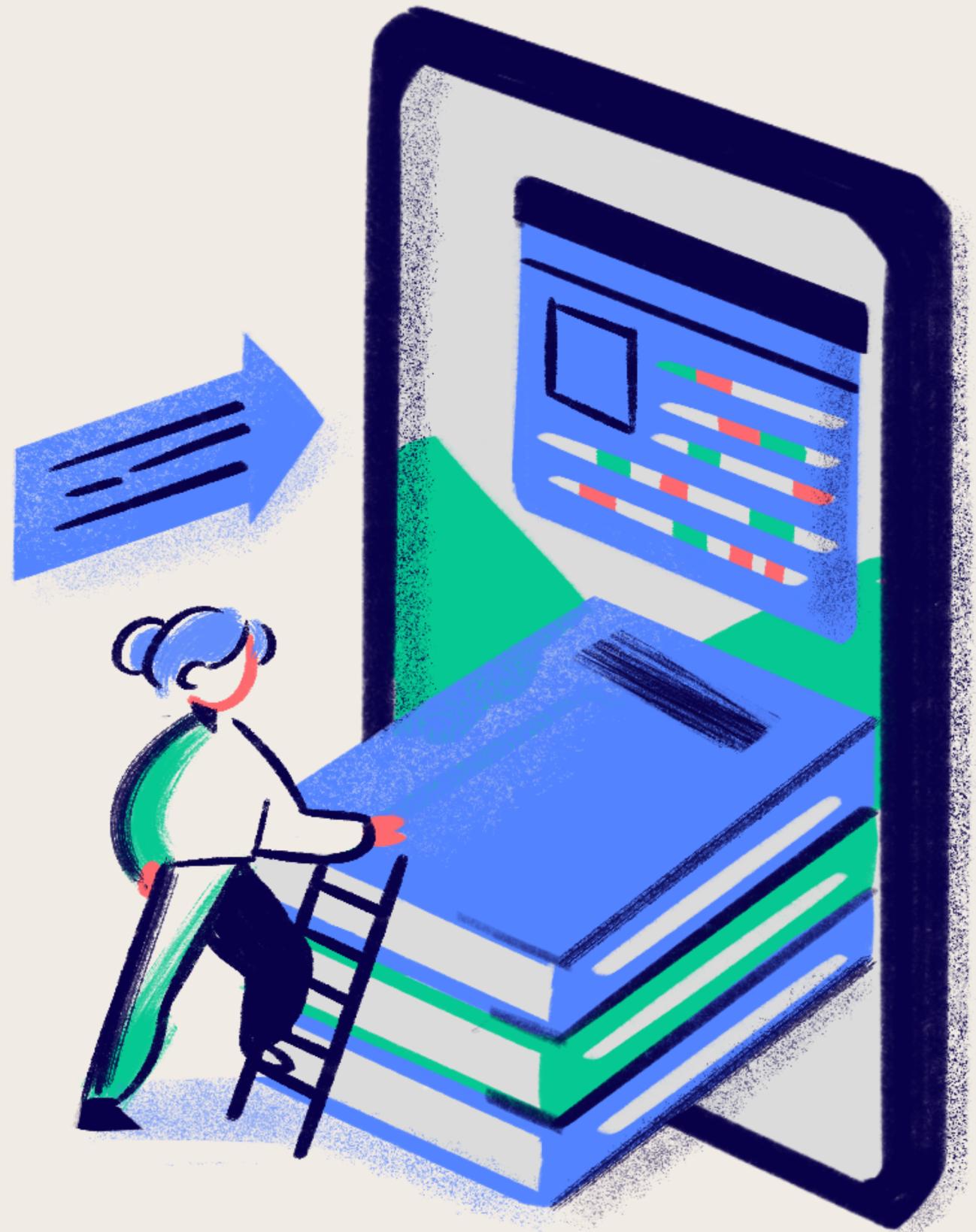


PRESENTED BY BAILEY WILLIAMS  
LONDON BSIDES 2024

# THREAT ANALYSIS IN MINUTES

AND OTHER AI SUPERPOWERS

[WWW.WHITERABBITNEO.COM](http://WWW.WHITERABBITNEO.COM)



