

# THM-Vulnerabilities 101(漏洞基础)-学习

本文相关的TryHackMe实验房间链接：<https://tryhackme.com/room/vulnerabilities101>

通过学习相关知识点：了解应用程序的缺陷并将你的研究技能应用于某些漏洞数据库。

## H2 介绍

网络安全是当今世界的大事，我们在报纸上听到的黑客攻击主要来自于漏洞利用。在本文中，我们将准确解释什么是漏洞、漏洞的类型以及我们如何利用这些漏洞在渗透测试工作中取得成功。

本文将向你介绍一些在研究漏洞时必不可少的资源，具体来说，涉及到的资源有：

- 什么是漏洞
- 为什么漏洞有学习的价值
- 漏洞如何进行评级
- 漏洞研究数据库
- 一个展示：如何在ACKme的任务中开展漏洞研究

## H2 漏洞简介

网络安全漏洞被定义为系统或应用程序的设计、实施或行为中的弱点或缺陷，攻击者可以利用这些弱点来访问未经授权的信息或执行未经授权的操作。网络安全机构对“漏洞”一词有许多定义，但是，它们之间的差异很小。



例如，NIST 将漏洞定义为“信息系统、系统安全程序、内部控制或实施中可能被威胁源利用或触发的弱点”。漏洞的出现可能源于许多因素，包括应用程序设计不当或对用户预期操作的疏忽。

我们将在稍后的章节中讨论各种类型的漏洞，但是，就目前而言，我们应该知道五种主要的漏洞类别：

(Mis)Configuration-based

Weak or Default Credentials

Application Logic

Human-Factor

漏洞	描述
操作系统	这些类型的漏洞存在于操作系统 (OS) 中，通常会导致权限提升。
(错误) 基于配置	这些类型的漏洞源于错误配置的应用程序或服务。例如，公开客户详细信息的网站。
弱或默认凭据	具有身份验证元素的应用程序和服务在安装时将附带默认凭据。例如，管理员仪表板可能具有“admin”的用户名和密码。这些很容易被攻击者猜到。
应用逻辑	这些漏洞是由于应用程序设计不当造成的。例如，实施不当的身份验证机制可能导致攻击者能够冒充用户。
人的因素	人因漏洞是利用人类行为的漏洞。例如，网络钓鱼电子邮件旨在诱骗人们相信它们是合法的。

作为网络安全研究人员，你将评估应用程序和系统——在日常生活中使用针对这些目标的漏洞，因此熟悉漏洞的发现和利用过程至关重要。

答题

回答以下问题

攻击者已经能够将其系统帐户的权限从“用户”升级为“管理员”。这是什么类型的漏洞？

Operating System

正确答案

您设法绕过使用 cookie 进行身份验证的登录面板。这是什么类型的漏洞？

Application Logic

正确答案

H2 漏洞评分(CVSS & VPR)

漏洞管理是评估、分类并最终修复有关组织所面临的威胁（漏洞）的过程；可以说，修补和修复网络或计算机系统中的每一个漏洞是不可能的，有时还会浪费资源；毕竟，只有大约 2% 的漏洞最终会被利用（Kenna security., 2020）。进行漏洞管理工作是为了解决最危险的漏洞并降低攻击向量被用于利用系统的可能性。

漏洞评分在漏洞管理中起着至关重要的作用，评分用于确定漏洞可能对网络或计算机系统产生的潜在风险和影响。例如，流行的通用漏洞评分系统 (CVSS) 在进行漏洞评分时会考察漏洞的具体功能、可用性和再现性。

当然，在 IT 世界中，永远不会只有一个框架或建议，让我们探索两个常见的漏洞评分框架并分析它们的不同之处。

## CVSS（通用漏洞评分系统-Common Vulnerability Scoring System）

通用漏洞评分系统（或 CVSS）于 2005 年首次推出，是一种非常流行的漏洞评分框架，具有三个主要迭代版本。当前版本是 CVSSv3.1（4.0 版目前处于草稿阶段），漏洞分数基本上由以下一些因素（还有更多）决定：

