## Tecnológico de Costa Rica

## Victor Aymerich Quesada – 2023152436

## Luis Urbina -

## Instituto Tecnológico De Costa Rica, Campus Tecnológico Central

## Escuela de Ingeniería en Computación

## Seguridad del software

## Herson Tobias Esquivel Vargas

## 9/19/2025

## Proyecto 1

Herramienta seleccionada: Busy box 1.37.0/netoworking/httpd.c usando Debian 64 bits

2- Flow Finder: Hubo muy buenos resultados sin necesidad de una configuración muy elaborada por lo tanto se pudo usar un comando sencillo como:

flawfinder --columns --minlevel=1 busybox-source/busybox-1.37.0/networking/httpd.c > analysis\_results/flawfinder\_httpd\_detailed.txt

3- Flow Finder:

Resultados de herramienta:

**Resumen del análisis**

* **Total hallazgos:** 46
* **Nivel 4 (alto):** 14 hallazgos
  + Ejemplos:
    - fprintf en línea 315 → CWE-134 (format string).
    - sprintf en 725, 952, 1120, etc. → CWE-120 (buffer overflow).
    - strcpy en 920, 960, 2333, 2420 → CWE-120 (buffer overflow).
    - access en 1168 y 2448 → CWE-362/367 (race condition).
    - execv en 1709 → CWE-78 (command injection).
* **Nivel 3 (medio):** 1 hallazgo
  + getenv en 2876 → CWE-807 (insecure environment variable).
* **Nivel 2 (bajo):** 21 hallazgos
  + Varios atoi, memcpy, open, arrays estáticos (char buffer[256]).
* **Nivel 1 (informativo):** 10 hallazgos
  + Varios strlen sobre cadenas.

| **Línea** | **Función** | **CWE** | **Clasificación** | **Nota breve** |
| --- | --- | --- | --- | --- |
| 315 | fprintf | CWE-134 | Verdadero positivo | Uso con string no constante → riesgo de format string |

**Hallazgos de Flawfinder en httpd.c**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Línea** | **Nivel** | **Tipo** | **Función** | **CWE estimado** | **Clasificación** | **Nota breve** |
| 315 | 4 | format | fprintf | CWE-134 | VP | Uso con string no constante → format string attack |
| 725 | 4 | buffer | sprintf | CWE-120 | VP | Posible overflow en buffer local |
| 920 | 4 | buffer | strcpy | CWE-120 | VP | Copia sin límite → riesgo alto |
| 952 | 4 | buffer | sprintf | CWE-120 | VP | Overflow posible en parsing |
| 960 | 4 | buffer | strcpy | CWE-120 | VP | Copia sin límite |
| 1120 | 4 | buffer | sprintf | CWE-120 | VP | Uso inseguro de sprintf |
| 1168 | 4 | race | access | CWE-362/367 | VP | Condición de carrera TOCTOU |
| 1268 | 4 | buffer | sprintf | CWE-120 | FP | Uso con límites válidos |
| 1709 | 4 | exec | execv | CWE-78 | VP | Ejecución de comandos externos |
| 2333 | 4 | buffer | strcpy | CWE-120 | VP | Copia sin límite |
| 2420 | 4 | buffer | strcpy | CWE-120 | VP | Copia insegura |
| 2448 | 4 | race | access | CWE-362/367 | VP | Posible condición de carrera |
| 2876 | 3 | env | getenv | CWE-807 | VP | Dependencia de variable de entorno |
| 856 | 2 | conv | atoi | CWE-190 | FP | Input limitado, bajo riesgo |
| 1645 | 2 | proc | vfork | CWE-362 | FP | Riesgo irrelevante en Linux moderno |