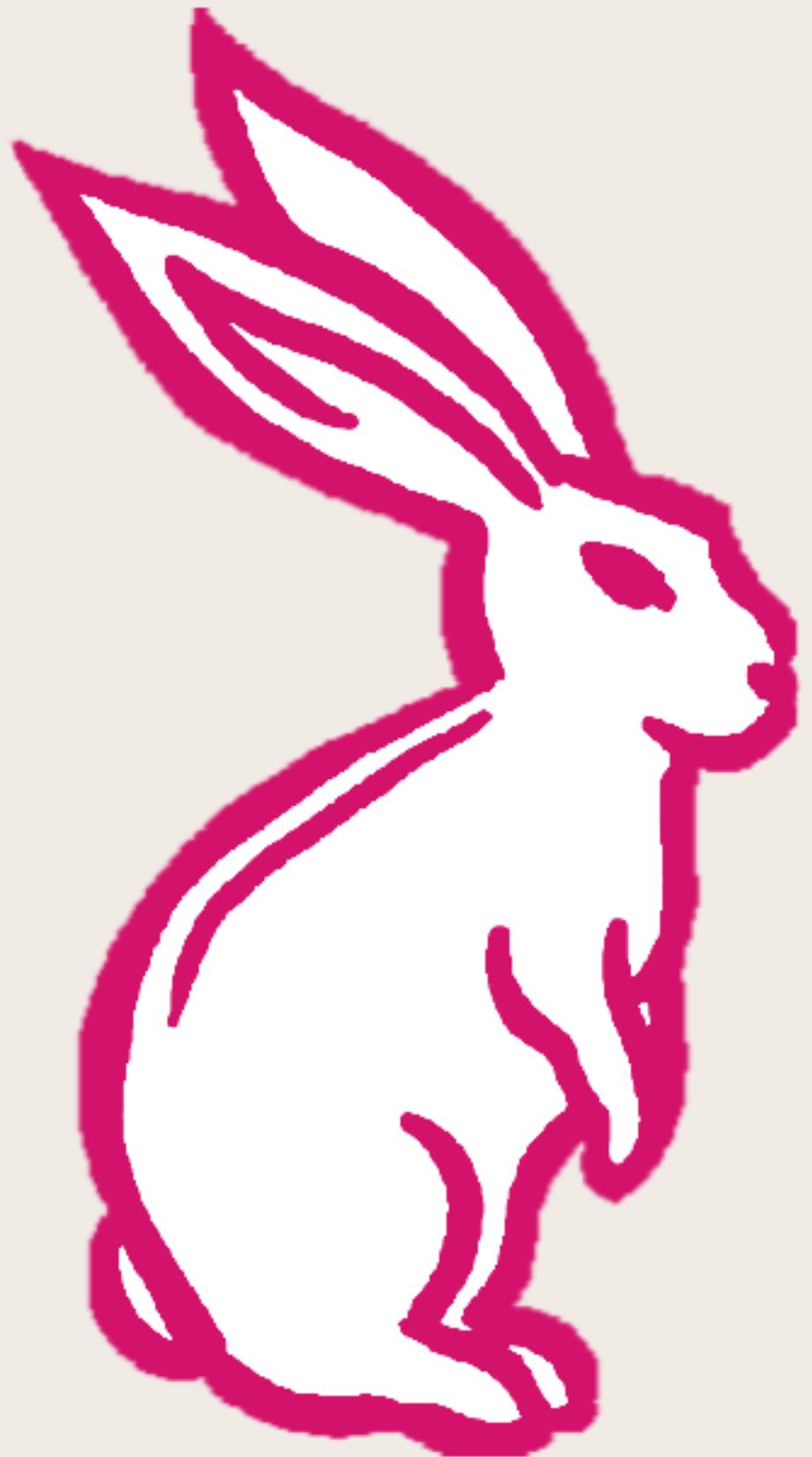
# ABOUT ME

- Bailey Williams
- Based out of Virginia, USA
- Cybersecurity and Political Science at Old Dominion University, Norfolk Virginia
- After graduation, I hope to help develop policies to reduce human susceptibility to social engineering attacks



