CyberSci Canada

A case study in community mismanagement.

Kohi, Hamed
0x.hamy.1@gmail.com
Date: July 12th, 2025

Table of Contents

CyberSci Canada: A case study in community mismanagement

TLDR: The CyberSci Incident

I discovered a security vulnerability at Royal Bank Canada (RBC) that allowed financial theft, which they classified as "intended behavior" while simultaneously requiring that I refrain from public disclosure. When I posted about this contradiction in CyberSci's Discord server where RBC was actively recruiting, my message was silently deleted without explanation.

CyberSci is a Canadian organization that serves as a **cyber talent pipeline for national security agencies** such as the Communications Security Establishment (CSE) and the Canadian Security Intelligence Service (CSIS). An organization fulfilling this critical role should actively encourage speaking out about security issues, particularly when vulnerabilities affect critical systems.

When I contacted CyberSci founder Tom Levasseur regarding the message deletion, he admitted that the organization avoids any criticism of its sponsors. He claimed that moderators had mistaken me for "some immature student," despite my name appearing on their contributor board. He then accused me of making "threats" when I stated that I would document how different organizations handled this security disclosure situation.

Given that Canadian national security agencies recruit cyber operators from CyberSci, Canada's national security training pipeline **may have been compromised** by financial relationships that prioritize sponsor comfort over legitimate security discourse and effective talent development.

Executive Summary

This analysis documents concerning patterns in how the CyberSci organization handles community discourse, particularly when it intersects with sponsor relationships. As a strong advocate for Canada's democratic principles including the fundamental right to

express professional opinions without institutional censorship, I find it troubling when financial institutions appear to influence community platforms to suppress legitimate security discourse.

This document examines an incident where my message in the CyberSci Discord server, which referenced concerns about **Royal Bank of Canada's (RBC)** vulnerability disclosure practices, was removed without explanation or notification.

The subsequent organizational response suggests a systematic prioritization of sponsor relationships over community transparency, **raising serious questions** about the independence of cybersecurity discourse in corporate-sponsored environments.

Initial Engagement with CyberSci Canada

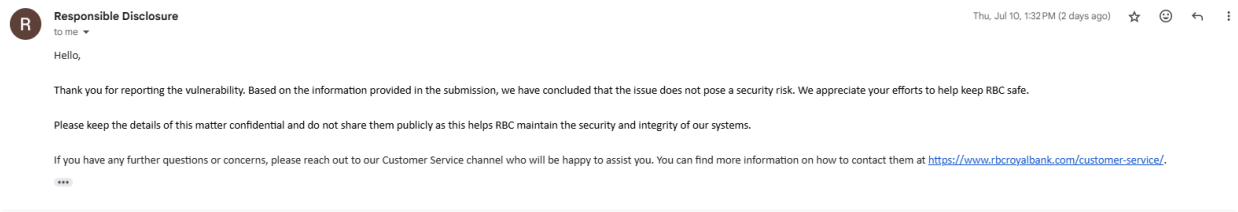
For accurate documentation purposes, I established first contact with CyberSci on March 7, 2025, reaching out to team member **Dmitriy Beryoza** to inquire about volunteer CTF design opportunities for their upcoming events. While the initial response indicated they did not require additional support at that time, Mr. Beryoza contacted me again on May 27, 2025, requesting my assistance in developing a challenge for their competition, which I agreed to provide.

It should be noted that Mr. Beryoza appears to have had no involvement in the subsequent incident documented in this analysis, and therefore detailed communications with him are not relevant to this case study.

Security Disclosure Analysis: RBC's Contradictory Response

On June 18, 2025, I identified and reported a security issue to **Royal Bank of Canada** through their **responsible disclosure** process. Following their standard review protocol, RBC requested verification after five days, which I provided. Their security team subsequently classified my finding as "**intended behavior**" rather than a vulnerability.

Screenshot:



However, despite this classification as intentional functionality, **RBC explicitly requested that I refrain from public disclosure of the technical details**. This presents a logical inconsistency: if the behavior is genuinely intended and represents legitimate functionality, there should be no objection to transparent discussion that could benefit their **17 million customers'** security awareness.

As a practitioner committed to responsible disclosure standards, I am honoring their non-disclosure request for the industry-standard 90-day period, with public documentation scheduled for September 18, 2025. My established track record in vulnerability disclosure includes successful publications involving multiple vendors such as Apache, OpenCart, Typo3 and Zencart.

