

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. Some nodes are highlighted with blue circles, and others with blue dots. The lines are thin and grey, creating a mesh-like structure.

Web Clients

Patch Notes

Weekly exercise on web fundamentals on Canvas:

https://canvas.colorado.edu/courses/126474/assignments/2495579?module_item_id=6750837

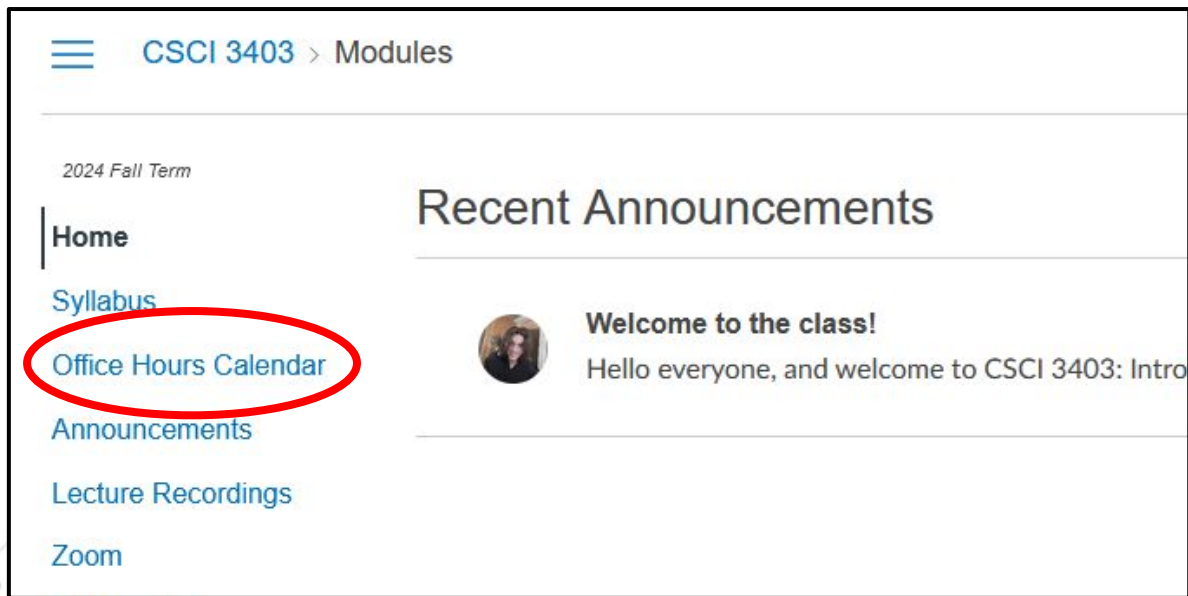
Patch Notes

Reminder to Alex: ask about AI usage

- Is it common? Is it helpful?

Patch Notes

Office hours calendar on Canvas:



≡ CSCI 3403 > Modules

2024 Fall Term

Home

[Syllabus](#)


[Office Hours Calendar](#)

[Announcements](#)

[Lecture Recordings](#)

[Zoom](#)

Recent Announcements

 **Welcome to the class!**
Hello everyone, and welcome to CSCI 3403: Intro

Web Fundamentals

The first half the the class will focus on **web security**: flaws which exist in websites.



Web Fundamentals

Pros:

- Very common (great for interviews!)
- Lots which can go wrong (which is a good thing?)
- Easy to get started

Web Fundamentals

Pros:

- Very common (great for interviews!)
- Lots which can go wrong (which is a good thing?)
- Easy to get started

Cons:

