



Breaking AI

Live coding and hacking
applications with Generative AI

+



snyk

Micah Silverman

Director, DevSecOps Acceleration  @Snyk



Java Developer (29 years)

Author

Open Source Contributor

DevSecCon chapter leader

Tinkerer

Chaotic Neutral



micah.silverman

Agenda

+

+

+

1

Introduction to AI in development 

2

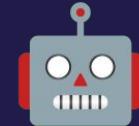
Building a conf schedule app with Copilot 

3

Learnings and takeaways 



AI in the world of Software Security



Managing application security is getting harder

**Developers introducing
code with growing
frequency**



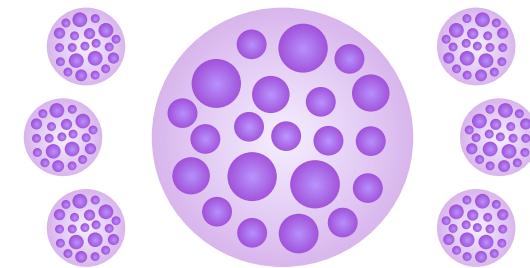
**Generative AI propels
productivity, but security issues
cause frustration**

**Applications more
complex than ever
before**



Visibility into overall security
posture is more difficult to
maintain

**Number & complexity of
issues in backlogs
continues to grow**



Difficult to ensure complete
coverage, identify and prioritize risk
to the business



Exploring the potential of AI 🤔



Common Uses in Development

- Adding comments
- Summarizing code
- Writing “readme”
- Refactoring code
- Providing templates
- Pair programming
- Generating code (the new Stack Overflow)

LLMs: Developer superpower...

... security concerns



92 %

Of **software developers**
Are already using AI
coding tools



Software developers using AI
tools completed tasks

57%

Faster than those who didn't.



Software developers using
AI tools were

27%

More likely to complete a
task than those who didn't



NYU

40%

Of **Co-Pilot generated
code contained
vulnerabilities**

Stanford

Developers wrote
significantly less secure code
than those without access.

**more likely to believe they
wrote secure code** than those
without access to the AI
assistant.



AI and Artificial Imagination



An exploration of hallucinatory possibilities





What is $5*9+4*3$? Give the answer first, then the explanation.



The answer is 51.

To get this answer, we need to first multiply 5 by 9, which gives us 45. Then, we multiply 4 by 3, which gives us 12. Finally, we add these two results together:

$$45 + 12 = 51$$

Therefore, $59+43$ equals 51.



Are you sure about the last result?



Yes, I am confident that the answer to $59+43$ is 51. If you think there might be an error, please let me know and I'll be happy to double-check my calculations.

Source: “chatGPT is confidently wrong” by Eelko de Vos



What is $45 + 12$?



$45 + 12$ is equal to 57.



And you earlier said it was 51?



I apologize for the mistake. I misunderstood the question earlier and made a calculation error in my response. The correct answer to $59+43$ is indeed 57. Thank you for bringing it to my attention.

Source: “chatGPT is confidently wrong” by Eelko de Vos

But...

TECH · A.I.

Over just a few months, ChatGPT went from correctly answering a simple math problem 98% of the time to just 2%, study finds

BY PAOLO CONFINO

July 20, 2023 at 8:29 AM GMT+9



Lawyer 'was unaware' ChatGPT could generate fake legal research, now faces sanctions

ELURA NANOS | May 30th, 2023, 10:01 am

Australian mayor readies world's first defamation lawsuit over ChatGPT content

By Byron Kaye ▾

April 5, 2023 2:52 PM EDT · Updated 2 months ago

S what is the world record for crossing the english channel entirely on foot

The world record for crossing the English Channel entirely on foot is held by Christof Wandratsch of Germany, who completed the crossing in 14 hours and 51 minutes on August 14, 2020. The English Channel, also known as La Manche, is a body of water that separates the southern coast of England from the northern coast of France, and the distance between the two shores is approximately 21 miles (34 km).

Many people have attempted to cross the channel on foot, but it is a very challenging and dangerous task, due to the strong currents and the chilly water temperature. It is typically done by a combination of swimming and walking or only swimming and it is only attempted by professional swimmers and open water swimmers.