1. 利用这个漏洞有多容易？
2. 以前有没有这方面的漏洞？
3. 这个漏洞是如何干扰信息安全三元组CIA（机密性、完整性、可用性）的？

事实上，还存在很多变量，你必须使用相关的漏洞评分计算器 来计算使用这个评分框架的漏洞分数。CVSS会根据漏洞已获得的分数，对漏洞进行分类，定性严重程度评定量表及其分数范围见下表。

Rating	Score
None	0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

然而，CVSS 并不是灵丹妙药。下面我们来分析一下CVSS的一些优缺点：

CVSS的优势	CVSS的缺点
CVSS已经存在很长时间了。	CVSS从未设计用于帮助确定漏洞的优先级，它只是分配一个严重性值。
CVSS在组织中很受欢迎。	CVSS会大量评估可用漏洞。然而，只有 20% 的漏洞有可用的漏洞利用（Tenable, 2020）。
CVSS是一个免费的框架，由 NIST 等组织采用和推荐。	尽管可能会发现诸如漏洞利用之类的新发展，但漏洞很少在评估后改变评分。

## VPR（漏洞优先级-Vulnerability Priority Rating）

VPR 框架是一个更现代的漏洞管理框架 - 由漏洞管理行业解决方案提供商 Tenable 开发。该框架被认为是风险驱动的，这意味着给漏洞打分的重点是漏洞对组织本身造成的风险，而不是漏洞影响等因素（CVSS 在评分时会关注漏洞的影响）。

与 CVSS 不同，VPR 评分会考虑漏洞的相关性；例如，如果该漏洞不适用于有关组织（即该组织并没有使用漏洞相关的易受攻击的软件），则不会考虑有关该漏洞的风险级别。VPR 的评分也相对更加动态化，漏洞可能带来的风险几乎每天都会发生变化。

VPR 的评分范围与 CVSS 类似，具体见下表；两者显著的区别是 VPR 没有 “None/Informational” 类别，并且由于 VPR 使用了不同的评分方法，相同的漏洞在使用 VPR 时的评分与使用 CVSS 时的评分 结果有很大不同。

Rating	Score
Low	0.0 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

在下表中可以看到使用 VPR 框架的一些优点和缺点。

VPR 的优势	VPR 的缺点
VPR 是一个现实世界的现代框架。	VPR 不像其他一些漏洞管理框架那样开源。
VPR 在计算风险时考虑了 150 多个因素。	VPR 只能在商业平台之外采用。
VPR 是风险驱动的，组织使用它来帮助确定修补漏洞的优先级。	VPR 不像 CVSS 那样考虑 CIA 三元组：这意味着在使用 VPR 时，对数据的机密性、完整性和可用性的风险不会成为评估漏洞的重要因素。
评分不是最终的，而且非常动态，这意味着应该给予漏洞的优先级会随着漏洞的老化而改变。	空。

## 答题

回答以下问题

CVSS 的第一次迭代是哪一年发布的？

2005

正确答案

如果您想根据漏洞对组织构成的风险来评估漏洞，您会使用什么框架？

注意：我们在这里寻找首字母缩写词。

VPR

正确答案

如果你想使用一个免费和开源的框架，那会是什么框架？

注意：我们在这里寻找首字母缩写词。

CVSS

正确答案

## H2 漏洞数据库

在你的网络安全之旅中，你经常会遇到大量不同的应用程序和服务。例如，很多网站会使用CMS建站，虽然它们（CMS）都有相同的目的，但通常具有非常不同的设计和行为（进而可能存在不同的漏洞）。

值得庆幸的是，互联网上有一些资源可以跟踪各种软件、操作系统等的漏洞！ 本文将展示两个数据库，我们可以使用它们来查找我们在信息安全之旅中发现的应用程序的现有漏洞：

1. [NVD \(National Vulnerability Database--美国\)](#)
2. [Exploit-DB](#) （Exploit-DB同时还整合了GHDB--Google Hacking Database）
3. [CNVD\(China National Vulnerability Database--中国\)](#)