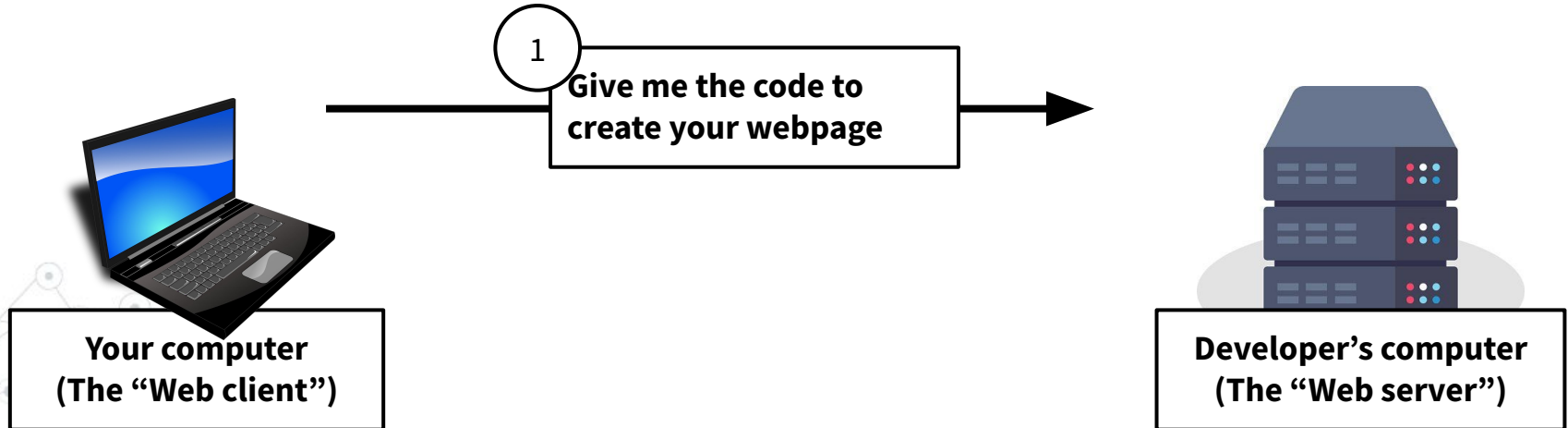
- We have to learn how websites work



What happens when you visit a webpage?

