i春秋:警惕您站上的文件内容检测绕过类上传漏洞

原创

喜欢散步 于 2015-06-01 04:07:55 发布 3853 收藏
文章标签： 漏洞 安全 入侵 渗透 初学

本文链接：https://blog.csdn.net/hope_smile/article/details/46298383

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 BurpSuite

实验目的
本课程带领大家学习利用修改文件内容，绕过上传验证，获取WebShell。通过亲身实验，验证绕过上传验证的可行性，从而提高自身的安全防御意识。

实验思路

1. 上传正常图片和一句话
2. 修改文件内容绕过上传检测
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

准备一张普通的图片，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，成功为 Upload Successful 失败这一行会显示失败信息）

观察蓝字部分（上传成功后文件的路径）

准备的是PHP环境,需要使用PHP的一句话，接着来制作一句话，新建一个空文本文档，将php的一句话写入到文本中,修改文件名为`yijuhua.php`并保存到桌面。

小i提示：

一句话是一种常见的网站后门，短小精悍,而且功能强大，隐蔽性非常好，在渗透测试过程中始终扮演着强大的作用。不同的环境需要选取与环境匹配的一句话。

一句话中`$_POST[‘这里是密码’]`，本例中我们以 `1` 为密码。

上传PHP文件，发现提示错误为`The File Is Not Picture`,因此得出结论，PHP文件被禁止上传。

服务器断可能是通过文件类型进行判断的，于是我们将`yijuhua.php`的改为`yijuhua.jpg`，进行上传尝试，发现也没有上传成功，所以我们可以判断：服务器端是通过文件内容进行验证的。

2

修改文件内容绕过上传检测

利用BurpLoader对上传文件内容进行修改

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`。

接着修改Firefox的代理设置，修改代理地址以及端口（设置与在BurpLoader中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-选项-网络-设置-手动配置代理，填入BurpLoader中设置的代理地址。

我们再打开BurpLoader抓包，进行截断浏览器给服务器发送的数据包，Proxy-Intercept 点击 intercept off 改为intercept on，截断的数据包将在关闭抓包的时候发送给服务端。

我们再将图片文件上传一次，返回查看被截断的数据包，在末尾加上几个空格后粘贴一句话，然后修改文件名的尾缀为.php利于之后使用中国菜刀进行连接。

小i提示：

空格的作用主要用于隔开图片文件和一句话，避免一句话解析混乱。

如果不修改尾缀上传上去的文件仍然是.jpg，则仍以.jpg解析，那么就无法执行PHP脚本（也就是一句话执行失败）。

关闭抓包（点击intercept on ->intercept off），上传数据,查看浏览器发现上传成功，复制File Name后面的信息（例如：uploadimg\1412865875.php ）。粘贴复制到网站地址后面，从而构造访问地址（例如：http://www.test.com\uploadimg\1412865875.php ），并复制访问地址。

3

获取WEBShell权限

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,之前我们在“一句话”中设置的密码是1，选择脚本类型为PHP，单击添加按钮，就会看到菜刀上出现一行信息，最后我们双击这条信息后，就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。

小i 知识点：

- 中国菜刀，是一款专业的网站管理软件，用途广泛，使用方便，小巧实用。只要支持动态脚本的网站，都可以用中国菜刀与一句话协作来进行管理。

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