PNNL-37642

Building Cybersecurity Educational Materials for Students

The Windfarm Capture-The-Flag Exercise

April 2025

Amy Pollom

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

**Available to DOE and DOE contractors from
the Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062
www.osti.gov
ph: (865) 576-8401
fox: (865) 576-5728
email: reports@osti.gov**

**Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov**

PNNL-37642

Building Cybersecurity Educational Materials for Students

The Windfarm Capture-The-Flag Exercise

April 2025

Amy Pollom

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Abstract

Securing and protecting critical infrastructure in an increasingly digital world is vital but it is all too often an afterthought. It is especially important that students become aware of internet safety and security at an early age. However, the availability of interactive and educational cybersecurity material targeted toward students is minimal in the United States. Here we show an example of interactive cyber security educational material that an educator can use in their classroom to encourage students to think about the interaction between real-world physical objects, cyber security, and information security. By putting together a “capture-the-flag” exercise, students can see in real time how hackers and cybercriminals exploit vulnerabilities and gain access information. The students try to “capture” the “flag” (i.e., information) in the wind farm by looking for oddities in the code or by taking advantage of weaknesses in everyday protocols. Students can also see how cybersecurity interacts with the power grid through the wind farm project scenario and how a hacker could cause serious problems to a critical infrastructure sector. Our goal for the project is getting students interested in cybersecurity and help them develop an awareness of how important having robust security systems is. We also hope that this project demonstrates the importance of introducing these concepts early and inspires others to create similar projects geared toward students.

Acknowledgments

This work was supported in part by the U.S. Department of Energy, Office of Science, Office of Workforce Development for Teachers and Scientists (WDTS) under the Science Undergraduate Laboratory Internship Program (SULI). Special thank you to David McKinnon, Nicole Castille Bentley, and Lisa Campbell for guidance and support.

Glossary

Arduino—An open-source electronics platform based on easy-to-use hardware and software. Arduino boards can read inputs and turn them into outputs (e.g., press a button to turn on a motor) (Arduino 2025).

Capture the flag (CTF) exercise—a term used in cybersecurity for exercises that challenge participants to exploit vulnerabilities and “capture” information. People can participate as individuals or on a team (Filipkowski 2025).

Flask—A lightweight Web Server Gateway Interface web application framework (Pallets 2025).

HTML—HyperText Markup Language is the basic scripting language used by web browsers to render pages on the World Wide Web (Hayes 2025).

JSON—JavaScript Object Notation is a text-based, human-readable data interchange format used to exchange data between web clients and web servers (Gillis 2025).

Micro:bit—The British Broadcasting Corporation (BBC) micro:bit is a pocket-sized computer that introduces users to how software and hardware work together. Contains a microcontroller, input and output devices, and an LED display (micro:bit 2025).

Python—An interpretative, interactive, object-oriented programming language (Python Software Foundation 2025).

Raspberry Pi—A very cheap computer that runs Linux while also providing a set of GPIO (general purpose input/output) pins, allowing you to control electronic components for physical computing and explore the Internet of Things (IoT) (Red Hat, Inc. 2025).

Web.Embedded C—A programming language that is used in the development of embedded systems (geeksforgeeks.org 2025).

Contents

Figures

1.0 Introduction

As daily life is increasingly conducted online, how to keep that personal data secure must be considered. In addition, students are introduced to technology at an increasingly younger age and they should be introduced to concepts for keeping themselves and their data safe. However, there is a dearth of educational material that teaches cybersecurity concepts to younger students. Our goal is to create an engaging project that teaches students appropriate cybersecurity concepts for different ages.

We built on and expanded a previous capture-the-flag (CTF) project, revamping the code and adding interactive elements to allow multiple students to participate at one time. CTFs are often held online and as competitions. One example is CyberForce, a competition for college students that is run by the Argonne National Lab (and other national labs such as Pacific Northwest National Laboratory) and sponsored by the Department of Energy. They can be ongoing events and tend to be geared toward college age and higher, such as the National Cyber League and HackTheBox. A few are geared toward a high school audience, such as PicoCTF. But few are geared towards younger students. We eventually plan to release this project online so that teachers can use this project in the classroom.