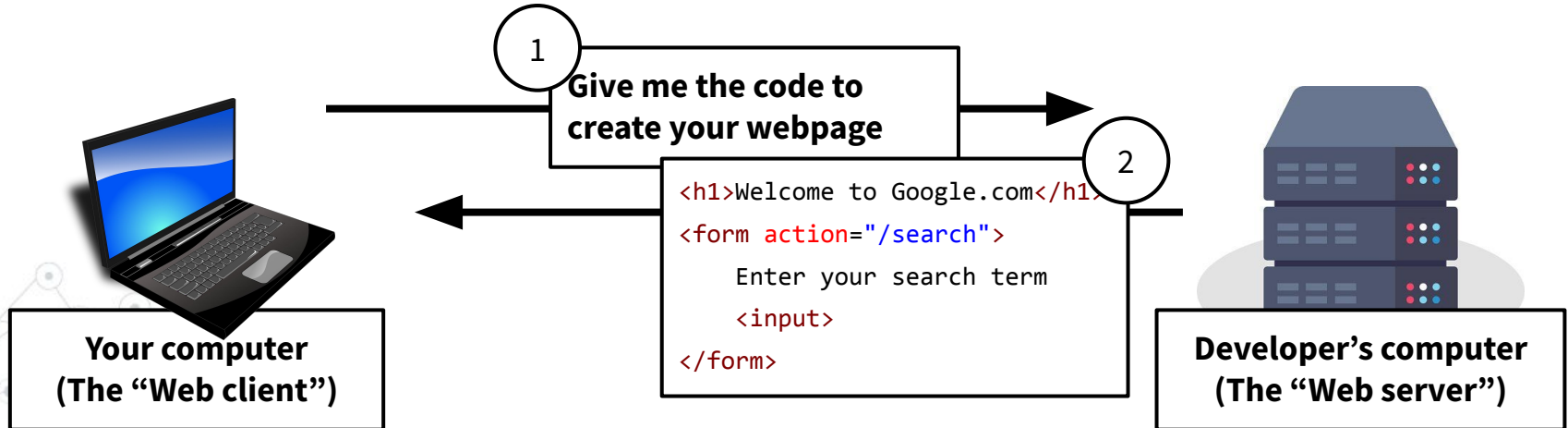
Web Fundamentals

1. Your computer (the “client”) asks for the website from the web developer’s computer (the “server”)



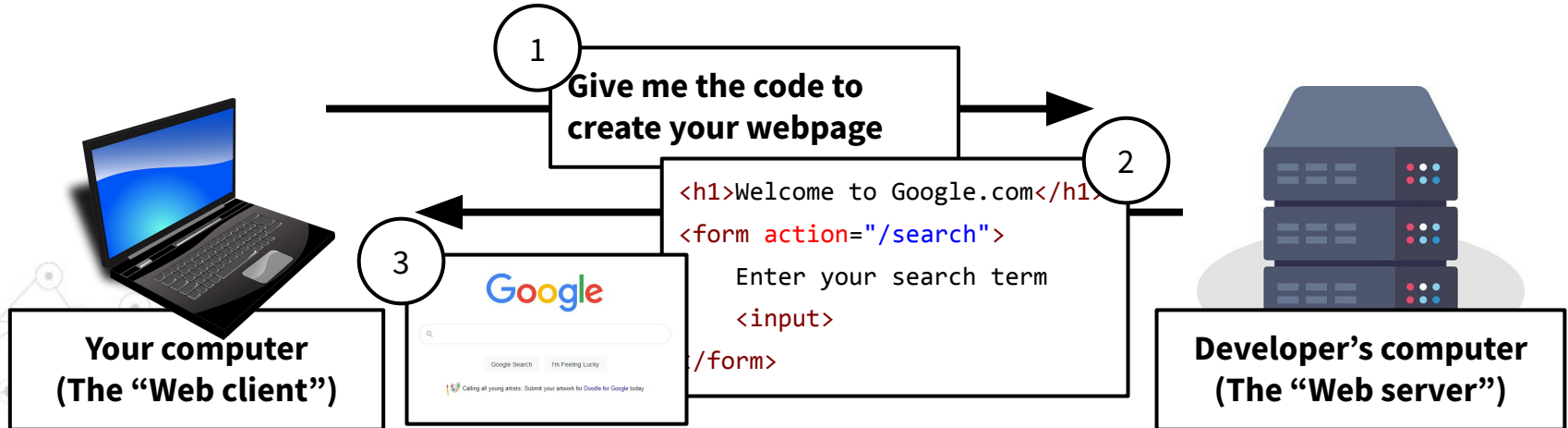
Web Fundamentals

1. Your computer (the “client”) asks for the website from the web developer’s computer (the “server”)
2. The server sends the code needed to create the website



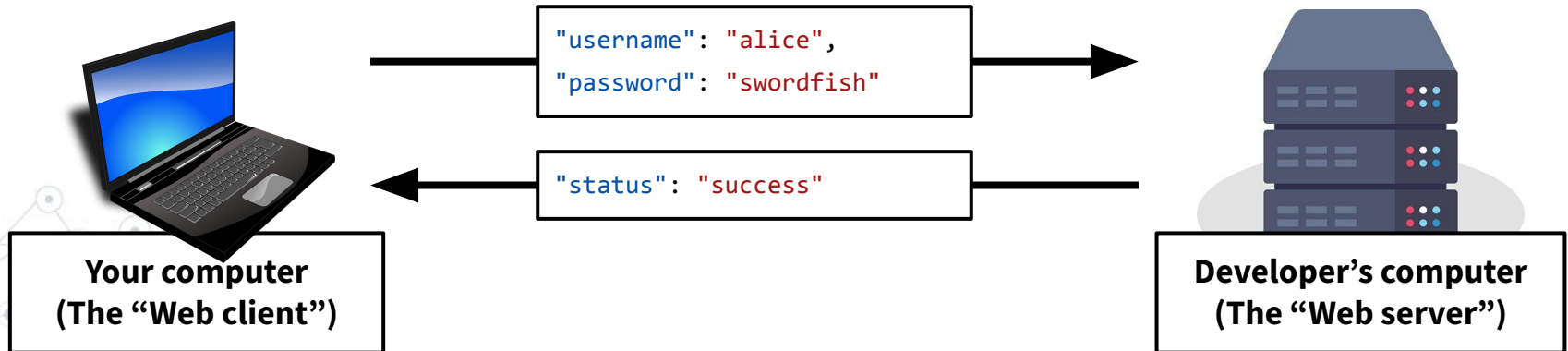
Web Fundamentals

1. Your computer (the “client”) asks for the website from the web developer’s computer (the “server”)
2. The server sends the code needed to create the website
3. The client runs the code to display the website



Web Fundamentals

(Optionally: Additional data can be sent back and forth afterwards such as logging in, updating chat messages, etc)



Web Fundamentals

This means web developers write two sets of code: One which runs on the client, and one which runs on the server.

- Client code: Displays the webpage
- Server code: Responds to messages from the client

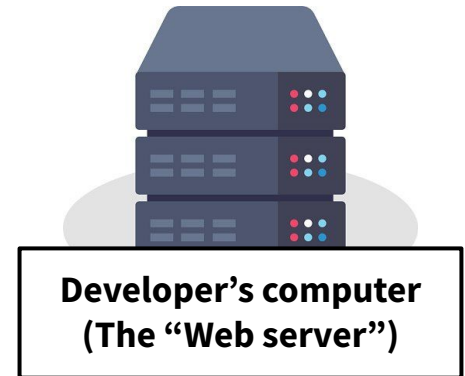




Client-side code

Client-side code

Client-side code: Code that is run on the user's computer which visually displays the webpage



