

Clickjacking Protection

<https://campus.barracuda.com/doc/76284722/>

Clickjacking (also known as *UI redressing* and *iframe overlay*) is a malicious technique where a user is tricked into clicking on a button or link on a website using hidden clickable elements inside an invisible iframe. This attack hijacks clicks intended for the visible page and routes the user to an application and/or domain on another page. The Barracuda Web Application Firewall as a Service uses the X-Frame-Options HTTP response header to detect and prevent iframe-based clickjacking. The X-Frame-Options header is inserted to indicate whether a browser should be allowed to render a page in a iframe, and if allowed, the iframe origin that needs to be matched.

Note: If your website is rendered inside a iframe, do not enable clickjacking protection because it will prevent rendering the website inside the iframe. To prevent this issue, clickjacking protection is *not enabled* by default.

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.