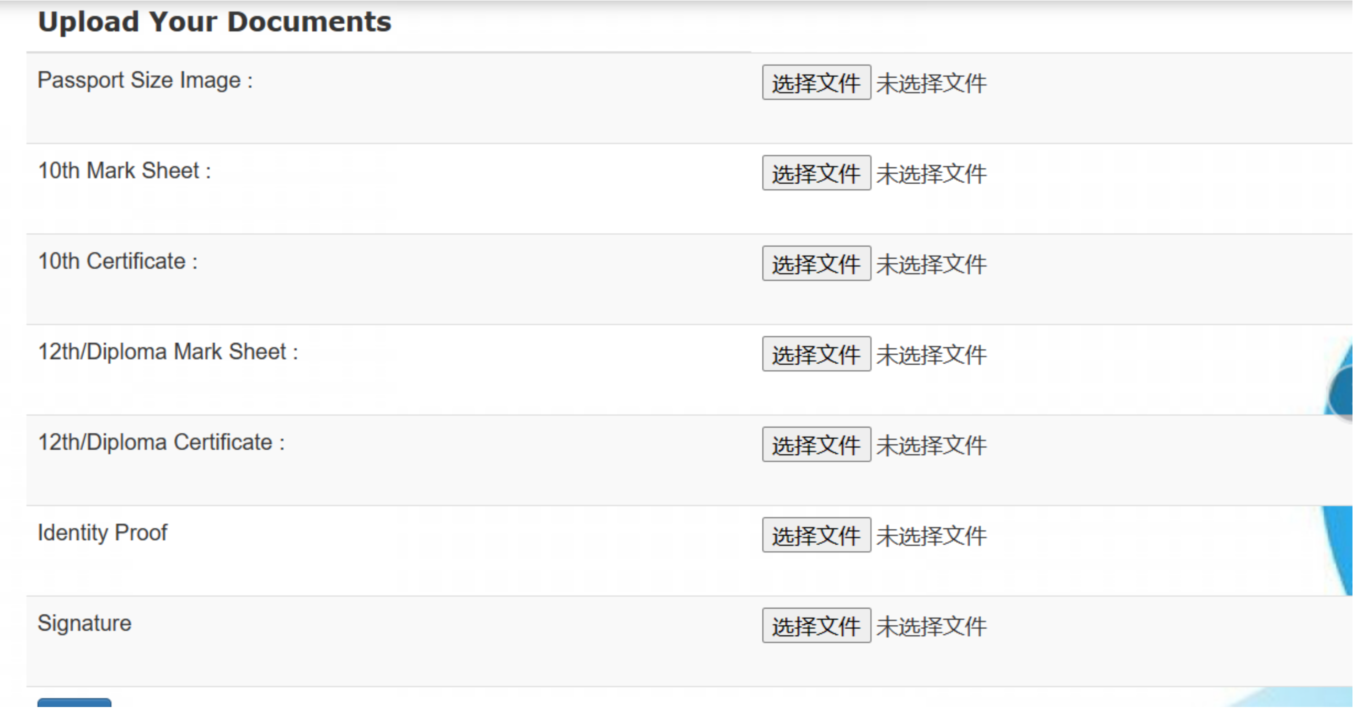
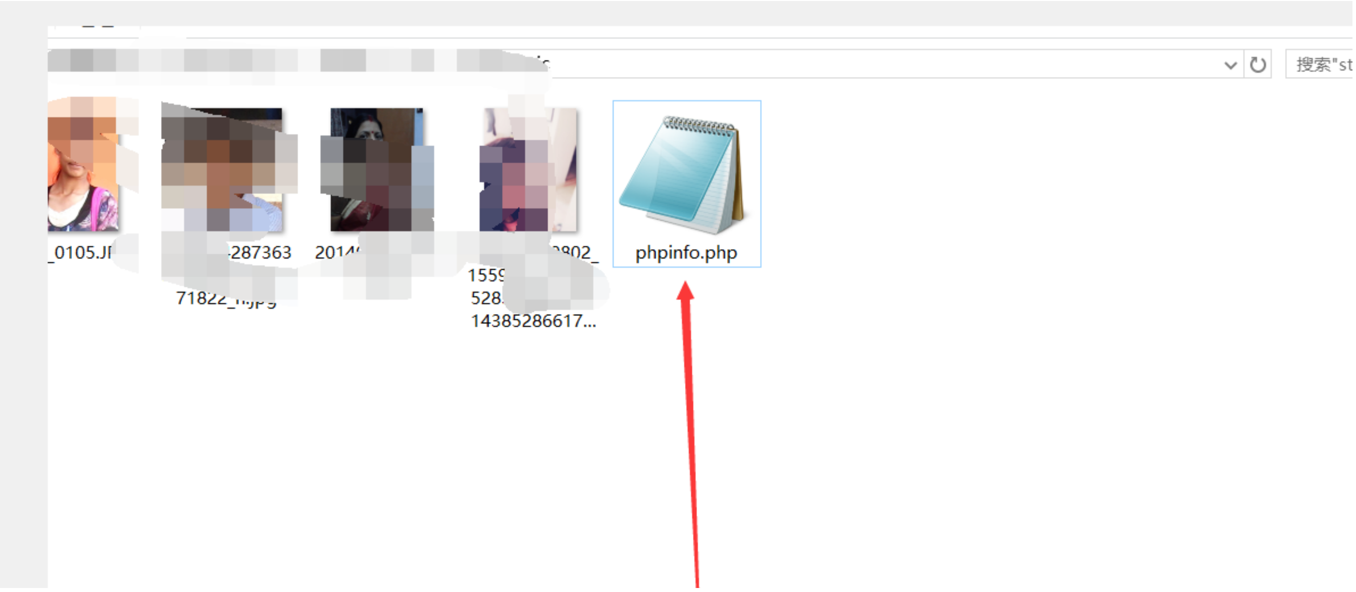
Admission Management System has a file upload (RCE) vulnerability