Client-side code

View the code for a page: Right click > View Source



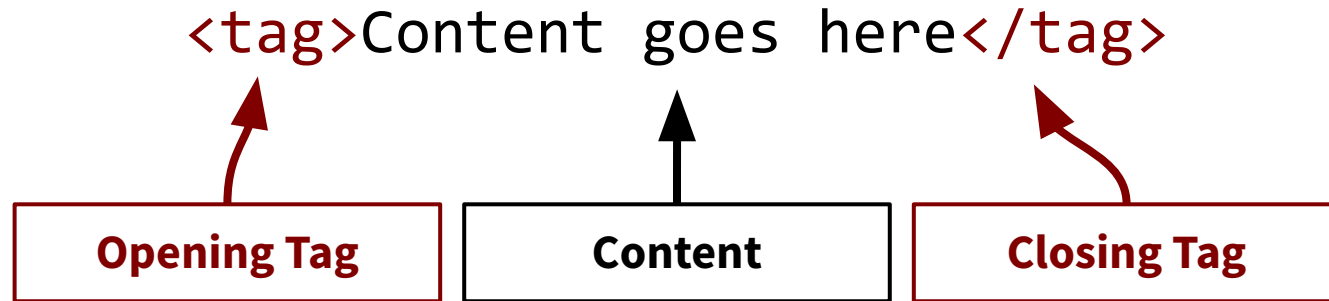
Client-side code

HyperText Markup Language (HTML): The language of the web, determines how a webpage looks and acts

```
<h1>Welcome to Google.com</h1>
<form action="/search">
  <label for="search">
    Enter your search term
  </label>
  <input name="search">
</form>
```

Client-side code

HTML works by enclosing content in **tags**, where different tags have different meanings



Client-side code

Tags can be nested, for example a **table** tag contains multiple rows, each with multiple columns:

```
<table>  
  <tr>  
    <td>Name</td>  
    <td>Email</td>  
    <td>Phone</td>  
  </tr>  
</table>
```



Name	Email	Phone
------	-------	-------




[Live demo]

Client-side code

Tags can have **attributes**: key/value pairs which determine how they should be treated

```
</img>
```



Opening tags can have optional key/value attributes which change their behavior

Client-side code

HTML Demo

```
<h1>This is my website!</h1>
```

```
<label>Username</label>
```

```
<input type="text"></input>
```

```
<label>Password</label>
```

```
<input type="password"></input>
```

```
<button>Submit</button>
```

Client-side code

HTML contains two sub-languages: CSS and JavaScript

- **CSS:** Change the appearance of HTML
- **JavaScript:** Add interactivity and functionality

(CSS does not really matter for security, but we will discuss JavaScript in depth later)

Client-side code

CSS: Changes appearance. Contained in a `<style>` tag. Rarely impacts security, so we will mostly ignore it.

```
<header>Welcome to my blog!</header>
```

```
<p>Here is some content</p>
```

```
<style>
```

```
  header {
```

```
    color: green;
```

```
    background-color: red;
```

```
  }
```

```
</style>
```



Welcome to my blog!

Here is some content

Client-side code

JavaScript: A full-featured programming language. Contained within a `<script>` tag. Allows the code to perform nearly any action.

- We will cover this more in depth later on

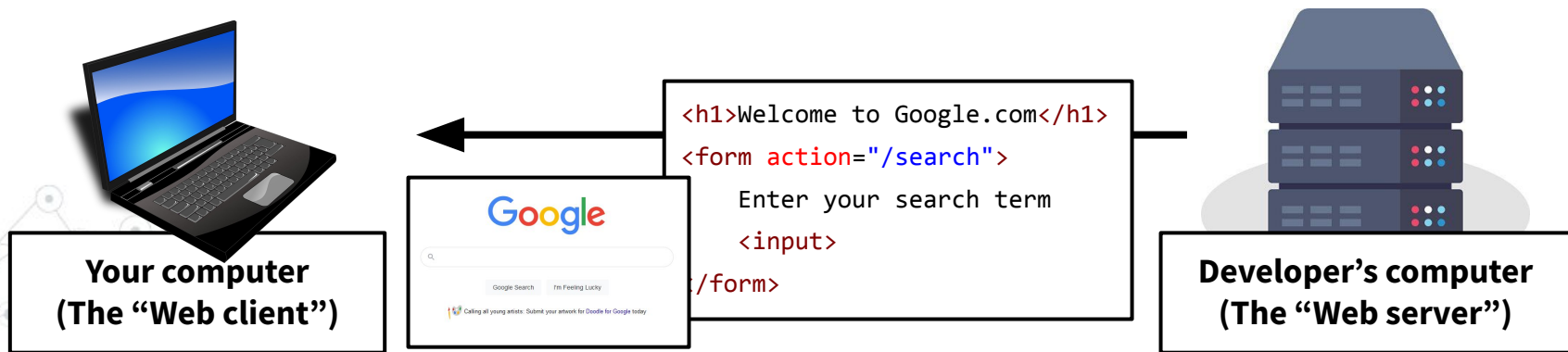
```
<button id="my_button">Click me!</button>
<script>
  my_button.onclick = function () {
    alert("You clicked the button!");
  }
</script>
```



Any security problems here?

