

Unrestricted file upload vulnerability was found in `"/Membership/edit_member.php"` of the Kashipara Live Membership System v1.0 allows attackers to execute arbitrary code via uploading a crafted PHP file.

**Affected Vendor:** KASHIPARA (<https://www.kashipara.com/>)

**Product Official Website URL:** Live Membership System  
(<https://www.kashipara.com/project/php/12997/live-membership-system-in-php-php-project-source-code>)

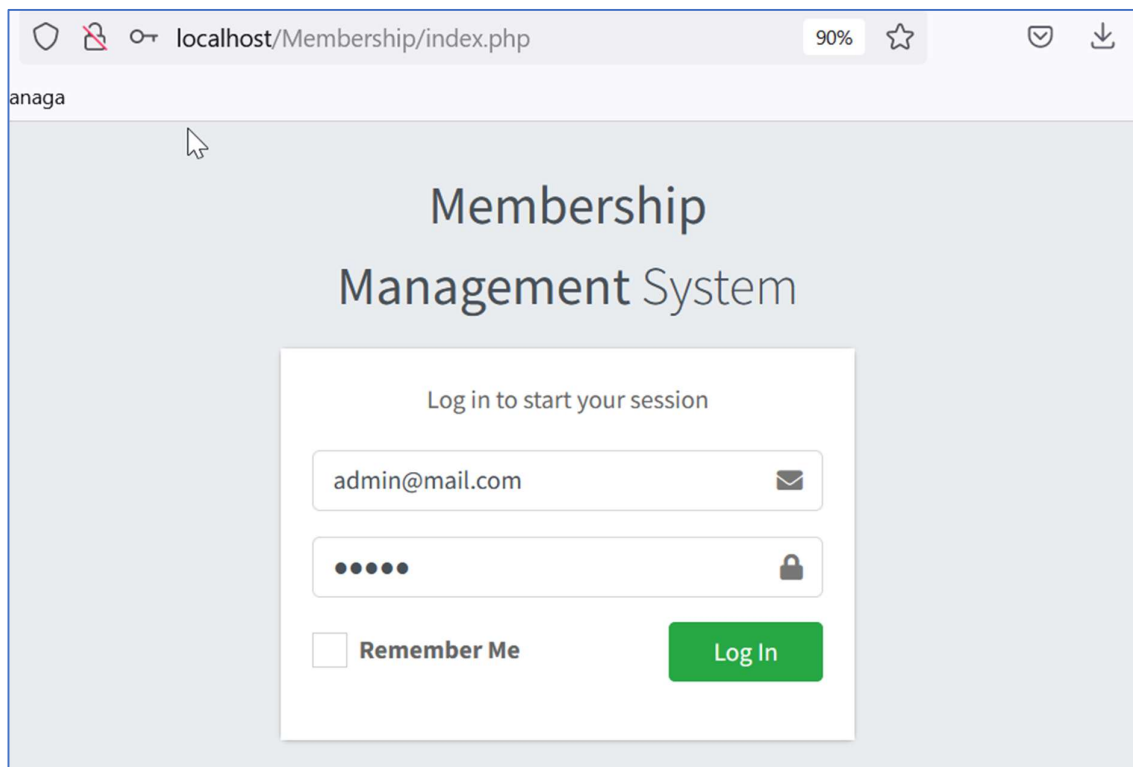
**Version:** 1.0

**Affected Components:**

- **Affected Code File:** `/Membership/edit_member.php`

**Steps:**











1. Login as admin user in the Live Membership System v1.0 (URL: <http://localhost/Membership/index.php>)



2. After successful login, go to menu "Manage Members".

3. Try to edit profile details of any member (member = "Testing Member") by clicking on the edit action button.

The screenshot shows a web application interface for managing members. The left sidebar contains a navigation menu with the following items: Dashboard, Membership Types, Add Members, Manage Members (highlighted with a red box), Renewal, Membership Report, Revenue Report, Settings, and Logout. The main content area is titled 'Manage Members' and displays a table of members. The table has columns: #, Fullname, Contact, Email, Address, Type, Status, and Actions. The row for 'Testing Member' (CA-519259) is highlighted with a red box, and its 'Actions' column contains an edit icon.