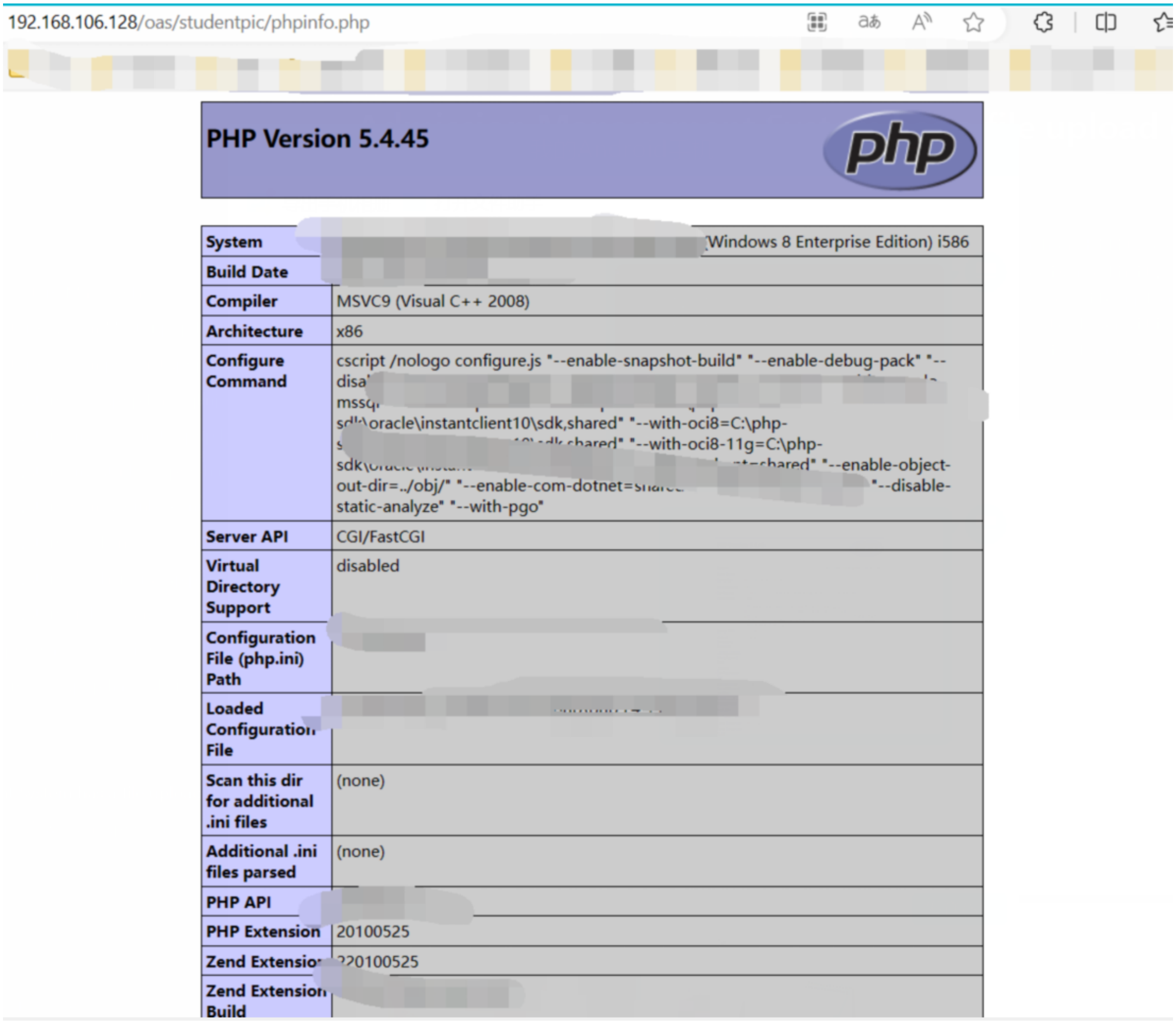
```
Admission Management System has a file upload (RCE) vulnerability, vulnerability exists
in student_avatar.php file, Can upload any format of the file, and there is no limit, the
file name is the file name when uploaded, developers should limit the type of file
uploaded by users, otherwise it will lead to users to obtain server permissions, steal
sensitive data, serious or even lead to server crash, a large number of user privacy
disclosure.
```