2.0 What is the Need for a Windfarm CTF?

Our CTF addresses an educational gap in available teaching aids and projects that can introduce cybersecurity concepts at an elementary to middle school level. The idea is that teachers can introduce age-appropriate concepts through this project to their classrooms.

First, a CTF “kit” is needed that teachers can easily and readily assemble and use in their classrooms. This kit allows students to dive deep into the project and build something that is known to work rather than creating a project from scratch with all the attendant problems that come with it. This is also a longer project, which is a good introduction to hands-on building and coding. The energy theme prompts students to think about the local power system ecosystems.

Second, the CTF is a hands-on demonstration model that facilitates in-depth interactions. The challenges range from easy to hard. It has a hands-on, visual, real-world component through the Windfarm board that students can see, hear, and touch. The turbines are mounted on servos that spin, and a student can turn a dial to speed the turbines up or down. Other students can “hack” the system by using micro:bits—by pressing a button, the student can tell one of the turbines to speed up or slow down out of sync with the other turbines. Students can navigate the website, clicking on links and searching for hidden information.

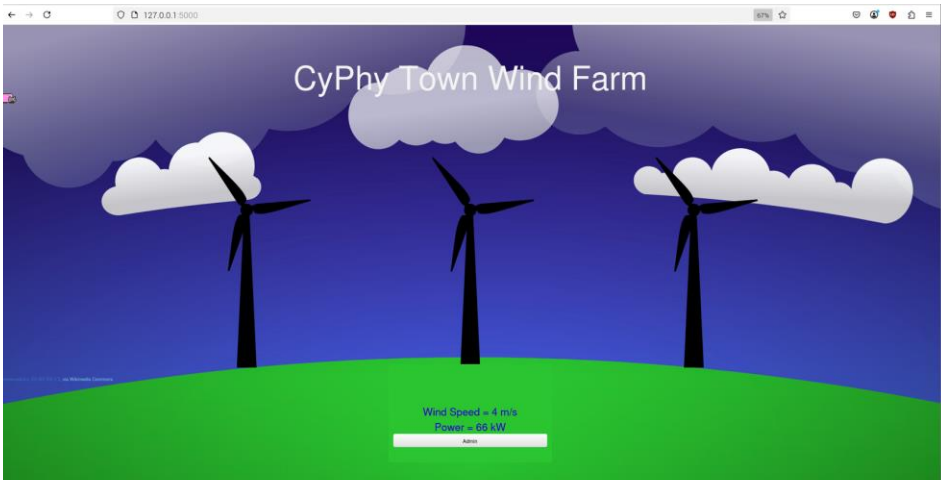
Third, the CTF can be used for quick interactions in science fairs and classrooms. It is an interactive, attention-grabbing project that can draw in a crowd. Once the audience is interested, the demonstration of “hacking” a system is quick and intuitive. It also can support more than one student at a time through the addition of multiple micro:bits to the demonstration. Students can spend as much or as little time with the project and will come away with new insights into cybersecurity and how it can be used to protect everyday and critical systems.

This CTF was created for STEM outreach activities such as the 2025 “Introduce a Girl to Engineering Day” as part of the national engineers week activities held at the Richland Public library. This event is an opportunity for girls to meet and interact with female engineers and learn more about careers in STEM. As mentioned above, the Windfarm CTF is a way for girls or any student to start thinking about cybersecurity and how they interact with technology on a day-to-day basis, as well as how cybersecurity is woven into the power grid. We intend to present this CTF at the similar events to see how students engage with the project.