# WHAT IS WHITERABBITNEO

- Uncensored, open-source AI model
- Uses the best current software engineering LLM as the foundational model, which is then trained on red-team and cybersecurity data
- WhiteRabbitNeo is and will always be free open-source and community-driven
- Promotes human-in-the-loop AI usage



# WHY IS WHITERABBITNEO IMPORTANT?

- Allows red and blue teams to stay up-to-date on the latest trends in cybersecurity
- Reduces tedium in cybersecurity by doing time-intensive research, allowing cybersecurity professionals to focus on crafting attacks
- Teaching tool for beginner security professionals.

The screenshot shows a KINDO application window. On the left, there's a code editor with a file named 'sec.py' containing the following SQLite database creation script:

```
import sqlite3

# Create a connection to the database
conn = sqlite3.connect("users.db")
cursor = conn.cursor()

# Create a users table if it doesn't exist
cursor.execute(
    """
    CREATE TABLE IF NOT EXISTS users (
        id INTEGER PRIMARY KEY,
        username TEXT,
        password TEXT
    )
    """
)
```

On the right, there's a panel with the title 'KINDO'. It contains a question: 'Are there any security issues with this code?'. Below the question, a message states: 'The provided Python script includes several vulnerabilities that could lead to security breaches if not addressed properly. Here are some critical points to consider:'. A numbered list follows, with the first item being: '1. SQL Injection Vulnerability: The user input is directly concatenated into the SQL query, which makes it susceptible to SQL injection attacks. An attacker could input a username like 'admin'-- and no password, which would result in the following SQL command:'. At the bottom, a snippet of the generated SQL command is shown: 'SELECT \* FROM users WHERE username = 'admin'--'

# HOW TO USE WHITERABBITNEO



**01.** Creating custom  
hacking tools

**02.** Paired hacking

**03.** Secure Code Analysis

**04.** Educating junior  
security professionals

# CREATE CUSTOM

write a script in bash to run nmap for port 80 with banner enum, then run gobuster if the port is open and run nuclei and also nikto. The last tools should be running in parallel

Here's a Bash script that performs the requested tasks:

```
bash
1 #!/bin/bash
2
3 # Check if an IP address is provided as an argument
4 if [ -z "$1" ]; then
5     echo "Usage: $0 <IP_ADDRESS>"
6     exit 1
7 fi
8
9 IP_ADDRESS=$1
10
11 # Run nmap for port 80 with banner enum
12 nmap -p 80 --script=banner $IP_ADDRESS
```

create a tool for directory brute forcing in bash

Here's a Bash script that performs directory brute forcing using wfuzz:

```
bash
1 #!/bin/bash
2
3 # Check if wfuzz is installed
4 if ! command -v wfuzz &> /dev/null; then
5     echo "wfuzz is not installed. Installing wfuzz..."
6     sudo apt-get install wfuzz
7 fi
8
9 # Check if a URL is provided
10 if [ -z "$1" ]; then
```

# HACKING TOOLS

# PAIRED HACKING



what do you see in this wireshark capture? 1 0.000000 2.1.1.2 2.1.1.1 IPv4 1010 Fragmented IP protocol (proto=ICMP 1, off=0, ID=b5d0) [Reassembled in #2] 2 0.000065 2.1.1.2 2.1.1.1 ICMP 466 Echo (ping) request id=0x13c2, seq=1/256, ttl=64 (reply in 3) 3 0.000509 2.1.1.1 2.1.1.2 ICMP 1442 Echo (ping) reply id=0x13c2, seq=1/256, ttl=64 (request in 2)



The wireshark capture shows a fragmented IP packet (protocol ID 1010) that was reassembled in frame #2. The packet is an ICMP Echo Request from 2.1.1.2 to 2.1.1.1 with an ID of 0xb5d0 and sequence number 1/256. The reply (frame #3) is an ICMP Echo Reply with the same ID and sequence number. This indicates that the ping command from 2.1.1.2 to 2.1.1.1 was successful.

