

Planned Flags for NullCon CTF 2026

February 7, 2026

Abstract

This document contains the collection of flags used throughout our Capture The Flag (CTF) security challenge. Each flag represents the successful completion of a specific task, vulnerability exploitation, or investigative step within the competition. Participants should handle these flags responsibly and avoid sharing them outside the intended challenge environment. Developer should keep this document and single flags confidential as well.

PLEASE NOTE: If the document has to be published before the competition, each challenge author is responsible to securely redact the flags used by his or her services!

1 Flag Format

The flag format `ENO{...}` follows a structured and intentionally constrained pattern commonly used in Capture The Flag (CTF) competitions to ensure both consistency and unambiguous identification of valid solutions. In this scheme, every legitimate flag begins with the fixed prefix “ENO”, immediately followed by a pair of curly braces that enclose the flag’s substantive content. The material inside the braces typically consists of an alphanumeric string, often augmented with underscores, mixed-case letters, or leetspeak substitutions. These stylistic choices serve two purposes: they make the flag human-readable while still allowing challenge designers to embed subtle hints, thematic references, or obfuscation techniques.

A representative example—`ENO{th1s_is_4n_eXample}`—illustrates the typical composition. The prefix anchors the flag to the event or organizing body, while the internal token demonstrates the flexible yet controlled syntax permitted within the braces. This structure is intentionally simple enough to be recognized across diverse challenge categories (cryptography, forensics, web exploitation, etc.) yet sufficiently distinctive to prevent accidental collisions with unrelated text. By standardizing the format, organizers streamline automated validation, reduce ambiguity during submissions, and reinforce a coherent identity across the competition’s technical artifacts.

2 Flag Generation Algorithm



3 Flag Distribution

Take only the flag associated with your challenge. The flag will only work for the intended challenge.

3.1 Computational Artefact Deconstruction and Behavioral Inference

The [REDACTED] is [REDACTED] { [REDACTED] }, [REDACTED] the [REDACTED] [REDACTED] of the [REDACTED] [REDACTED] [REDACTED]. The [REDACTED] [REDACTED] is [REDACTED] { [REDACTED] }, [REDACTED] [REDACTED] [REDACTED] a [REDACTED] [REDACTED] with the [REDACTED] [REDACTED]. The [REDACTED] [REDACTED] is [REDACTED] { [REDACTED] }, [REDACTED] that the [REDACTED] [REDACTED] [REDACTED] has been [REDACTED] [REDACTED]. The [REDACTED] [REDACTED] is [REDACTED] { [REDACTED] }, [REDACTED] [REDACTED] [REDACTED] [REDACTED] the [REDACTED] to [REDACTED] a [REDACTED] [REDACTED]. The [REDACTED] [REDACTED] is [REDACTED] { [REDACTED] }, [REDACTED] [REDACTED] [REDACTED] of the [REDACTED] and its [REDACTED] [REDACTED].

3.2 Computational Epistemology and Algorithmic Hermeneutics

The first flag is `ENO[semantic.3.inference.initialized]`, marking the moment participants successfully extract meaning from an intentionally opaque computational construct. The second flag is `ENO[semantic.3.inference.initialized]`, awarded upon demonstrating a structured understanding of a process that initially appears arbitrary or chaotic. The third flag is `ENO[semantic.3.inference.initialized]`, obtained when a participant's analytical framework aligns with the system's hidden operational logic. The fourth flag is `ENO[semantic.3.inference.initialized]`, representing mastery over the recursive interpretive steps required to fully decode the challenge's epistemic structure.

3.3 Applied Cryptanalytic Methodologies and Information Obfuscation Studies

The first flag is [REDACTED], awarded upon correctly interpreting the foundational transformation applied to the encoded message. The second flag is [REDACTED], signifying the participant's ability to extract meaningful structure from an intentionally noisy cryptographic construct. The third flag is [REDACTED], obtained after navigating the algebraic constraints underlying the challenge's numerical system. The fourth flag is [REDACTED], granted once the hidden key material has been isolated through analytical reasoning or computational strategy. The fifth flag is [REDACTED], marking the moment when the internal logic of a cryptographic scheme has been fully reconstructed. The sixth flag is [REDACTED], representing the culmination of the participant's efforts in breaking, bypassing, or otherwise subverting the intended security mechanism.

3.4 Dynamic Systems Perturbation and Exploitability Studies



3.5 Interoperable Protocol Forensics and Network Phenomenology

████ first flag █████ ENO{██████████}, earned █████ isolating █████ interpreting █████ latent meaning embedded within █████ fragmented protocol exchange. █████ second flag █████ ENO{██████████}, awarded upon demonstrating insight into █████ disparate network layers influence █████ another’s observable behavior. █████ third flag █████ ENO{██████████}, obtained █████ classifying irregular communication patterns █████ tracing █████ phenomenological origins. █████ fourth flag █████ ENO{██████████}, granted █████ participants successfully reveal █████ hidden structural alignment—████ misalignment—████ interoperating systems.

3.6 Distributed Hypermedia Systems Analysis and Vulnerability Exploration

The first flag is [REDACTED]{[REDACTED]}, obtained by identifying and exploiting a subtle flaw in the service’s handling of user-supplied data. The second flag is [REDACTED]{[REDACTED]}, awarded upon demonstrating an understanding of how weak state-management practices can be manipulated to escalate privileges. The third flag is [REDACTED]{[REDACTED]}.

granted when participants successfully uncover and leverage a hidden or improperly validated pathway within the application's request-processing flow.

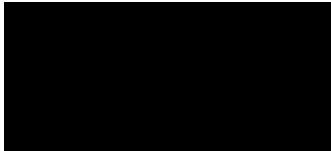
3.7 Computational Ontology Reconciliation and Symbolic Discontinuity Analysis



3.8 Practical Offensive Systems Manipulation and Privilege Subversion

[REDACTED]

3.9 Synthetic Logic Manipulation and Constraint Subversion Theory



4 Signatures

The final flag document has to be signed by at least two organizers.