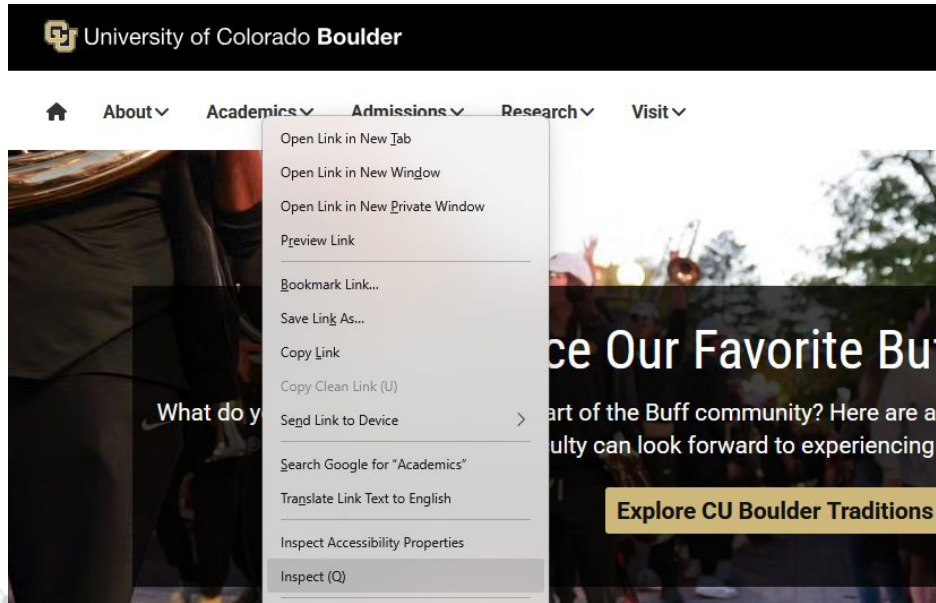
Client-side code

Once any code sent to the web client, it can be read or modified in any way by that client!



Client-side code

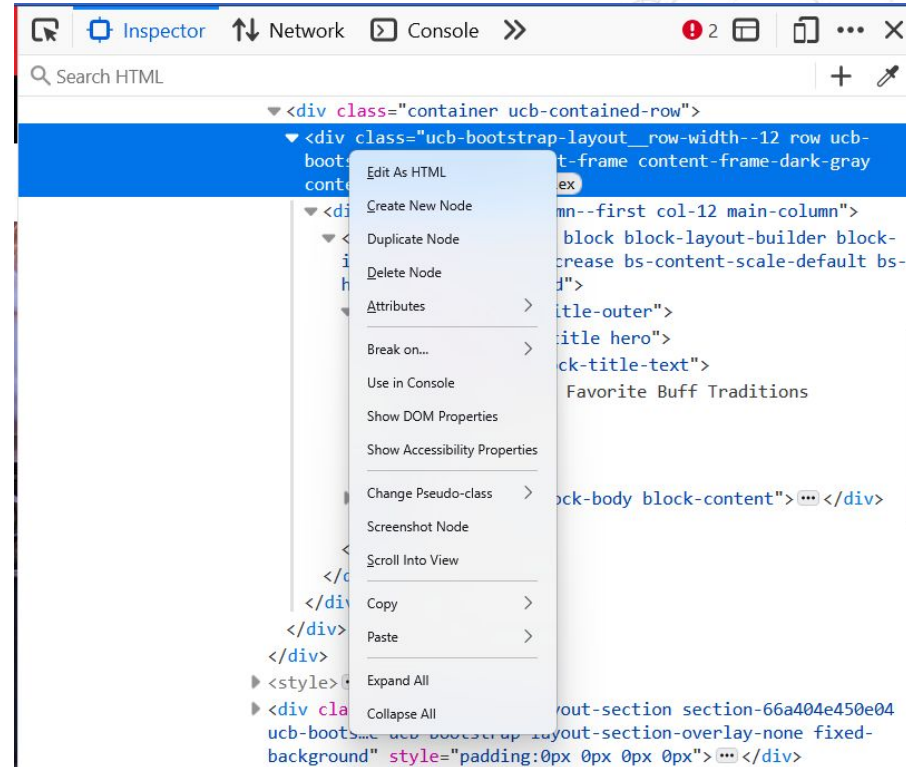
Right-click “Inspect” on a webpage will open the browser Developer Tools menu:



Client-side code

The this can be used to edit or delete HTML items

- Reloading the page will download a fresh, unmodified copy





This is a problem in real life
all the time

Client-side code

Missouri teachers' Social Security numbers at risk on state agency's website

From the Essential reading: Governor threatens Post-Dispatch after discovery of data vulnerability series

Josh Renaud Oct 14, 2021 0





Though no private information was clearly visible [...] teachers' Social Security numbers were contained in the HTML source code of the pages involved.

