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:

Operating System

(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



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:

<u>CVSS</u> 的优势	<u>CVSS</u> 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。
<u>CVSS</u> 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和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。

<u>VPR</u> 的优势	VPR的缺点
VPR 是一个现实世界的现代框架。	<u>VPR</u> 不像其他一些漏洞管理框架那样开源。
<u>VPR</u> 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。
<u>VPR</u> 是风险驱动的,组织使用它来帮助确定修补漏洞的优先级。	WPR 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



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)

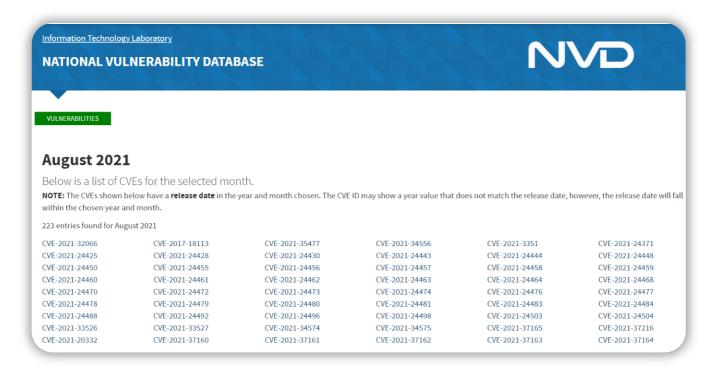
在深入研究以上两个资源之前,让我们确保我们对一些基本关键术语的理解是一致的:

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 (<u>PoC</u>)	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。

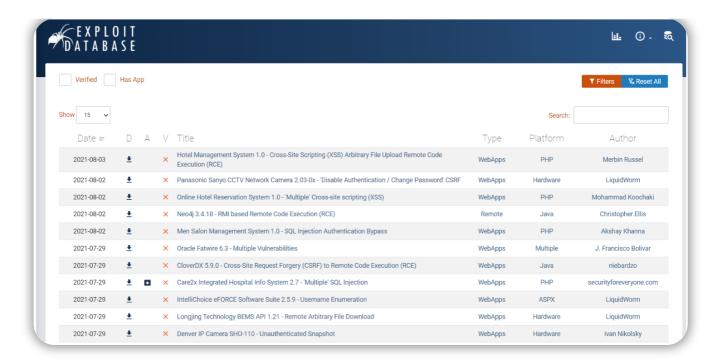


虽然该网站有助于跟踪新漏洞,但在搜索特定应用程序或场景的漏洞时效果并不佳。

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。

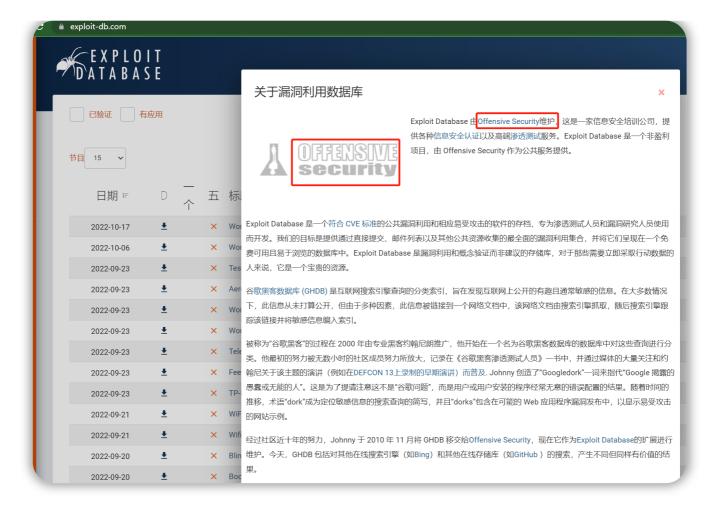
我们可以使用 Exploit-DB 来查找用于利用特定漏洞的代码片段(称为POC-概念证明)。



