

# Fourteen new types of attacks on web browsers detected

December 2 2021



Using the XSinator.com tool, the researchers analysed numerous combinations of browsers and operating systems for their vulnerability to XS-Leaks. Credit: RUB, Marquard

IT security experts have identified 14 new types of attacks on web

browsers that are known as cross-site leaks, or XS-Leaks. Using XS-Leaks, a malicious website can grab personal data from visitors by interacting with other websites in the background. The researchers from Ruhr-Universität Bochum (RUB) and Niederrhein University of Applied Sciences tested how well 56 combinations of browsers and operating systems are protected against 34 different XS-Leaks.

To this end, they developed the [website XSinator.com](https://www.xsinator.com), which allowed them to automatically scan browsers for these leaks. Popular browsers such as Chrome and Firefox, for example, were vulnerable to a large number of XS-Leaks. "XS-Leaks are often [browser](#) bugs that have to be fixed by the manufacturer," says Lukas Knittel, one of the Bochum authors of the paper.

The researchers published their findings online and at the ACM Conference on Computer and Communications Security, which was held as a virtual event in mid-November 2021. At the conference, Lukas Knittel, Dr. Christian Mainka, Dominik Noß and Professor Jörg Schwenk from the Horst Görtz Institute for IT-Security at RUB as well as Professor Marcus Niemietz from the Niederrhein University of Applied Sciences received a Best Paper Award for their study. The study took place within the Cluster of Excellence "CASA—Cyber Security in the Age of Large-Scale Adversaries."

## How XS-Leaks work

XS-Leaks bypass the so-called same-origin policy, one of a browser's main defenses against various types of attacks. The purpose of the same-origin policy is to prevent information from being stolen from a trusted website. In the case of XS-Leaks, attackers can nevertheless recognize individual details of a website. If these details are tied to [personal data](#), those data can be leaked. For example, emails in a webmail inbox could be read from a malicious site, because the search function would

respond in a different way depending on whether there were results for a search term or not.

In order to systematically analyze XS-Leaks, the group first identified three characteristics of such attacks. Based on these, they then derived a formal model that aids in understanding XS-Leaks and helps in detecting new attacks. As a result, the researchers identified 14 new attack categories.

**More information:** XSinator.com: From a Formal Model to the Automatic Evaluation of Cross-Site Leaks in Web Browsers, PDF: [xsinator.com/paper.pdf](https://xsinator.com/paper.pdf)

Provided by Ruhr-Universitaet-Bochum

Citation: Fourteen new types of attacks on web browsers detected (2021, December 2) retrieved 20 March 2024 from <https://techxplore.com/news/2021-12-fourteen-web-browsers.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--