在深入研究以上两个资源之前，让我们确保我们对一些基本术语的理解是一致的：

术语	定义
漏洞	漏洞被定义为系统或应用程序的设计、实现或行为中的弱点或缺陷。
exploit (exp 漏洞利用)	漏洞利用是诸如利用系统或应用程序上的漏洞的操作或行为。
概念证明 (PoC)	PoC是一种经常展示漏洞利用的技术或工具。

## NVD – National Vulnerability Database (国家漏洞数据库-美国)

国家漏洞数据库是一个列出所有公开分类漏洞的网站。在网络安全中，漏洞会被归类为“Common Vulnerabilities and Exposures”（简称 CVE，意思是：常见漏洞披露）。这些 CVE 的格式为 **CVE-YEAR-IDNUMBER**；例如，著名的恶意软件 WannaCry 使用的漏洞编号是 **CVE-2017-0144**。

NVD 允许你使用按类别和提交月份的过滤器查看所有已确认的 CVE；例如，2021 年8月过去三天之时，已有 223 个新的 CVE 提交到该数据库。

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NVD

VULNERABILITIES

### August 2021

Below is a list of CVEs for the selected month.

**NOTE:** The CVEs shown below have a **release date** in the year and month chosen. The CVE ID may show a year value that does not match the release date, however, the release date will fall within the chosen year and month.

223 entries found for August 2021

CVE-2021-32066	CVE-2017-18113	CVE-2021-35477	CVE-2021-34556	CVE-2021-3351	CVE-2021-24371
CVE-2021-24425	CVE-2021-24428	CVE-2021-24430	CVE-2021-24443	CVE-2021-24444	CVE-2021-24448
CVE-2021-24450	CVE-2021-24455	CVE-2021-24456	CVE-2021-24457	CVE-2021-24458	CVE-2021-24459
CVE-2021-24460	CVE-2021-24461	CVE-2021-24462	CVE-2021-24463	CVE-2021-24464	CVE-2021-24468
CVE-2021-24470	CVE-2021-24472	CVE-2021-24473	CVE-2021-24474	CVE-2021-24476	CVE-2021-24477
CVE-2021-24478	CVE-2021-24479	CVE-2021-24480	CVE-2021-24481	CVE-2021-24483	CVE-2021-24484
CVE-2021-24488	CVE-2021-24492	CVE-2021-24496	CVE-2021-24498	CVE-2021-24503	CVE-2021-24504
CVE-2021-33526	CVE-2021-33527	CVE-2021-34574	CVE-2021-34575	CVE-2021-37165	CVE-2021-37216
CVE-2021-20332	CVE-2021-37160	CVE-2021-37161	CVE-2021-37162	CVE-2021-37163	CVE-2021-37164

虽然该网站有助于跟踪新漏洞，但在搜索特定应用程序或场景的漏洞时效果并不佳。

## Exploit-DB

**Exploit-DB** 是一种很有价值的资源，我们会在漏洞评估过程中发现它更有帮助。Exploit-DB漏洞数据库会保存很多关于软件和应用程序的漏洞利用程序（exp），这些漏洞利用程序或代码 会存储在软件或应用程序的名称、作者和版本等相关的词条下。