答题





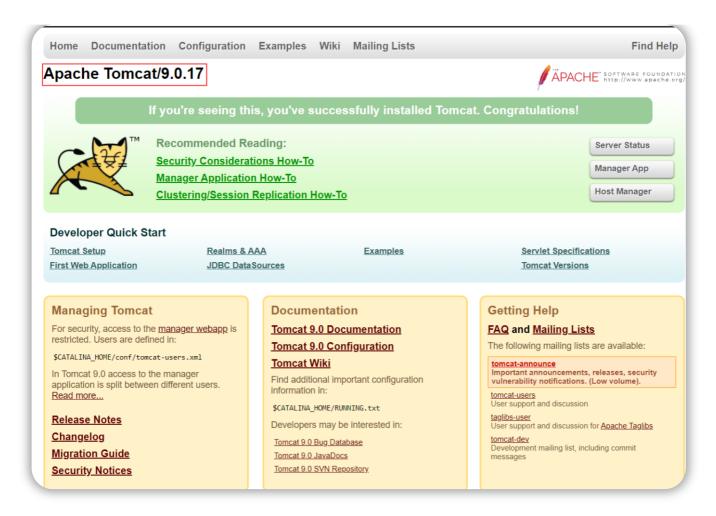


H2 一个查找漏洞的简单示例

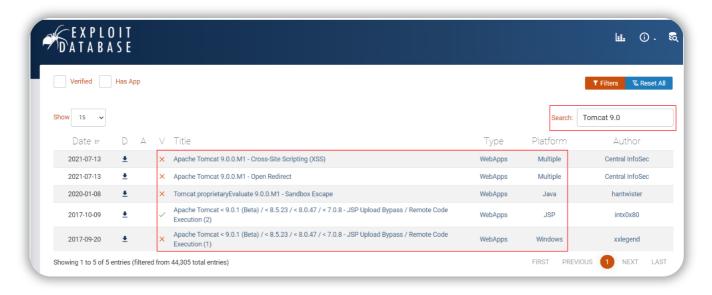
在本小节中,将展示发现一个小漏洞的过程,以及对漏洞数据库的一些研究,最终我们将获得更有价值的漏洞和漏洞利用(exp)。

