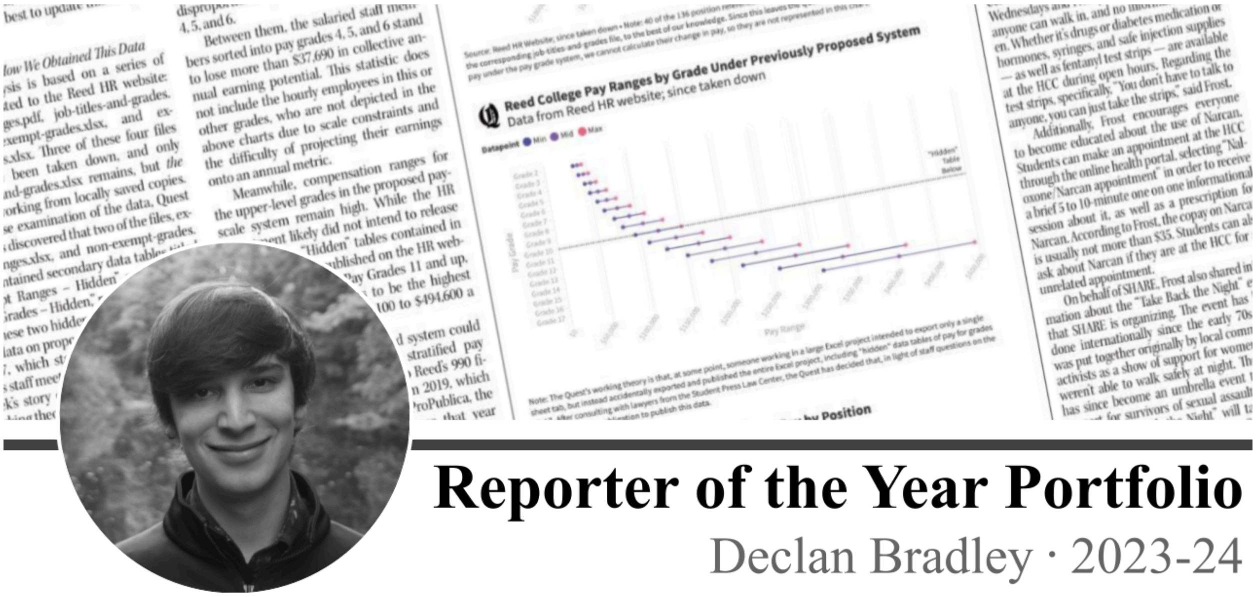


Reporter of the Year Portfolio

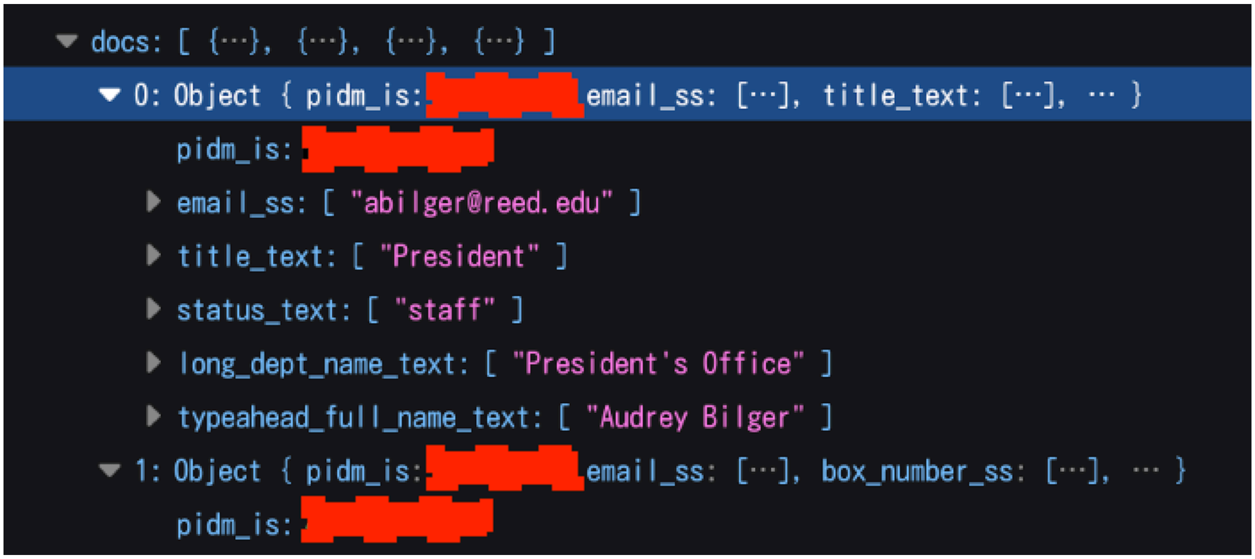
Declan Bradley · 2023-24

THE REED COLLEGE QUEST

Flaw in Campus Directory Exposes ID Numbers of Students, Staff, Faculty, Alumni

SEPTEMBER 28, 2023 / declanrjb.com/portfolio/systems_flaw/final.html

2nd Place National News Writing, Fall Clips and Clicks, Associated Collegiate Press



```
▼ docs: [ {…}, {…}, {…}, {…} ]
   ▼ 0: Object { pidm_is: [redacted] email_ss: […], title_text: […], … }
        pidm_is: [redacted]
      ▶ email_ss: [ "abilger@reed.edu" ]
      ▶ title_text: [ "President" ]
      ▶ status_text: [ "staff" ]
      ▶ long_dept_name_text: [ "President's Office" ]
      ▶ typeahead_full_name_text: [ "Audrey Bilger" ]
   ▼ 1: Object { pidm_is: [redacted] email_ss: […], box_number_ss: […], … }
        pidm_is: [redacted]
```

