Task 13 : 6. Vulnerable and Outdated Components

Vulnerable and Outdated Components

Occasionally, you may find that the company/entity you're pen-testing is using a program with a well-known vulnerability.

For example, let's say that a company hasn't updated their version of WordPress for a few years, and using a tool such as WPScan, you find that it's version 4.6. Some quick research will reveal that WordPress 4.6 is vulnerable to an unauthenticated remote code execution(RCE) exploit, and even better, you can find an exploit already made on Exploit-DB.

As you can see, this would be quite devastating because it requires very little work on the attacker's part. Since the vulnerability is already well known, someone else has likely made an exploit for the vulnerability already. The situation worsens when you realise that it's really easy for this to happen. If a company misses a single update for a program they use, it could be vulnerable to any number of attacks.

Answer the questions below :

1. Read about the vulnerability.
A. No answer needed