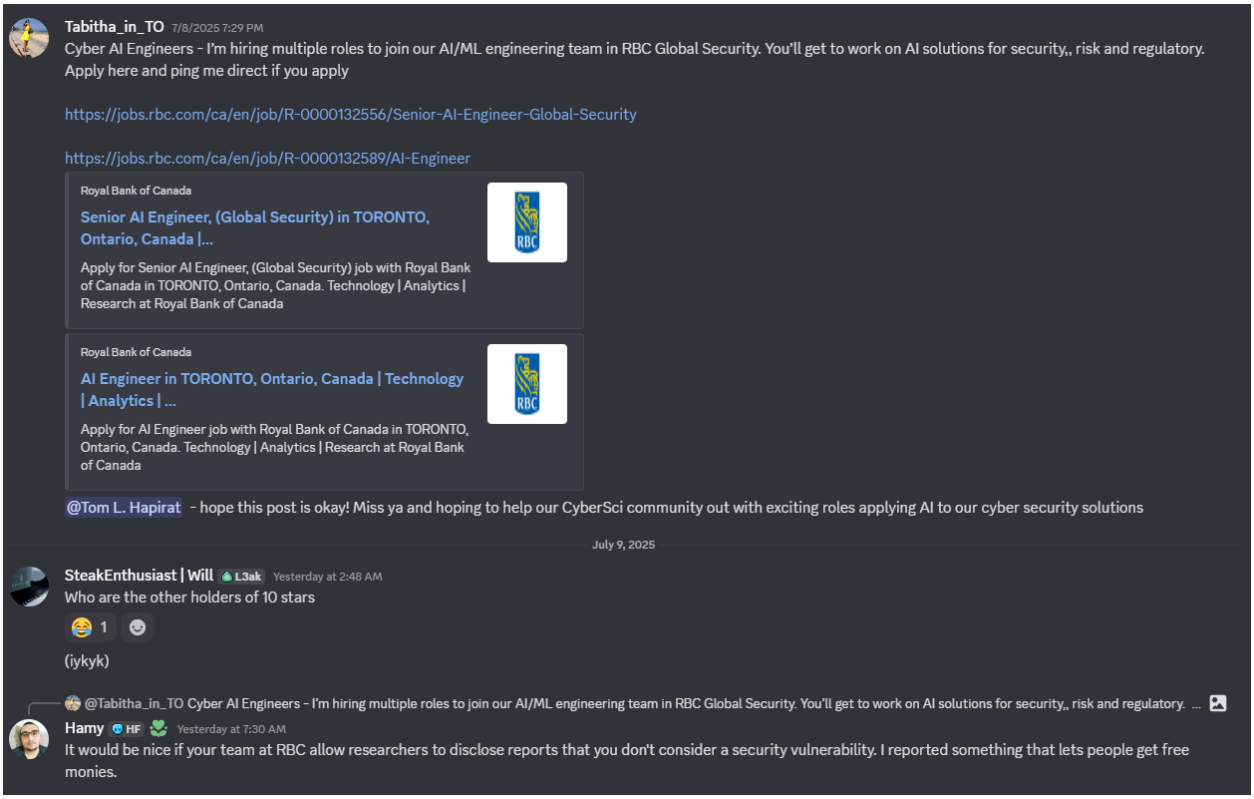
These disclosures, documented on my research blog, demonstrate a consistent pattern of methodical, evidence-based security research. The volume of vulnerabilities disclosed on **May 24, 2025,** alone, provides clear evidence of my commitment to advancing cybersecurity through responsible disclosure practices.

The contradiction inherent in RBC's position such classifying behavior as "**intended**" while simultaneously restricting discussion of this "feature" raises important questions about transparency in financial sector security practices.