Editors' Note: The following story was scheduled to appear in print and online on Friday, September 29. On September 22, The Quest *alerted IT in good faith that the article would go to print the following week to give the department time to fix the massive security vulnerabilities detailed within. Forty minutes ago, IT sent* ***an email*** *to all Reed community members minimizing the seriousness of those vulnerabilities in a seeming attempt to get ahead of the* Quest's *coverage. The following is that coverage, as it will appear in print tomorrow. More coverage to follow live as we learn more.*

Read all of our most-updated coverage here.

Investigative reporting by the *Quest* confirmed that a vulnerability allowed any IRIS user and in some cases the general public, to access ID numbers and clone ID cards of any Reed community member.

After first being alerted to the existence of a critical vulnerability in the IRIS system by a student who wished to remain anonymous, *Quest* reporters were able to independently confirm that the college's "campus directory" — which is accessible to all students — had unintentionally exposed the Reed ID numbers of all students, staff, and faculty.

Furthermore, while the original vulnerability has now been closed, the *Quest* has reason to believe that one or more users retained locally saved copies of a spreadsheet that allows them to continue to obtain ID numbers for any user, leaving students, staff, and faculty continuously vulnerable to impersonation. Student sources have also asserted the existence of further vulnerabilities in the college's harassment reporting system which, while unconfirmed, potentially exposed ID numbers for alumni in addition to current students, staff, and faculty.

Investigative reporting by the *Quest* also confirmed that the properties of Reed College ID cards are based directly on the owner's ID number. Such magnetic swipe cards do little more than encode simple information — a line or two of text — on a physical object. In the case of Reed ID cards, that information seems to be a simple text file containing the user's ID number followed by their name. Combined with the ease of obtaining exposed ID numbers, this means that any user could clone the ID card of any other user using a simple magnetic read/write device — standard models of which connect to a laptop through USB and cost about $90 from Amazon.

Using such cloned ID cards, users could then spend board points, swipe through locked doors (including those meant to be closed to students), or otherwise impersonate the target to any automated system at Reed that identifies community members by their ID cards.

This raised concerns for some reporters about the security of the Reed Research Reactor, which the *Quest* was able to confirm uses swipe cards as at least one of its security steps. While Reactor Operators are forbidden to reveal the security protocols of the reactor control room, one student who underwent reactor training confirmed anonymously that there are "a few more steps" necessary to gain access to the reactor than simply presenting a standard swipe card, which means the reactor is at least somewhat secured against this vulnerability.

While the *Quest* only learned of the vulnerability during the first week of September, the anonymous source claimed it had been known by "multiple people in Reed CS [computer science]" since at least early 2023.

In an email to the *Quest*, Reed Cybersecurity Architect Payam Damghani confirmed that the college was first alerted to the issue by a student worker in IT in May 2023, which the *Quest* has independently confirmed. Despite this, the vulnerability remained open through the beginning of September 2023, four months later, and reporters did not observe a patch to the IRIS system until September 16 — eleven days after the IT department was contacted by the *Quest* on September 5.

The original source claimed that students had made "several" fruitless attempts to alert the college to the seriousness of the issue, although the *Quest* has been unable to confirm this beyond the original May report. The source said that they had chosen to come to the *Quest* with this information at least partially because "it seemed like the only way to get any of this fixed." "I know it had been brought up internally previously but nothing seemed to have been done about it," the source said, "it didn't seem like they would have any motivation to fix it without external pressure."

The *Quest* first formally alerted Mr. Damghani and Information and Security Officer Valerie Moreno to the existence of the vulnerability on the afternoon of September 5. When neither Mr. Damghani nor Ms. Moreno responded by noon on September 8, a *Quest* reporter, considering it an urgent issue, approached Director of Instructional Technology Services Trina Marmarelli — a professional in a different division of IT who is not involved in systems security — in her office. The *Quest* reporter asked if the IT department had received the alert. Ms. Marmarelli did not seem previously aware of the details of the case but promised to pass along the request. The *Quest* received a response from Mr. Damghani soon after.

Anonymous sources within IT say that, since that date, the existence of the vulnerability — and students' knowledge of it — has been kept secret even from many Reed IT professionals. At an all-staff meeting of IT on September 13, only a brief mention of IRIS maintenance was made, and the flaw was alluded to, “only in the vaguest possible terms.”

Director of Technology Infrastructure Services Gabe Leavitt, meanwhile, said in an email to the *Quest* on September 8 that he was not told of the paper’s attempt to notify the department until that afternoon, three days after it was originally sent.