Upload Your Documents

Passport Size Image :	选择文件 未选择文件
10th Mark Sheet :	选择文件 未选择文件
10th Certificate :	选择文件 未选择文件
12th/Diploma Mark Sheet :	选择文件 未选择文件
12th/Diploma Certificate :	选择文件 未选择文件
Identity Proof	选择文件 未选择文件
Signature	选择文件 未选择文件



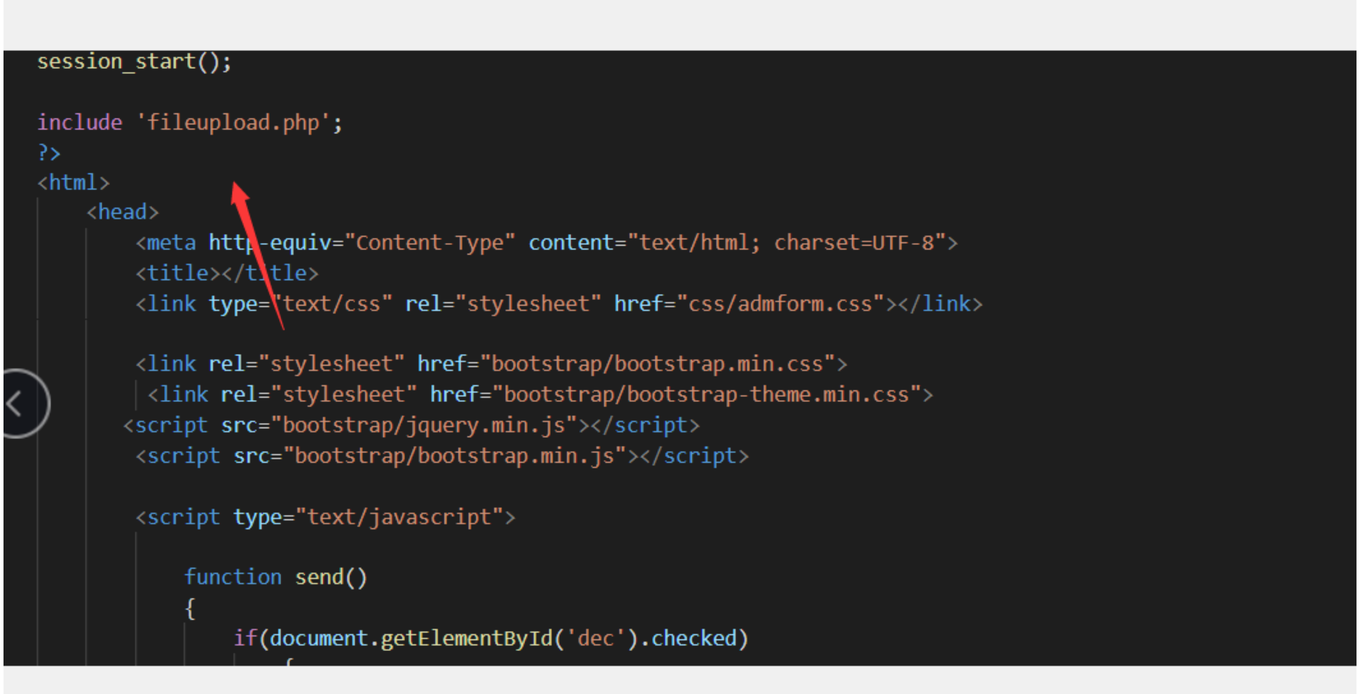


192.168.106.128/oas/studentpic/phpinfo.php

[redacted]

PHP Version 5.4.45

System	[redacted] Windows 8 Enterprise Edition) i586
Build Date	[redacted]
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disa [redacted] sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-s [redacted] sdk,shared" "--with-oci8-11g=C:\php-sdk [redacted] "--enable-object-out-dir=../obj/" "--enable-com-dotnet= [redacted] "--disable-static-analyze" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	[redacted]
Loaded Configuration File	[redacted]
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	[redacted]
PHP Extension	20100525
Zend Extension	220100525
Zend Extension Build	[redacted]