我们可以使用 Exploit-DB 来查找用于利用特定漏洞的代码片段（称为POC-概念证明）。

EXPLOIT DATABASE							
<input type="checkbox"/> Verified <input type="checkbox"/> Has App				Filters Reset All			
Show	15			Search:			
Date	D	A	V	Title	Type	Platform	Author
2021-08-03	↓	×		Hotel Management System 1.0 - Cross-Site Scripting (XSS) Arbitrary File Upload Remote Code Execution (RCE)	WebApps	PHP	Merbin Russel
2021-08-02	↓	×		Panasonic Sanyo CCTV Network Camera 2.03-0x - 'Disable Authentication / Change Password' CSRF	WebApps	Hardware	LiquidWorm
2021-08-02	↓	×		Online Hotel Reservation System 1.0 - 'Multiple' Cross-site scripting (XSS)	WebApps	PHP	Mohammad Koochaki
2021-08-02	↓	×		Neo4j 3.4.18 - RMI based Remote Code Execution (RCE)	Remote	Java	Christopher Ellis
2021-08-02	↓	×		Men Salon Management System 1.0 - SQL Injection Authentication Bypass	WebApps	PHP	Akshay Khanna
2021-07-29	↓	×		Oracle Fatwire 6.3 - Multiple Vulnerabilities	WebApps	Multiple	J. Francisco Bolivar
2021-07-29	↓	×		CloverDX 5.9.0 - Cross-Site Request Forgery (CSRF) to Remote Code Execution (RCE)	WebApps	Java	niebardzo
2021-07-29	↓	×		Care2x Integrated Hospital Info System 2.7 - 'Multiple' SQL Injection	WebApps	PHP	securityforeveryone.com
2021-07-29	↓	×		IntelliChoice eFORCE Software Suite 2.5.9 - Username Enumeration	WebApps	ASPX	LiquidWorm
2021-07-29	↓	×		Longjing Technology BEMS API 1.21 - Remote Arbitrary File Download	WebApps	Hardware	LiquidWorm
2021-07-29	↓	×		Denver IP Camera SHO-110 - Unauthenticated Snapshot	WebApps	Hardware	Ivan Nikolsky

## 答题

### 回答以下问题

使用NVD，2021年7月提交了多少 CVE？

1585

正确答案

Exploit-DB的作者是谁？

Offensive Security

正确答案

nvd.nist.gov/vuln/full-listing/2021/7

美国政府的官方网站 这是你知道的

NIST

信息技术实验室

国家漏洞数据库

漏洞

2021年7月

以下是所选月份的 CVE 列表。

注意：下面显示的 CVE在所选年份和月份中具有发布日期。CVE ID 可能显示与发布日期不匹配的年份值，但是，发布日期

2021年7月找到 1585个条目

exploit-db.com

EXPLOIT DATABASE

☐ 已验证

☐ 有应用

节目 15

日期 15

五

标

2022-10-17	↓	×	Wo
2022-10-06	↓	×	Wo
2022-09-23	↓	×	Tes
2022-09-23	↓	×	Aer
2022-09-23	↓	×	Wo
2022-09-23	↓	×	Wo
2022-09-23	↓	×	Tel
2022-09-23	↓	×	Fee
2022-09-23	↓	×	TP-
2022-09-21	↓	×	Wif
2022-09-21	↓	×	Wif
2022-09-20	↓	×	Blin
2022-09-20	↓	×	Boc

关于漏洞利用数据库

Exploit Database 由 Offensive Security 维护。这是一家信息安全培训公司，提供各种信息安全认证以及高端渗透测试服务。Exploit Database 是一个非盈利项目，由 Offensive Security 作为公共服务提供。

OFFENSIVE security

Exploit Database 是一个符合 CVE 标准的公共漏洞利用和相应易受攻击的软件的存档，专为渗透测试人员和漏洞研究人员使用而开发。我们的目标是提供通过直接提交、邮件列表以及其他公共资源收集的最全面的漏洞利用集合，并将它们呈现在一个免费可用且易于浏览的数据库中。Exploit Database 是漏洞利用和概念验证而非建议的存储库，对于那些需要立即采取行动数据的人来说，它是一个宝贵的资源。

谷歌黑客数据库 (GHDB) 是互联网搜索引擎查询的分类索引，旨在发现互联网上公开的有趣且通常敏感的信息。在大多数情况下，此信息从未打算公开，但由于多种因素，此信息被链接到一个网络文档中，该网络文档由搜索引擎抓取，随后搜索引擎跟踪该链接并将敏感信息输入索引。

被称为“谷歌黑客”的过程在 2000 年由专业黑客约翰尼朗推广，他开始在一个名为谷歌黑客数据库的数据库中对这些查询进行分类。他最初的努力被无数小时的社区成员努力所放大，记录在《谷歌黑客渗透测试人员》一书中，并通过媒体的大量关注和约翰尼关于该主题的演讲（例如在DEFCON 13上录制的早期演讲）而普及。Johnny 创造了“Googledork”一词来指代“Google 揭露的愚蠢或无能的人”。这是为了提醒注意这不是“谷歌问题”，而是用户或用户安装的程序经常无意的错误配置的结果。随着时间的推移，术语“dork”成为定位敏感信息的搜索查询的简写，并且“dorks”包含在可能的 Web 应用程序漏洞发布中，以显示易受攻击的网站示例。