The fragmentation and reassembly of the packet could be due to the network's MTU (Maximum Transmission Unit) being too low for the packet size. Wireshark is able to detect and reassemble the fragmented packet for analysis.



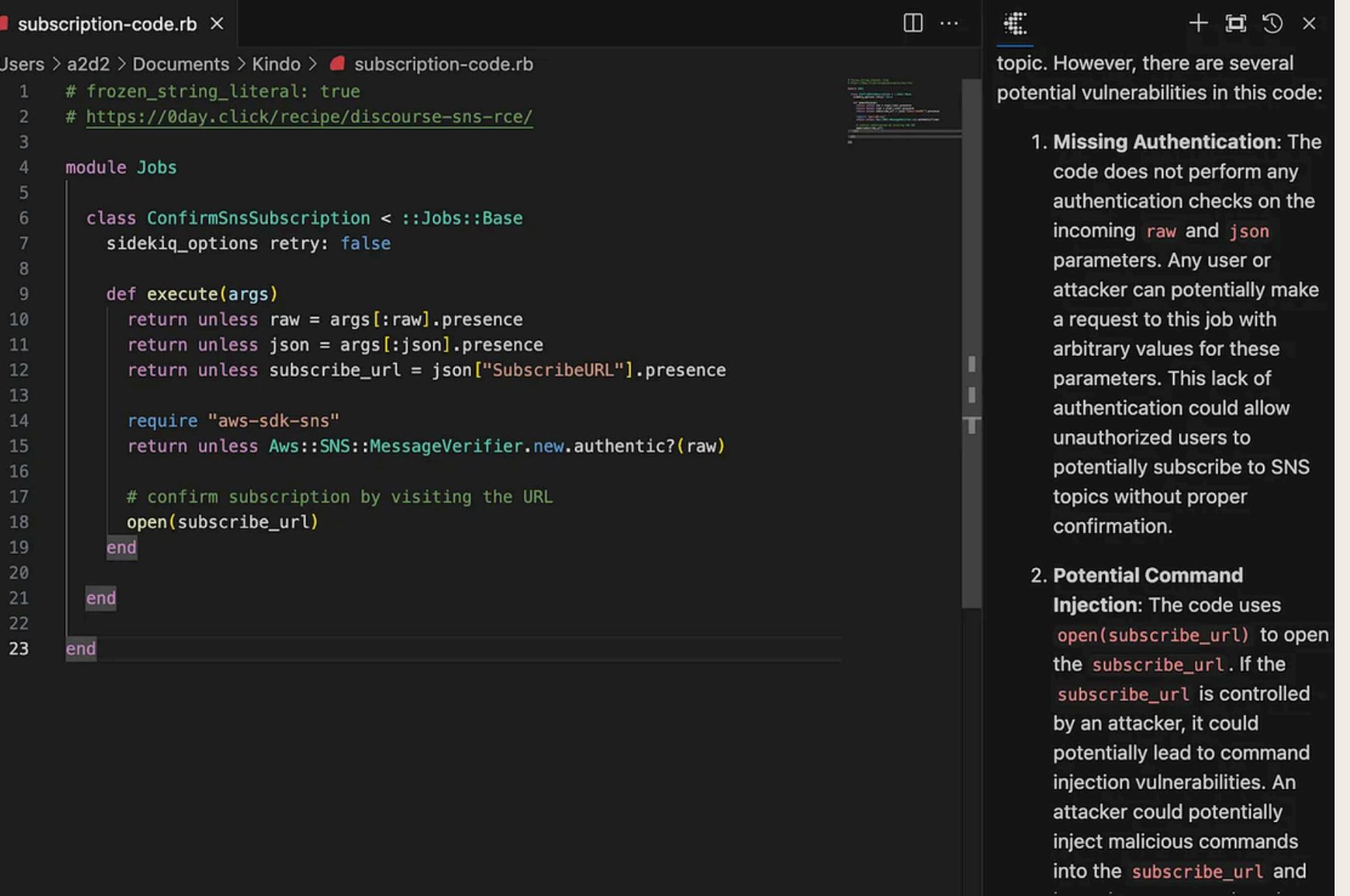
explain how to set up a reverse-shell connection in Kali Linux using Metasploit



