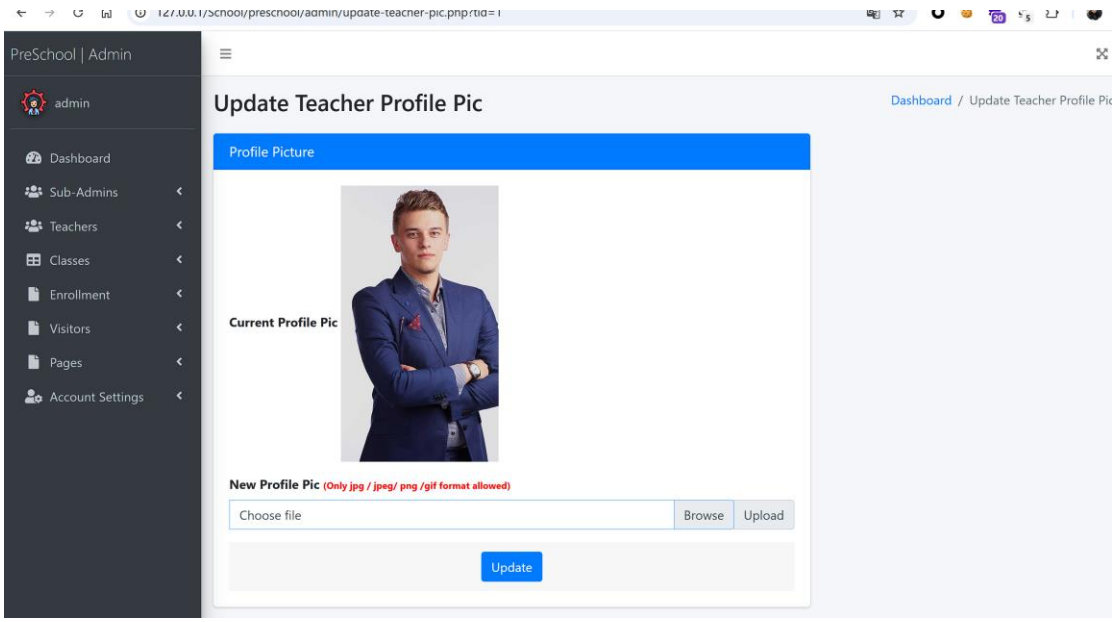
There is an issue with the current profile pic parameter in the update-teacher-pic.chp file, which leads to a directory traversal vulnerability. The issue that was traversed due to this feature being a replacement image function was deleted.

