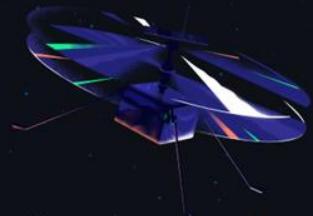




GitHub Copilot Training for Developers

Andrew Scoppa



AGENDA

GitHub Copilot - Introduction

Best practices & prompt engineering

In-class coding demos using copilot and copilot chat

Secure coding

Wrap-up, Q&A

GitHub Copilot Introduction

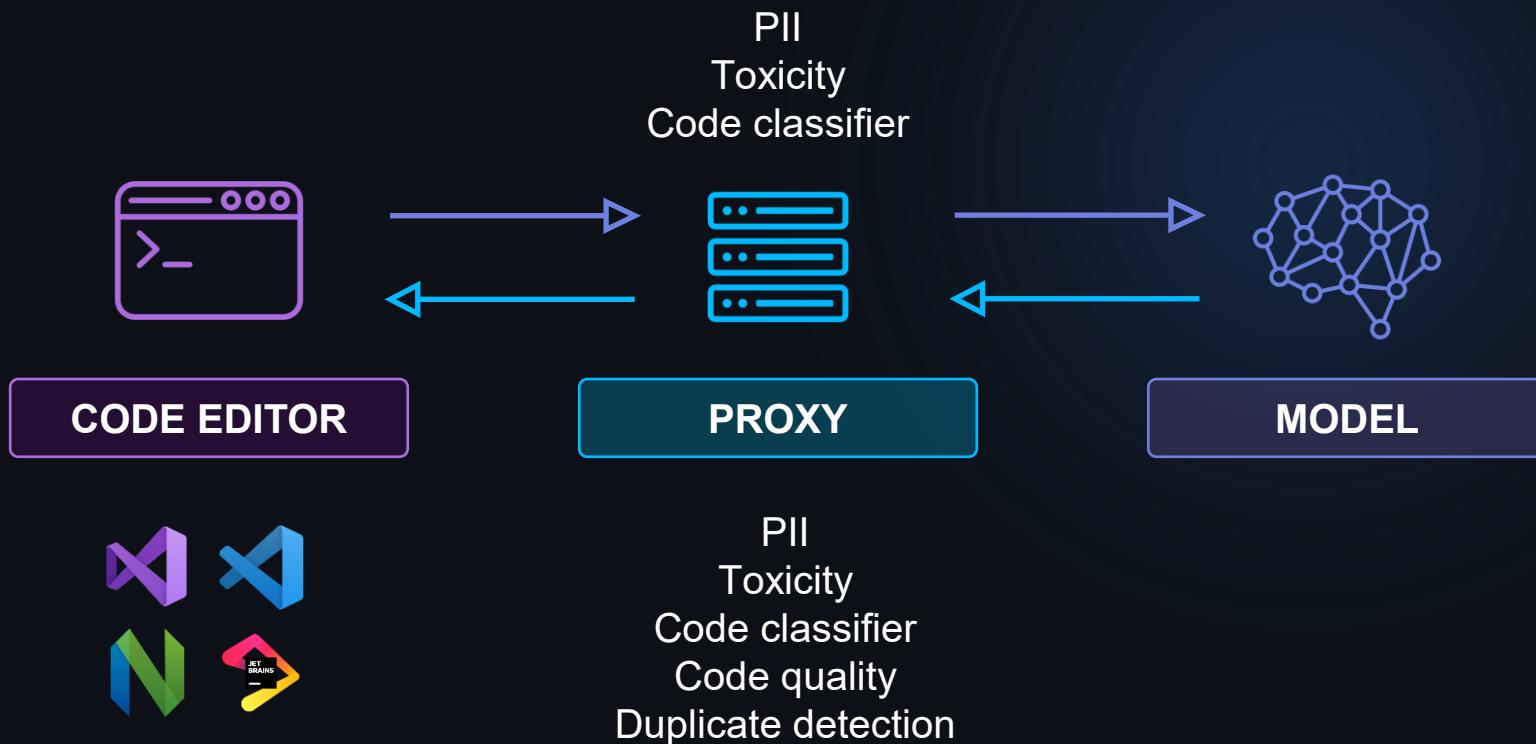


Let's start with a high-level overview of GitHub Copilot

- GitHub Copilot is there to enhance daily work
 - It's an intelligent “pair-programmer”
 - Like a smart assistant or mentor by your side
- Powered by OpenAI
 - Copilot uses a transformative model
 - Think of something like Google Translate
- Trained on large datasets to ensure accuracy
 - Languages with large representation produce best results
- Copilot generates new code in a probabilistic way
 - Unlikely to produce the same code as a snippet that occurred in training.



Data flow through the Copilot ecosystem



Copilot vs Copilot Chat

Copilot

Direct Code Writing

Your “coding assistant”

Solo Development

Copilot Chat

In-Depth Interactive Assistance

Your “research assistant”

Collaborative Scenarios

GitHub Copilot + Chat



Helps developers stay in the flow throughout the entire SDLC



Using Different LLM Models with Copilot

- Several models to choose from including

GPT 5 - Next-generation successor to GPT-4o, geared toward deeper multi-step reasoning, tool orchestration, and extended trusted context windows.

Claude 3.5 Sonnet - Balanced model delivering strong reasoning, long-context handling, and fast iterative responses at moderate cost.

o3-mini (OpenAI) - Lightweight reasoning-optimized model variant focused on fast iterative problem solving (code, logic puzzles, structured planning) with lower latency and cost versus larger flagship models.

- Be aware of costs

Costs mainly come from tokens (input/output/context), model tier (mini / base / pro), and embedding storage/lookups.

Cut them by shortening prompts, limiting context, caching, and choosing right-sized models.



Chatting with Copilot

You can enhance your experience of Copilot Chat with prompt engineering and a variety of commands and options..

