



Generative AI and the future of development

Christopher Harrison

Senior Developer Advocate, GitHub

@geektrainer



**Will AI replace
developers?**

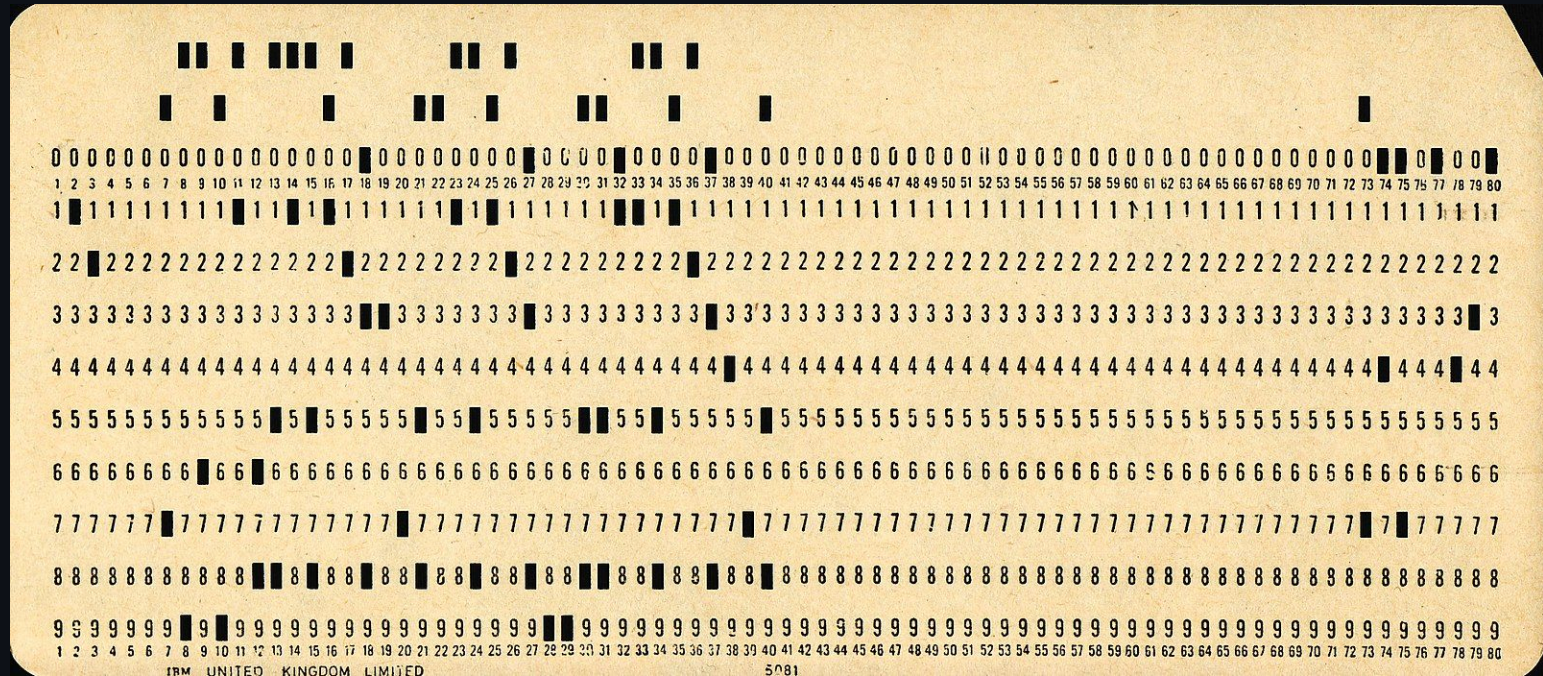
Short answer: No

Longer answer:
Also no

**We sometimes
overhype technology**

**We're always
improving how we
create software**

We've moved beyond these



We've created many languages

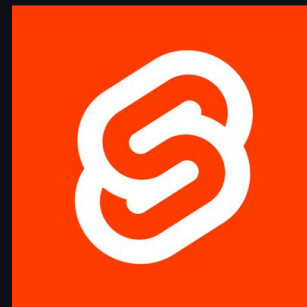
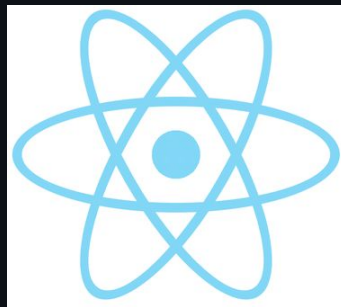
- Assembly
- FORTRAN
- FLOW-MATIC
- COBOL
- C, C++
- Python
- Java
- JavaScript
- C#
- Scratch
- Scala
- F#
- PowerShell
- Go
- TypeScript
- Swift

**Let's talk about
web frameworks...**

jQuery was revolutionary

```
$('#button').click(function () {  
    alert('Hello, world!');  
});
```

And now we've got...