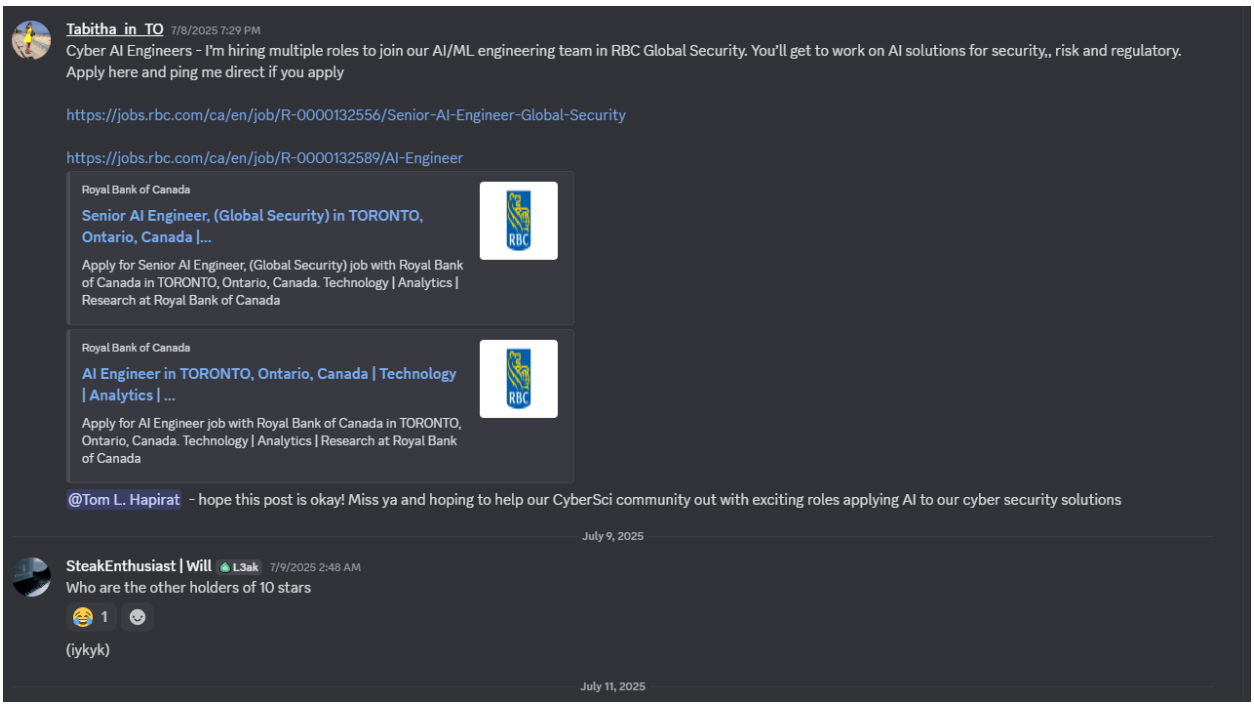
Timeline documentation

Following RBC's response to my security disclosure, I observed recruitment activity within the **CyberSci Discord server** where RBC representatives were posting AI Engineer positions. Given the context of my recent interaction with RBC's security assessment process, I felt it appropriate to share my experience regarding their vulnerability disclosure practices for the benefit of community members who might be considering these opportunities.

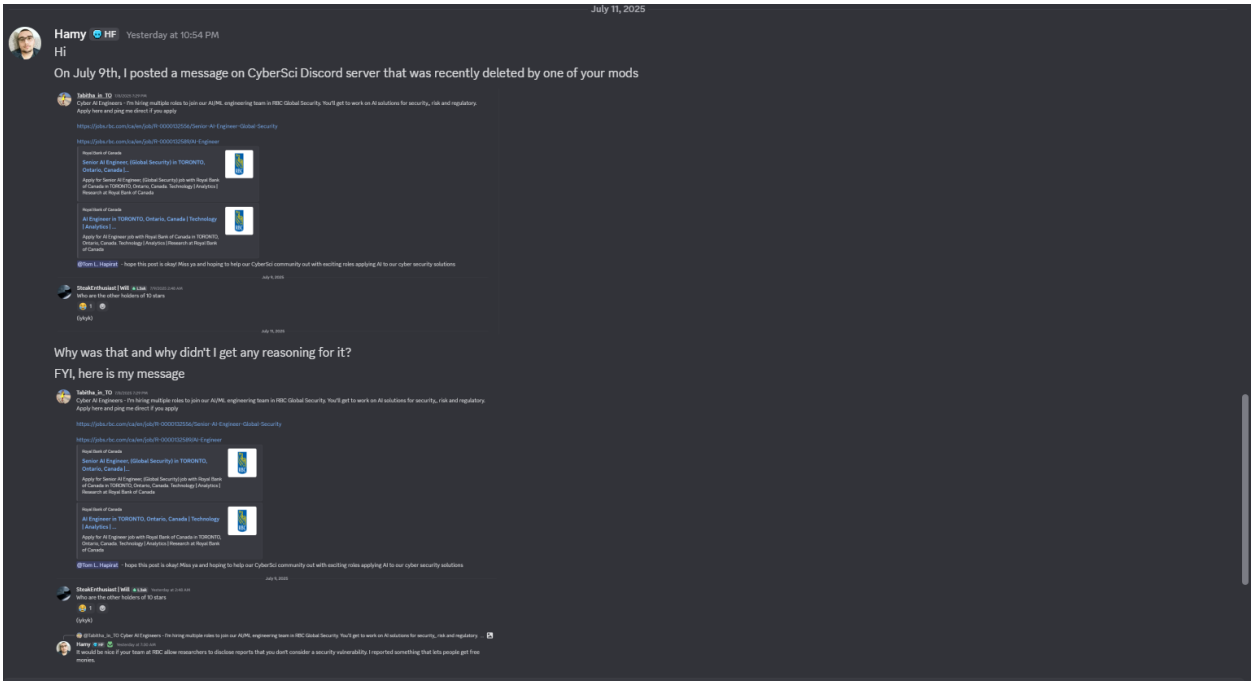
I posted the following message in the CyberSci Discord server expressing concerns about RBC's disclosure handling, posted on **July 9th 2025**:



Upon checking the Discord channel on **July 11, 2025**, at approximately **11:00 PM**, I discovered that my message had been removed without notification:



Following the message deletion, I sent a private inquiry to CyberSci leadership (Tom Levasseur) on **July 11, 2025**, requesting clarification regarding the removal:



This was also sent by me as a follow-up shortly after:

The optics don't look very good, the RBC did ask me multiple times not to disclose an "intended issue" and then I was silenced in your Discord server when I mentioned the same thing. This could mean that whoever deleted my message either didn't know about my contributions to your nationals CTF or didn't care.

When I eventually disclose this vulnerability after 90 days, I will mention how this was handled on HackFest vs CyberSci, the HackFest team didn't delete my message, they helped me understand the situation better through constructive dialogue.

I received the following reply from Tom Levasseur on **July 12th 2025** at around **1:30 AM**:

First I've heard of this. Glad the Hackfest team explained the problem to you. After your help at Nationals, you should have been contacted directly by whoever deleted your post. But no one on our organizing team would ever, ever use the CyberSci server to get into a back-and-forth with one of our sponsors. We all know that would be a horrible thing to do. So they must have thought you were just some immature student.

What surprised me - a lot - about your message here is your last paragraph. You've decided to publicly criticize our program over this incident. This CyberSci vs Hackfest thing feels like either a threat or retaliation. That's some serious escalation right there. I like communication too but , as you said yourself, it needs to be constructive.

When I referenced my intention to document the contrast in organizational responses, the founder characterized this as **'either a threat or retaliation'** and **'serious escalation'**.

On **July 12th 2025**, I sent the following message to Tom and didn't get any further responses:

My contributions is listed on this document posted by one of your organizers:

https://github.com/CyberSCI/PastChallenges/tree/main/challenges/nationals-2024-25

Additionally, I had also posted a message on Discord with writeup of my challenge so I find it hard to believe that someone mistook me for some "immature student".

Your organization probably lacks proper contributor recognition mechanisms or they disregarded my contribution due to potential bias. My message didn't break any listed rules, there are no rules on your server that says "Don't criticize our sponsors".

The fact that you think it's acceptable to delete messages from "immature students" without explanation shows that there may be "respect tiers" or

respect based on someone's status which is pretty dehumanizing in itself. Everyone should be treated equal.

My focus is on equal treatment of all, whether you are some “immature primary school student” or the Prime Minister, you deserve the same equal treatment without prejudice based on perceived status.

The Pattern Recognition Framework

The communication sequence from CyberSci leadership exhibits a recognizable pattern commonly observed when organizations face accountability requests. This framework, well-documented in organizational psychology literature, typically manifests through four distinct phases:

1. Initial Deflection The response "*First I've heard of this*" serves to distance leadership from the incident, suggesting either inadequate organizational oversight or deliberate plausible deniability.

2. Responsibility Displacement Language such as "*whoever deleted*" and "*they must have thought*" systematically shifts responsibility to unnamed individuals or processes.

3. Victim Reversal The characterization of legitimate documentation requests as "*threats*" or "*retaliation*" represents a classic reversal technique where the party seeking accountability becomes framed as the aggressor.

