

# [网络安全自学篇] 六十六.Vulnhub靶机渗透之DC-1提权和Drupal漏洞利用（二）

原创

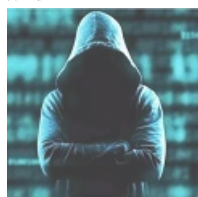
[Eastmount](#) 于 2020-04-11 20:28:01 发布 7455 收藏 27

分类专栏: [网络安全自学篇](#) 文章标签: [Web渗透](#) [Vulnhub](#) [网络安全](#) [DC-1](#) [漏洞利用](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/Eastmount/article/details/105442329>

版权



[网络安全自学篇](#) 专栏收录该内容

107 篇文章 2590 订阅 ¥19.90 ¥99.00

订阅专栏

这是作者的网络安全自学教程系列, 主要是关于安全工具和实践操作的在线笔记, 特分享出来与博友们学习, 希望您们喜欢, 一起进步。前文分享了Vulnhub靶机渗透的环境搭建和JIS-CTF题目, 采用Nmap、Dirb、中国蚁剑、敏感文件分析、SSH远程连接、Shell提权等获取5个flag。本文将讲解DC-1提权和Drupal漏洞利用, 通过信息收集、CMS漏洞搜索、Metasploit反弹shell、提权及数据库爆破获取flag。本文是一篇Web渗透的基础性文章, 希望对您有所帮助。

作者作为网络安全的小白, 分享一些自学基础教程给大家, 主要是关于安全工具和实践操作的在线笔记, 希望您们喜欢。同时, 更希望您能与我一起操作和进步, 后续将深入学习网络安全和系统安全知识并分享相关实验。总之, 希望该系列文章对博友有所帮助, 写文不易, 大神们不喜勿喷, 谢谢! 如果文章对您有帮助, 将是我创作的最大动力, 点赞、评论、私聊均可, 一起加油喔~

## 文章目录

### 一.DC-1题目描述及环境配置

#### 1.题目描述

#### 2.环境搭建

### 二.Vulnhub靶机渗透详解

#### 1.信息收集

#### 2.CMS漏洞搜索

#### 3.Metasploit漏洞利用

#### 4.敏感信息分析获取flag1和flag2