

## WEB 漏洞-文件上传之后端黑白名单绕过

# WEB漏洞-文件上传

## ① 初识

- 什么是文件上传漏洞?
- 文件上传漏洞有哪些危害?
- 文件上传漏洞如何查找及判断?
- 文件上传漏洞有哪些需要注意的地方?
- 关于文件上传漏洞在实际应用中的说明?

## ② 验证/绕过

- 前端
  - JS类防护
- 黑名单
  - 特殊解析后缀
  - .htaccess解析
  - 大小写绕过
  - 点绕过
  - 空格绕过
  - ~\$\$DATA绕过
  - 配合解析漏洞
  - 双后缀名绕过
- 后端
  - 白名单
    - MIME绕过
    - %00截断
    - 0x00截断
    - 0x0a截断
  - 内容及其他
    - 文件头检测
    - 二次渲染
    - 条件竞争
    - 突破getimagesize
    - 突破exif\_imagetype

## ③ 漏洞/修复

- 解析漏洞
  - IIS6/7.X
  - Apache
  - Nginx
- CMS漏洞
  - 某CMS上传1
  - 某CMS上传2
  - 某CMS上传3
- 其他漏洞
  - 编辑器漏洞
    - ckeditor
    - ewebeditor
    - ckeditor
    - kindedit
    - .....
  - CVE等漏洞
    - CVE-2015-5254
    - CVE-2017-12615
    - CVE-2019-2618
    - .....
  - 安全修复
    - 方案

## ④ WAF绕过

- safedog
- BT(宝塔)
- XXX云盾

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

简要上传表单代码分析解释

---

### 演示案例：

✧ uploadlabs 关卡分析

---