Client-side code

Missouri teachers' Social Security numbers at risk on state agency's website

From the Essential reading: Governor threatens Post-Dispatch after discovery of data vulnerability series

Josh Renaud Oct 14, 2021 0

This content requires a subscription!

\$1 FOR 6 MONTHS

Special Introductory Offer

SIGN UP

*offer available for new customers only

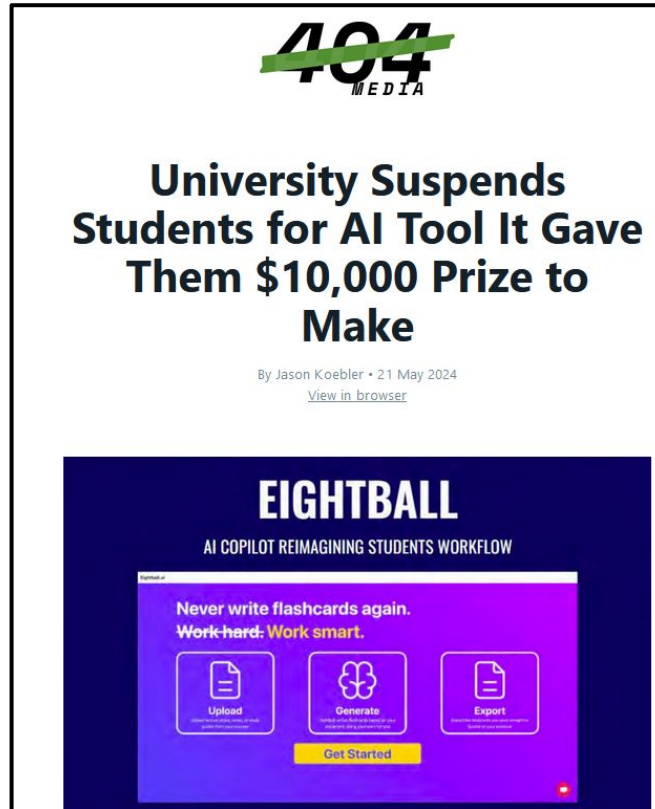
Already subscribed? [Log in](#) | [Return to homepage](#)

Client-side code

Turns out the news website I just quoted is also vulnerable...

```
cle-recommend-items', 4);
int "><div class="ad-col visible-sm"><div class="tnt-ads-container text-center hidden-print hidden-xs"><div style="min-height:90px; min-width:728px;"
xt"><p>"We have worked with our data team and the Office of Administration Information Technology Services Division to get that search tool pulled do
xt"><p>It wasn't immediately clear how long the Social Security numbers and other sensitive information had been vulnerable on the DESE website, nor
xt"><h2>'A serious flaw'</h2></div><div id="tncms-region-article_instory_top" class="tncms-region hidden-print"></div><div class="lee-article-text"><
xt"><p>The newspaper asked Shaji Khan, a cybersecurity professor at the University of Missouri-St. Louis, to confirm the findings. He called the vuln
xt"><p>Khan urged the state to perform a thorough audit to ensure no other web applications contain similar vulnerabilities.</p></div><div class="hid
xt"><p>According to McGowin, such an audit had begun Tuesday and was still underway at noon Wednesday. She said that as far as she was aware, no other
cle_instory_middle" class="tncms-region hidden-print"><div id="tncms-block-1245342" class="tncms-block"></div></div><div class="lee-article-text"><p>
xt"><p>The 2015 audit found that DESE was unnecessarily storing students' Social Security numbers and other personally identifiable information in it
xt"><p>The public has a right to see certain kinds of data about teachers because they are public employees, Clemens said. But he wants his members'
xt"><p>"We think certificated teachers deserve the same privacy rights as anybody else," he said.</p></div><div class="hidden-print"><div class="ad-
xt"><h2>100,000 at risk</h2></div><div class="lee-article-text"><p>McGowin said Tuesday that the department would discuss its findings with the newsp
><div class="ad-col visible-sm"><div class="tnt-ads-container text-center hidden-print hidden-xs"><div style="min-height:90px; min-width:728px;" clas
><div class="ad-col visible-lg visible-md"><div class="tnt-ads-container text-center hidden-print hidden-xs"><div style="min-height:250px; min-width:
xt"><p>In reality, the Post-Dispatch discovered the vulnerability and confirmed that the nine-digit numbers were indeed Social Security numbers. The
xt"><p>Post-Dispatch attorney Joseph Martineau, of Lewis Rice, responded to DESE's statements late Wednesday:</p></div><div class="hidden-print"><div
xt"><p>The reporter did the responsible thing by reporting his findings to DESE so that the state could act to prevent disclosure and misuse," Marti
xt"><p>"For DESE to deflect its failures by referring to this as 'hacking' is unfounded. Thankfully, these failures were discovered."</p></div><div c
s="asset-tagline text-muted"><!-- tagline suppressed in site component --></div><div id="lee-series-panel">
```

