

METHOD AND DEVICE FOR DETECTING INFORMATION LEAKAGE, SERVER, AND COMPUTER-READABLE STORAGE MEDIUM

[0001] The present application is the National Stage of International Application No. PCT/CN2017/089807, filed Jun.23, 2017, which claims the benefit of China Patent Application No. 201710164043.7, filed March 17, 2017 before the State Intellectual Property Office and entitled “Method and Device for Detecting Information Leakage, Server, and Computer-readable Storage Medium”, the entirety of which is hereby incorporated herein by reference.

[0002] TECHNICAL FIELD

[0003] The present disclosure relates to the technical field of information security, and more particularly relates to a method and a device for detecting information leakage, a server, and a computer-readable storage medium.

[0004] BACKGROUND

[0005] In order to guarantee user's information security, a server typically detects leakage of information through a web application vulnerability scanner. To do so, the server defines some specific keywords (e.g., “email,” or “username,”) in advance that correspond to some sensitive information, and then compares the parameter included in a scanned record against the predefined keywords, so that when any parameter that is consistent with any one of the keywords shows up in the scanned record, it would indicate that plaintext transmission of sensitive information is being used, which would also indicate the risk of information leakage. However, if the parameter “USERNAME” appears in a newly developed system http request while the specific keywords include the keyword “username” but not the keyword “USERNAME”, the parameter “USERNAME” would not be matched or identified; the same goes with the parameter “uname” that shows up in the http request leaving it unidentified, resulting in plaintext transmission of the sensitive information, hence the risk of information leakage.

[0006] Since the above method just roughly detects the presence of any plaintext transmission of sensitive information, it requires security testers to invest more efforts

advance through machine learning, and obtaining a matching degree between the parameter and the keyword based on the matching result:

matching the parameter included in the request message against the keyword obtained in advance through machine learning to determine a first matching degree between the parameter and the keyword; and

determining the matching degree between the parameter and the keyword based on the first matching degree and a context of the parameter in the request message.

20. The computer-readable storage medium according to claim 18, wherein, the computer-readable storage medium is further configured to perform the operation of matching a parameter included in the request message against a keyword obtained in advance through machine learning, and obtaining a matching degree between the parameter and the keyword based on the matching result:

splitting the parameter included in the request message into a first sub-parameter and a second sub-parameter according to keywords obtained in advance through machine learning;

matching the keywords obtained in advance through machine learning against the first sub-parameter and the second sub-parameter respectively to determine a first probability of matching between the first sub-parameter and a first keyword and a second probability of matching between the second sub-parameter and a second keyword; and

determining the matching degree between the parameter and the keyword based on the first probability, the second probability, and a context of the parameter in the request message.