i春秋:通过案例学安全—再现杰奇网站漏洞环境

转载

喜欢散步 于 2015-06-01 03:56:29 发布 5659 收藏
文章标签： 漏洞 安全 初学 渗透 入侵
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 firebug

实验目的
本课程带领大家学习利用JS验证绕过杰奇CMS1.7上传验证，获取WebShell。课程旨在教会大家提高自身的安全防御意识的同时，学会修补漏洞。

实验思路

1. 找到上传功能
2. 尝试上传图片和木马
3. 删除验证方法绕过上传
4. 修改过滤白名单绕过上传
5. 防御方案

实验步骤
1

找到上传功能

输入www.test.com打开目标网站。

单击新用户注册，注册一个用户，这里注册的用户是test。

在个人空间中寻找上传功能，位置在个人空间--我的空间--相册--上传图片。

2

尝试上传图片和木马

正常图片上传成功，返回图片路径。

上传WEBShell返回错误提示。

> **小i提示：**
>
> - 如何判断是本地验证呢？很多情况下感觉速度较快的返回信息则认为有可能是本地验证，但是有的时候需要根据抓报以及跟踪上传代码来分析出是否为本地验证。

3

删除验证方法绕过上传

打开firebug 点击 按钮，将光标选择上传模块。

<form onsubm:t="return checkFile()"是他的验证的框架，将它删除并编辑保存。

验证框架的代码进行删除之后，页面不会对我们上传文件的类型进行检测。

再重新选择yijuhua.php进行上传。

文件已经上传成功，保存在upload/yijuhua 将他复制到地址的后面，这个地址就是我们WEBSshell的连接地址。

4

修改过滤白名单绕过上传

打开Firebug查看代码，可以看到限制语句，可以判断为js前端验证。

> **小i提示：**
>
> - Firebug的打开方式是在火狐浏览器窗口页面中右键鼠标，最下面有“使用Firebug查看元素”,更详细的使用方法请查看百度经验

在Firebug中修改JS代码绕过本地验证上传WEBShell。单击Firebug中的编辑功能，修改或者在类型后面加上PHP，让JS代码允许上传PHP文件。

上传WEBShell，提示上传成功，并返回路径。

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