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"。

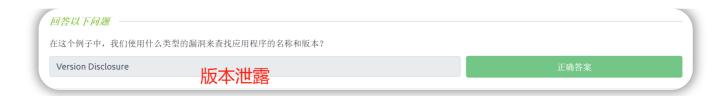


有了这些信息,我们就可以使用 Exploit-DB 上的搜索过滤器来查找可能适用于 "Apache Tomcat 9.0.17" 的相关漏洞利用程序或者代码。

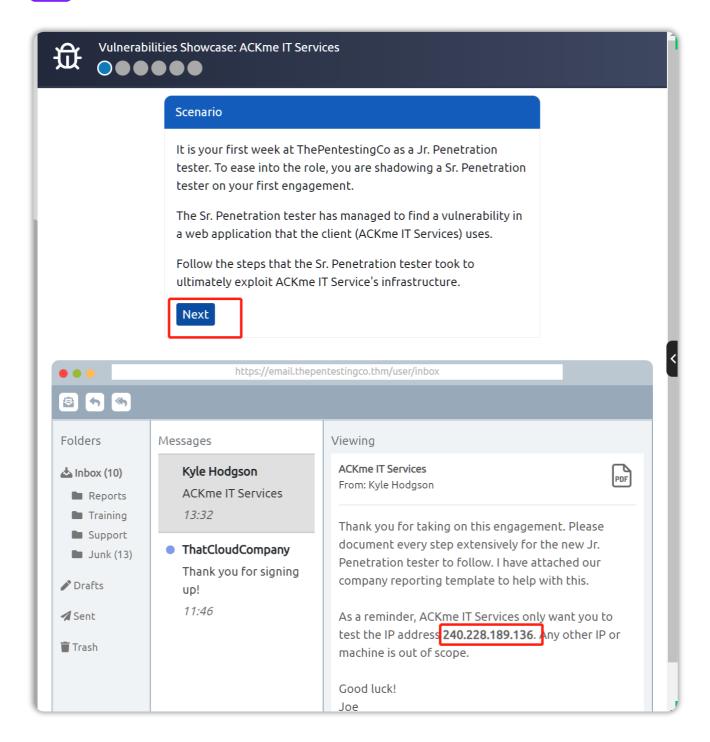


在搜索 Exploit-DB 之后,对于这个特定版本的应用程序,总共有 5 个漏洞可能对我们有用,我们需要自行筛选出对我们有用的漏洞和exp(漏洞利用程序)。

答题

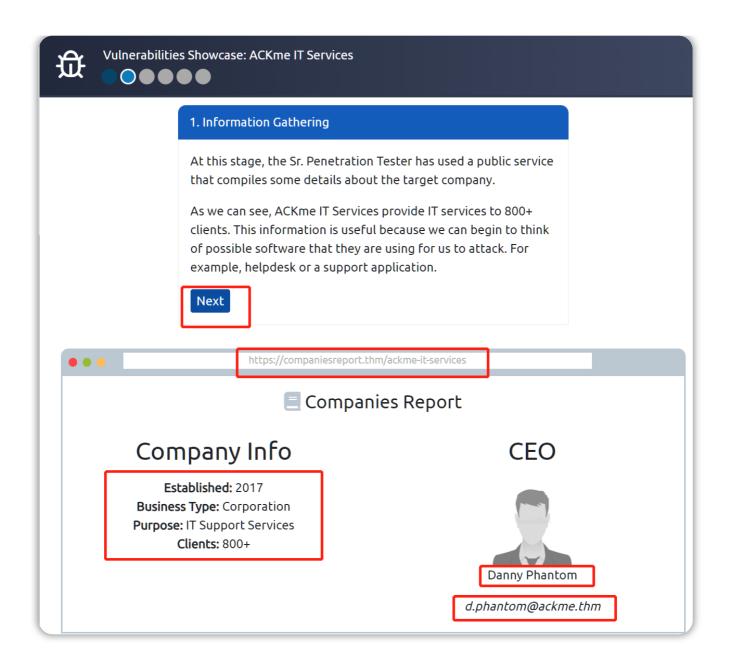


H2 展示:对Ackme的应用程序进行漏洞利用



1.信息收集

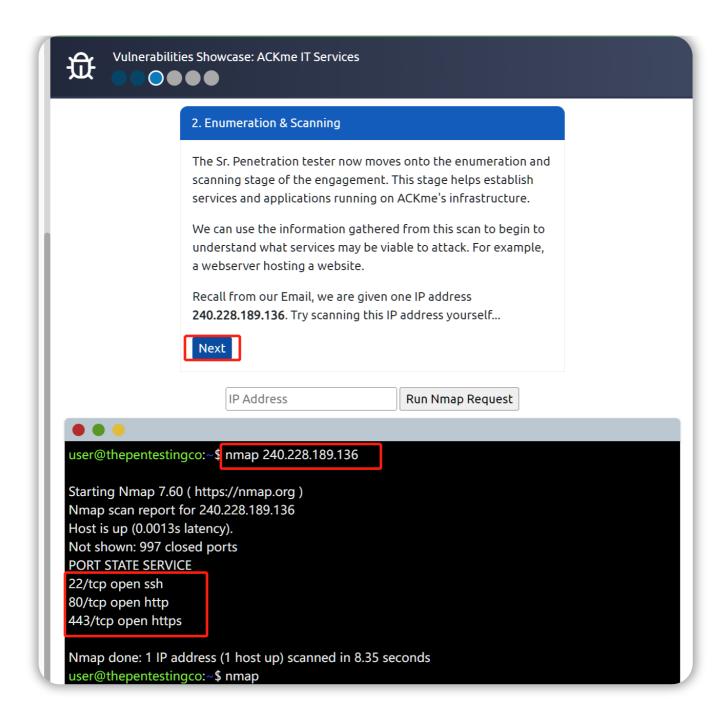
在这个阶段,渗透测试员使用了一项公共服务,该服务涉及了有关目标公司的一些详细信息。正如我们所见,ACKme IT Services 为 800 多个客户提供 IT 服务。这些信息很有用,因为我们可以开始考虑我们可能用作攻击目标的一些软件。 例如,帮助台(helpdesk)或支持应用程序(support application)。



