Configuring Parameter Protection

https://campus.barracuda.com/doc/17106000/

Parameter protection defends the service from attacks based on parameter values in the absence of a parameter profile. It is a replacement for the settings that can otherwise be found under a parameter profile, and applies to all parameters when profiles are not being used. It defines strict limitations in form fields and other parameters. It deep inspects user input when a FORM is submitted. This allows users to set up validation rules for FORM parameters.

Special characters such as " ' ", " ; " or ' ' are used to embed SQL expressions in parameter values. SQL keywords such as "OR," "SELECT," "UNION" can be embedded in parameter values to exploit vulnerabilities. Special characters such as '<' or keywords such as "<script>," "<img" are used to embed html tags in parameter values in the case of Cross-Site Scripting attacks. Keywords such as "xp_cmdshell" are used in System Command Injection attacks.

To configure parameter protection, go to **SECURITY > Security Policies**, select a policy, and scroll down to the **Parameter Protection** section. See the Online Help on the Barracuda Load Balancer ADC for detail instructions on how to configure parameter protection.

© 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.