#	Fullname	Contact	Email	Address	Type	Status	Actions
CA-053289	Demo Member	7777777770	member@demo.com	77 demo	Premium	Active	 
CA-159695	Member A	1111111100	membera@test.com	11 test	Silver	Active	 
CA-373031	Demo Test	7412121455	demo@test.com	77 address	Gold	Active	 
CA-519259	Testing Member	1212121212	testing@mail.com	77 demo	Basic	Expired	 
CA-610243	Qwerty	1010101012	qwerty@mail.com	77 asd	Gold	Expired	 

4. Upload the PHP shell file in the "Member Photo" section with below details:

- File Name: **Shell2.php**
- File content: **<?php phpinfo();?>**

localhost/Membership/edit\_member.php?id=10

### Edit Members

Edit Member Details

<b>Full Name</b>	<b>Date of Birth</b>
Testing Member	12/12/1985
<b>Contact Number</b>	<b>Email</b>
1212121212	testing@mail.com
<b>Address</b>	<b>Country</b>
77 demo	demooo
<b>Postcode</b>	<b>Occupation</b>
1111	demodemo

**Member Photo**

Browse... Shell2.php

Leave it blank if you don't want to change the photo.

Submit

Intercept HTTP history WebSockets history Options

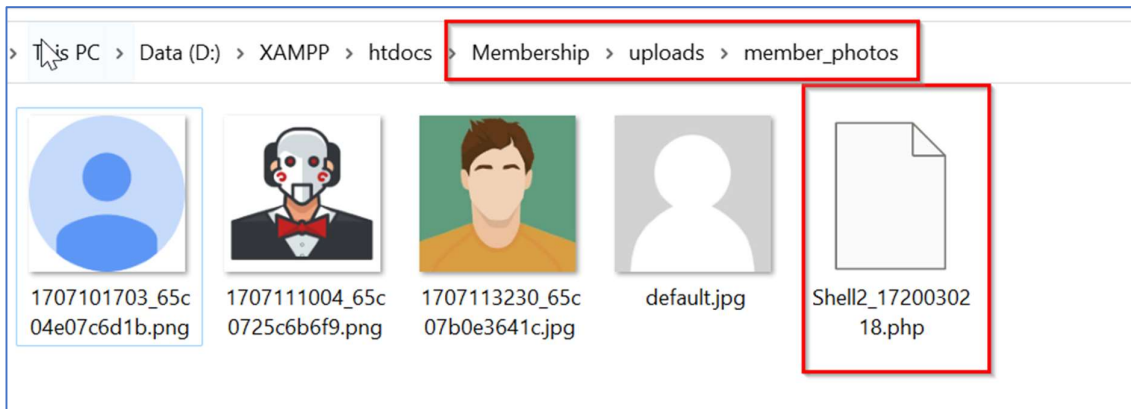
Request to http://localhost:80 [127.0.0.1]

Forward Drop Intercept is on Action Open Browser

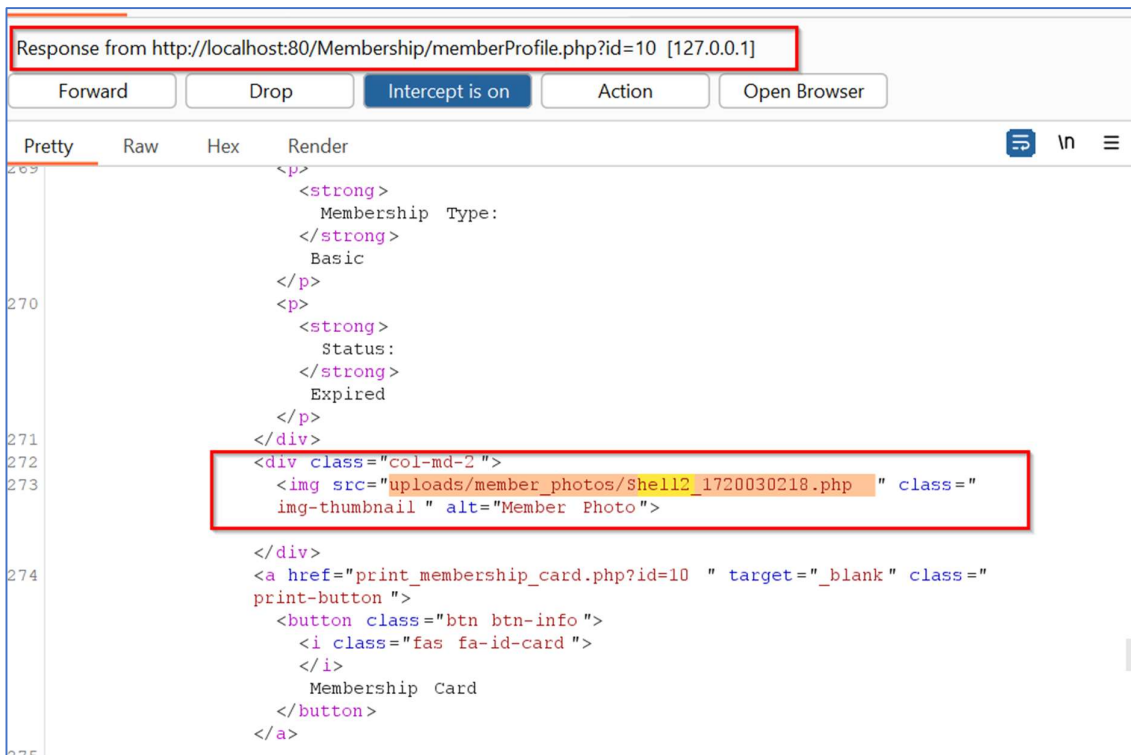
Pretty Raw Hex

```
38 -----82048041120206244241273002826
39 Content-Disposition : form-data ; name="email"
40
41 testing@mail.com
42 -----82048041120206244241273002826
43 Content-Disposition : form-data ; name="address"
44
45 77 demo
46 -----82048041120206244241273002826
47 Content-Disposition : form-data ; name="country"
48
49 demooo
50 -----82048041120206244241273002826
51 Content-Disposition : form-data ; name="postcode"
52
53 1111
54 -----82048041120206244241273002826
55 Content-Disposition : form-data ; name="occupation"
56
57 demodemo
58 -----82048041120206244241273002826
59 Content-Disposition : form-data ; name="photo"; filename="Shell12.php"
60 Content-Type : application/octet-stream
61
62 <?php phpinfo();?>
63 -----82048041120206244241273002826--
64
```

