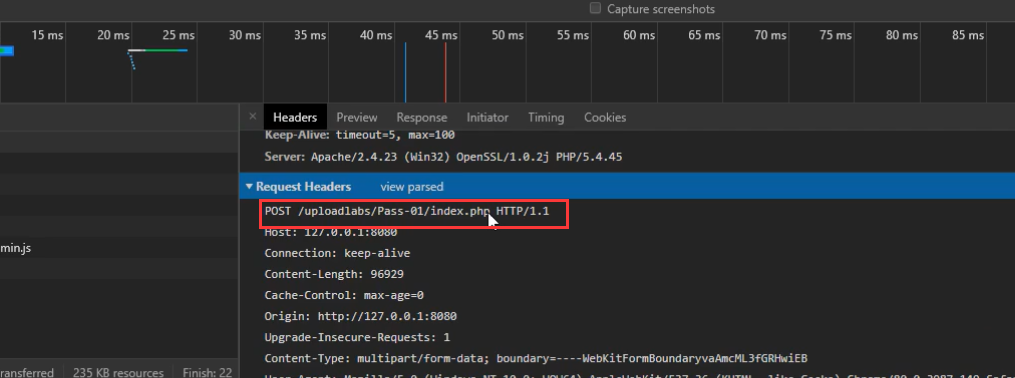
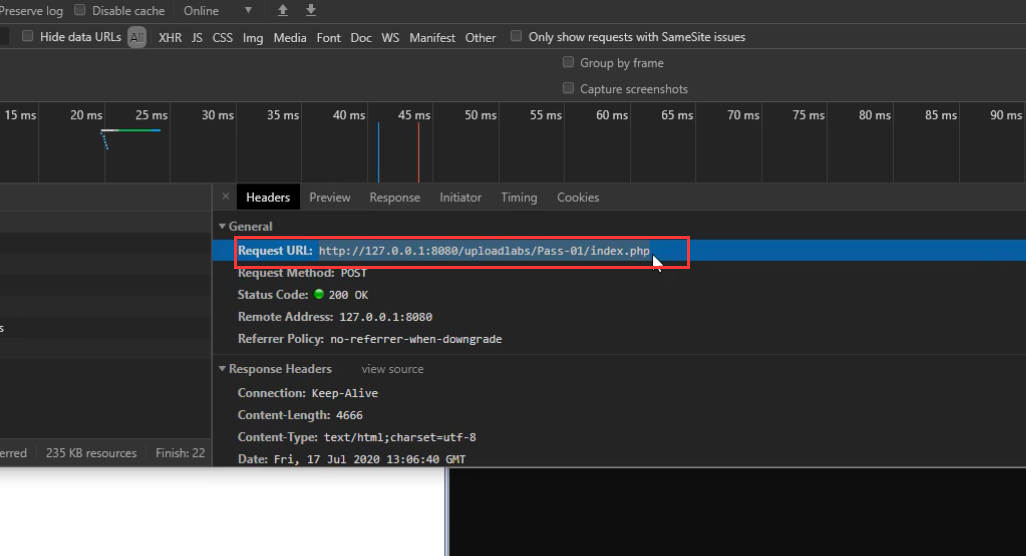
# 10.文件上传

1. 初识
   1. 什么是文件上传漏洞？
   2. 文件上传有哪些危害？
   3. 文件上传漏洞如何查找及判断？
   4. 文件上传漏洞有哪些需要注意的地方？
   5. 冠以文件上传漏洞在实际应用中的说明？
2. 验证/绕过
   1. 前端
      1. 35类防护
      2. 前端验证
         1. 禁用js脚本（不推荐）
         2. 删除指定的js脚本并修改或添加action指令

