**Browser security** is the application of [Internet security](https://en.wikipedia.org/wiki/Internet_security) to [web browsers](https://en.wikipedia.org/wiki/Web_browser) in order to protect [networked](https://en.wikipedia.org/wiki/Computer_network) data and [computer systems](https://en.wikipedia.org/wiki/Computer_system) from breaches of privacy or [malware](https://en.wikipedia.org/wiki/Malware). Security exploits of [browsers](https://en.wikipedia.org/wiki/Web_browser) often use [JavaScript](https://en.wikipedia.org/wiki/JavaScript) — sometimes with [cross-site scripting](https://en.wikipedia.org/wiki/Cross-site_scripting) (XSS)[[1]](https://en.wikipedia.org/wiki/Browser_security#cite_note-mozilla-noscript-1) — sometimes with a secondary payload using [Adobe Flash](https://en.wikipedia.org/wiki/Adobe_Flash).[[2]](https://en.wikipedia.org/wiki/Browser_security#cite_note-mozilla-betterprivacy-2) Security exploits can also take advantage of [vulnerabilities](https://en.wikipedia.org/wiki/Vulnerability_(computing)) (security holes) that are commonly exploited in all [browsers](https://en.wikipedia.org/wiki/Web_browser) (including [Mozilla Firefox](https://en.wikipedia.org/wiki/Mozilla_Firefox),[[3]](https://en.wikipedia.org/wiki/Browser_security#cite_note-Firefox_vulnerability_confirmed-3) [Google Chrome](https://en.wikipedia.org/wiki/Google_Chrome),[[4]](https://en.wikipedia.org/wiki/Browser_security#cite_note-Chrome_dirty_dozen-4) [Opera](https://en.wikipedia.org/wiki/Opera_(web_browser)),[[5]](https://en.wikipedia.org/wiki/Browser_security#cite_note-Opera_severe_hole-5) [Microsoft Internet Explorer](https://en.wikipedia.org/wiki/Microsoft_Internet_Explorer),[[6]](https://en.wikipedia.org/wiki/Browser_security#cite_note-time_to_drop_IE6-6) and [Safari](https://en.wikipedia.org/wiki/Safari_(web_browser))[[7]](https://en.wikipedia.org/wiki/Browser_security#cite_note-7)).

**Security**

Web browsers can be breached in one or more of the following ways:

* Operating system is breached and malware is reading/modifying the browser memory space in privilege mode[[8]](https://en.wikipedia.org/wiki/Browser_security#cite_note-8)
* Operating system has a malware running as a background process, which is reading/modifying the browser memory space in privileged mode
* Main browser executable can be hacked
* Browser components may be hacked
* Browser plugins can be hacked
* Browser network communications could be intercepted outside the machine[[9]](https://en.wikipedia.org/wiki/Browser_security#cite_note-9)

The browser may not be aware of any of the breaches above and may show user a safe connection is made.

Whenever a browser communicates with a website, the website, as part of that communication, collects some information about the browser (in order to process the formatting of the page to be delivered, if nothing else).[[10]](https://en.wikipedia.org/wiki/Browser_security#cite_note-10) If malicious code has been inserted into the website's content, or in a worst-case scenario, if that website has been specifically designed to host malicious code, then vulnerabilities specific to a particular browser can allow this malicious code to run processes within the browser application in unintended ways (and remember, one of the bits of information that a website collects from a browser communication is the browser's identity- allowing specific vulnerabilities to be exploited).[[11]](https://en.wikipedia.org/wiki/Browser_security#cite_note-11) Once an attacker is able to run processes on the visitor's machine, then exploiting known security vulnerabilities can allow the attacker to gain privileged access (if the browser isn't already running with privileged access) to the "infected" system in order to perform an even greater variety of malicious processes and activities on the machine or even the victim's whole network.[[12]](https://en.wikipedia.org/wiki/Browser_security#cite_note-12)