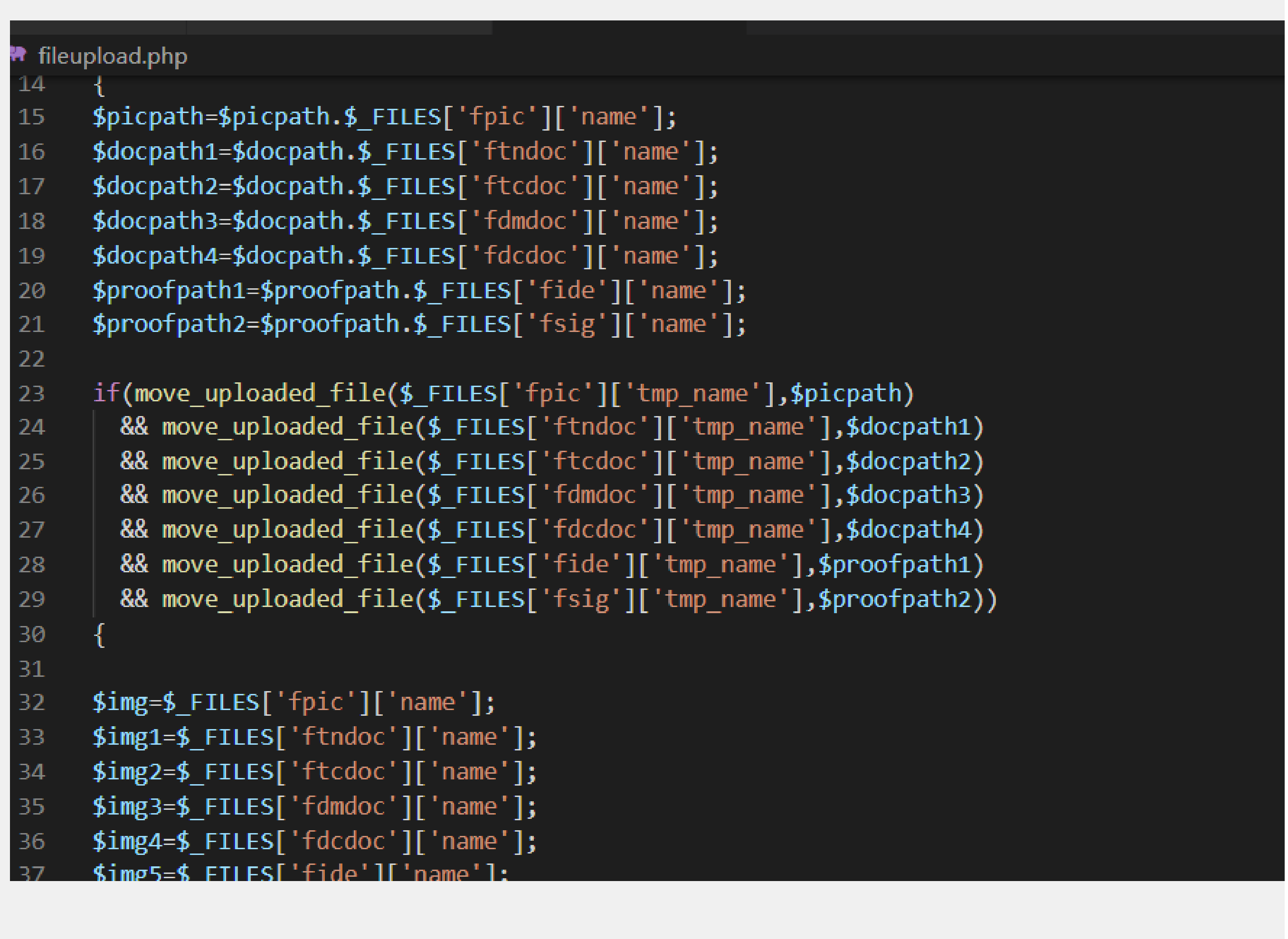
```
session_start();

include 'fileupload.php';
?>
<html>
    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
        <title></title>
        <link type="text/css" rel="stylesheet" href="css/admform.css"></link>

        <link rel="stylesheet" href="bootstrap/bootstrap.min.css">
         <link rel="stylesheet" href="bootstrap/bootstrap-theme.min.css">
       <script src="bootstrap/jquery.min.js"></script>
        <script src="bootstrap/bootstrap.min.js"></script>

        <script type="text/javascript">

            function send()
            {
                if(document.getElementById('dec').checked)
```



```
{
$picpath=$picpath.$_FILES['fpic']['name'];
$docpath1=$docpath.$_FILES['ftndoc']['name'];
$docpath2=$docpath.$_FILES['ftcdoc']['name'];
$docpath3=$docpath.$_FILES['fdmdoc']['name'];
$docpath4=$docpath.$_FILES['fdcdoc']['name'];
$proofpath1=$proofpath.$_FILES['fide']['name'];
$proofpath2=$proofpath.$_FILES['fsig']['name'];

if(move_uploaded_file($_FILES['fpic']['tmp_name'],$picpath)
  && move_uploaded_file($_FILES['ftndoc']['tmp_name'],$docpath1)
  && move_uploaded_file($_FILES['ftcdoc']['tmp_name'],$docpath2)
  && move_uploaded_file($_FILES['fdmdoc']['tmp_name'],$docpath3)
  && move_uploaded_file($_FILES['fdcdoc']['tmp_name'],$docpath4)
  && move_uploaded_file($_FILES['fide']['tmp_name'],$proofpath1)
  && move_uploaded_file($_FILES['fsig']['tmp_name'],$proofpath2))
{

$img=$_FILES['fpic']['name'];
$img1=$_FILES['ftndoc']['name'];
$img2=$_FILES['ftcdoc']['name'];
$img3=$_FILES['fdmdoc']['name'];
$img4=$_FILES['fdcdoc']['name'];
$img5=$_FILES['fide']['name'];
```