Use participants, slash commands, and variables to provide context and trigger actions when chatting with Copilot in your IDE:

- **Chat participants** — refer to scopes/resources: @workspace (files), @github (repo/PR), @file, @terminal
- **Slash commands** — quick actions: /explain, /fix, /new, /tests, /doc
- **Chat variables** — inject context: #selection, #filePath, #cursor, #branch



Prompt Engineering



What is a Prompt?



In the context of Copilot, a prompt is a piece of code or natural language description that is used to generate code suggestions. It is the input that Copilot uses to generate its output.

- The Copilot Team

What is Prompt Engineering?



Prompt Engineering is the strategic crafting of user inputs to guide the AI towards producing desired code outputs.

This involves techniques like role prompting, contextual detailing, and iterative refinement, which collectively enhance the interaction between the developer and Copilot.

Structured Prompt Engineering

- Define Goal

- One sentence on what you want.

- Provide Context

- Key constraints, environment, and inputs.

- Include Sources and Links

- Only the needed code/spec links or snippets.

- Specify Expectations

- Exact output format and style.

Example:

Role-play as a senior Python reviewer mentoring a programmer.

Goal: Generate deterministic pytest unit tests for the Producer–Consumer in apps/python/ex1.

Context: Python 3.13, stdlib only; use delay=0 in tests; enforce ValueError on negative count or delay; stop on unique SENTINEL; queue empty after run.

Sources: apps/python/ex1/specs.md and the files producer.py, consumer.py, run.py, logging_utils.py, __init__.py in copilot-base.

Expectations: Output exactly one test file (tests/test_producer_consumer.py) in a single fenced code block with the filepath comment; cover count=0 and normal flow; assert sentinel consumed once; keep assertions concise; no prose; ≤80 lines.



Use Prompting Across the SDLC

Observe the technique being used in the following prompt:

“You are an experienced C++ software engineer.