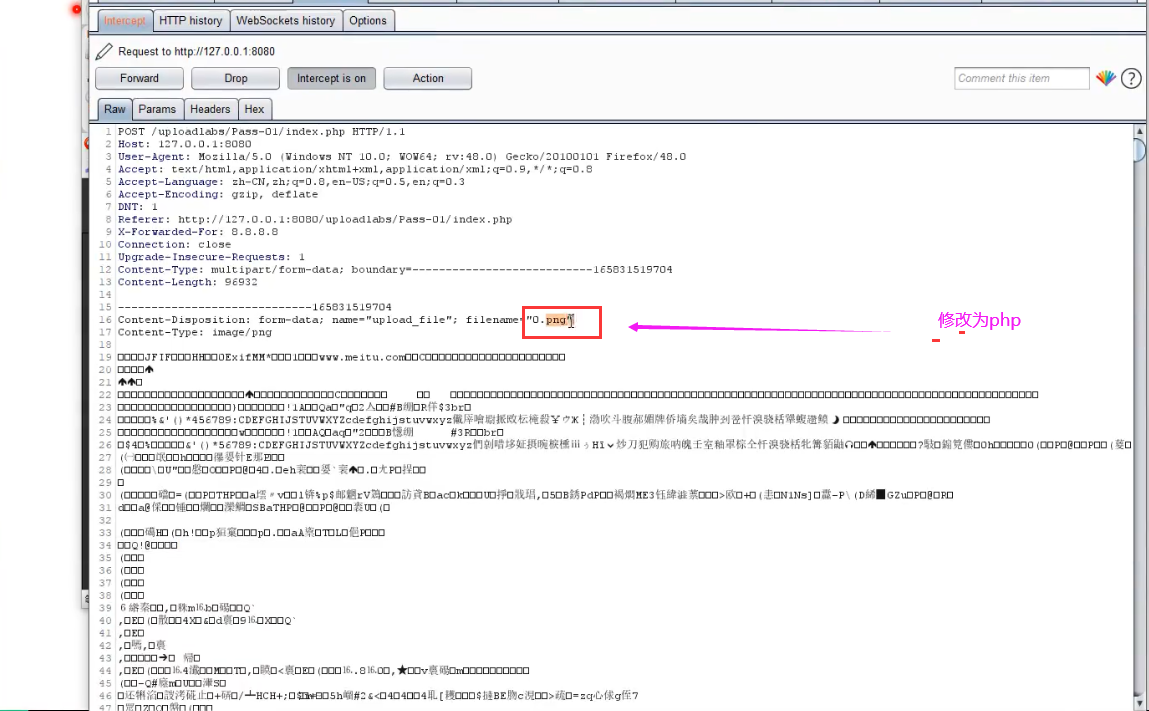




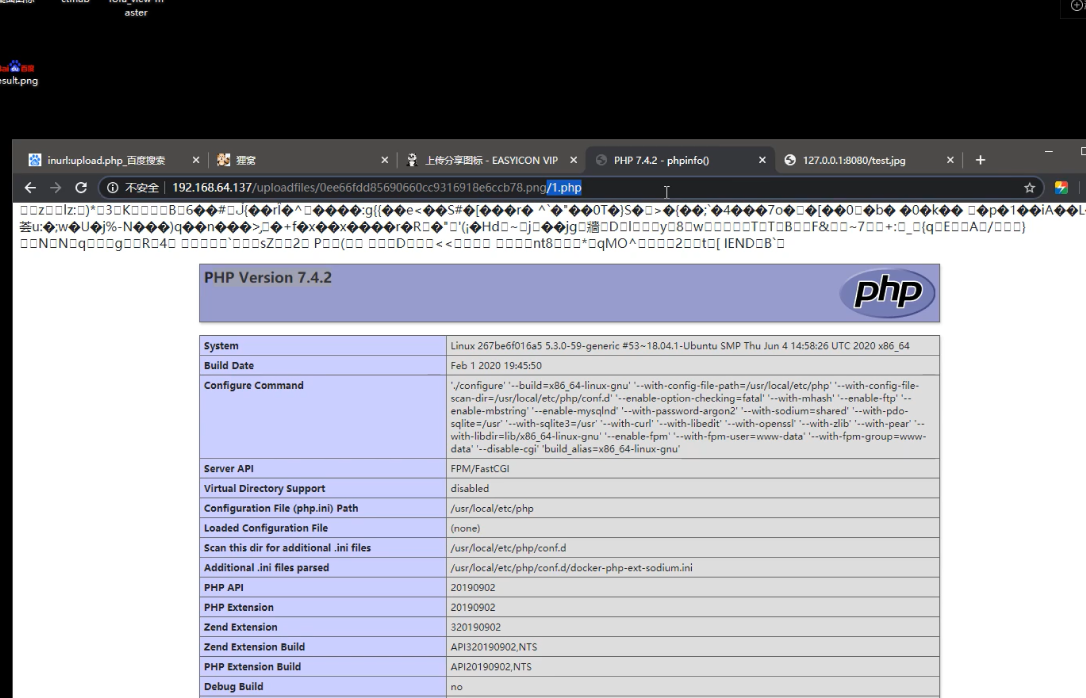


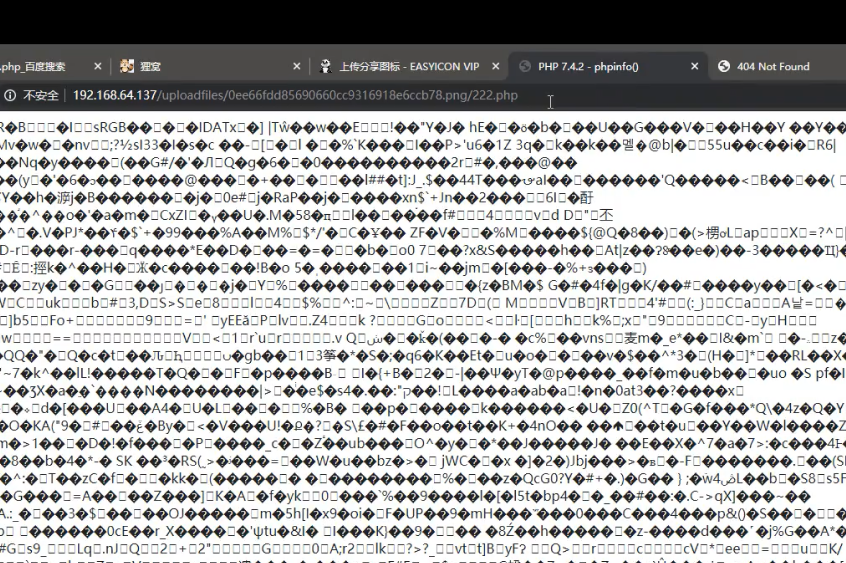


* + - 1. burp抓包修改后缀（有些网站不行）
         1. 有些网站和js写的代码只在本地运行，没有发送现象，抓不到包



* 1. 后端
     1. 黑名单
        1. 特殊解析后缀
        2. .htaccess解析
        3. 大小写绕过
        4. 点绕过
        5. 空格绕过
        6. ::$$QATA绕过
        7. 配合解析漏洞





* + - 1. 双后缀名绕过
    1. 白名单
       1. MIME绕过
       2. %OO截断
       3. OxOO截断
       4. OxOa截断
    2. 内容及其他
       1. 文件头检测
       2. 二次渲染
       3. 条件竞争
       4. 突破getimagesize
       5. 突破exif\_imagetype

1. 漏洞/修复
   1. 解析漏洞
      1. IIS6/7.x
      2. Apache
      3. Nginx
   2. CMS漏洞
      1. 某CMS上传1
      2. 某CMS上传2
      3. 某CMS上传3
   3. 其他漏洞
      1. 编辑器漏洞
         1. fckeditor
         2. ewebeditor
         3. ckediter
         4. kindedit
         5. ……
      2. CVE等漏洞
         1. CVE-2015-5254
         2. CVE-2017-12615
         3. CVE-2019-2618
      3. 安全修复
         1. 方案
2. WAF绕过
   1. safedog
   2. bt
   3. xxx云盾
3. 利用思路
   1. 常规类
      1. 扫描获取上传
      2. 会员中心上传
      3. 后台系统上传
      4. 各种途径上传
   2. CMS类
      1. 已知CMS源码
   3. 编辑器类
      1. ckedittor
      2. fckeditor
      3. kindeditor
      4. xxxxeditor
   4. 其他类/CVE
      1. 代码审计
      2. 平台/三方应用等