

Parameter Protection

<https://campus.barracuda.com/doc/76284735/>

Parameter Protection defends web applications from attacks sent inside URL parameters.

Parameters that contain special characters might have SQL or HTML tagging expressions embedded in them. Embedded SQL keywords like `OR`, `SELECT`, or `UNION` in a parameter, or system commands such as `xp_cmdshell` can exploit web application vulnerabilities. These attack patterns can be configured in Parameter Protection, and if a web request parameter matches, the request is not processed.

© 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.