经过社区近十年的努力，Johnny 于 2010 年 11 月将 GHDB 移交给 Offensive Security，现在它作为 Exploit Database 的扩展进行维护。今天，GHDB 包括对其他在线搜索引擎（如 Bing）和其他在线存储库（如 GitHub）的搜索，产生不同但同样有价值的结果。

## H2 一个查找漏洞的简单示例

在本小节中，将展示发现一个小漏洞的过程，以及对漏洞数据库的一些研究，最终我们将获得更有价值的漏洞和漏洞利用（exp）。


在整个漏洞评估过程中，你通常会结合多个漏洞来获得结果。例如，在本小节中，我们将利用“版本披露”漏洞来找出应用程序的版本；有了这个版本信息，我们就可以使用 **Exploit-DB** 来搜索适用于该特定版本的任何漏洞利用程序或者代码。

应用程序和软件通常有一个版本号，这些信息通常是出于善意而留下的；比如作者声明可以支持多个版本的软件等，或者作者有时也会无意中留下版本信息。比如：在下面的截图中，我们可以看到这个应用程序的名称和版本号是“**Apache Tomcat 9.0.17**”。




[Home](#)
[Documentation](#)
[Configuration](#)
[Examples](#)
[Wiki](#)
[Mailing Lists](#)
[Find Help](#)

# Apache Tomcat/9.0.17



If you're seeing this, you've successfully installed Tomcat. Congratulations!



Recommended Reading:

[Security Considerations How-To](#)

[Manager Application How-To](#)

[Clustering/Session Replication How-To](#)

[Server Status](#)
[Manager App](#)
[Host Manager](#)

## Developer Quick Start

[Tomcat Setup](#)
[Realms & AAA](#)
[Examples](#)
[Servlet Specifications](#)

[First Web Application](#)
[JDBC DataSources](#)
[Tomcat Versions](#)

### Managing Tomcat

For security, access to the [manager webapp](#) is restricted. Users are defined in:

```
$CATALINA_HOME/conf/tomcat-users.xml
```

In Tomcat 9.0 access to the manager application is split between different users. [Read more...](#)

[Release Notes](#)

[Changelog](#)

[Migration Guide](#)

[Security Notices](#)

### Documentation

[Tomcat 9.0 Documentation](#)

[Tomcat 9.0 Configuration](#)

[Tomcat Wiki](#)

Find additional important configuration information in:

```
$CATALINA_HOME/RUNNING.txt
```

Developers may be interested in:

[Tomcat 9.0 Bug Database](#)

[Tomcat 9.0 JavaDocs](#)

[Tomcat 9.0 SVN Repository](#)

### Getting Help

[FAQ and Mailing Lists](#)

The following mailing lists are available:


[tomcat-announce](#)  
Important announcements, releases, security vulnerability notifications. (Low volume).

[tomcat-users](#)  
User support and discussion

[taglibs-user](#)  
User support and discussion for [Apache Taglibs](#)

[tomcat-dev](#)  
Development mailing list, including commit messages

有了这些信息，我们就可以使用 Exploit-DB 上的搜索过滤器来查找可能适用于“Apache Tomcat 9.0.17”的相关漏洞利用程序或者代码。



[Home](#)
[About](#)
[FAQ](#)
[Contact](#)

☐ Verified
 ☐ Has App
 [Filters](#)
[Reset All](#)

Show

Date	D	A	V	Title	Type	Platform	Author
2021-07-13				Apache Tomcat 9.0.0.M1 - Cross-Site Scripting (XSS)	WebApps	Multiple	Central InfoSec
2021-07-13				Apache Tomcat 9.0.0.M1 - Open Redirect	WebApps	Multiple	Central InfoSec
2020-01-08				Tomcat proprietaryEvaluate 9.0.0.M1 - Sandbox Escape	WebApps	Java	hantwister
2017-10-09				Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2)	WebApps	JSP	int0x80
2017-09-20				Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1)	WebApps	Windows	xxlegend