3.0 What is Our Windfarm CTF Approach?

The Windfarm project was part of a series of projects created in 2017 by previous interns that focused on the power grid. During COVID, the challenge wasn't used so there were several years where the CTF was not updated. Then in 2025, the decision was made to update the Windfarm CTF. One goal of the update was to create a more interactive experience for students. The first order of business was making sure the code still ran when connected to the Windfarm board. Initially the code did not run at all, erroring out when connected. This was not unexpected given that five years had passed since the software was last updated. The Arduino code had to be updated from Embedded C version 5 to version 7—two full version levels. The backend Flask framework coded in Python was also updated. Updates to the JSON encoding enabled the ability to send encrypted messages to the Arduino. JSON messages are used to move commands and data between the Raspberry Pi computer and the Arduino microprocess board. CTF data includes wind speed data, if the turbines are on or off, and at what speed the turbines are spinning. The Arduino also sends information about the power "generated" in kilowatts from the wind farm. The wind speed and power generation data are passed to the Raspberry Pi front end where they are displayed on the main page of the Windfarm CTF website.

The second task was to update the CTF website to make it more visually interesting and interactive. The main web page now has a background image that displays a hill and sky for the wind farm turbines to be displayed on.



CyPhy Town Wind Farm

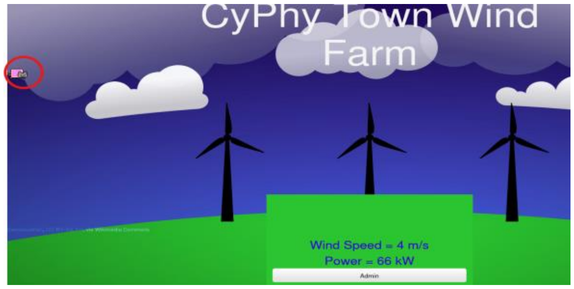
Wind Speed = 4 m/s

Power = 66 kW

Figure 1. Updated Main Page

Several user-interface changes were made to how the wind speed and power generated are displayed. There are also flags hidden in the main page that users can search for.

One of the challenges of creating CTF flags is making it just difficult and interesting enough for players to want to find them without being so difficult they get discouraged. One such flag is an image of the internet-famous rainbow "nyancat" (visible on the left of the screen shown in Figure 1 and circled in Figure 2), which when clicked leads the player to a hidden/secret page that the student "hacker" can use to "vandalize" the messages shown on the Windfarm board's 7-segment display modules.

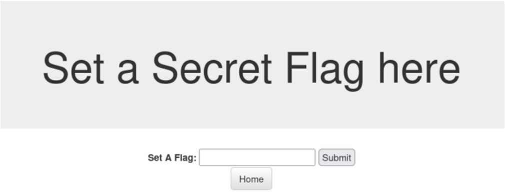


CyPhy Town Wind Farm

Wind Speed = 4 m/s

Power = 66 kW

Figure 2. Nyancat Icon

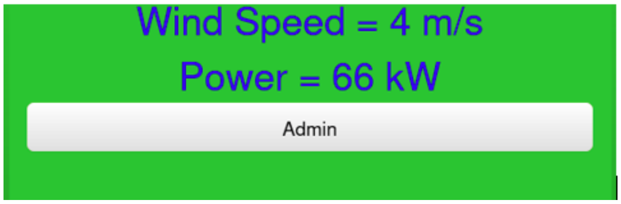


Set a Secret Flag here

Set A Flag:

Figure 3. Secret Flag Webpage

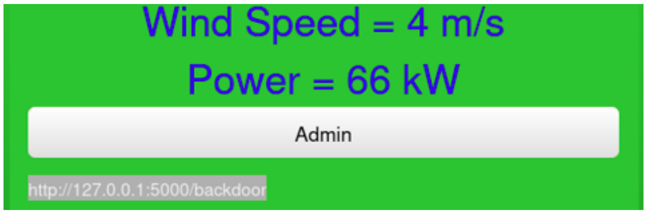
Another flag is hidden in the green grass of the hill—a link to a secret “backdoor” that allows players to access admin controls without a password.