The *Quest* was initially hesitant to publish information that would make the vulnerability easier to replicate, and on September 12 Mr. Damghani suggested that a 90-day embargo on the story would be “industry standard.” However, the shutdown of the IRIS system for “maintenance” between September 16 and 17 appeared to patch the most public-facing parts of the vulnerability, which sources from both within and without Reed IT have assured the *Quest* are no longer functional.

On the afternoon of September 22, a lawyer with the Student Press Law Center assured the *Quest* that coverage of the vulnerability would likely be protected, and that reporters may even have been “too responsible” in delaying their story to give the IT department time to fix the issue.

Prior to the patch, users were identified in the IRIS database by an 8-digit number known as a PIDM. Such PIDMs were stored openly in the URL strings for each user’s page — obtaining one was as simple as searching for that user, clicking on their name, and then copying their PIDM from the address bar in any browser. (URLs followed the format: “**https://iris.reed.edu/directory/campus/[PIDM**]”)

This was intentional. In an email to the *Quest*, Mr. Damghani said that PIDMs “were originally intended by Reed IT to be a publicly-visible unique user identifier specifically for use by web applications.”

However, students discovered that PIDMs were calculated by simply taking a user’s Reed ID number and adding a fixed constant. For example, if a student’s ID number was 20001000, their PIDM would be 20002000 (20001000 + 1000). While the actual fixed offset was not 1000, and the *Quest* will withhold the true value, the value seemed to be consistent across all Reed community members.

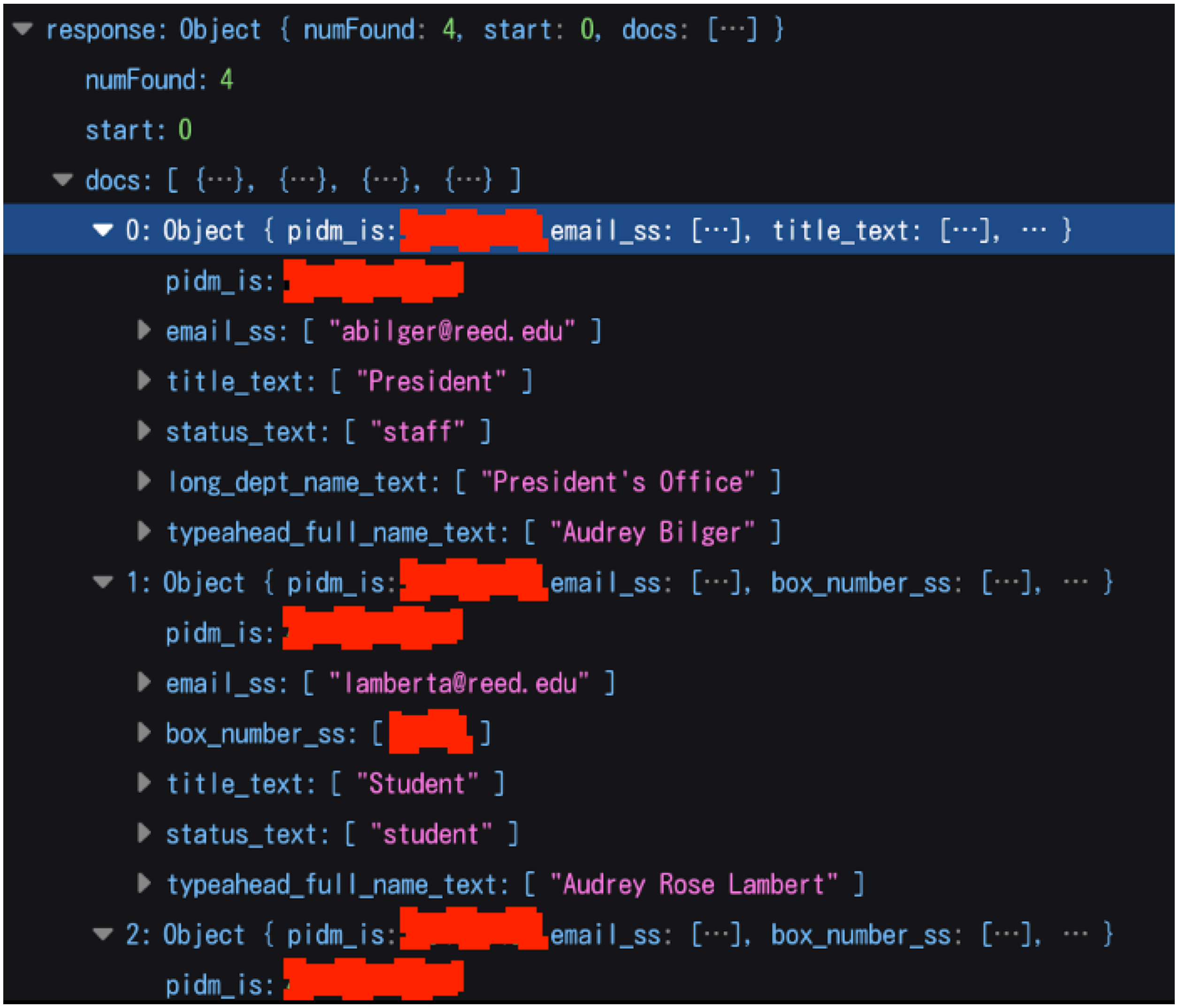
While reporters were careful not to access sensitive data themselves, the *Quest* was able to independently confirm that the fixed offset method correctly produced ID numbers to a high rate of accuracy across all students, staff, and faculty, something not even the original source had been able to confirm at scale. This meant that any student, after calculating the difference between their own ID number and PIDM with a simple phone calculator, could extrapolate the ID number of any other student, faculty, or staff member, up to and including the level of the president.