**We're making
things more
difficult...**

**...at the same time
we're making it
easier...**

...and opening dev
to “non-devs”.

**There's still a
never-ending
demand for
software**

**How can
generative AI
support developers?**

Offload boilerplate code

```
# Create a speaker with name, bio, email and linkedin url
class Speaker(models.Model):
    name = models.CharField(max_length=100)
    bio = models.TextField()
    email = models.EmailField()
    linkedin = models.URLField()
    def __str__(self):
        return self.name
```

Generate unit tests

```
1 // import models
2
3 const { Speaker, Talk } = require('../src/api/models');
4
5 // test validation for speaker
6 describe('Unit Tests', () => {
  test('speaker should be invalid if name is empty', async () => {
    const speaker = new Speaker();


    speaker.validate((err) => {
      expect(err.errors.name).toBeDefined();
    });
  });

  test('speaker should be invalid if bio is empty', async () => {
    const speaker = new Speaker();

    speaker.validate((err) => {
      expect(err.errors.bio).toBeDefined();
    });
  });
});
```


Inline upskilling

GITHUB COPILOT




Hi @lefrightleft, how can I help you?

I'm powered by AI, so surprises and mistakes are possible. Make sure to verify any generated code or suggestions, and [share feedback](#) so that we can learn and improve.




lefrightleft

Can you explain what cross-site scripting is?



GitHub Copilot

Cross-site scripting (XSS) is a type of security vulnerability that allows an attacker to inject malicious code into a web page viewed by other users. This can allow the attacker to steal sensitive information, such as login credentials or personal data, from the users who view the page. In the context of the warning you provided, it means that the value of `queueNamePrefix` is not being properly sanitized, and could potentially contain malicious code that could be executed by a user's browser.



How can I prevent cross-site scripting attacks in my web application?

Ask Copilot a question or type '/' for topics


CQSUserPageServlet.java — ghas-demo-2023

J CQSUserPageServlet.java 9 X

src > com > comcast > cqs > controller > J CQSUserPageServlet.java

```
330 out.println("<td>"+(attributes.get("DelaySeconds") != null ? attributes.get("DelaySeconds")+
331 out.println("<td>"+(attributes.get("ReceiveMessageWaitTimeSeconds") != null ? attributes.get("Re
332 out.println("<td>"+(attributes.get("NumberOfPartitions") != null ? attributes.get("NumberofParti
333 out.println("<td>"+(attributes.get("NumberOfShards") != null ? attributes.get("NumberOfShards")+
334 out.println("<td>"+(attributes.get("IsCompressed") != null ? attributes.get("IsCompressed")+
335 out.println("<td>"+(attributes.get("ApproximateNumberOfMessages") != null ? attributes.get("Appr
336 out.println("<td>"+(attributes.get("ApproximateNumberOfMessagesNotVisible") != null ? attributes
337 out.println("<td>"+(attributes.get("ApproximateNumberOfMessagesDelayed") != null ? attributes.ge
338
339 out.println("<td><a href='/webui/cquser/message?userId="+ user.getUserId()+ "&queueName="+ Ut
340 out.println("<td><a href='/webui/cquser/permissions?userId="+ user.getUserId() + "&queueName="+
341 out.println("<td><a href='\" onclick='\"window.open(\"/webui/cquser/editqueueattributes?queueName=
342
343 out.println("<input type='hidden' name='queueNamePrefix' value='"+(queueNamePrefix != null ? que
```

GitHub Security Alert



Cross-site scripting vulnerability due to a user-provided value.

Cross-site scripting

Directly writing user input (for example, an HTTP request parameter) to a web page, without properly sanitizing the input first, allows for a cross-site scripting vulnerability.

Recommendation

To guard against cross-site scripting, consider using contextual output encoding/escaping before writing user input to the page, or one of the other solutions that are mentioned in the reference.

Example

The following example shows the `page` parameter being written directly to the page, leaving the website vulnerable to cross-site scripting.

```
public class XSS extends HttpServlet {
    protected void doGet(HttpServletRequest request, HttpServletResponse response)
        throws ServletException, IOException {
        // BAD: a request parameter is written directly to the Servlet response stream
        response.getWriter().print(
            "The page \"" + request.getParameter("page") + "\" was not found.");
    }
}
```

References

- OWASP: XSS (Cross Site Scripting) Prevention Cheat Sheet

**How to get the most
out of the tools?**

Provide context

Be specific

**Good code begets
good code**

Find the flow

**Offload the boring
and focus on the
bigger issues**

**What if I get
bad code?**

How I wrote code before generative AI

Write code based on
experience

Find snippets in
documentation

Find snippets in
forums

**Keep your
DevOps flow
even with
generative AI**

Peer review

IP checks

Code quality scans

Security scans

In the end...

**Generative AI is a
tool to help you be
more productive as
a developer**

Thank you