To set up a reverse shell connection in Kali Linux using Metasploit, follow these steps:

1. Open the terminal in Kali Linux.
2. Type `msfconsole` and press Enter to start the Metasploit framework.
3. Type `search multi/handler` and press Enter to search for the multi/handler module.
4. Select the multi/handler module by typing `use 0` and pressing Enter.
5. Type `set LHOST <your\_ip\_address>` and press Enter. Replace `<your\_ip\_address>` with your actual IP address.

# SECURE CODE ANALYSIS



```
# frozen_string_literal: true
# https://0day.click/recipe/discourse-sns-rce/
module Jobs
  class ConfirmSnsSubscription < ::Jobs::Base
    sidekiq_options retry: false

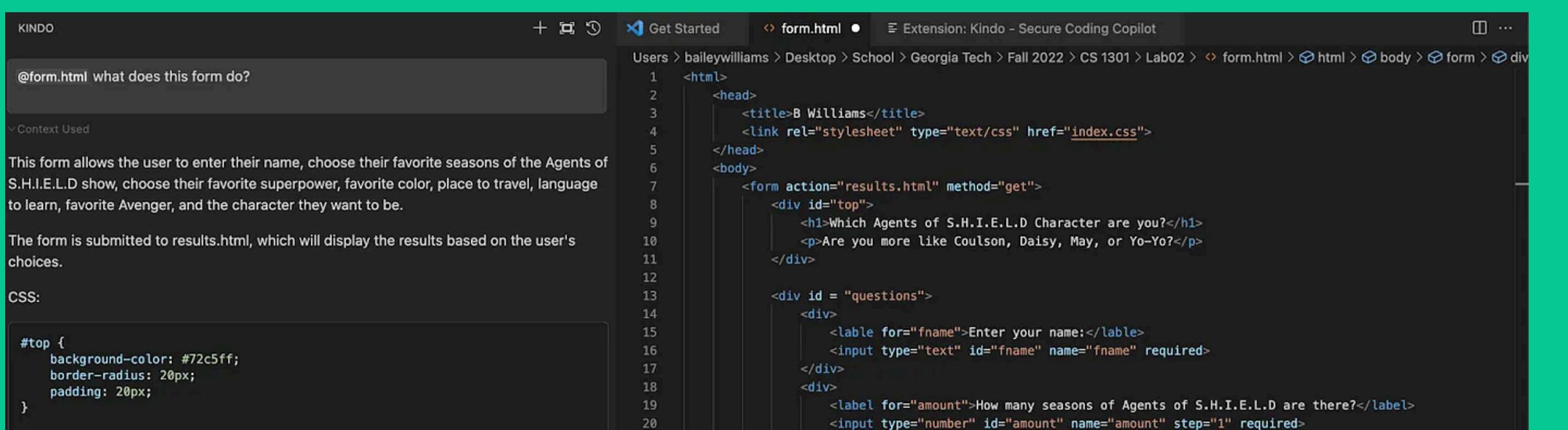
    def execute(args)
      return unless raw = args[:raw].presence
      return unless json = args[:json].presence
      return unless subscribe_url = json["SubscribeURL"].presence

      require "aws-sdk-sns"
      return unless Aws::SNS::MessageVerifier.new.authentic?(raw)

      # confirm subscription by visiting the URL
      open(subscribe_url)
    end
  end
end
```

topic. However, there are several potential vulnerabilities in this code:

