i春秋:警惕您站上的MIME类型绕过漏洞

转载

喜欢散步 于 2015-06-01 04:01:17 发布 2320 收藏
文章标签： 初学 渗透 入侵 安全 漏洞
实验环境

- 实验环境
  - 操作机：`Windows XP`
  - 目标机：`Windows 2003`
- 目标网址：`www.test.com`
- 实验工具：中国菜刀 `burp`

实验目的
MIME的作用：使客户端软件，Web服务器使用MIME来说明发送数据的种类， Web客户端使用MIME来说明希望接收到的数据种类。本课程带领大家了解MIME头部信息过滤不严带来的严重后果以及防御方法，使大家了解到提高自身的上传漏洞防御能力的重要性。

实验思路

1. 上传正常图片和一句话
2. 修改MIME绕过上传检测
3. 获取WEBShell权限
4. 防御方案

实验步骤
1

上传正常图片和一句话

上传正常的图片以及上传一句话，查看区别，准备一个普通的图片，使用`*.jpg`在电脑上进行搜索，可以看到很多图片，复制一张图片放到桌面上，改名为`tupian.jpg`。

打开上传地址，选取准备好的图片，上传图片。

> **小i提示：**
>
> 上传地址就是可以上传文件的地方
>
> 本次实验用的是一个测试网址http://www.test.com 作为目标网站

上传成功后，观察返回的页面信息。

小i提示：

观察红字部分（上传是否成功）

观察蓝字部分（上传后文件的路径）

2

修改MIME绕过上传检测

我们可以尝试使用BurpLoader修改文件的类型来绕过其防御。首先打开BurpLoader，选择 Proxy->Options，设置BurpLoader代理地址，默认为127.0.0.1、端口：8080。

设置IE的代理地址，勾选为 LAN 使用代理服务器,修改下面的代理地址以及端口（设置与在BurpLoader设置的代理地址相同：127.0.0.1、端口：8080）。

小i提示：：

- **不同浏览器设置代理的方法不相同， 此处我们以IE浏览器为例，首先点击右上角的工具-internet选项-连接-局域网设置-代理服务器勾选并设置。**

选择 BurpLoader 的 Proxy->Intercept 将抓包的状态从关闭改为打开。

在浏览器上传PHP文件，回到BurpLoader看到MIME信息（Content-type）为text/plain。

关闭抓包，发送刚刚的PHP文件，接着返回浏览器，重新选择图片文件，打开抓包，上传图片，查看MIME为image/pjpeg，复制MIME信息。

再次上传时则需要再次进行此操作，重新关闭抓包，发送刚刚的图片文件，接着返回浏览器，重新选择PHP文件，打开抓包，上传PHP文件，粘贴刚刚复制的MIME信息，然后关闭抓包，BurpLoader自动发送PHP文件。

3

获取WEBShell权限

上传成功后，我们需要访问文件，这时可直接复制文件路径（File Name后面的内容，即是一句话的路径），将复制的地址粘贴至网站地址后面，从而构造访问地址，并复制构造好的地址。

例：http://www.test.com/uploading/1412780873.php

使用中国菜刀软件打开webshell地址

打开中国菜刀软件并填入复制的访问地址，填入你设定的密码,这里设置的密码是1，选择脚本类型为PHP，单击添加按钮，最后我们双击指定条目后的可以看到目标网站的目录，这样我们就成功获取到目标网站的WEBShell权限。

4

防御方案

1.客户端检测，使用JS对上传图片检测，包括文件大小、文件扩展名、文件类型等

2.服务端检测，对文件大小、文件路径、文件扩展名、文件类型、文件内容检测，对文件重命名

3.其他限制，服务器端上传目录设置不可执行权限