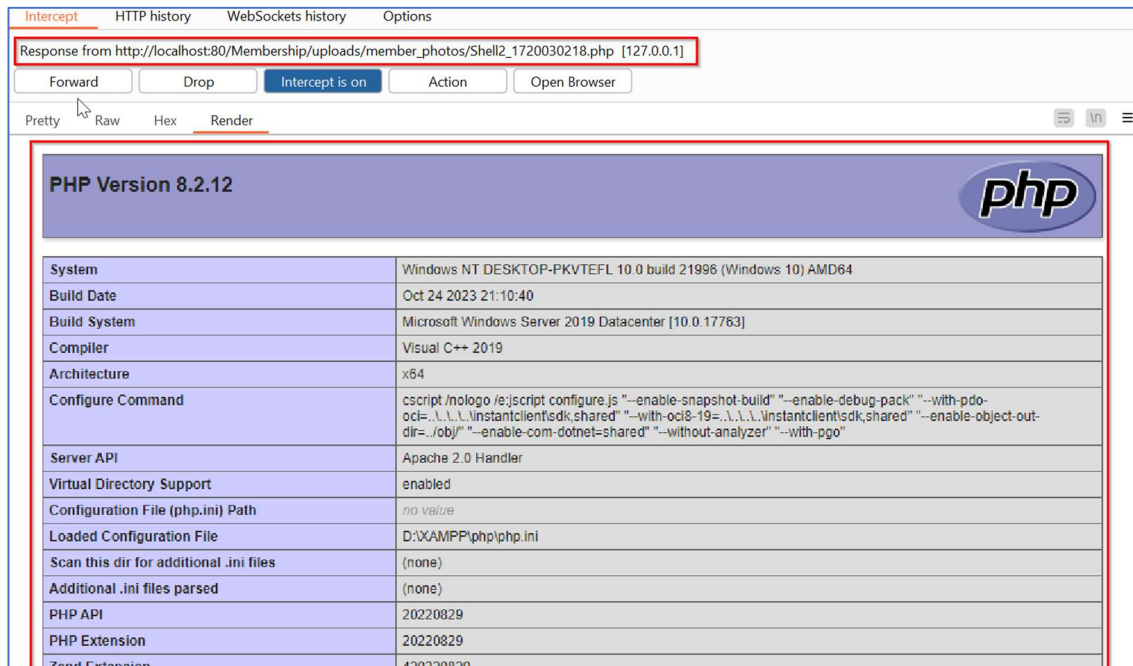
5. The PHP file is uploaded successfully. The file is stored in the “/uploads/member\_photos” folder by name “Shell2\_1720030218.php”.



6. Now try to access the profile image of that user. URL:  
<http://localhost/Membership/memberProfile.php?id=10>



7. The uploaded PHP file can be accessed by URL:  
[http://localhost/Membership/uploads/member\\_photos/Shell2\\_1720030218.php](http://localhost/Membership/uploads/member_photos/Shell2_1720030218.php)
8. Finally, arbitrary system commands can be executed through the uploaded malicious PHP file.



#### **Solution/Good Reads:**

The file types allowed to be uploaded should be restricted to only those that are necessary for business functionality.

- [https://owasp.org/www-community/vulnerabilities/Unrestricted\\_File\\_Upload](https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload)
- <https://cwe.mitre.org/data/definitions/434.html>