- Provide a detailed explanation of how Copilot can assist in each phase of the SDLC, including planning, design, development, testing, deployment, and maintenance.
- Include specific C++ examples of tasks or activities within each phase where Copilot can be particularly beneficial.”
- The output should be formatted as markdown with clear delineation of phases.

Interactive Coding with Copilot

To help Copilot generate accurate suggestions when writing code:

- Add a top-level comment block describing the purpose of the file
- Front load as many imports as needed (import / include / requires / etc.)
- Create a detailed comment block describing the purpose of an operation or UDT
- Use sample code as a starting point
- Have related content open in other tabs



AI Prompt Techniques

Zero Shot Prompt

```
1 //Write a JavaScript function that finds
2 //the maximum value in an array.
3 function max(array) {
4     return Math.max.apply(null, array);
5 }
```

One-Shot Prompt

```
1 ✓ //Create a JavaScript function, `findMax`, that takes an array of strings as input
2     //and returns the string with the maximum length.
3     //Ensure that the function works correctly for arrays that are empty,
4     //as well as arrays that contain both strings and numbers.
5 ✓ function findMax(array) {
6     var max = array[0].length;
7     array.map(v => max = Math.max(max, v.length));
8     result = array.filter(v => v.length == max);
9     return result;
10 }
```



Helpful Patterns

- * Use descriptive variable names to make your intentions clear.

```
totalSampleCount = 1000
```

- * Maintain consistent naming conventions for variables and functions.

i.e. using camelCase for variable names consistency

- * Define method signatures with unambiguous parameter names and types.

```
double calculateAverageSampleSize(unsigned long samples[], size_t size)
```

- * Use comments to explain the purpose of the code.

This function 'palindrome' takes an array of strings
as input and returns true if a palindrome is found.



Helpful Patterns

- * Specify error handling scenarios.

Exit where the input is NULL and throw and exception if the input out of range [min, max] inclusive.

- * Describe control flow structures.

Write a while loop to print the first 'n' values in the fibonnaci sequence.

- * Show examples of how to use the code.

```
int samples[] = {1, 2, 3, 4, 5};  
double average = calculateAverageSampleSize(samples, 5);  
printf("Average: %f\n", average); // Average: 3.0
```

- * Test your code.

Write a test suite to verify the correctness of the code.

