

Gym Management System Any file upload execution command

The existence point of the vulnerability is in admin/add_exercises. PHP, and no filtering is done on file upload, resulting in the uploading of malicious files with command execution function to obtain server information.

```
//Text Data Variables
$user_name= $_POST['user'];
$exer_name= $_POST['exercise'];
$day_name= $_POST['day'];
$sets= $_POST['sets'];

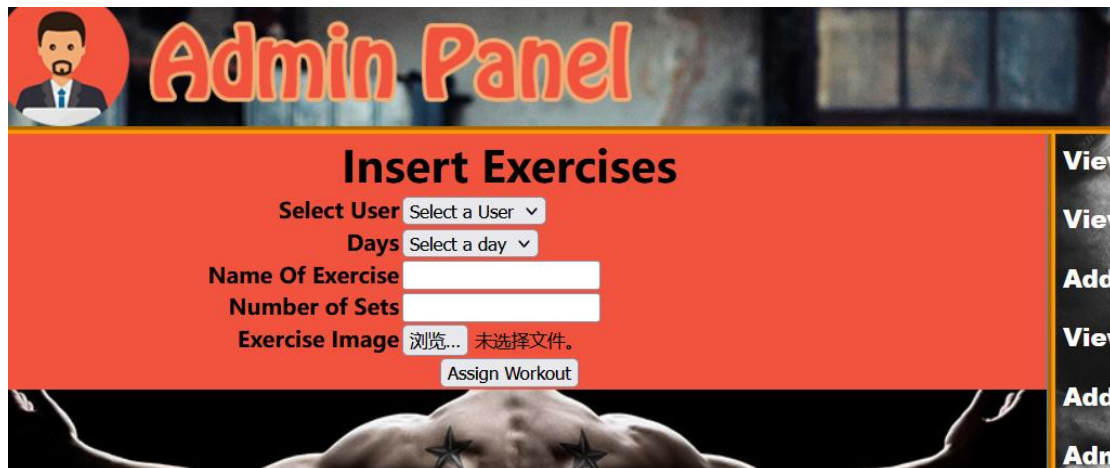
// Image Name
$exercise_img= $_FILES['exer_img']['name'];

//Images Temp Name
$temp_name= $_FILES['exer_img']['tmp_name'];

//Validations
if($user_name==''){
    echo "<script>alert('Please Fill All The Fields!')</script>";
    exit();
}
elseif ($exer_name=='') {
    echo "<script>alert('Please Fill All The Fields!')</script>";
    exit();
}
elseif ($day_name=='') {
    echo "<script>alert('Please Fill All The Fields!')</script>";
    exit();
}
elseif ($sets=='') {
    echo "<script>alert('Please Fill All The Fields!')</script>";
    exit();
}
elseif ($exercise_img=='') {
    echo "<script>alert('Please Fill All The Fields!')</script>";
    exit();
}
}
else{
    move_uploaded_file($temp_name, "exercise_images/$exercise_img");

    //Query For Inserting Workout Into Database
```

Hole location



Admin Panel

Insert Exercises

Select User

Days

Name Of Exercise

Number of Sets

Exercise Image 未选择文件。

View
View
Add
View
Add
Adm

Vulnerability to prove

PHP Version 7.3.4	
System	Windows NT DESKTOP-PG96EO3 10.0 build 19042 (Windows 10) AMD64
Build Date	Apr 2 2019 21:50:57
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cmd /c "nololo configure.js --enable-snapshot-build --enable-debug-pack --disable-zts --with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared --with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared --enable-object-out-dir=../obj/" --enable-com-dotnet=shared --without-analyzer --with-pgo
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	C:\phpstudy_pro\Extensions\php\php7.3.4nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,NTS,VC15

Download the source code:

<https://www.sourcecodester.com/php/15515/gym-management-system-project-php.html>