Regenerate response

AI will be wrong...

...and when it is wrong....

It doesn't know it's wrong!

snyk



What about the Code?



AI Coding

create me a basic express app which takes a name in the request params and returns a html page that shows the user their name.



```
const express = require('express');
const app = express();

app.get('/name/:name', (req, res) => {
  const name = req.params.name;
  const html = `
    <html>
      <head>
        <title>User Name</title>
      </head>
      <body>
        <h1>Hello, ${name}!</h1>
      </body>
    </html>
  `;
  res.send(html);
});

app.listen(3000, () => {
  console.log('Server started on port 3000');
})|
```

Prompt provided to Bard, GPT-3.5 + GPT-4

- **name** parameter output without sanitization
- Results in typical reflected Cross-Site Scripting vulnerability

AI Securing Code



NoSQL injection is a potential vulnerability when working with NoSQL databases like MongoDB. While the provided code is not susceptible to NoSQL injection, it's important to be aware of this security risk and take appropriate measures to prevent it.

NoSQL injection occurs when untrusted user input is directly concatenated with a database query, allowing an attacker to manipulate the query and potentially access or modify data in unintended ways. In the provided code, Mongoose handles the interaction with the MongoDB database, and it automatically sanitizes and escapes user input to prevent NoSQL injection.



The code you provided is safe from NoSQL injection because it uses the `bodyParser` middleware to sanitize all incoming requests. The `bodyParser` middleware will sanitize the request body before it is passed to the Mongoose model. This helps to prevent attackers from injecting malicious code into the database.

Bad advice to developers

- Both GPT + Bard stated code was not vulnerable and gave invalid advice!
- GPT-4 did notice the bug when specifically asked about NoSQLi - but failed when asked generic "Is there any vulnerability in this code?"

Know how your IP will be used

Whoops, Samsung workers accidentally leaked trade secrets via ChatGPT

ChatGPT doesn't keep secrets.

By [Cecily Mauran](#) on April 6, 2023



A major whoopsie from Samsung. Credit: Getty Images



Coding Patch Conference App



Create Homepage

Requires top banner and
product listing table

1

Create Homepage



Requires speaker and product database

1

2

Make talks table searchable

Take user input and filter the results based on matches in the talk's name and description or speaker name

Create Homepage

Requires a speaker and
a talk.

%';

```
update talk set
start_date = dateadd(hour,-2,CURRENT_TIMESTAMP),
end_date = dateadd(hour,1,CURRENT_TIMESTAMP)
where speaker_id = 1;
```

--

Take user input and filter the results based on matches in the talk's name and description or speaker name

Create Homepage



Requires speaker and product database

1

2

Make talks table searchable

Take user input and filter the results based on matches in the talk's name and description or speaker name