"Oh, yeah, I have Audrey Bilger's ID," said one student, casually, while speaking with a *Quest* reporter.

Even more significantly, further vulnerabilities in the autocomplete function of the IRIS database allowed any user to obtain a spreadsheet of all Reed community members containing each person's name, PIDM number, and position at the college (job title, status as a student, etc.)

For the more technical reader, the autocomplete function sent whatever input the user typed to a remote database containing all possible search results and then returned the matching rows. However, the URL format of the search function allowed anyone with basic programming knowledge to simply send the star character (*) — which in computer science stands for "everything" — as an input. Any user could therefore simply request results matching "everything," and the system would promptly dispense the entire database as a pre-formatted JSON or CSV table.

Critically, these files of all PIDM data could then be easily downloaded by the user and saved to their computer. While this access has now been cut off, the *Quest* has been and will be, unable to confirm how many users accessed this data or currently retain local copies of it.



```
▼ response: Object { numFound: 4, start: 0, docs: […] }
     numFound: 4
     start: 0
   ▼ docs: [ {…}, {…}, {…}, {…} ]
     ▼ 0: Object { pidm_is: [redacted] email_ss: […], title_text: […], … }
         pidm_is: [redacted]
       ▶ email_ss: [ "abilger@reed.edu" ]
       ▶ title_text: [ "President" ]
       ▶ status_text: [ "staff" ]
       ▶ long_dept_name_text: [ "President's Office" ]
       ▶ typeahead_full_name_text: [ "Audrey Bilger" ]
     ▼ 1: Object { pidm_is: [redacted] email_ss: […], box_number_ss: […], … }
         pidm_is: [redacted]
       ▶ email_ss: [ "lamberta@reed.edu" ]
       ▶ box_number_ss: [ [redacted] ]
       ▶ title_text: [ "Student" ]
       ▶ status_text: [ "student" ]
       ▶ typeahead_full_name_text: [ "Audrey Rose Lambert" ]
     ▼ 2: Object { pidm_is: [redacted] email_ss: […], box_number_ss: […], … }
         pidm_is: [redacted]
```

A screenshot of the system dispensing identity data for college president Audrey Bilger and the three other people at Reed named Audrey, provided to the Quest by a student source. The PIDMs have been removed by the Quest to protect privacy but were easily accessible to the source and any other IRIS user.

The *Quest* contacted IT on September 25 to ask how many copies of the data were downloaded during the at least four months it was available, and if the department had any way to ascertain that number. Mr. Damghani responded, “We are investigating potential access to the affected systems. We currently do not have any conclusive information that would indicate widespread access to or abuse of the affected systems that would be a violation of the college’s Computer User Agreement.”

While the IRIS system appears to have been overhauled, student, staff, and faculty ID cards are physical, non-connected objects that can't be altered remotely. That means that the only way to completely protect Reed ID cards from the risk posed by the ID spreadsheet is to recall them and physically run each one through a read/write machine. This would also likely require the college to reset all student, staff, and faculty ID numbers to new — ideally random — values.

When the *Quest* asked IT if the college plans to carry out such a mass rewrite of ID cards, and when, Mr. Damghani repeated his exact words that the department does not "have any conclusive information" that would suggest "widespread access" to the system, and added that, "[IT is] working with our vendor to implement ISO codes for our card access system which would in turn address the issue of the unique identifier."

Meanwhile, since the overhaul was implemented over the weekend of the 16th, student sources have continued to test the vulnerabilities of the system. One, who would only speak on the condition of anonymity, claimed to have identified a further flaw in the college's harassment reporting form that simply printed the raw Reed ID numbers of all students, faculty, staff, *and alumni* — both making the step of converting between PIDMs and IDs unnecessary and raising the number of affected individuals into the thousands.

Critically, this flaw also bypassed the 'directory visibility' property, meaning that even community members who had opted out of the campus directory were still at risk. The *Quest* alerted IT to this new flaw on September 25, but will not print the details of the vulnerability, even though it had been fixed by the time the paper went to print on Wednesday night.

Further such flaws, which had not been fixed at the time of publication, continue to expose PIDM numbers of either students or Reed employees through at least three different avenues — all of which the *Quest* alerted IT to on the 25th. One of these also overrides the 'directory visibility' property.

While it is important to note that, since the September 16 update, these vulnerabilities only return ten rows of data at a time, there is nothing to stop users from simply making repeated requests until all of the data is eventually returned.

The *Quest* has not been able to independently confirm these vulnerabilities, but reporters have seen screenshots that seem to demonstrate their existence. If real, these gaps in security remained open after the weekend overhaul of IRIS — and there is no way for individual users to protect themselves or their information.