4. Communication Policing Statements about communication needing to be "*constructive*" establish arbitrary standards for acceptable discourse, typically used to dismiss criticism that doesn't conform to organizational preferences.

The Logical Contradiction Highlight

The founder stated that “**no one on our organizing team would ever use the CyberSci server to get into a back-and-forth with one of our sponsors**”, an acknowledgment that sponsor criticism is systematically avoided, while simultaneously claiming the deletion was due to mistaking an established contributor for “**some immature student.”**

Casual Dehumanization

The fact that Tom thinks it's acceptable to delete messages from "**immature students**" without explanation shows their community values. They have different **tiers of respect** based on **who they think you are**, rather than **treating all community members with basic courtesy**.

Why am I posting this now?

I've deliberately waited several weeks before addressing this incident publicly, believing professional **disagreements should be resolved through direct dialogue**. This measured approach reflects my standard practice, as demonstrated in my previous "Contao CVE Fraud" analysis, **where I similarly allowed substantial time for private resolution**.

Throughout this period, I remained available for constructive dialogue with CyberSci leadership. Unfortunately, despite my continued willingness to engage, **no such outreach occurred**.

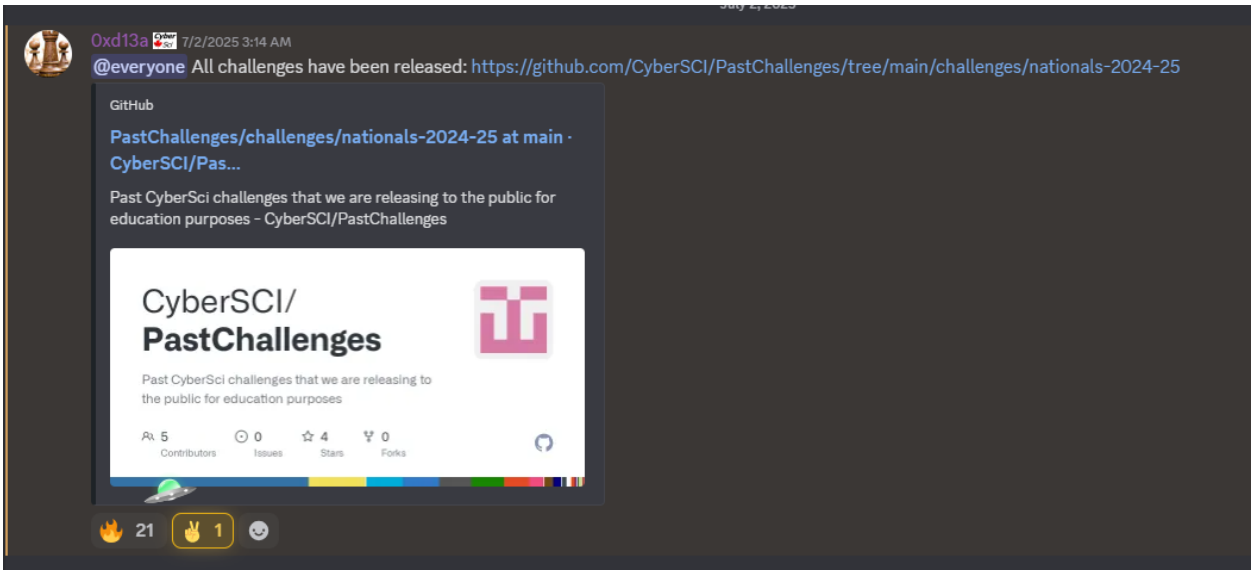
After careful consideration and consultation with community colleagues, I've concluded that documenting this experience **serves the broader cybersecurity community's** interest in understanding organizational accountability practices. Having **formally disengaged from CyberSci's** platforms, I can now provide this analysis from a position of complete **professional detachment**.

Contributor Recognition Analysis: Documented Evidence

The explanation provided by CyberSci leadership regarding moderation staff's unfamiliarity with established contributors **warrants examination** against available documentation. **Tom Levasseur's** assertion that moderators mistook an established contributor for "**some immature student**" raises questions about organizational knowledge management systems.

