CLAIMS

1. A computer implemented method for preventing a server from being attacked, the method comprising:

in response to receiving a page request sent by a browser, obtaining (201)

a page URL in the page request;

randomly extracting a page script from a plurality of page scripts that exist in a predetermined script library and are corresponding to the page URL, wherein different script execution parameter acquisition logic is used in the plurality of page scripts (202);

sending (203) the randomly extracted page script to the browser, so that the browser executes the page script to obtain a script execution parameter;

in response to receiving a page verification request sent by the browser, determining (204) whether the page verification request is expired;

in response to determining that the page verification request is expired, outputting (205a) error prompt information indicating page expiration; or

in response to determining that the page verification request is unexpired, verifying (205b) whether the script execution parameter comprised in the page verification request is valid; and

if the script execution parameter is invalid, rejecting the page request (206b).

2. The method according to claim 1, wherein the script execution parameter acquisition logic comprises obtaining a token value in encrypted cookie information.

3. The method according to claim 1, wherein before randomly extracting a page script from a plurality of page scripts that exist in a predetermined script library and are corresponding to the page URL, the method further comprises:

configuring page scripts corresponding to each page URL in the predetermined script library and identifier information corresponding to the page scripts.

4. The method according to claim 1, wherein determining whether the page verification request is expired comprises:

determining whether a request time of the page verification request is later than the sum of a

predetermined time period and a time for the browser to execute the page script; and

in response to determining that the request time of the page verification request is later than the sum of a predetermined time period and a time for the browser to execute the page script, determining that the page verification request is expired; or

in response to determining that the request time of the page verification request is not later than the sum of a predetermined time period and a time for the browser to execute the page script, determining that the page verification request is not expired.

5. The method according to any one of claims 1 to 4, wherein the page request further comprises identifier information of the page script executed by the browser, and wherein verifying whether the script execution parameter comprised in the page verification request is valid comprises:

searching the predetermined script library for a page script corresponding to the identifier information, wherein the predetermined script library further stores identifier information corresponding to each page script; and

verifying, based on the page script corresponding to the identifier information, whether the script execution parameter comprised in the page verification request is valid.

6. The method according to claim 5, wherein verifying, based on the page script corresponding to the identifier information, whether the script execution parameter comprised in the page verification request is valid comprises:

obtaining a local script parameter based on the page script corresponding to the identifier information;

determining whether the local script parameter is the same as the script execution parameter comprised in the page verification request; and

in response to determining that the local script parameter is the same as the script execution parameter comprised in the page verification request, determining that the script execution parameter is valid; or

in response to determining that the local script parameter is not the same as the script execution parameter comprised in the page verification request, determining that the script execution parameter is invalid.

7. The method according to any one of claims 1 to 6, wherein rejecting the page request is based on a user identity information included in the page verification request.

8. The method according to claim 7, wherein the user identity information comprises cookie information generated by the server.

9. A device for preventing a server from being attacked, the device comprising a plurality of modules configured to perform the method of any one of claims 1 to 8.