VULNERABILITIES 101

1. <u>Introduction:</u>

2. <u>Introduction to Vulnerabilities (Categories):</u>

- **Operating System:** These types of vulnerabilities are found within Operating Systems (OSs) and often result in privilege escalation.
- **(Mis)Configuration-based:** These types of vulnerability stem from an incorrectly configured application or service. (Website exposing customer details)
- **Weak or Default Credentials:** Applications and services that have an element of authentication will come with default credentials when installed.
  (Username and password of "admin")
- **Application Logic:** These vulnerabilities are a result of poorly designed applications. (Poorly Authentication Mechanisms)
- **Human-Factor:** Human-Factor vulnerabilities are vulnerabilities that leverage human behavior. (Phishing emails)

3. <u>Scoring Vulnerabilities (CVSS & VPR):</u>

CVSS → Common Vulnerability Scoring System
https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

VPR → Vulnerability Priority Rating
(Same as CVSS But no : *"None/Information"* Rating)

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

4. <u>Vulnerability Databases:</u>

- NVD (National Vulnerability Database): https://nvd.nist.gov/vuln/full-listing
- Exploit-DB: https://exploit-db.com/
- PoC (Proof of Concept): Demonstrates the exploitation of a vulnerability.

5. <u>An Example of Finding a Vulnerability</u>

6. <u>Showcase: Exploiting Ackme's Application:</u>

7. <u>Conclusion:</u>