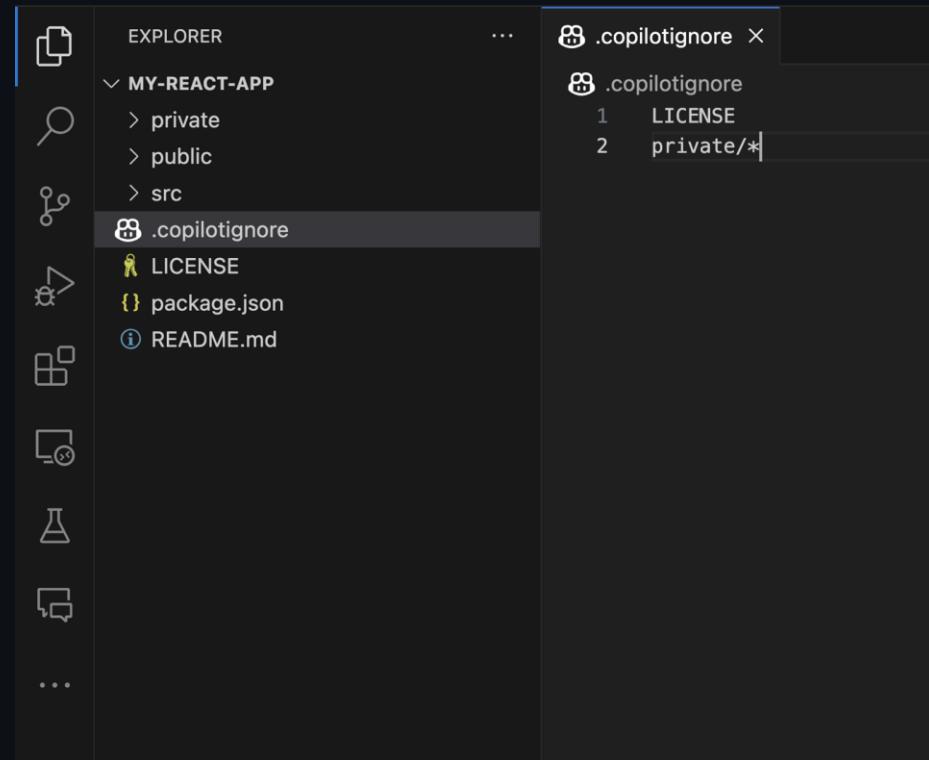


Secure coding



Block files from Copilot

Use `.copilotignore` to block files and folders from being used by Github Copilot



Copilot Restricted Content feature

- The Copilot Restricted Content feature allows repository owners to control the usage of Copilot across their codebases.
- This includes specific files, folders, or entire repositories, even if they're not hosted on GitHub.
- The goal is to provide CfB customers a flexible way of controlling what content Copilot can access for prompt crafting and where it can insert code.

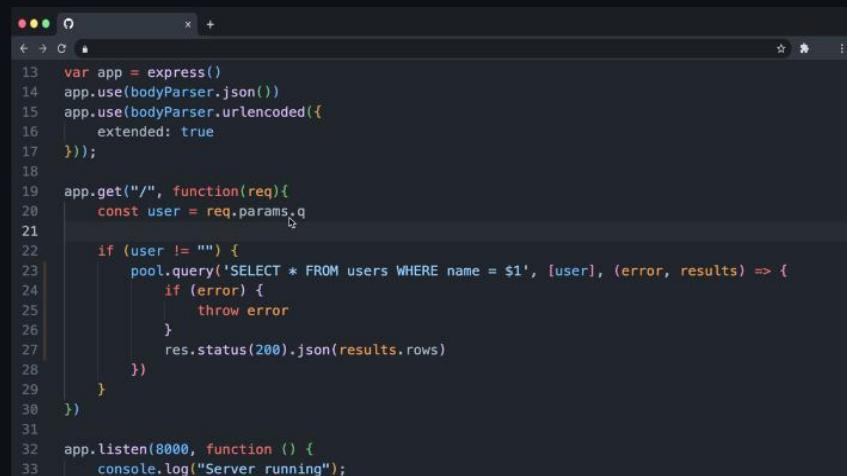
The screenshot shows the GitHub Copilot interface for managing restricted content. On the left, a sidebar lists organization settings like General, Features, Access, and Copilot. The 'Copilot' section is expanded, showing 'Restricted content' (Beta). The main area is titled 'Restricted content' and 'Restricted paths'. It explains that Copilot won't access paths listed here. It supports YAML syntax with fnmatch notation. A text input box contains the following YAML rules:

```
1  /*+: [**/.env*]
2
3  marais-testing-repo:
4    - */src/kernel.rs*
5
6  git@github.com:primer/react.git:
7    - *e2e/*
8
9  git@gitlab.com:openicity-labs/surreal-react.git:
10   - *fly.toml*
11   - **/surrealdbjs/*
```

Below the input box, instructions say to use `Control + Shift + m` to toggle focus between tabs. A note at the bottom says 'Use separate lines to choose what folders and files will be ignored by GitHub Copilot'. At the bottom right are 'Discard changes' and 'Save changes' buttons.

