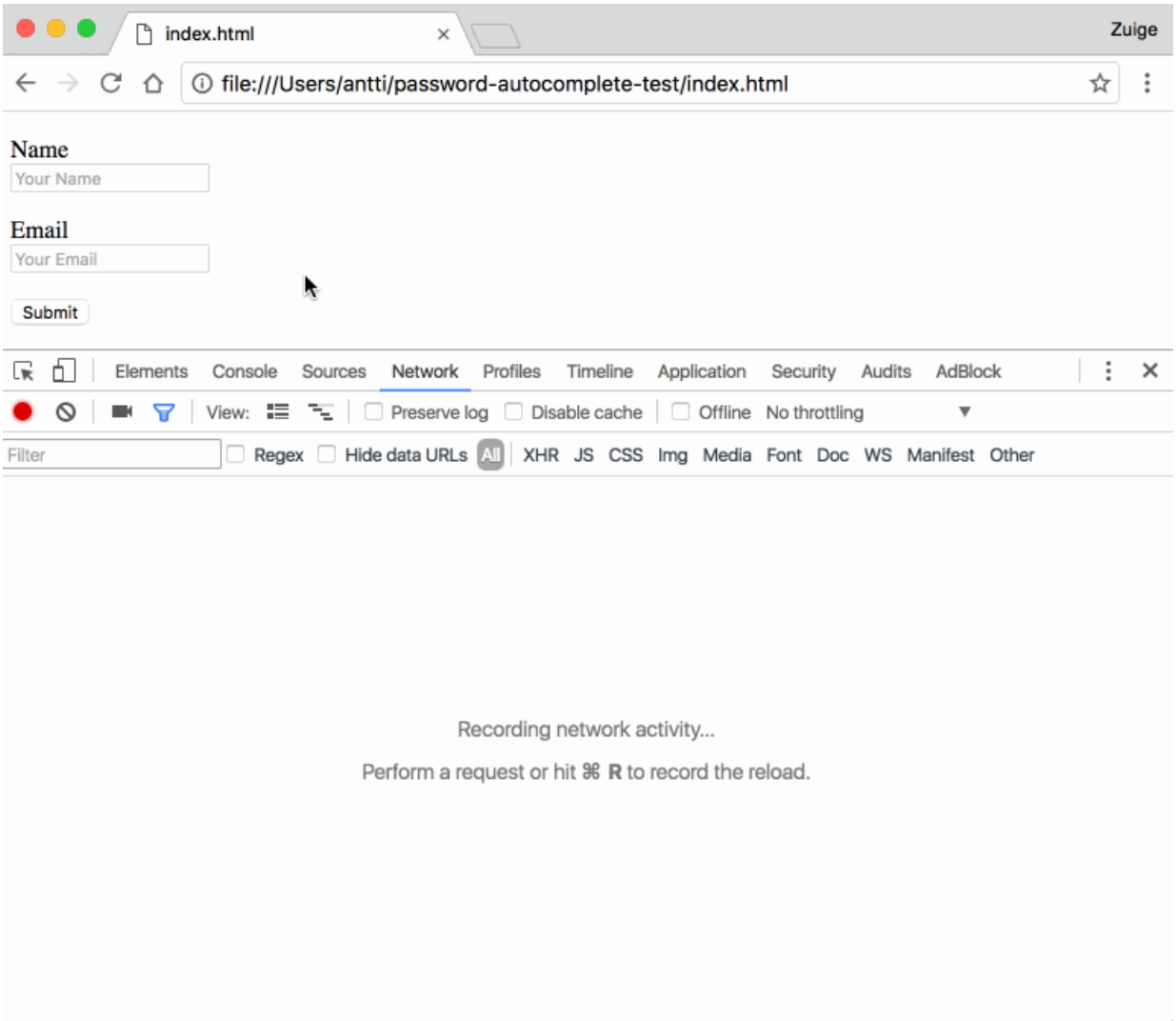
Finnish developer shows how browser autofill profiles can be exploited to leak information

January 12 2017, by Nancy Owano



(Tech Xplore)—Some phishing attack. Numerous sites this week have reported the dangers of a phishing attack made possible by the browser you use. *The Guardian* was one of the sites having a look at how private information can be leaked.

What is behind all this? Hidden text boxes. All roads lead to a trouble spot in the form of browser autofill profiles.

Autofill systems in general are designed for user convenience, so that you can avoid the tedium of having to repeat standard information, such as address. Not everyone thinks they are so grand.

Catalin Cimpanu in *BleepingComputer* looks at browser autofill profiles, an addition to modern-day browsers, as a phishing vector. Via hidden fields, attackers can collect information from users which the user unknowingly sends to the attacker when submitting a form. The user already created a profile of details entered inside web forms. So when forms have to be filled, there is preset information for form fields, which is designed to spare the user some time.

Darren Pauli in *The Register* on Tuesday detailed what goes on in such an attack effort: "The attack vector is manifest when victims select autofill while filling out registration forms: attackers hide sensitive fields like street address, date of birth, and phone number, displaying only basic entry boxes like name and email."

Cimpanu noted that, "Unless the user looks at the page's source code, he won't know that the form also contains six more fields named Phone, Organization, Address, Postal Code, City, and Country."

Finnish web developer and hacker Viljami Kuosmanen made the discovery. If clicked on a phishing site, a user's sensitive information could go into boxes the user cannot see. There is a proof of concept that

was provided by Kuosmanen.

What's the take-home? That autofill you use for convenience may reveal information to phishers using hidden text boxes on sites.

Samuel Gibbs on Tuesday in *The Guardian* noted Google's Chrome, Apple's Safari and Opera browsers were included. Reports said some plugins and add-ons may also be affected.

How did Kuosmanen spot this? In an email to *BleepingComputer*, he discussed how.

"The idea for the demo came after I was annoyed about Chrome autofilling wrong fields on an ecommerce site. I then went on to see which details Chrome had saved for autofill about me and was surprised about how much information is available," Kuosmanen added.

Then he experimented to see what was the range of form fields that Chrome would fill in. He had an idea to test hidden form fields.

"I thought it would be a good idea to demonstrate this issue as a gif," he said in *BleepingComputer*.

One interesting side note as in *The Register*: Autofilling credit card and financial data forms will trigger additional prompts and extra warnings on Chrome when sites do not offer HTTPS.

See how Firefox is missing from this list? *The Guardian* said according to a Mozilla engineer, "Mozilla's Firefox is immune to the problem, as it does not yet have a multi-box autofill system and cannot be tricked into filling text boxes by programatic means." (Several reports said Mozilla was working on the feature.)

How to avoid this kind of phishing attack: Disable the autofill system within their browser or extension settings, said Gibbs.

More information: github.com/anttiviljami/browser-autofill-phishing