Client-side code



<https://www.404media.co/email/cc1d5860-9db9-4ffe-a77b-21b5e65adef9>

Alex Curtiss | CSCI 3403



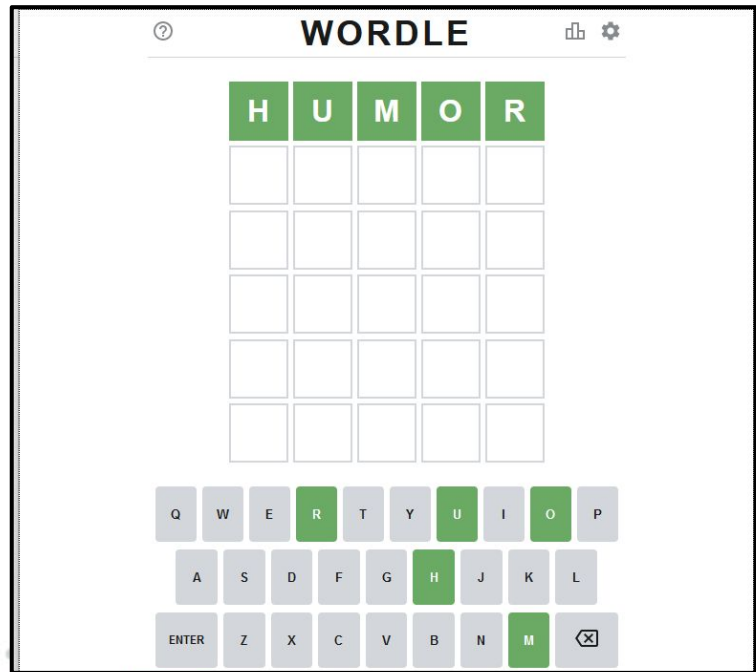
“

“the university changed the settings within Canvas and “hid the button that generates Canvas [API] tokens”

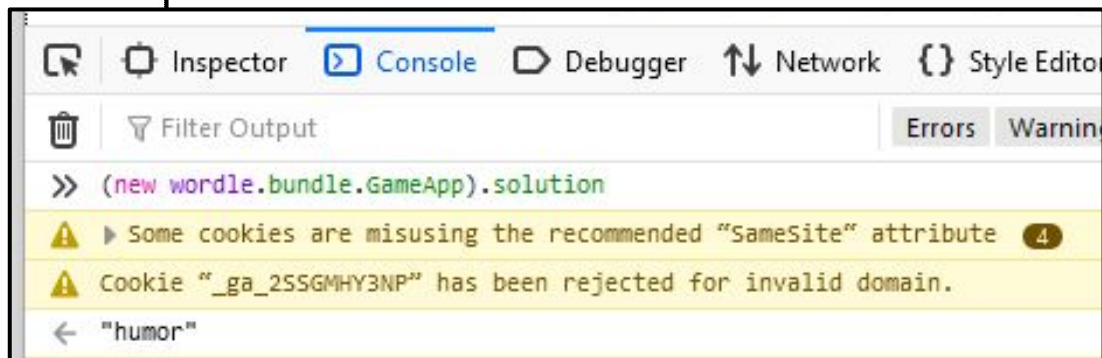
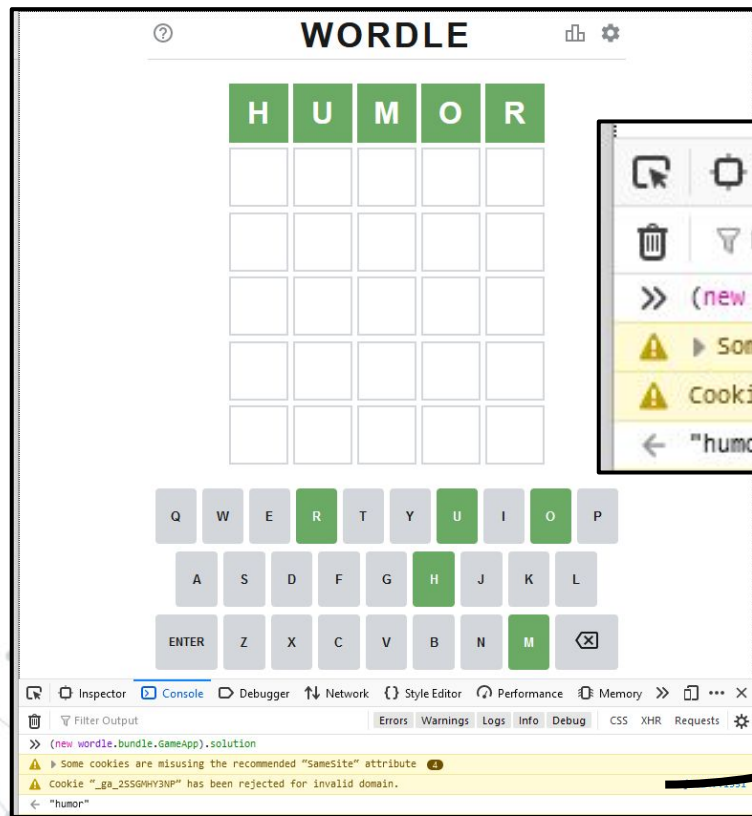


