**Webpage Spoofing**

**Other names: URL spoofing, Website Spoofing**

**Description 1**

Web Spoofing is a security attack that allows an adversary to observe and modify all web pages sent to the victim's machine, and observe all information entered into forms by the victim. Web Spoofing works on both of the major browsers and is not prevented by "secure" connections. The attacker can observe and modify all web pages and form submissions, even when the browser's "secure connection" indicator is lit. The user sees no indication that anything is wrong. [1]

**Definition 2**

Website spoofing is the act of creating a website, as a hoax, with the intention of misleading readers that the website has been created by a different person or organization. Normally, the spoof website will adopt the design of the target website and sometimes has a similar URL. A more sophisticated attack results in an attacker creating a "shadow copy" of the World Wide Web by having all of the victim's traffic go through the attacker's machine, causing the attacker to obtain the victim's sensitive information. The objective may be fraudulent, or to criticize or make fun of the person or body whose website the spoofed site purports to represent. [2]

**Definition 3**

URL spoofing is the attempt to mislead a user to a different (often malicious) website by imitating or “spoofing” a legitimate URL. [3] **(not sure about this reference)**

**Reference**

[1] <http://sip.cs.princeton.edu/WebSpoofing/>

[2] <https://en.wikipedia.org/wiki/Website_spoofing>

[3] <https://www.expressvpn.com/internet-privacy/internet-security-technical-glossary/url-spoofing/>