文件上传 URL 防盗链使用说明

概述

为了防止恶意人员获取上传地址，非法上传，上传服务器支持 URL 验证。即针对每次上传，采用经过加密的 URL，这个 URL 有一定的时效性，超过有效时间，则不能再用该 URL 上传。
合法的上传者必须通过有效的方式获得合法的 URL，才能上传文件到服务器。

使用步骤

1、修改上传服务器的配置文件 conf/config.xml

在上传服务器的根节点 hywebfileserver 里 添加如下配置节点 authentication

```
<authentication
    enable="1"
    key="38408956"
/>
```

其中：
enable：表示 URL 认证是否生效，如果为 1，则生效，否则为 0，则不生效。
key：为 URL 生成的加密密码，这个密码不能公开在客户端，应该仅保存在服务器端，这个密码是自定义的。配置了这个密码，需要把这个密码通知给 CMS 系统。
CMS 系统 URL 生成算法的代码里的密码也需要跟这个密码值一致。

2、URL 生成步骤与算法

2.1 构造 三个参数，参数的名称与意义如下：

变量名称	含义
siteid	站点 ID，这是用户自定义的站点 ID，具体意义取决于你自己，用没有含义的值也行。
userid	用户 ID，为上传的用户 ID，具体含义由你自己确定
stm	时间戳，为该 URL 的有效期的截至时间戳，即过了这个时间戳，则 URL 就无效了。时间戳的起点为 1970-01-01T00:00:00Z.，**stm** 为距离起点时间的秒数；与 PHP 语言的 **time** 函数返回的值含义一致。 C 语言函数 time_t time(time_t *t); 返回的值也满足此参数 为了保证 URL 有一定的时效性，建议 **stm = time() + 有效时长**

以上参数的名称是固定的，不能变，**siteid 与 userid** 参数的含义由你自己确定，如果实在无法确定，用随机数也行。**stm 为时间戳，不能随便定义，要求确保是时间戳。**

2.2 用以上参数加上配置文件中的 Key 生成一个 magic 值

算法如下：

```
md5(siteid + userid + stm + key)
```

生成 hash 值的 PHP 代码如下：

```php
<?php

function make_videoUploadUrl($siteid, $userid, $maxTimestamp, $password)
{
    $str = $siteid . $userid . $maxTimestamp . $password;
    $hash = md5($str);
    $url = "/upload/video?siteid=$siteid&userid=$userid&stm=$maxTimestamp&magic=$hash";

    return $url;
}

//测试数据
$siteid = '001';
$userid = 'user001';
//当前时间起 1 小时之内有效
$maxTimestamp = time() + 3600;
$password = '38408956';

$UploadUrl = make_videoUploadUrl($siteid, $userid, $maxTimestamp, $password);

echo $UploadUrl;
```

2.3 用生成的 magic 值构造 URL

构造的 URL 算法为：
上传地址 + **siteid** + **userid** + **stm** +**magic**

譬如，如下就是构造的一个上传 URL：

```
var upload_file_url =
uploadsrv_addr+'/upload/video?siteid=001&userid=user001&
stm=1669368493&magic=778c1cbb0c2b3771e367d362e7d28f80';
```

上传服务器会用传入的 URL 参数 **siteid、userid 与 stm** 在服务器端加上 配置的密码重新计

算 magic 值，如果计算得到的值与你传入的值一致则该 URL 就是合法的 URL；在比较 **magic** 值一致的情况下再比较当前时间戳是否小于 **stm** 参数传入的时间戳，如果小于 stm 参数给定的时间戳，则该 URL 可以上传文件，否则，不能上传文件，服务器拒绝该连接。

3、提示：

构造 URL 的算法代码一定要放在服务器端，由服务器端通过某种机制返回给客户端，如果放在客户端，则 key 参数很容易被人获知，恶意人员可以根据 key 参数来自行构建上传 URL。

文件扩展名验证设置说明

上传服务器支持限制上传文件类型，通过如下方式设置。

在上传服务器配置文件的 **upload** 节点或其子节点 **item** 添加 **allow** 属性，**allow** 属性为文件扩展名（**含点号**）列表，由半角逗号","或分号";“分开，例如：

```
allow=".mp4;.avi;.rm;.doc"
```

一旦在 **upload** 节点配置了 **allow** 属性，则上传服务器就会对文件扩展名过滤，同时不再支持无扩展名的文件上传，**item** 节点为 **upload** 节点的子节点，如果 **item** 节点也配置了 **allow** 属性，则用子节点自己的配置，否者用 **upload** 节点的配置。

每个 **item** 节点可以独立配置接受的文件扩展名用于分别接受不同的文件类型。

如果希望一个节点支持任意文件类型，解决办法为 不配置 **upload** 节点的 **allow** 属性，在 **upload** 节点下添加一个不配置 **allow** 属性 的节点。

附录：

一个支持 URL 验证的配置文件如下：

```
<?xml version="1.0" encoding="UTF-8"?>
<hywebfileserver version="1.0">
    <serverconfig
        port="8021"
        root="html"
        tempdir="temp"
        logdir="log"
    />
   <authentication
                enable="1"
                key="38408956"
    />
    <vdirectory>
        <location name="videos" path="/Uploads/videos" />
        <location name="images" path="/Uploads/images" />
        <location name="audios" path="/Uploads/audio" />
        <location name="res" path="/Uploads" />
    </vdirectory>

    <upload dir="/Uploads" key="123456" dirformat="YMD"
baseurl="http://ip-to-fix:8021/res">
        <item id="audio" dir="/Uploads/audio"
key="123456" baseurl="http://ip-to-fix:8021/audios"/>
        <item id="image" dir="/Uploads/images"
key="123456" baseurl="http://ip-to-fix:8021/images" />
        <item id="video" dir="/Uploads/videos"
 key="123456" baseurl="http://ip-to-fix:8021/videos" allow=".mp4;.mpg;.dat;.jpg"/>
        <item id="document" dir="/Uploads/document"
key="123456" baseurl="http://ip-to-fix:8021/res/document" />
    </upload>
</hywebfileserver>
```