Wind Speed = 4 m/s

Power = 66 kW

Figure 4. Green-On-Green-Text (Invisible)



Wind Speed = 4 m/s

Power = 66 kW

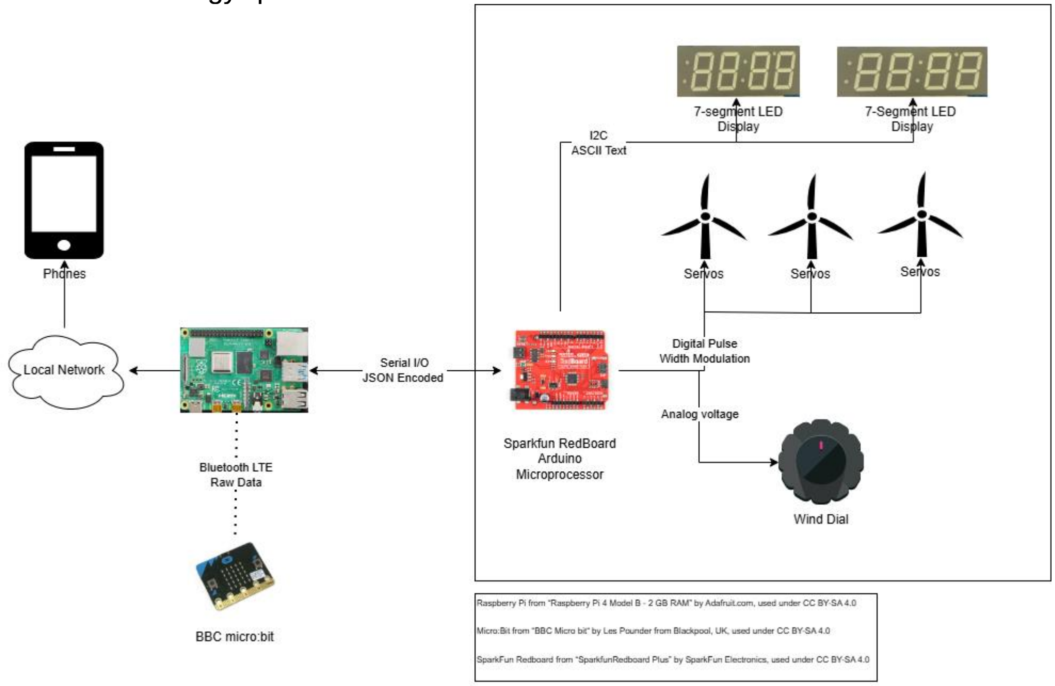
http://127.0.0.1:5000/backdoor

Figure 5. Green-On-Green-Text (Highlighted)

If a student decides to investigate the web page by looking at its elements in a web browser, they can find a secret message that prints to the console. If they click on one of the wind turbines displayed on the main page, that turbine will turn off on the board. The Windfarm board also has a hidden covert channel. When the Windfarm board is running, one of the colons on the 7-segment displays blinks on and off. The blinking is subtle, but nonetheless the blinking transmits a secret message in Morse code.

The micro:bits were added in 2025 so that more students could interact with the Windfarm board. But for the micro:bits to work with the Windfarm board, these small device had a way to communicate to the wind farm system. The Arduino board that is currently in use for our project does not support any sort of wireless protocol or Bluetooth. The Raspberry Pi, however, does have this functionality. While this is still a work in progress at the time of writing this paper, we have a plan for proceeding with this addition. We intend to set up the micro:bits to send a signal to the Raspberry Pi if one of the two buttons is pushed: if button A is pushed, the device will send a signal to the Pi to slow down, and to speed up if button B is pushed. The Pi will be listening for a signal, either through the Flask framework or via a separate program that will be run in conjunction with the Windfarm code. The signal will then be converted into a JSON message and sent to the Arduino as a command to speed up or slow down a turbine. Three micro:bits will be programmed and will correspond to one of the three turbines on the Windfarm board. Once completed, four students will be able to physically interact with the Windfarm board instead of just one.