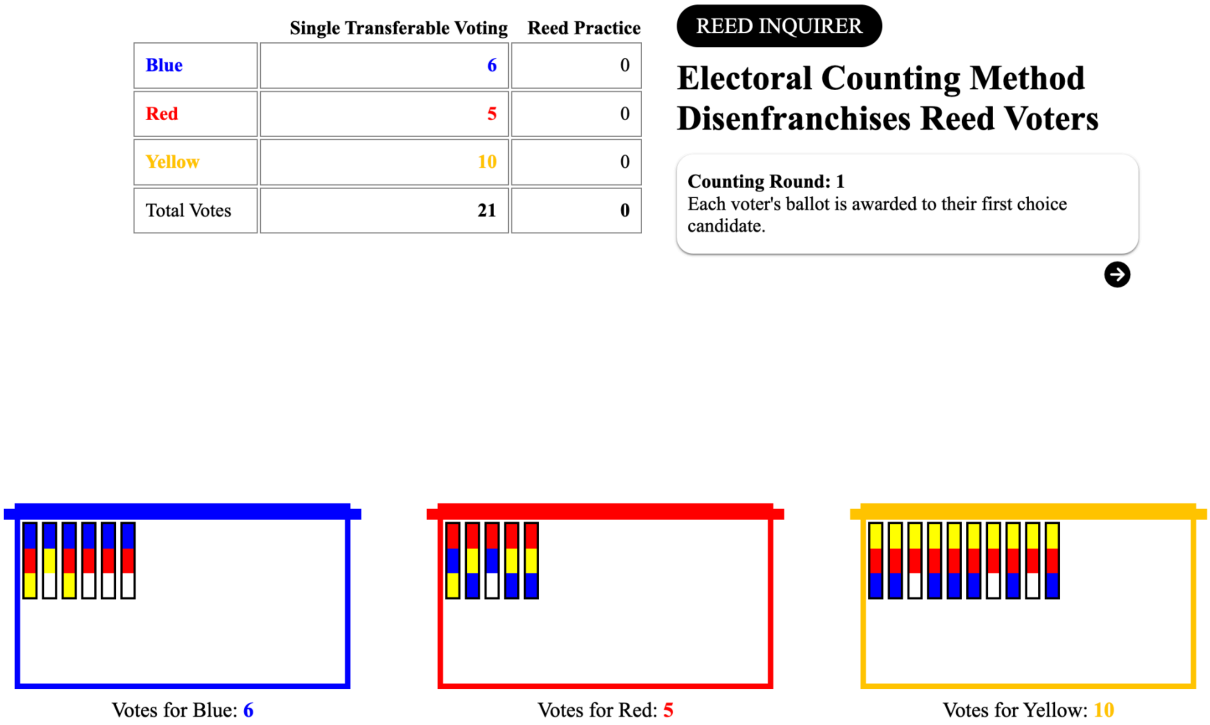
This is a developing story and the Quest *will continue to follow it in the coming hours.*

THE REED INQUIRER

Electoral Counting Method Disenfranchises Reed Voters

APRIL 24, 2024 / reedinquirer.org/ranked-choice.html

Prior Election Czars' decision to count votes according to their own method, rather than using the Single Transferable Voting method recommended by the Senate Elections Handbook, disenfranchised many student voters, an investigation by *The Inquirer* found.



	Single Transferable Voting	Reed Practice
Blue	**6**	0
Red	**5**	0
Yellow	**10**	0
Total Votes	**21**	**0**

REED INQUIRER

Electoral Counting Method Disenfranchises Reed Voters

Counting Round: 1
Each voter's ballot is awarded to their first choice candidate.

Votes for Blue: **6**

Votes for Red: **5**

Votes for Yellow: **10**

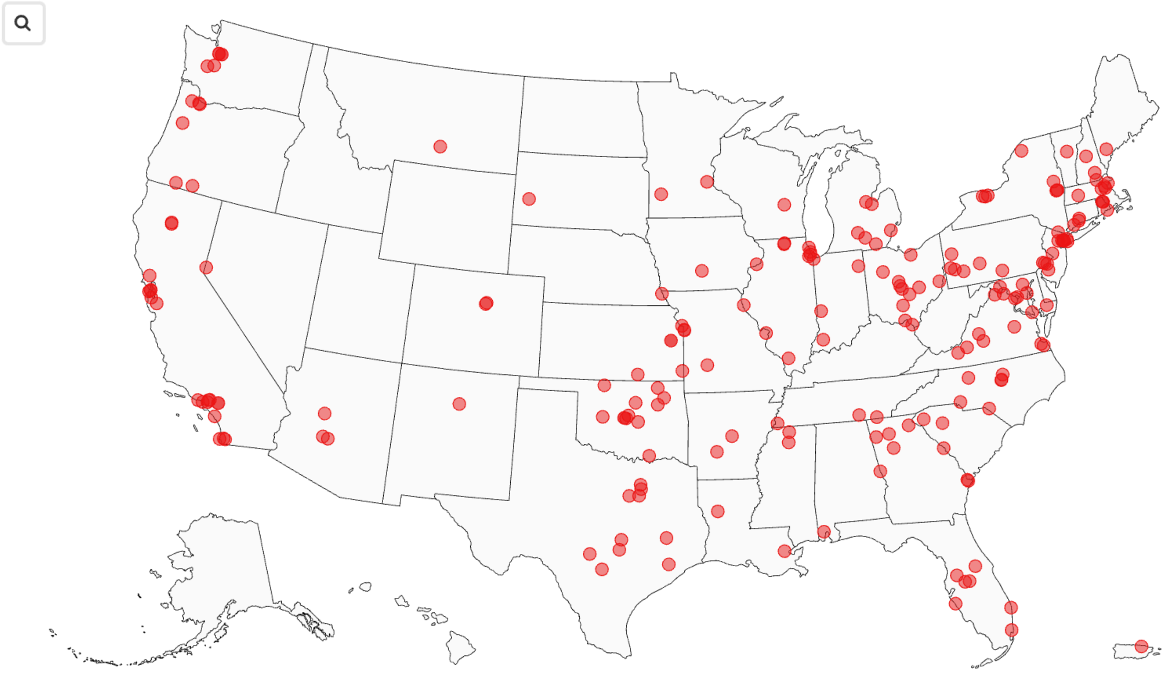
Read the interactive story online.

