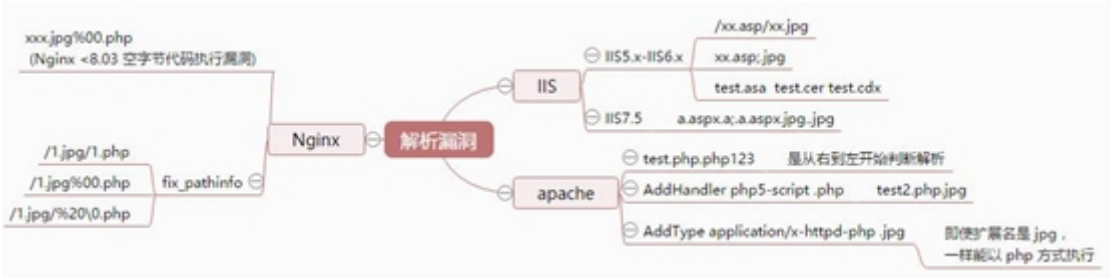
Day22　WEB漏洞–文件上传之内容逻辑数组绕过

> 图片一句话制作方法：　copy 1.png /b + shell.php /a webshell.jpg
>
> 文件头检测
>
> 图像文件信息判断
>
> 逻辑安全=二次渲染
>
> 逻辑安全-条件竞争
>
> 目录命名-x.php/.
>
> 脚本函数漏洞-CVE-2015-2348
>
> 数组接受+目录命名

22.1 解析漏洞



- 这段代码存在逻辑判断问题，可以通过逻辑竞争来进行注入。

```
#靶场17关代码
$is_upload = false;
$msg = null;

```

```php
if(isset($_POST['submit'])){
    $ext_arr = array('jpg','png','gif');
    $file_name = $_FILES['upload_file']['name'];
    $temp_file = $_FILES['upload_file']['tmp_name'];
    $file_ext = substr($file_name,strrpos($file_name,".")+1);
    $upload_file = UPLOAD_PATH . '/' . $file_name;

    if(move_uploaded_file($temp_file, $upload_file)){
        if(in_array($file_ext,$ext_arr)){
            $img_path = UPLOAD_PATH . '/'. rand(10, 99).date("YmdHis").".".$file_ext;
            rename($upload_file, $img_path);
            $is_upload = true;
        }else{
            $msg = "只允许上传.jpg|.png|.gif类型文件！";
            unlink($upload_file);
        }
    }else{
        $msg = '上传出错！';
    }
}
}
```

- 20关代码可以采用数组注入

```php
$is_upload = false;
$msg = null;
```

```php
if(!empty($_FILES['upload_file'])){
    //检查MIME
    $allow_type = array('image/jpeg','image/png','image/gif');
    if(!in_array($_FILES['upload_file']['type'],$allow_type)){
        $msg = "禁止上传该类型文件!";
    }else{
        //检查文件名
        $file = empty($_POST['save_name']) ? $_FILES['upload_file']['name'] : $_POST['save_name'];
        if (!is_array($file)) {
            $file = explode('.', strtolower($file));
        }

        $ext = end($file);
        $allow_suffix = array('jpg','png','gif');
        if (!in_array($ext, $allow_suffix)) {
            $msg = "禁止上传该后缀文件!";
        }else{
            $file_name = reset($file) . '.' . $file[count($file) - 1];
            $temp_file = $_FILES['upload_file']['tmp_name'];
            $img_path = UPLOAD_PATH . '/' .$file_name;
            if (move_uploaded_file($temp_file, $img_path)) {
                $msg = "文件上传成功! ";
```

```
                $is_upload = true;
            } else {
                $msg = "文件上传失败！";
            }
        }
    }else{
        $msg = "请选择要上传的文件！";
    }
```

详情参考uploads过关手册

资源：

```
https://www.smi1e.top/文件解析漏洞总结/
```