i春秋:警惕您站上的空字节截断目录路径检测绕过类上传漏洞

转载

喜欢散步 于 2015-06-01 04:07:13 发布 4219 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 BurpSuite

实验目的
本课程带领大家学习通过空字节截断，绕过验证，获取WebShell。使大家亲身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WEBShell
2. 截断目录绕过上传检测
3. 获取WEBShell权限
4. 防御方案

实验步骤
1

上传正常图片和WEBShell

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）

这里服务器端准备的是PHP环境,需要使用PHP的一句话，接着我们来制作一句话，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(一句话中$_POST[‘这里是密码’]，本例中我们以 1 为密码)。

> **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

上传PHP文件，发现提示错误，得出结论PHP文件被禁止上传。

2

截断目录绕过上传检测

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IE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-internet选项->连接->局域网设置->代理服务器勾选并设置。

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PHP文件的尾缀改为.jpg，filename后面的信息是我们本地的地址，Content-Disposition : from-data ; name=”path”后面一行uploadimg是我们保存的地址。

现在我们将uploadimg改为uploadimg/1.php .jpg ，接着我们来到 Proxy->intercept->Hex找到1.php .jpg这个被修改过的代码，找到同一行的数字20，改为00 按一下回车，返回。

小i知识点：

- 20(也就是空格字符的16进制)改成00(也就是一个截断字符的16进制）这样以来。截断字符后面的都会被截断，也就是忽略掉了，所以uploadimg/1.php .jpg 就变成了uploadimg/1.php 达到了我们上传PHP文件的目的。

返回Raw，看到uploadimg/1.php .jpg变成uploadimg/1.php□.jpg,原本的文件服务器保存路径从uploadimg/yijuhua.jpg变为uploadimg/1.php。

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，复制上传框下面的信息，舍弃掉后面的.jpg（例如：uploadimg\1.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\1.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