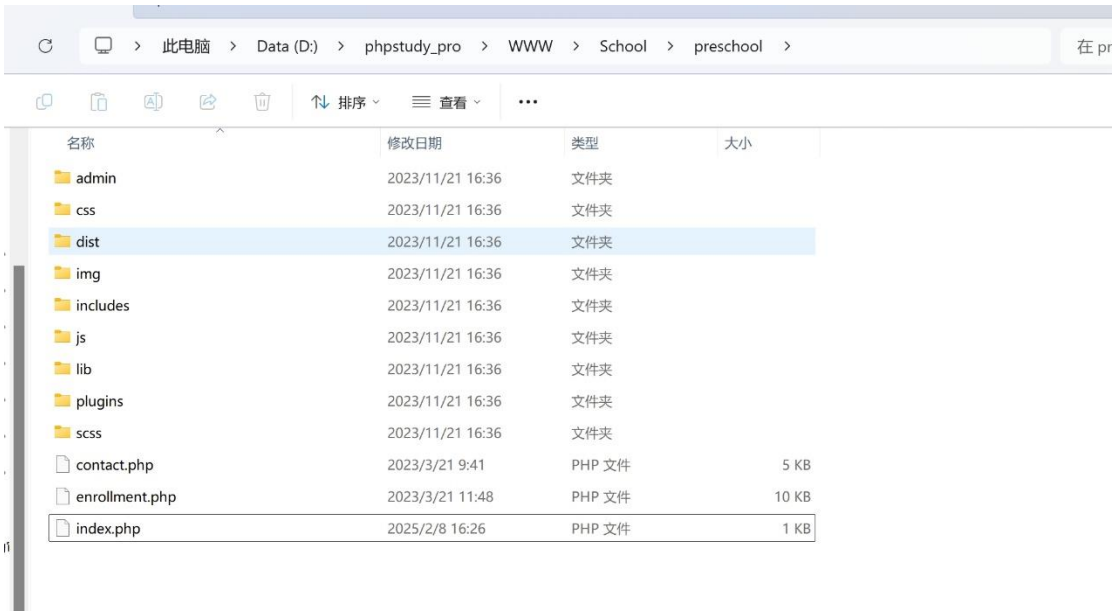
update-teacher-pic.php

```php
<?php session_start();
//Database Connection
include('includes/config.php');
//Validating Session
if(strlen($_SESSION['aid'])==0)
  {
header('location:index.php');
}
else{
//Code for update lawyer image
if(isset($_POST['submit'])){

$lid=intval($_GET['tid']);
//Getting Post Values
$currentpic=$_POST['currentprofilepic'];
$oldprofilepic='teacherspic'.'/'.$currentpic;
$profilepic=$_FILES["profilepic"]["name"];
//get the image extension
$extension = substr($profilepic,strlen($profilepic)-4,
strlen($profilepic));
//allowed extensions
$allowed_extensions = array(".jpg","jpeg",".png",".gif");
//Validation for allowed extensions .in_array() function
searches an array for a specific value.
if(!in_array($extension,$allowed_extensions))
{
echo "<script>alert('Invalid format. Only jpg / jpeg/ png /
gif format allowed');</script>";
}
else
{
//rename the image file
$newprofilepic=md5($profilepic).time().$extension;
//Code for move image into directory
move_uploaded_file($_FILES["profilepic"]["tmp_name"],
"teacherspic/".$newprofilepic);

```

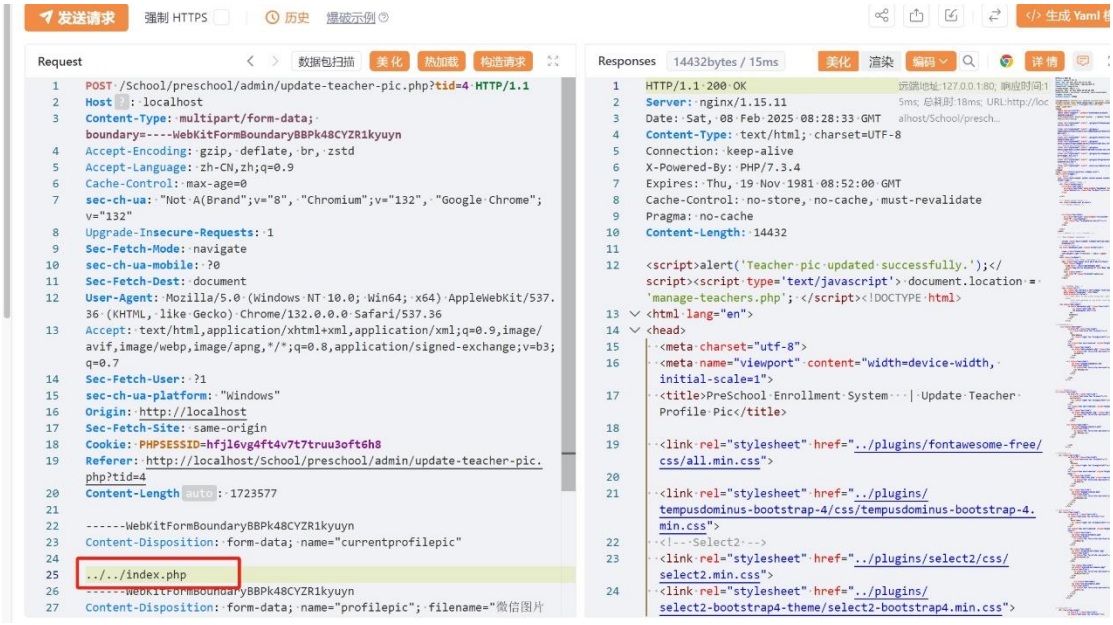
Log in to the backend management page, Update Teacher Profile Pic




View the index.php file in the directory




Problem Parameters:currentprofilepic




Index.php file has been deleted