Create Homepage



Requires customer and product info to be available

Allow users to personalise profiles

Users can upload their own avatar to their profile

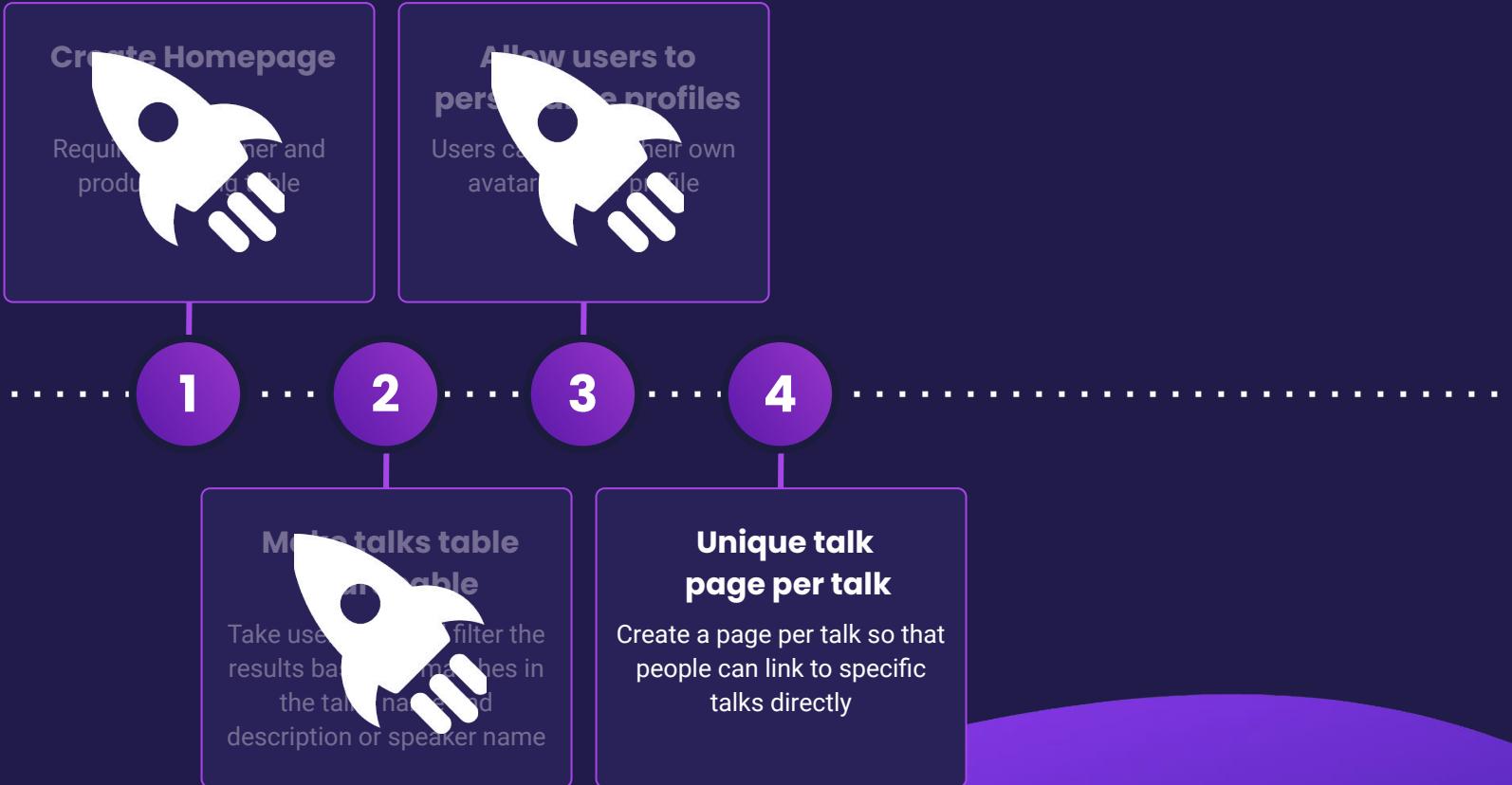
1

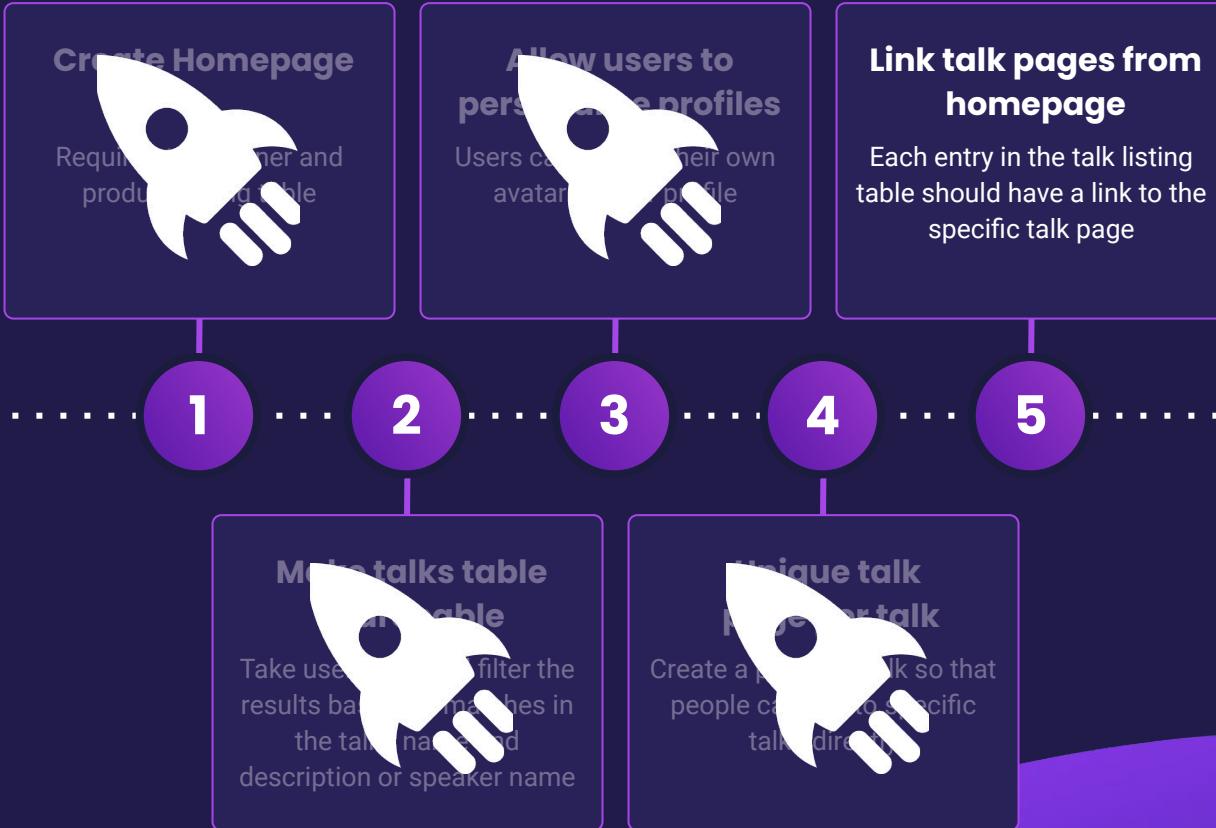
2

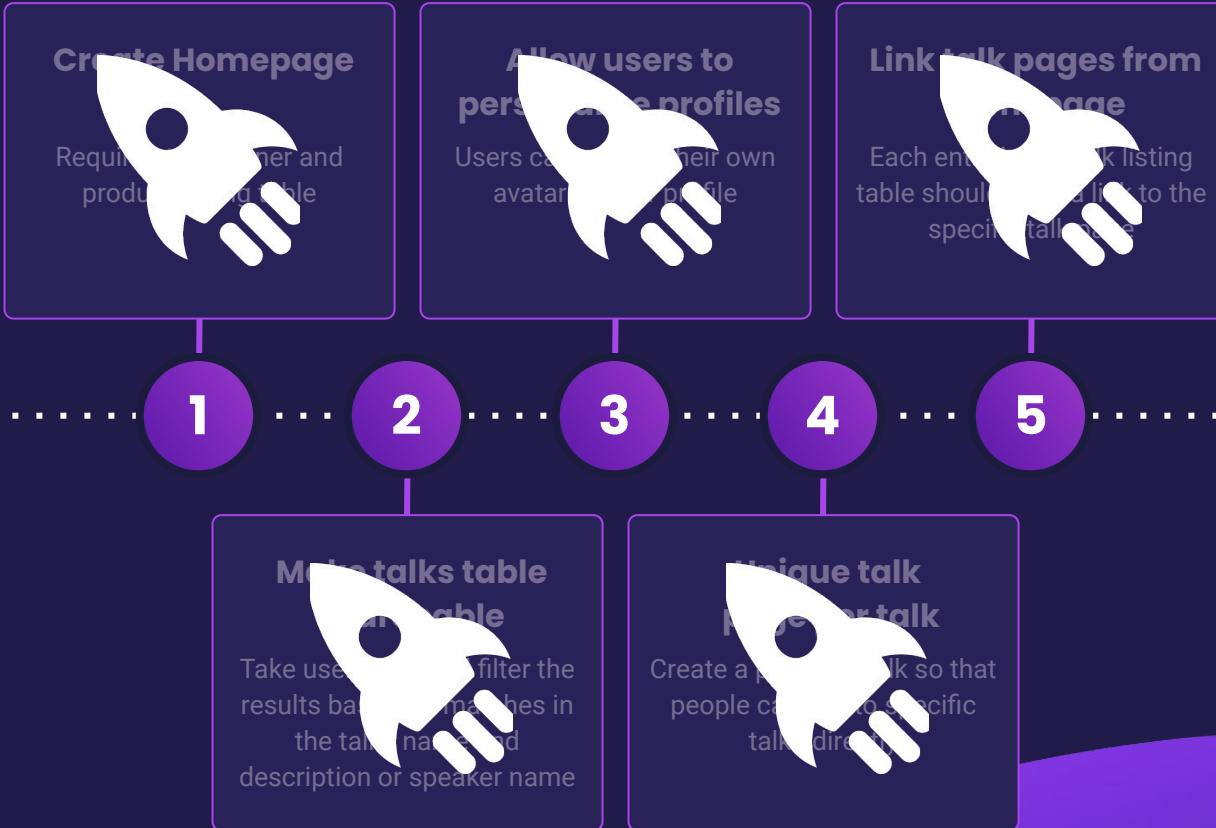
3

Make talks table filterable

Take user input to filter the results based on matches in the talk name and description or speaker name









