Day21　WEB漏洞–文件上传之后端黑白名单绕过

21.1 文件上传常见验证

- 后缀名，类型、文件头等
- 后缀名:黑名单、白名单
- 文件类型:MIME信息
- 文件头:内容头信息
- 方法：查看源码、抓包修改包信息

注意:

```
%00截断：可以把这个放在文件名内，绕过检测。
get：　会自动解码
post：不会自动解码，所以想以post提交数据%00需要把它进行url解码
```

21.2 过滤规则

```php
<?php
include '../config.php';
include '../common.php';
include '../head.php';
include '../menu.php';

$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
```

```php
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array('.asp','.aspx','.php','.jsp');
        $file_name = trim($_FILES['upload_file']['name']);
        $file_name = deldot($file_name);//删除文件名末尾的点
        $file_ext = strrchr($file_name, '.');
        $file_ext = strtolower($file_ext); //转换为小写
        $file_ext = str_ireplace('::$DATA', '', $file_ext);//去除字符串::$DATA
        $file_ext = trim($file_ext); //收尾去空

        if(!in_array($file_ext, $deny_ext)) {
            $temp_file = $_FILES['upload_file']['tmp_name'];
            $img_path = UPLOAD_PATH.'/'.date("YmdHis").rand(1000,9999).$file_ext;
            if (move_uploaded_file($temp_file,$img_path)) {
                 $is_upload = true;
            } else {
                $msg = '上传出错！';
            }
        } else {
            $msg = '不允许上传.asp,.aspx,.php,.jsp后缀文件！';
        }
    } else {
```

```
31          $msg = UPLOAD_PATH . '文件夹不存在,请手工创
    建! ';
32      }
33  }
34  ?>
```

21.3 靶场

uploads