Copilot and Secure Coding

- AI-based vulnerability system that helps prevent insecure coding patterns (e.g. SQL script injection)
- Vulnerability filters are applied only to the Copilot-generated suggestion itself
 - ✖ It cannot detect downstream vulnerabilities introduced by the code e.g. on deployment infrastructure
 - ⓘ We recommend taking the **same precautions** you take with code written by engineers (linting, code scanning, etc.)
- Copilot Chat can be used to query code for known vulnerabilities



```
var app = express()
app.use(bodyParser.json())
app.use(bodyParser.urlencoded({
  extended: true
}));

app.get("/", function(req){
  const user = req.params.q
  if (user != "") {
    pool.query('SELECT * FROM users WHERE name = $1', [user], (error, results) => {
      if (error) {
        throw error
      }
      res.status(200).json(results.rows)
    })
  }
})
app.listen(8000, function () {
  console.log("Server running");
})
```

Detection & Remediation

- Prompt for insecure coding patterns
- Use GHAS Code Scanning results
- Write custom CodeQL queries
- Increase your knowledge of secure coding patterns
- Create custom Secret Scanning patterns

 stebje

It looks like this code is insecure. Help me understand what the issue is and how to resolve it.

 GitHub Copilot

Yes, this code is vulnerable to SQL injection attacks. The issue is that the `search` parameter is directly concatenated into the SQL query string without any sanitization or validation. This means that an attacker could potentially inject malicious SQL code into the query, which could lead to data theft or destruction.

To fix this issue, you should use parameterized queries instead of concatenating strings. Parameterized queries use placeholders for the input values, which are then bound to the query separately. This ensures that the input values are properly sanitized and validated before being used in the query.

Here's an example of how to use parameterized queries with the `pg` library:

```
const search = req.params.q;

if (search != "") {
  const query = "SELECT * FROM users WHERE name = $1";
  const values = [search];
  pool.query(query, values, (err, res) => {
    console.log(err, res);
    pool.end();
  });
}
```

In this example, the `$1` placeholder is used for the `search` parameter, and the actual value is passed in as an array of values to the `pool.query()` function. This ensures that the `search` parameter is properly sanitized and validated before being used in the query.

```
4   const pool = new Pool(config: {
5     user: 'postgres',
6     host: 'localhost',
7     database: 'postgres',
8     password: 'process.env.POSTGRES_PW',
9     port: 5432,
10    });
11
12
13  var app = express();
14  app.use(bodyParser.json());
15  app.use(bodyParser.urlencoded({ extended: true }));
16
17  app.get('/', function (req, res) {
18    const search = req.params.q;
19
20    if (search != "") {
21      var query = "SELECT * FROM users WHERE name = $" + search + "'";
22      pool.query(queryTextOrConfig: query, callback: (err, res) => {
23        console.log(message: err, optionalParams: { res });
24        pool.end();
25      });
26    }
27  });
28
29  app.listen(port: 8000, callback: function () {
30    console.log(message: 'Example app listening on port 8000!');
31  });
32
```



Copilot + GHAS

GitHub Copilot and GitHub Advanced Security (GHAS) serve different purposes and are not replacements of each other.

- Copilot is not a replacement of GHAS features
- Copilot can be used in tandem with GHAS
 - features to detect and remediate vulnerabilities earlier during the SDLC
 - GHAS Code scanning results
 - GHAS Secret scanning



Security & Trust

Copilot Trust Center

- Security
- Privacy
- Data flow
- Copyright
- Labor market
- Accessibility
- Contracting

The screenshot shows the GitHub Copilot Trust Center page. At the top, there's a navigation bar with links for Resources, Why GitHub, Collections, Topics, Type, a search bar, and buttons for Enterprise trial and Contact Sales. The main title "GitHub Copilot Trust Center" is prominently displayed. Below the title, a subtitle reads: "We enable developers and organizations to maximize their potential by prioritizing security, privacy, compliance, and transparency as we develop and iterate on GitHub Copilot." There are five categories listed below: Security, Privacy, IP and Open Source, Labor Market, and Accessibility. On the right side, there's a video player titled "Trust Center Overview" showing a video thumbnail with a white cat silhouette and a red play button. A black arrow points to the "Watch on YouTube" button.



Wrap Up



Thank you