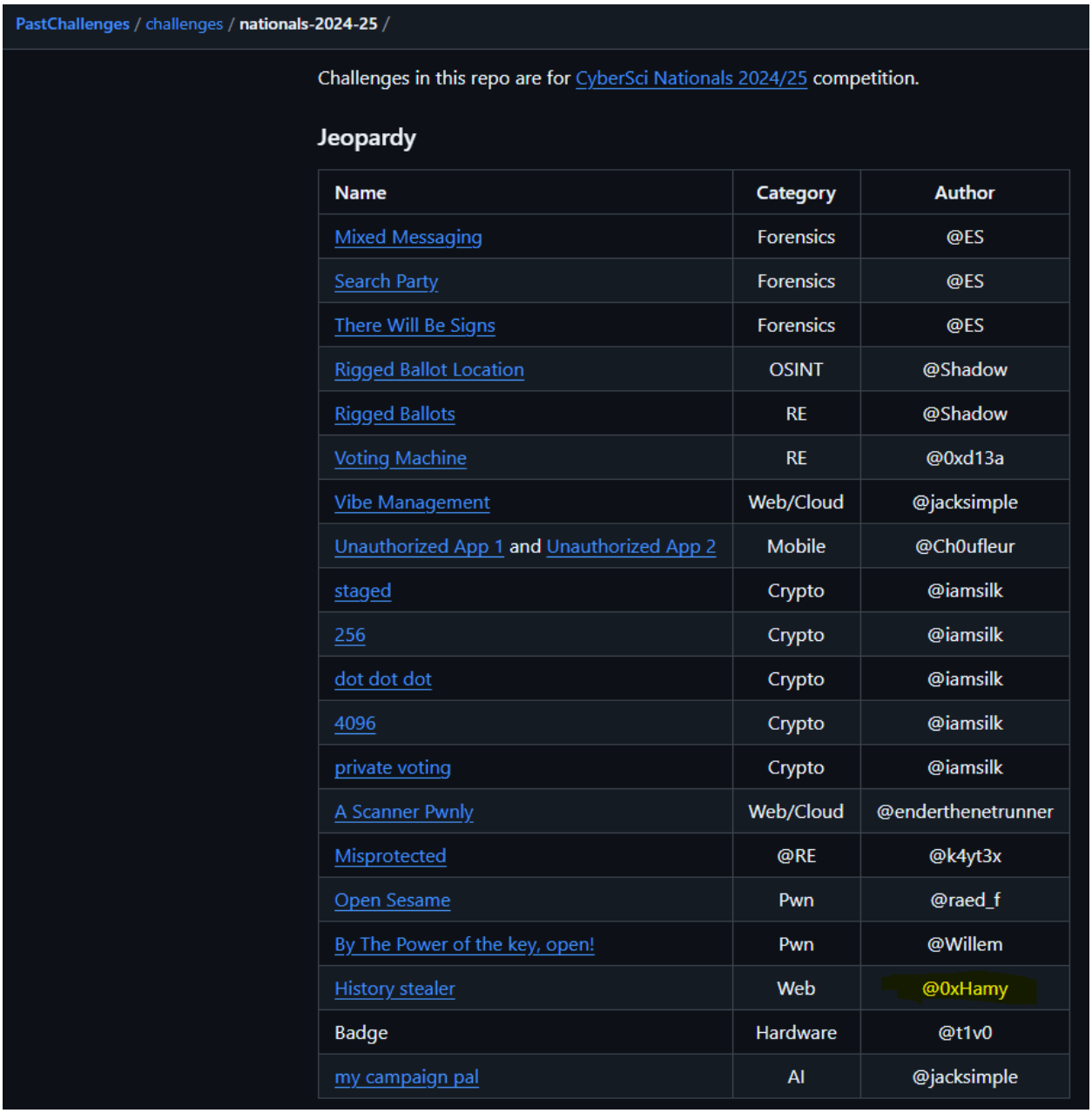
Public Acknowledgment Documentation

On **July 2, 2025**, CyberSci published the following announcement recognizing CTF contributors:



The [GitHub documentation clearly displays my name] among the recognized contributors, indicating formal organizational acknowledgment of my participation and

contributions to their competition:



PastChallenges / challenges / nationals-2024-25 /

Challenges in this repo are for CyberSci Nationals 2024/25 competition.