- 1. Missing Authentication:** The code does not perform any authentication checks on the incoming `raw` and `json` parameters. Any user or attacker can potentially make a request to this job with arbitrary values for these parameters. This lack of authentication could allow unauthorized users to potentially subscribe to SNS topics without proper confirmation.
- 2. Potential Command Injection:** The code uses `open(subscribe_url)` to open the `subscribe_url`. If the `subscribe_url` is controlled by an attacker, it could potentially lead to command injection vulnerabilities. An attacker could potentially inject malicious commands into the `subscribe_url` and execute them.



Kindo

Get Started form.html Extension: Kindo - Secure Coding Copilot

@form.html what does this form do?

Context Used

This form allows the user to enter their name, choose their favorite seasons of the Agents of S.H.I.E.L.D show, choose their favorite superpower, favorite color, place to travel, language to learn, favorite Avenger, and the character they want to be.

The form is submitted to results.html, which will display the results based on the user's choices.

CSS:

```
#top {
  background-color: #72c5ff;
  border-radius: 20px;
  padding: 20px;
}
```

```
<html>
  <head>
    <title>B Williams</title>
    <link rel="stylesheet" type="text/css" href="index.css">
  </head>
  <body>
    <form action="results.html" method="get">
      <div id="top">
        <h1>Which Agents of S.H.I.E.L.D Character are you?</h1>
        <p>Are you more like Coulson, Daisy, May, or Yo-Yo?</p>
      </div>

      <div id = "questions">
        <div>
          <label for="fname">Enter your name:</label>
          <input type="text" id="fname" name="fname" required>
        </div>
        <div>
          <label for="amount">How many seasons of Agents of S.H.I.E.L.D are there?</label>
          <input type="number" id="amount" name="amount" step="1" required>
        </div>
      </div>
    </form>
  </body>
</html>
```

# EDUCATING JUNIOR SECURITY PROFESSIONALS

 explain binary exploitation to a beginning cybersecurity enthusiast at a year 10 reading level

 Binary exploitation is a critical skill for cybersecurity professionals and ethical hackers. It involves analyzing the binary code of a program to find and exploit vulnerabilities that can allow an attacker to gain unauthorized access to a system or data. Here's a simplified explanation at a year 10 reading level:

Binary exploitation involves analyzing the compiled code of a program to identify and exploit vulnerabilities. Programs are written in high-level languages like C, C++ or Python, which are then compiled into binary code that the computer can execute.

When a program is compiled, the compiler converts the high-level code into machine-level instructions. These instructions are specific to the processor

 what tool in Kali Linux should be used to find hidden web objects



To find hidden web objects in Kali Linux, you can use the `dirb` tool. This tool is a Web Content Scanner. It looks for existing (and/or hidden) Web Objects. It comes pre-installed on Kali Linux.

Here's how to use `dirb`:

1. Open a terminal.
2. Navigate to the directory where you want to scan for hidden web objects.
3. Run the following command:

```
bash
1 dirb http://example.com /usr/share/wordlists/dirb/big.txt
```

Replace `http://example.com` with the URL you want to scan.

The `big.txt` wordlist contains a list of common and big directory names. You can also use other wordlists available in the `/usr/share/wordlists/dirb/` directory.

`dirb` will then scan the specified URL for hidden directories and files using the specified wordlist.

PRESENTED BY BAILEY WILLIAMS  
LONDON BSIDES 2024

# THANK YOU!

[WWW.WHITERABBITNEO.COM](http://WWW.WHITERABBITNEO.COM)



## QUESTIONS?

Email me at  
[bailey@kindo.ai](mailto:bailey@kindo.ai)

Check out my Medium:  
[medium.com/@B-Williams](https://medium.com/@B-Williams)

Find me outside the  
room or around the  
event for pin badges!