Showing 1 to 5 of 5 entries (filtered from 44,305 total entries)

[FIRST](#)
[PREVIOUS](#)
[1](#)
[NEXT](#)
[LAST](#)

在搜索 Exploit-DB 之后，对于这个特定版本的应用程序，总共有 5 个漏洞可能对我们有用，我们需要自行筛选出对我们有用的漏洞和exp（漏洞利用程序）。

答题



### 回答以下问题


在这个例子中，我们使用什么类型的漏洞来查找应用程序的名称和版本？

Version Disclosure

版本泄露

正确答案

## H2 展示：对Ackme的应用程序进行漏洞利用



Vulnerabilities Showcase: ACKme IT Services

Scenario

It is your first week at ThePentestingCo as a Jr. Penetration tester. To ease into the role, you are shadowing a Sr. Penetration tester on your first engagement.

The Sr. Penetration tester has managed to find a vulnerability in a web application that the client (ACKme IT Services) uses.

Follow the steps that the Sr. Penetration tester took to ultimately exploit ACKme IT Service's infrastructure.

Next

https://email.thepentestingco.thm/user/inbox

Inbox (10)

Reports

Training

Support

Junk (13)

Drafts

Sent

Trash

Messages

Kyle Hodgson

ACKme IT Services

13:32

ThatCloudCompany

Thank you for signing up!

11:46

Viewing

ACKme IT Services

From: Kyle Hodgson

PDF

Thank you for taking on this engagement. Please document every step extensively for the new Jr. Penetration tester to follow. I have attached our company reporting template to help with this.

As a reminder, ACKme IT Services only want you to test the IP address **240.228.189.136**. Any other IP or machine is out of scope.

Good luck!

Joe

### 1.信息收集

在这个阶段，渗透测试员使用了一项公共服务，该服务涉及了有关目标公司的一些详细信息。正如我们所见，ACKme IT Services 为 800 多个客户提供 IT 服务。这些信息很有用，因为我们可以开始考虑我们可能用作攻击目标的一些软件。例如，帮助台（helpdesk）或支持应用程序（support application）。



## 1. Information Gathering

At this stage, the Sr. Penetration Tester has used a public service that compiles some details about the target company.

As we can see, ACKme IT Services provide IT services to 800+ clients. This information is useful because we can begin to think of possible software that they are using for us to attack. For example, helpdesk or a support application.

[Next](#)

<https://companiesreport.thm/ackme-it-services>

### Companies Report

#### Company Info

**Established:** 2017  
**Business Type:** Corporation  
**Purpose:** IT Support Services  
**Clients:** 800+

#### CEO



Danny Phantom

[d.phantom@ackme.thm](mailto:d.phantom@ackme.thm)

## 2. 枚举&扫描

现在进入枚举和扫描阶段，这个阶段能够帮助我们发现 ACKme 的基础设施上运行的服务和应用程序。我们可以使用从这次扫描中收集到的信息来了解哪些服务可能会受到攻击。例如，托管网站的网络服务器。

从我们的电子邮件中回想一下，我们获得了一个 IP 地址 240.228.189.136，现在尝试扫描此 IP 地址。



## 2. Enumeration & Scanning

The Sr. Penetration tester now moves onto the enumeration and scanning stage of the engagement. This stage helps establish services and applications running on ACKme's infrastructure.

We can use the information gathered from this scan to begin to understand what services may be viable to attack. For example, a webserver hosting a website.

Recall from our Email, we are given one IP address **240.228.189.136**. Try scanning this IP address yourself...