Note for judges: The entrant was responsible for both the writing and reporting of this in-depth feature story and the development, testing, and deployment of the HTML, CSS, and JavaScript code that governs its interactive structure.

THE REED INQUIRER

Non-Credible Bomb Threat Targeted Reed, 200+ Other Colleges, Data Shows

MARCH 21, 2024 / reedinquirer.org/#bomb-threat



Universities across the U.S. received the same non-credible threat email sent to Reed on Wednesday.

Reed's Office of Community Safety alerted campus early Wednesday, March 13, that the college had received an emailed threat of explosives and an accompanying shooting on campus. The threat was received by more than 200 institutions across the United States, and Director of Community Safety Gary Granger stated that "we have no reason to believe that Reed is specifically being targeted." Reed Community Safety alerted the Portland Police Bureau upon receiving the threat, and assured the Reed Community that the PPB was responding to the matter. At this time there have been no further developments to suggest that the threat was credible.

"The communication was distributed to more than 100 admissions offices across the United States, alerting them to the reported presence of four fertilizer-based explosive devices," Director

Granger wrote Wednesday, “two on campus premises (with one concealed underground), one within a vehicle, and another in possession of an unidentified individual. The identity of the person who disseminated this information remains unknown.”

The emailed threat, a copy of which Director Granger provided to reporters for the *Quest* and *The Inquirer*, was sent at 4:03 AM Wednesday to 301 email addresses associated with college admissions departments across the U.S. The message originated from a user identified as “AustralianHitler@dnmx.org.” Dnmx is an anonymity-focused email provider which, on its website, describes itself as “The Anonymous Email Service For The Dark Net.”

The threat message itself, a copy of which can be found here, read:

Four fertilizer-based explosives. Two around campus (one is buried), one
in my car, and one on me. As soon as I detonate the first three, it's guns
blazing. If law enforcement manages to trap me then the fourth one on me
goes kaboom. I'm hoping for a high kill count today!*

*Formatting preserved

In an email to reporters, Director Granger assessed the credibility of the threat as low, emphasizing the number of institutions targeted and the vague nature of the message. “Even in a high-risk environment (i.e., a place/organization that might be a high value target for a person or group), the vast majority of threats are simply that,” Director Granger wrote. “... Since this was sent to over 200 institutions, the credibility is pretty low. I don't believe we at Reed are at any increased risk.”

“However,” Director Granger continued, “in my 40+ years of dealing with bomb threats one [thing] has been true across time: one always responds as if the threat may be credible because not to do so invites a potentially avoidable disaster.”

By isolating the domain names hosting each targeted email address, *The Inquirer* was able to identify the websites of all institutions to receive the threat message. Reporters were then able to cross reference the targeted domains with the federal Integrated Post Secondary Education

Dataset (IPEDS) — a sprawling government database of U.S. colleges — identifying the names and street addresses of the institutions targeted, and by extension their latitudes and longitudes.

Overall, approximately 269 unique institutions in 48 U.S. states or territories received the threat message. Of these, 252 had domain names with exact matches in the IPEDs database. The remaining seventeen did not, however, indicating that those addresses were compiled and added to the target list from some reference list other than IPEDs.

Using Google Reverse search, reporters were able to identify that the seventeen unusual addresses appeared in a public file called colleges.txt, which contains a list of 1,717 colleges and their admissions email addresses. Of the 301 email addresses to receive the threat, 300 appear exactly in colleges.txt. Exactly one, the admissions email address for Robert Gordon University in Scotland, does not.

While *The Inquirer* has been unable to verify whether the colleges.txt source file was used to compile the list of targeted email addresses, it is hosted alongside an open source Python program, “sendmail.py,” which appears designed to help users solicit free t-shirts by sending mass emails to college admissions addresses. The program is hosted in a public GitHub repository titled “TikTokHacks,” which appears to have been created by the TikTok influencer @hoppuman, who uses the same username on both platforms.

