```
................................................................................
::  ANTIGRAVITY V7 // SINGULARITY ARTIFACT                                    ::
##  ID: 905ba1fb-42b3-414f-be78-0b60f9dd1dc0  |  CYCLE: 697B3351  |  ENTROPY: 0.004        ##
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

[00] :: SYNAPTIC_TELEMETRY
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
TARGET_HOST   :: api.nexus-commerce.io
INFECT_VECTOR :: EXPLOIT >> CWE-UNKNOWN
CONFIDENCE    :: 99.999% (Verified by Gamma)
HIVE_LATENCY  :: 47ms (Optimal)
RISK_STATE    :: [!] CRITICAL_MEMBRANE_RUPTURE

[01] :: HIVE_CONSENSUS (SYNC_NODE_04)
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
> OMEGA:  Perimeter protocols bypassed. Logic sanitization nonexistent.
> ZETA:   Resources steady. No thermal throttling required.
> VERDICT: System integrity compromised via EXPLOIT logic flaw.

[02] :: CHRONOLOGICAL_EVENT_STREAM
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
T+00.000  [ALPHA]  >>  HANDSHAKE_INIT  :: DATA_STREAM_ACTIVE
T+19.330  [BETA ]  >>  INJECTION_EXEC  :: Payload_217a
T+20.030  [GAMMA]  >>  STATE_CHANGE    :: SAFE -> COMPROMISED
T+38.880  [KAPPA]  >>  MEMORY_WRITE    :: Vector Stored

[03] :: RAW_EVIDENCE (HEX_DUMP_VIEW)
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
OFFSET    00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F  ASCII
00000000  7B 27 74 79 70 65 27 3A 20 27 6C 6F 67 69 63 5F  {'type': 'logic_
00000010  61 72 69 74 68 6D 65 74 69 63 5F 6F 76 65 72 66  arithmetic_overf
00000020  6C 6F 77 27 2C 20 27 70 61 79 6C 6F 61 64 27 3A  low', 'payload':
00000030  20 27 2D 39 32 32 33 33 37 32 30 33 36 38 35 34   '-9223372036854

[04] :: REMEDIATION (GENETIC_PATCH)
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
EST_EFFORT: 1.5 HOURS  |  SEVERITY: EXTINCTION_LEVEL

[ARCHITECTURAL_ADAPTATION]
> Implement Strict Schema Validation (Zod/Pydantic) at Gateway.
> Enforce unsigned integer boundaries for all transaction inputs.

[CODE_INJECTION]
# FILE: services/cart_service.py
  def update_quantity(item_id: str, qty: int):
+     if qty < 1: raise SecurityException("Negative Quantity")
+     if qty > MAX: raise LogicException("Overflow Attempt")
      return db.update(item_id, qty)

--------------------------------------------------------------------------------
[SIG] {hashlib.sha256(report_content.encode()).hexdigest()[:64]} // VERIFIED
................................................................................
```