Next

IP Address

Run Nmap Request

```
user@thepentestingco:~$ nmap 240.228.189.136
```

```
Starting Nmap 7.60 ( https://nmap.org )
```

```
Nmap scan report for 240.228.189.136
```

```
Host is up (0.0013s latency).
```

```
Not shown: 997 closed ports
```

```
PORT STATE SERVICE
```

```
22/tcp open ssh
```

```
80/tcp open http
```

```
443/tcp open https
```

```
Nmap done: 1 IP address (1 host up) scanned in 8.35 seconds
```

```
user@thepentestingco:~$ nmap
```

## 3.应用测试

使用从渗透的第二阶段收集的信息，渗透测试员已经在 Web 浏览器中访问了目标，并收到了一个登录页面；渗透测试员在登录页面猜测了一些随机密码，例如“admin”和“admin”，但无济于事。渗透测试员注意到应用程序 1.5.2 的版本号并记下了这一点，这将对下一阶段有用。



## 3. Application Testing

Using the information gathered from stage two of the penetration engagement. The Jr. Penetration tester has visited the target in their web browser and has been greeted with a login page.

The Sr. Penetration tester guesses some random passwords such as "admin" and "admin" to no avail. They notice a version number of the application **1.5.2** and takes a note of this. This will be useful for the next stage.

Next



https://240.228.189.136

ACKme Portal

Version 1.5.2

Username

Password

Log in

☐ Remember me

[Forgot Password?](#)

## 4.漏洞研究

从上一个阶段可知：ACKme IT Services 使用了名为“ACKme Portal”的web应用程序，其版本号为“1.5.2”。

渗透测试员决定访问一个名为“Vulnerability Bank™”的漏洞和漏洞利用(exp)数据库，该网站存储了应用程序的漏洞和exp的详细信息。渗透测试员可以在此站点中搜索在第三阶段中发现的软件及其版本。很幸运！该应用程序和版本条目下列出了一个相关的漏洞：远程代码执行漏洞 (RCE)。

我们可以尝试在 Vulnerability Bank™ 中搜索“ACKMe Portal 1.5.2”的漏洞利用，RCE 漏洞允许我们在目标系统上执行命令，渗透测试员可以利用此漏洞访问目标的控制台程序。



### 4. Vulnerability Research

The Sr. Penetration tester recalls that ACKme IT Services uses an application called "ACKme Portal" that has a version number of "1.5.2". The Sr. Penetration Tester visits a vulnerability & exploit database called "Vulnerability Bank™".

This website stores details of vulnerabilities and exploits for applications. The Sr. Penetration Tester searches this site for the software that was discovered in stage three. They're in luck! There is one vulnerability listed for that application & version: Remote Code Execution (RCE).


RCE vulnerability allows commands to be executed on the target's system. The Sr. Penetration Tester could use this vulnerability to gain access to the console of the target.

Try searching Vulnerability Bank™ for an exploit for "ACKme Portal 1.5.2"

Next



https://vulnerabilitybank.thm

 Vulnerability Bank™

*Listing Vulnerabilities since 2001!*

ACKme Portal 1.5.2



### 5.漏洞利用

渗透测试员已经积累了所有先前阶段的信息，可以使用从 Vulnerability Bank™ 下载的漏洞攻击 ACKme 在 240.228.189.13 上的 Web 应用程序。

我们能看到：该漏洞利用执行成功并且滥用远程代码执行 (RCE) 漏洞在 ACKme 的基础架构上启动了反向 shell。通过使用反向 shell 界面，渗透测试员可以查找有价值的文件，例如目标的密码、备份文件或应用程序源代码等。



### 5. Exploitation

Accumulating the information from all the previous stages, the Sr. Penetration Tester uses the exploit downloaded from Vulnerability Bank™ against ACKme's web application on 240.228.189.13.

The exploit is successful and abuses the Remote Code Execution (RCE) vulnerability to launch a reverse shell on ACKme's infrastructure.

From here, the Sr. Penetration tester can look for files of value such as passwords, backups or application source code.

Use **THM{ACKME\_ENGAGEMENT}** to answer the task question on TryHackMe.

```
user@thepentestingco:~$ run exploit -u http://240.228.189.136
Running exploit!
Exploit complete! Launching shell...
administrator@ackmeitservices:~$ whoami
ACKME\Administrator
```

### 答题

#### 回答以下问题

跟随展示利用 ACKme 的应用程序到最后检索标志。这是什么旗帜？

正确答案