A sample message provided alongside the Python program reads:

> Dear [CollegeName] Admissions,
>
> I am a TikToker named Hoppuman (430,000 followers). I'm working on a project where I promote schools and universities based on their college tshirts!
> If you would like your college promoted I would love to show it on my page (past episodes in this series have gotten 1M+ views).
> If you're willing could you please send your best school shirt to:
>
> [redacted]

> Thank you,
>
> James

The program also comes with a manual, "READ THIS FIRST.txt", which instructs users to "edit Messages.txt to change the message you want to send." The manual includes a disclaimer that "I am not responsible for all the mail you will get because of this."

Late Wednesday, a local Fox 65 station in Kentucky reported that nearby Asbury university had received an emailed threat of “multiple bombs on campuses and that there would be an active shooter threat.” The university, Fox reporter Madylin Goins wrote, “was one of 200 colleges and universities that received bomb and shooting threats on Wednesday.”

Asbury’s contact email address does not appear in the threat message received by Reed, but does appear in the TikTokHacks GitHub repository. *The Inquirer* reached out to Fox 65 with its findings in an attempt to confirm whether the threat message received by Asbury used the same language as the one received by Reed, and whether the 200 colleges referenced were distinct from those targeted in the same batch as Reed, but did not receive a response in time for publication.

The threats came the same day that the U.S. House of Representatives voted overwhelmingly in support of the so-called “TikTok ban,” a bill that would force Chinese parent company ByteDance to sell TikTok within six months or face a ban of the app on U.S. soil. The bill now faces a difficult road to approval in the Senate, per a New York Times assessment, but President Biden has said he would sign it into law if passed. The Biden administration has long argued that Chinese ownership of TikTok “poses grave national security risks to the United States, including the ability to meddle in elections,” but some lawmakers — and many TikTok users — have opposed the bill on free speech grounds. It was not immediately clear if there was any connection between the timing of the threats and the House vote.

This is a developing story, and *The Inquirer* will continue to follow it as more information becomes available.

THE REED COLLEGE QUEST

Silo Review: The Flamekeepers

AUGUST 23, 2023 / declanrjb.com/portfolio/silo/final.html

3rd Place National Opinion Writing, Fall Clips and Clicks, Associated Collegiate Press

In a particularly haunting scene of the Apple TV+ series *Silo*, a military interrogator makes his prisoner an offer. If she fails to cooperate, he'll lock her in a windowless concrete cell several miles beneath the Earth's surface, never to see the sun again. If she gives up the names of her allies, he'll do the exact same thing — but he'll keep her plied with a steady supply of painkillers. That way, she can let her remaining years slip away, lost in hallucinations of beachside sunsets she can never see with her own eyes. Because in the Silo, only in dreams can you ever be truly free.

Much has been written about *Silo* since it became a surprise hit late last year. *The Verge* called it "a small town mystery set at the end of the world." *The New York Times*, "a cautionary tale about tech." And it is all of those things and more. But it is also, in its bones, a horror story — one made all the more frightening by the lack of traditional jump scares or raging monsters. The show is frightening not because it's shocking, but because it's addictive — melding the sinewy grace of a whodunnit with the creeping sense of inevitable doom familiar to readers of Shakespeare or Homer.

Silo's is a world initially light on both details and explanation — as many characters will be eager to tell you throughout the series' premiere: "We do not know why we are here. We do not know who built the Silo." All they do know is that the hundred story concrete habitat they call home serves to protect them from the dangers of the outside world. The "windows" of the Silo, no matter where in the building they're found, all look out on the same view — a short stretch of blasted, poisoned ground culminating in a single dead tree at the top of a small hill. The perfectly preserved bodies of "cleaners" — political dissidents who made the fatal mistake of expressing a desire to leave the Silo — litter the hillside, their corpses left as a warning to future generations.

Dissident "cleaners" are exiled from the safety of the Silo with only a few minutes of oxygen in their suits and a single piece of wool with which to clean the habitat's exterior camera.

Yet for some residents of the Silo, that warning has never been enough to suppress a hunger for answers. Allison Becker (Rashida Jones), is a systems programmer and master hacker, one who harbors a growing suspicion that the Silo's "population control program" of enforced sterilization is not the beneficent system she has always been told. Meanwhile, her husband, Sheriff Holston

Becker (David Oyelowo), makes his living confiscating dangerous "relics" that pose a threat to order in the Silo, including, at one point, what appears to be a pez dispenser.

As questions pile up for the Beckers and for Mayor Jahn's, effective ruler of the Silo, some of them begin to question whether their self-contained world is really the safe haven it seems. Their search for answers will take them into the heart of the bizarre but undeniably enticing world of the Silo, a world where the retrofuturist aesthetic of *Loki* or *Brazil* becomes tinged with the gritty dystopian cynicism of *Snowpiercer* or *Blade Runner*.

Systems programmer Allison (Rashida Jones) searches for answers to the mysteries of her futuristic world from behind the screen of a bizarrely anachronistic Unix terminal.

By the time Rebecca Ferguson's protagonist Juliette Nichols makes her first appearance in episode three, most of these people will be dead. And therein lies what makes *Silo* such a remarkable piece of storytelling. It is not a story about people. It is a story about what consumes people. Whether it be love, or grief, or simply the aching desire to know, most of the series' characters are driven, inexorably, to fight the irresistible, to strive for the impossible, to reach for the sun and burn themselves up trying.

