Vulnerabilities 101

Understand the flaws of an application and apply your researching skills on some vulnerability databases.

Task 2 Introduction to Vulnerabilities

Question	Answer
An attacker has been able to upgrade the permissions of their system account from "user" to "administrator". What type of vulnerability is this?	Operating System
You manage to bypass a login panel using cookies to authenticate. What type of vulnerability is this?	Application Logic

Task 3 Scoring Vulnerabilities (CVSS & VPR)

Question	Answer
What year was the first iteration of CVSS published?	2005
If you wanted to assess vulnerability based on the risk it poses to an organisation, what framework would you use? Note: We are looking for the acronym here.	VPR
If you wanted to use a framework that was free and open-source, what framework would that be? Note: We are looking for the acronym here.	CVSS

Task 4 Vulnerability Databases

Question	Answer
Using NVD, how many CVEs were published in July 2021?	1554
Who is the author of Exploit-DB?.	offsec

Task 5 An Example of Finding a Vulnerability

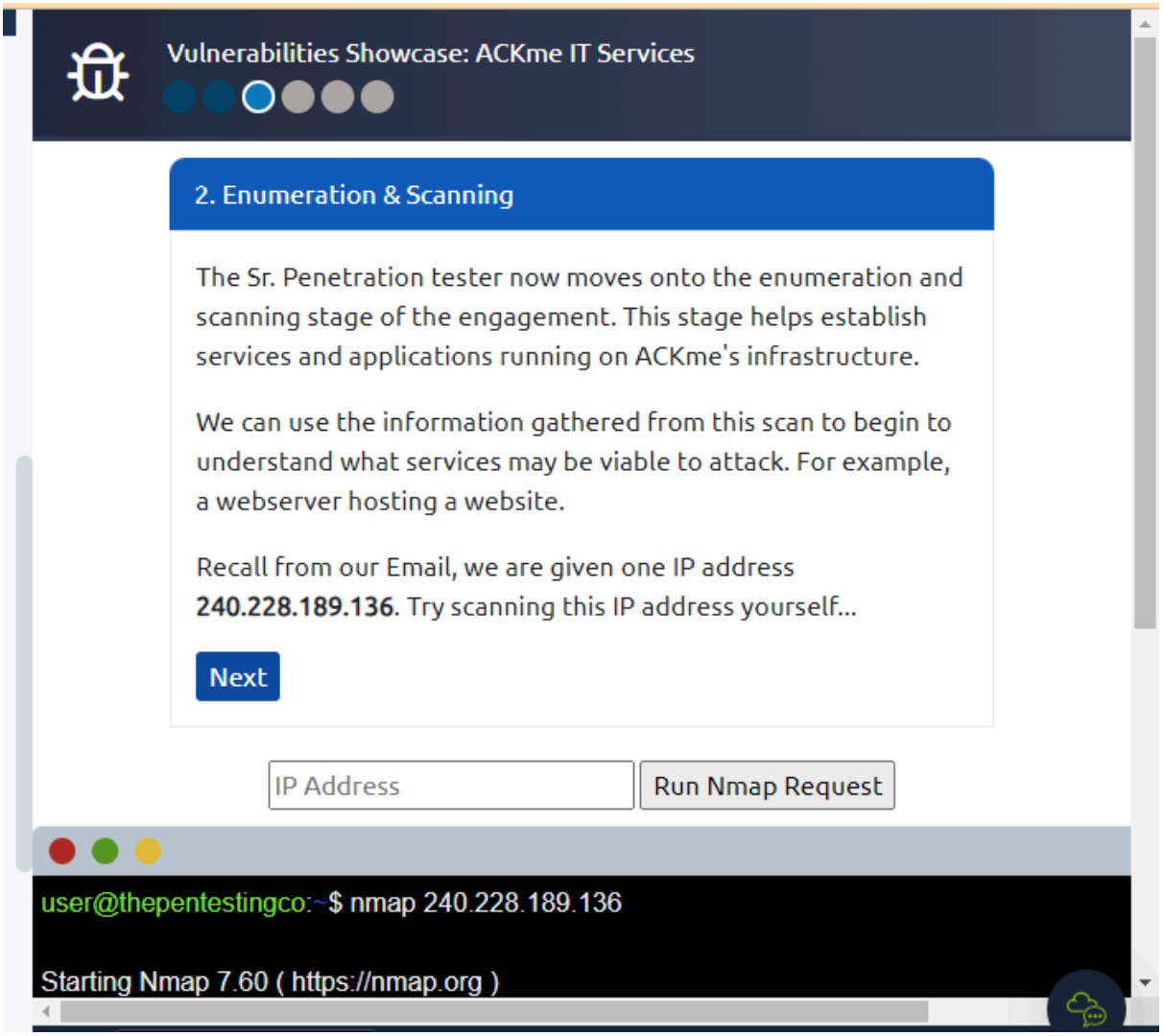
Question	Answer
What type of vulnerability did we use to find the name and version of the application in this example?	Version Disclosure

Task 6 Showcase: Exploiting Ackme's Application

Follow along with the showcase of exploiting ACKme's application to the end to retrieve a flag. What is this flag?

Answer: **THM{ACKME_ENGAGEMENT}**

➔ I deployed the site attached to this task and followed the steps that the Sr. Penetration Tester took to exploit a vulnerability against ACKme IT Service's infrastructure.


Vulnerabilities Showcase: ACKme IT Services
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)

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