Learnings

Best Practices & Resources





Takeaways



Education and awareness

- Write up policies and company guidelines
- Focus on security vulns, sensitive data and IP and human interaction
- Make education actionable making sure repeatable steps can be taken

Don't trust. Verify.

- Treat AI code like it's from an inexperienced dev/app sec engineer
- Test/validate everything
- Pair ChatGPT, Co-Pilot with AST in the IDE



Micah Silverman



micah.silverman



dogeared



SPECIAL THANKS TO ALL OUR AWESOME CAMP SPONSORS!

Unspecified



DATASTAX



PROPELAUTH



FOR DEVELOPERS



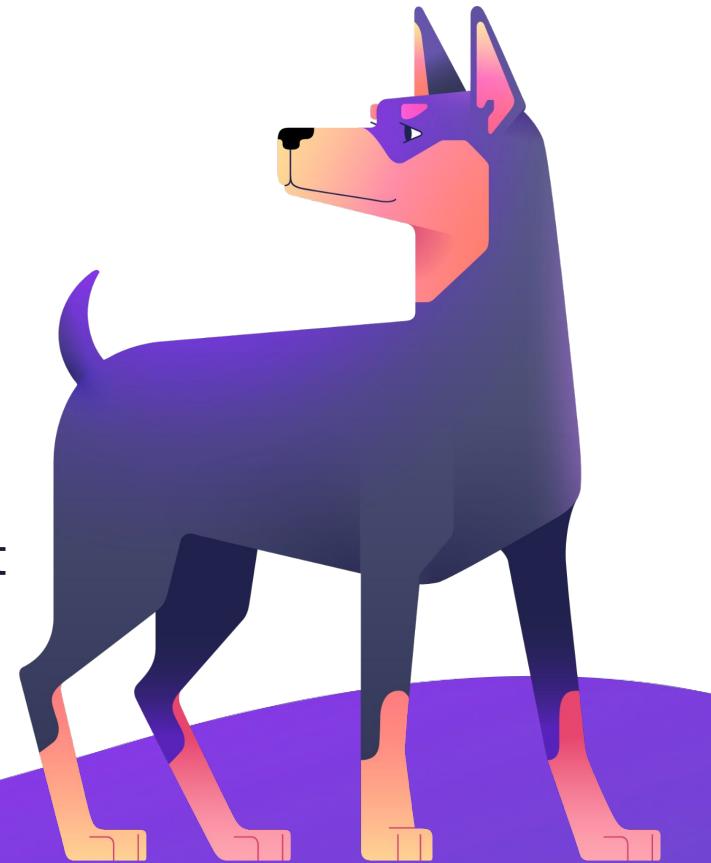
FORMERLY GRAPECITY, INC.





Q&A

Secure Your GenAI Code from the Start





Thank You!

Secure Your GenAI Code from the Start