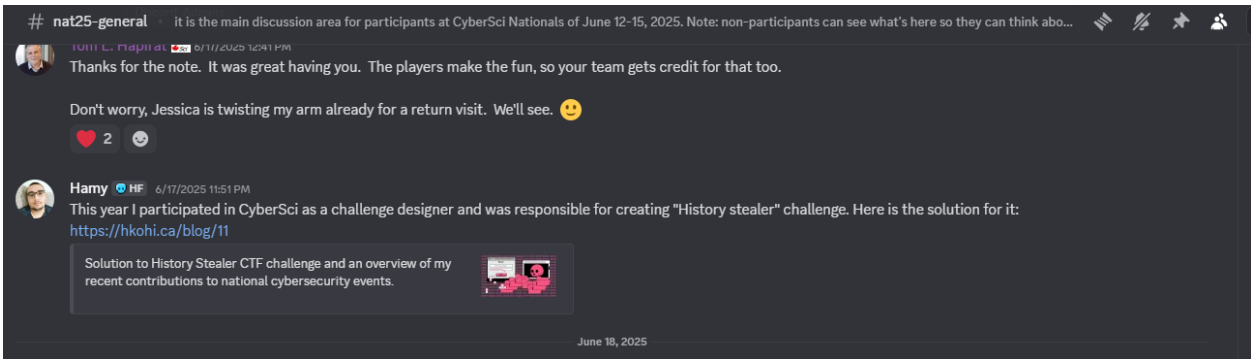
Jeopardy

Name	Category	Author
Mixed Messaging	Forensics	@ES
Search Party	Forensics	@ES
There Will Be Signs	Forensics	@ES
Rigged Ballot Location	OSINT	@Shadow
Rigged Ballots	RE	@Shadow
Voting Machine	RE	@0xd13a
Vibe Management	Web/Cloud	@jacksimple
Unauthorized App 1 and Unauthorized App 2	Mobile	@Ch0ufleur
staged	Crypto	@iamsilk
256	Crypto	@iamsilk
dot dot dot	Crypto	@iamsilk
4096	Crypto	@iamsilk
private voting	Crypto	@iamsilk
A Scanner Pwnly	Web/Cloud	@enderthenetrunner
Misprotected	@RE	@k4yt3x
Open Sesame	Pwn	@raed_f
By The Power of the key, open!	Pwn	@Willem
History stealer	Web	@0xHamy
Badge	Hardware	@t1v0
my campaign pal	AI	@jacksimple

My name on Discord is “Hamy”, my username on Discord is “0xHamy”. It’s difficult to mistake me for someone else **unless you lack critical thinking** while making decisions.

Community Engagement Evidence

Additional evidence of my established presence within the CyberSci community includes technical content sharing, such as the "**History Stealer**" challenge writeup posted directly in their Discord server:



Organizational Knowledge Management Analysis

The existence of comprehensive public documentation acknowledging my contributions, combined with active community participation, suggests that moderation staff either:

1. Lack access to contributor recognition systems
2. Do not consult available documentation before taking moderation actions
3. Operate without established protocols for identifying community contributors

This documentation indicates a disconnect between organizational **rhetoric about valuing contributors** and operational practices for recognizing and protecting those same contributors during community interactions.

Conclusion: Canada’s security posture

If CyberSci's approach to handling a simple question about vulnerability disclosure is to delete messages and **gaslight contributors**, what does that say about the cybersecurity mindset they're cultivating in the people who will end up protecting **Canada's most sensitive systems**?

Here's an organization that supposedly trains the next generation of cybersecurity professionals, yet their response to transparency and accountability is immediate **censorship** followed by **defensive deflection**.

The fact that RCMP, CSIS, and CSE actively recruit from CyberSci means this broken mentality is being directly imported into Canada's **most critical security infrastructure**.

Now imagine that same mentality applied to someone working at CSE who discovers a critical vulnerability in government systems, or a CSIS analyst who identifies concerning patterns in sensitive data handling. Is the country’s national cyber talent pipeline compromised or corrupted by mega corporations? Your guess is as good as mine.

The vulnerability disclosure process is the foundation of responsible cybersecurity practice. If CyberSci's training environment teaches future professionals that questioning disclosure processes is unwelcome, we're creating a generation of cybersecurity workers who will stay quiet when they should be speaking up. These positions require moral courage to speak truth to power when systems are failing. But if the training ground teaches people that asking uncomfortable questions leads to censorship and retaliation, **we're systematically selecting for compliance over competence**.

Your healthcare data, financial records, and personal information are being protected by people who may have internalized the lesson that institutional harmony matters more than security transparency. **That should keep every Canadian awake at night**.