Students found a workaround [...] right clicking on the Canvas website, clicking “View Source,” and copy-pasting the credential.

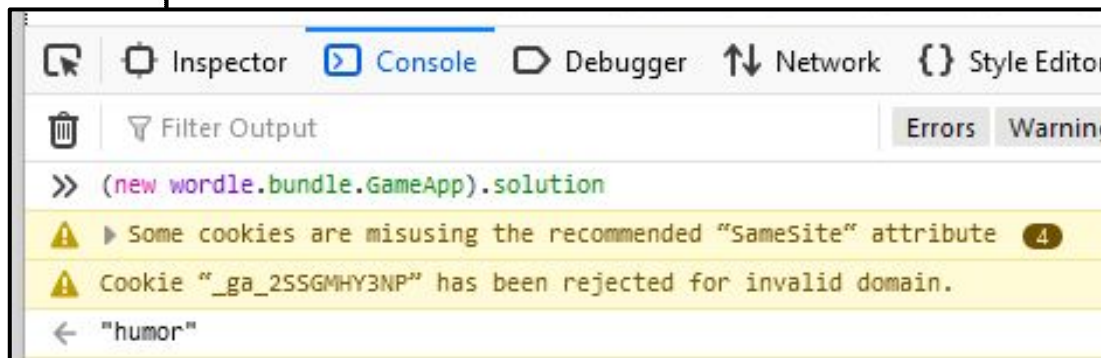
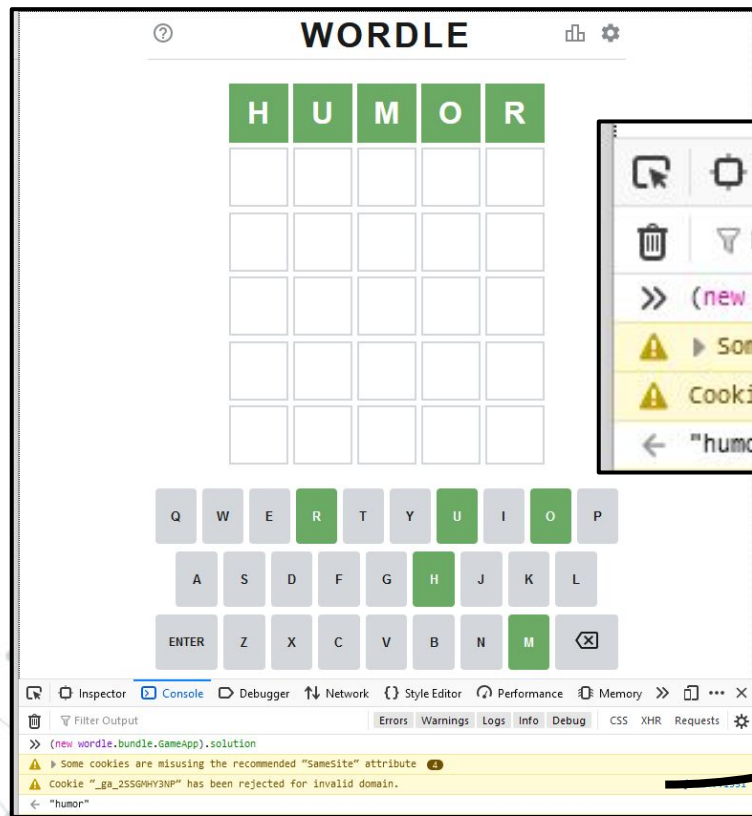
Client-side code



Client-side code



Client-side code



They have changed it so this one line no longer works, but you can still find the answers.

Recap

- **Clients and servers** and how they communicate
- **HTML:** The language web client code is written in
- **Security takeaway:** The user can easily read and modify web client code



See ya'!