Below is a diagram of the physical windfarm as well as the connections between the individual elements. The microprocessor speaks to other parts of the board with various methods: the LED displays use the Inter-Integrated Circuit (I2C)[1] protocol and receives ASCII[2] text from the microprocessor, the servos communicate via pulse width modulation[3], and the wind dial communicates via analog voltage. The microprocessor talks with the Raspberry Pi using a Serial[4] connection and with JSON encoded I/O. The micro:bits talk with the Raspberry Pi with the Bluetooth Low Energy[5] protocol.



Raspberry Pi from "Raspberry Pi 4 Model B - 2 GB RAM" by Adafruit.com, used under CC BY-SA 4.0

Micro:Bit from "BBC Micro bit" by Les Pounder from Blackpool, UK, used under CC BY-SA 4.0

SparkFun Redboard from "SparkfunRedboard Plus" by SparkFun Electronics, used under CC BY-SA 4.0

Figure 6. Logical Diagram of Windfarm Project

[1] I2C is a protocol that allows "peripheral" chips to communicate with "controller" chips (SFUptownMaker 2025)

[2] ASCII stands for American Standard Code for Information Interchange, and is a 7-bit code for standard characters (Injosoft AB 2025)

[3] PWM is a way of creating an analog signal from digital pulses (Liebold 2025)

[4] Serial communication is used between the Arduino board and a computer or other devices (Arduino 2025)

[5] BLE is a protocol designed for very low power operation which transmits data in the 2.4GHz unlicensed ISM frequency band (Bluetooth 2025).

In Figure 7 one can see an example physical layout of the Windfarm CTF components.

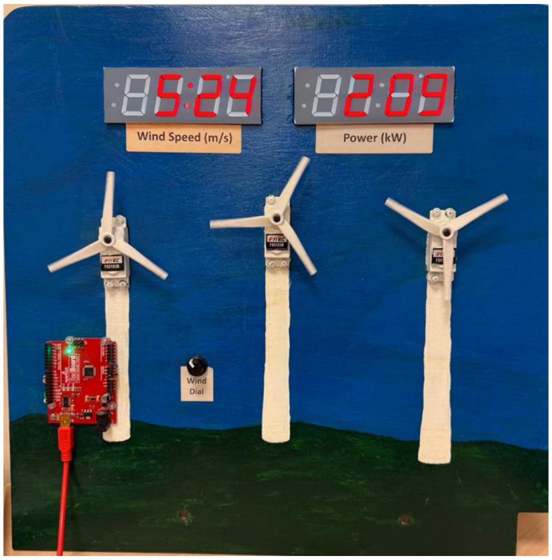


Figure 76. Windfarm Physical Board

Another task of this 2025 Windfarm CTF update was generating detailed notes for those who will come after us so they can edit and use this project. This report is an important first step in that process, as previous iterations of this project do not have a write-up to accompany the code. And finally, the updated code has been checked into the stash for future use.

4.0 What are the Benefits of a Windfarm CTF?

The main benefit of the CTF project is its ease of use for educators and students to assemble a hands-on, physical model with provided code. Whether it is a teacher putting this project together for a classroom or a student just starting their journey in cybersecurity and complex systems, our hope is that this project gets students thinking about cybersecurity in an interesting and interactive way.

