Browser extensions could capture passwords and sensitive info as plain text

October 30 2023, by Jason Daley

PhD student Asmit Nayak is investigating ways that browser extensions could extract passwords and other sensitive data from popular websites. Nayak, along with fellow PhD student Rishabh Khandelwal and Kassem Fawaz, a UW–Madison associate professor of electrical and computer engineering, first discovered the issue while investigating Google login webpages. Credit: Joel Hallberg

When you type a password or credit card number into a website, you

expect that your sensitive data will be protected by a system designed to keep it secure.

That's not always the case, according to a group of digital security researchers at the University of Wisconsin–Madison. They found that some popular websites are vulnerable to browser extensions that can extract user data like passwords, credit card information and social security numbers from HTML code. A preprint of their work has already created a buzz in tech circles.

The team includes Rishabh Khandelwal and Asmit Nayak, Ph.D. students who work with Kassem Fawaz, a UW–Madison associate professor of electrical and computer engineering. The trio first discovered the issue while investigating Google login webpages.

"We were just messing around with login pages, and in the HTML source code we could see the password in plain text," says Nayak. "We thought, 'This is interesting. Why is this happening? Is it possible that other websites are doing something similar?' Then we started digging deeper."

They discovered a big issue. The researchers found that a huge number of websites—about 15% of more than 7,000 they looked at—store sensitive information as plain text in their HTML source code. While many security measures keep hackers from accessing this data, the team hypothesized that it might be possible to find it using a browser extension.

Browser extensions are add-ons that, using small bits of code, allow users to customize their internet experience, for example by blocking ads or improving time management. Browser developers sometimes introduce experimental features via extensions while also allowing third-party developers to offer their own extensions for users to try. The researchers

found that a malevolent extension could use code written in a common programming language to grab users' login information, passwords and other protected data.

"Combining what we know about extensions and about websites, an extension can very easily access users' passwords," says Fawaz. "It's not something that actually is happening, but there is nothing preventing it."

Surveying the extensions available for the Google Chrome browser, the team found that 17,300, or 12.5% of the available browser extensions, had the necessary permissions to exploit this vulnerability. To see if it was feasible for such an extension to make it into circulation, they developed their own extension and submitted it to the Chrome Web Store, describing it as an AI assistant offering ChatGPT-like functions on websites. The store approved the extension. The team was careful not to release the extension to the public and quickly deleted it after it was approved, demonstrating that it was possible for such an exploit to get in under the radar. The researchers emphasize that at no point was there any harm to users.

Khandelwal says that most likely a real hacker wouldn't follow the same path.

"Somebody who's malicious does not need to start from scratch," he says. "They can get access to existing extensions, for instance, by buying one with lots of users and tweaking the code a little bit. They could maintain the functionality and get access to the passwords very easily."

Fawaz says it's likely that the vulnerability isn't an oversight; instead, browser security is configured this way to let popular password manager extensions access password information. For its part, in a statement to the researchers, Google says that it is looking into the matter but does not consider this a security flaw, especially if permissions for the

extensions are configured correctly.

Fawaz, however, is still concerned, and he hopes his research will convince websites to rethink the way they handle this sensitive information. His team proposes alerts to let users know when sensitive data is being accessed by browser extensions, as well as tools for developers to protect these data fields.

"It's a dangerous thing," Fawaz says. "This is something that people really need to know: Passwords aren't always safe on browsers."

More information: Asmit Nayak et al, Exposing and Addressing Security Vulnerabilities in Browser Text Input Fields, *arXiv* (2023). DOI: 10.48550/arxiv.2308.16321

Provided by University of Wisconsin-Madison