2.枚举&扫描

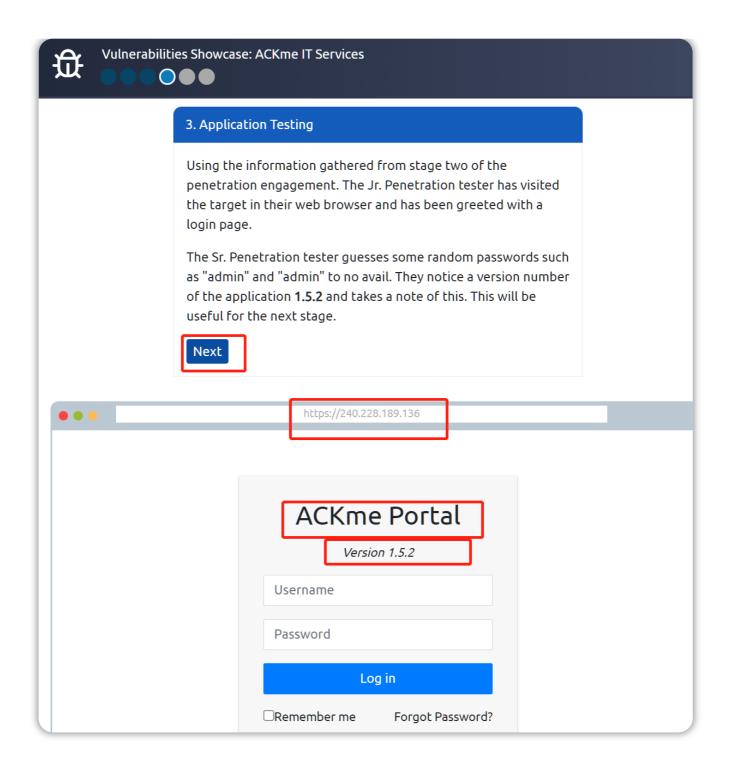
现在进入枚举和扫描阶段,这个阶段能够帮助我们发现在 ACKme 的基础设施上运行的服务和应用程序。 我们可以使用从这次扫描中收集到的信息来了解哪些服务可能会受到攻击。 例如,托管网站的网络服务 器。

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。



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。

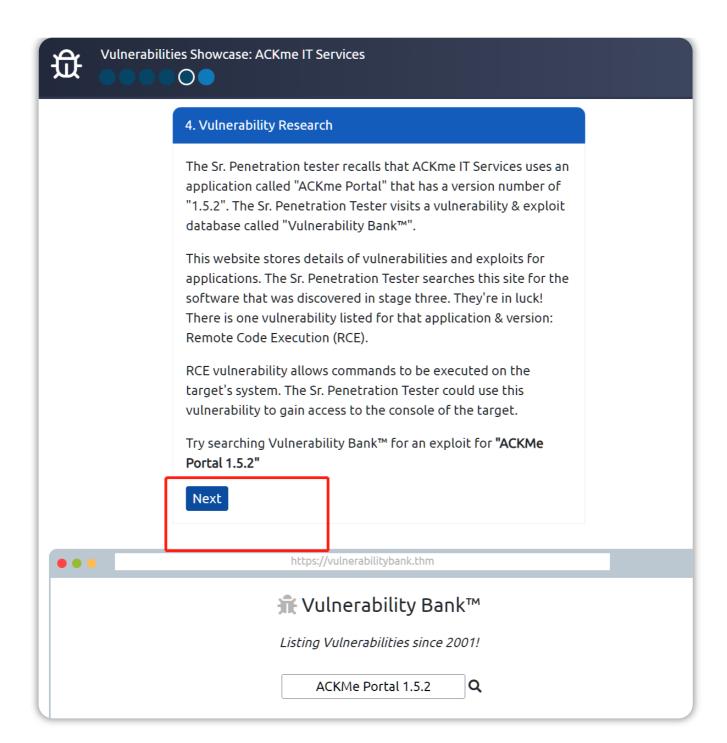


4.漏洞研究

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。



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。



Vulnerabilities Showcase: ACKme IT Services



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?

THM{ACKME_ENGAGEMENT}

正确答案