What made this a good SULI internship project also would make it a great student project. Future students can also learn about using HTML to design user-friendly websites, and the process of creating and embedding flags for students to find. Students could also need to learn how to problem-solve hardware and software issues, as we did when we needed to replace the analog dial of the Windfarm parts because it stopped working. Students will need to understand how to will use the Bluetooth Low Energy Protocol to have the micro:bits communicate with the Raspberry Pi. For now, we have set up the micro:bits so that a user can control the speed of the turbine servos of the wind farm, but future students may have other ideas and concepts they will want to try out. The SULI interns working on this project over the years have had programming backgrounds, so future students can also learn programming while also exploring cybersecurity concepts and exploits. Our goal is that students will want to continue programming and also understand the importance of including security measures in their code—code that won't be "hacked" or exploited in the future.

5.0 Conclusion

Our goal was creating a CTF project that was geared toward younger students, would be engaging, and students can learn about concepts like web development and the different ways websites can be exploited. Additionally, the windfarm project is a good “maker” project that students can build in or out of a classroom setting, even if the focus isn’t on the cybersecurity aspects. Through updates and expansions to the initial code on the Raspberry Pi and the introduction of micro:bits, we have significantly updated an interesting project that can be used in the classroom and in other educational settings. Our future plan is to put the code online with a step-by-step guide for teachers to either assemble this project themselves or make it a classroom project for students. The code can be further developed if students and teachers would like to expand the project.

6.0 References

Arduino. 2025. *Serial.* April 9. https://docs.arduino.cc/language-reference/en/functions/communication/serial/.

—. 2025. *What is Arduino?* March 13. https://docs.arduino.cc/learn/starting-guide/whats-arduino/.

Bluetooth. 2025. *Bluetooth technology overview.* Accessed April 9, 2025. https://www.bluetooth.com/learn-about-bluetooth/tech-overview/.

Filipkowski, Ben. 2025. *Capture the Flag: What you should know about cybersecurity CTFs.* March 13. https://fieldeffect.com/blog/capture-the-flag-cybersecurity.

geeksforgeeks.org. 2025. *Embedded C.* March 13. https://www.geeksforgeeks.org/embedded-c/.

Gillis, Alexander S. 2025. *JSON (JavaScript Object Notation).* March 13. https://www.theserverside.com/definition/JSON-Javascript-Object-Notation.

Hayes, Adam. 2025. *HyperText Markup Language (HTML): What It Is and How It Works.* March 13. https://www.investopedia.com/terms/h/html.asp.

Injosoft AB. 2025. *ASCII Table.* April 9. https://www.ascii-code.com/.

Laserlicht. 2019. *Wikimedia Commons, CC BY-SA 4.0.* July 3. Accessed April 3, 2025. https://commons.wikimedia.org/w/index.php?curid=80140657.

Les Pounder from Blackpool, UK. 2016. *Wikimedia Commons - BBC Microbit, CC BY-SA 2.0.* February 22. Accessed April 3, 2025. Wikimedia Commons, CC BY-SA 4.0.

Liebold, Aaron. 2025. *Intro to Arduino: Pulse Width Modulation (PWM).* April 9. https://nightshade.net/knowledge-base/electronics-tutorials/arduino/intro-to-arduino-pulse-width-modulation-pwm-links/.

micro:bit. 2025. *What is a micro:bit?* March 13. https://support.microbit.org/support/solutions/articles/19000013983-what-is-a-micro-bit.

Pallets. 2025. *Flask.* March 13. https://flask.palletsprojects.com/en/stable/.

Python Software Foundation. 2025. *General Python FAQ.* March 13. https://docs.python.org/3/faq/general.html#what-is-python.

Red Hat, Inc. 2025. *What is a Raspberry Pi?* March 13. https://opensource.com/resources/raspberry-pi.

SFUptownMaker. 2025. *I2C.* April 9. https://learn.sparkfun.com/tutorials/i2c/all.

SparkFun Electronics. 2021. *Wikimedia Commons, CC BY 2.0.* June 22. Accessed April 3, 2025. https://commons.wikimedia.org/wiki/File:SparkFun_RedBoard_Plus_(51307373383).jpg.

**Pacific Northwest
National Laboratory**

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354

1-888-375-PNNL (7665)

www.pnnl.gov