<UWE-484-N>: <Description/Title>

# The Basics

**Authors**: <Your names here>

**Disclosure Date**: 05/13/2024

**Product**: tinyserv

**Reporter(s):** CSE 484 staff

**Exploit sample**: see sploitN.sh

# The Exploit

**Exploit strategy (2p) -** What does the exploit do? What are the key parts of the exploit?:

**Exploit primitives (2p) -** What new capabilities (if any) does an attacker gain from successful exploitation of the vulnerability?These are small, process-space or environment-related building blocks used to construct full exploit chains such as: write arbitrary data to arbitrary memory locations, overwrite local variables, overwrite heap data, crash the program, send data on the network, read from local files, escalate privileges, etc.:

# The Vulnerability[[1]](#footnote-0)

**Vulnerability details** **(3p) -** Provide details about the vulnerability. Also, if applicable, provide the vulnerable file(s), function(s), and line number(s):

**Bug class (CWE) (1p) -** Visit [this page](https://cwe.mitre.org/data/definitions/699.html) (<https://cwe.mitre.org/data/definitions/699.html>) and provide the name and CWE identifier number of the bug class that best fits the vulnerability. You will need to expand the dropdowns/bullets to see all the options for each category.:

**Severity/priority score (2p) -** Rate the severity of the vulnerability as one of low, medium, or high, and explain your choice in terms of the vulnerability and the provided exploit:

**Thoughts on how this vulnerability might have been found by the attacker (1p)** **-** What did the attacker do (what tools, techniques, etc.) to find this vulnerability?

# The Patch

**Proposed patch plan (2p)** - This must be something you can implement in code for tinyserv; do not say something like “use stack canaries” for your answer to this question**:**

**Killing the bug class (bonus 1p) -** What could the tinyserv project do to prevent more vulnerabilities of this CWE type from appearing anywhere in this codebase in the future? Explain some advantages and disadvantages of your solution**:**

1. If an exploit uses more than one vulnerability, then when asked about “the vulnerability”, answer for all vulnerabilities instead. [↑](#footnote-ref-0)