In some ways that trope — the indomitable truth seeker who refuses to give up in the face of impossible odds, the one person who sees clearly in a world of lies — has been far overused in genre fiction. It should not be innovative. It should not feel new. And yet, in *Silo*, it does.

Juliette (Rebecca Ferguson) and George (Ferdinand Kingsley) long for a sky they'll never see.

Partially, I think, that's because the series takes a cue from Philip K. Dick in its understanding that there is a very fine line between insight and madness. It's all well and good to cheer for characters who doubt reality in fiction — in fact, Hollywood has a long tradition of it — but in the real world, when someone says, "everything you know is a lie and the shadow government is out to get me," it's usually a sign that they need to seek help from a mental health professional. The fact that, in this particular case, the characters of *Silo* happen to be right is mostly a coincidence.

That's what makes *Silo* so darkly thrilling to watch. At some level, you know that the Silo is not such a terrible place to live. Sure, it's all a lie — the government is watching you and the whole thing is probably some kind of eugenics experiment — but as the cant of the Silo intones: "We only know that here is safe, and there is not." Generations of citizens have probably felt at least some suspicion that their history, the story of themselves, was a lie — yet they chose to live that lie, to laugh and cry and fall in love in an unreal world, rather than risk their lives for a truth that offered no guarantees of a better future. Yet, in every world, there are those that keep the flame. Those who, for better or worse, cannot tolerate a lie — even if it means facing great personal danger. The **ones who walk away from Omelas**.

In every world, there are those that keep the flame.

Silo is the story of those people. The ones who were told to accept life as it was given to them and screamed no. I want to go out. The ones who died for the truth, and for each other, without ever reaching their goal. So I say that while *Silo* is a cautionary tale, it's not about big tech. It's a warning about the terrible banality of lies, about the seductive quality of any simple narrative of good and evil, safe and unsafe — especially the ones peddled by those with the trappings of authority.

Silo is a reminder that none of us want to live in a world where we rely on the mad to speak the truth. For all of our sakes, I hope we take that warning seriously.

Declan Bradley

Student Journalist at Reed College

Writer, programmer, and aspiring data journalist, my work has been cited in *The Oregonian* and *The Hill*, and has appeared in *Nightingale Magazine* and been nationally recognized by the Associated Collegiate Press. See my portfolio at declanrjb.com.

EXPERIENCE

The Reed Inquirer — *Founder and Co-Editor*

MARCH 2024 - PRESENT

Co-founded a student publication specializing in data journalism and investigative reporting.

Automated Webscraper — *The Associated Press*

JANUARY 2024 - PRESENT

Worked with a team to scrape, fact check, and report results live on election nights. Was given personal responsibility to oversee results scraping for Los Angeles and Orange County California on Super Tuesday 2024.

Reed College Data Lab — *Data Science Student Specialist*

JANUARY 2023 - PRESENT

Worked on long-term data science projects for the college as well as assisting faculty and student researchers with hands-on data and statistics.

Reed Magazine — *Intern*

JANUARY 2024 - PRESENT

The Reed College Quest — *Editor*

DECEMBER 2022 - DECEMBER 2023

Held ultimate responsibility for all editorial decisions. Broke stories that led to institutional policy changes to protect student data, and won the publication's first Associated Collegiate Press awards in recent memory.

National College Media Conference, Associated Collegiate Press — *Speaker*

MARCH 2023

Gave talks on review writing, mobile app development in Swift, and webscraping with rvest and RSelenium.

Data Visualization Society Mentorship Program

JUNE 2023 — AUGUST 2023 | nightingaledvs.com/dvs-mentorship-data-journalism

Worked with Julia Wolfe, Americas Graphics Editor at Reuters and former Data Visualization Editor for FiveThirtyEight, on a project of my own design, which used web scraping and language processing techniques to visualize presidential rhetoric.

ReThink Media — *Data Science Intern*

MAY 2023 - JULY 2023

Was given wide-ranging independence and responsibility, developing new general-purpose R scripts for analysis and visualization of national poll data.

CONTACT

Email: declanrjb@gmail.com

Phone: 616-914-9525

SKILLS

R for Data Science (tidyverse)

Webscraping (Python, rvest, RSelenium)

Data Visualization (Flourish, ggplot2, Sigma.js, Tableau)

Web Development (CSS, HTML, JavaScript)

Programming (Python, C, C++)

Spanish (Working Proficiency)

AWARDS

2023 Multimedia Story of the Year, 1st Place Interactive Graphic, Associated Collegiate Press

2nd Place News Writing, ACP Fall 2023

3rd Place Opinion Writing, ACP, Fall 2023

Best of Show Diversity, Equity, and Inclusion Reporting, National College Media Conference Fall 2023

2nd Place Opinion Writing, ACP, Spring 2023

Best of Show News Website Design, National College Media Conference Spring 2023

Innovation Pacemaker Award, National Scholastic Press Association, 2022

2022 Honorary All-State Student Journalist Staff, Michigan Interscholastic Press Association

1st Place Review Writing, Michigan Interscholastic Press Association 2020-21 and 2021-22

National Merit Scholar, 2022

1st Place Opinion Writing, NSPA Fall 2021