

CLAIMS:

1. A method of scanning website vulnerability, comprising:

reading a vulnerability scan task in a scan task pool;

finding a website corresponding to the vulnerability scan task, acquiring access data of the website, and obtaining a popularity coefficient of the website according to the access data;

acquiring historical vulnerability scan data and a vulnerability risk level table, and obtaining a security risk coefficient of the vulnerability scan task according to the historical vulnerability scan data and the vulnerability risk level table;

acquiring update time data of the vulnerability scan task, and calculating a time coefficient of the vulnerability scan task according to the update time data;

inputting the popularity coefficient, the security risk coefficient, and the time coefficient into a preset priority evaluation model for processing, and obtaining an execution priority weight of the vulnerability scan task; and

executing vulnerability scan tasks in the scan task pool in descending order according to the execution priority weights;

wherein the acquiring historical vulnerability scan data and the vulnerability risk level table, and obtaining the security risk coefficient of the vulnerability scan task according to the historical vulnerability scan data and the vulnerability risk level table comprises:

acquiring a first historical vulnerability scan data of the website corresponding to the vulnerability scan task, and obtaining a task risk characteristic value of the vulnerability scan task according to the first historical vulnerability scan data and the vulnerability risk level table;

acquiring a second historical vulnerability scan data of the scan task pool, and obtaining a website risk characteristic value of the website corresponding to the vulnerability scan task according to the second historical vulnerability scan data and the vulnerability risk level table; and

calculating the security risk coefficient of the vulnerability scan task according to the task risk characteristic value and the website risk characteristic value; and

wherein the acquiring a first historical vulnerability scan data of the website corresponding to the vulnerability scan task, and obtaining a task risk characteristic value of the vulnerability scan task according to the first historical vulnerability scan data and the vulnerability risk level table comprises:

acquiring a vulnerability attribute of a historical scan security vulnerability of the website corresponding to the vulnerability scan task;

finding a risk score corresponding to the vulnerability attribute in the vulnerability risk level table;

summing risk scores of the historical scan security vulnerabilities of the vulnerability scan task to obtain a risk value of the vulnerability scan task;

summing risk scores of the historical scan security vulnerabilities of the corresponding website to obtain a risk value of the corresponding website; and

calculating the task risk characteristic value of the vulnerability scan task according to the risk value of the corresponding website and the risk value of the vulnerability scan task.

2. The method of scanning website vulnerability of claim 1, wherein the acquiring update time data of the vulnerability scan task, and calculating the time coefficient of the vulnerability scan task according to the update time data comprises:

acquiring scan time data of all the vulnerability scan tasks in the scan task pool, and calculating a scan time characteristic value of the read vulnerability scan task according to the scan time data;

acquiring a content update time data of all the vulnerability scan tasks in the scan task pool, and calculating an update time characteristic value of the read vulnerability scan task according to the content update time data; and

obtaining the time coefficient of the read vulnerability scan task according to the scan time characteristic value and the update time characteristic value.

3. The method of scanning website vulnerability of claim 2, wherein the acquiring the content update time data of all the vulnerability scan tasks in the scan task pool, and

calculating the update time characteristic value of the read vulnerability scan task according to the content update time data comprises:

- acquiring a first time when the latest task content of the read vulnerability scan task being updated;

- finding a vulnerability scan task with the shortest task content update time interval and a vulnerability scan task with the longest task content update time interval in the scan task pool, and calculating an update time interval of the two found vulnerability scan tasks; and

- calculating the update time characteristic value according to the first time and the update time interval.

4. A device of scanning website vulnerability comprising:

- a task reading module configured to read a vulnerability scan task in a scan task pool;

- a popularity coefficient obtaining module configured to find a website corresponding to the vulnerability scan task, acquire access data of the website, and obtain a popularity coefficient of the website according to the access data;

- a security risk coefficient obtaining module configured to acquire historical vulnerability scan data and a vulnerability risk level table, and obtain a security risk coefficient of the vulnerability scan task according to the historical vulnerability scan data and the vulnerability risk level table;

- a time coefficient obtaining module configured to acquire update time data of the vulnerability scan task, and calculate a time coefficient of the vulnerability scan task according to the update time data;

- a priority weight obtaining module configured to input the popularity coefficient, the security risk coefficient, and the time coefficient into a preset priority evaluation model for processing, and obtain an execution priority weight of the vulnerability scan task; and

- a scan task execution module configured to execute vulnerability scan tasks in the scan task pool in descending order according to the execution priority weights;

wherein the security risk coefficient obtaining module comprises:

- a task risk coefficient obtaining module configured to acquire a first historical vulnerability scan data of the website corresponding to the vulnerability scan task, and obtain a task risk characteristic value of the vulnerability scan task according to the first historical vulnerability scan data and the vulnerability risk level table;

- a website risk coefficient obtaining module configured to acquire a second historical vulnerability scan data of the scan task pool, and obtain a website risk characteristic value of the website corresponding to the vulnerability scan task according to the second historical vulnerability scan data and the vulnerability risk level table; and

- a risk coefficient calculation module configured to calculate the security risk coefficient of the vulnerability scan task according to the task risk characteristic value and the website risk characteristic value; and

 - wherein the task risk coefficient obtaining module comprises:

 - an attribute obtaining module configured to acquire a vulnerability attribute of a historical scan security vulnerability of the website corresponding to the vulnerability scan task;

 - a score searching module configured to find a risk score corresponding to the vulnerability attribute in the vulnerability risk level table;

 - a task risk value obtaining module configured to sum risk scores of the historical scan security vulnerabilities of the vulnerability scan task to obtain a risk value of the vulnerability scan task;

 - a website risk value obtaining module configured to sum risk scores of the historical scan security vulnerabilities of the corresponding website to obtain a risk value of the corresponding website; and

 - a risk characteristic value calculation module configured to calculate the task risk characteristic value of the vulnerability scan task according to the risk value of the corresponding website and the risk value of the vulnerability scan task.

5. The device of scanning website vulnerability of claim 4, wherein the time coefficient obtaining module comprises:

a scan time coefficient obtaining module configured to acquire scan time data of all the vulnerability scan tasks in the scan task pool, and calculate a scan time characteristic value of the read vulnerability scan task according to the scan time data;

an update time coefficient obtaining module configured to acquire a content update time data of all the vulnerability scan tasks in the scan task pool, and calculate an update time characteristic value of the read vulnerability scan task according to the content update time data; and

a time coefficient calculation module configured to obtain the time coefficient of the read vulnerability scan task according to the scan time characteristic value and the update time characteristic value.

6. The device of scanning website vulnerability of claim 4, wherein the time coefficient obtaining module comprises:

a scan time coefficient obtaining module configured to acquire scan time data of all the vulnerability scan tasks in the scan task pool, and calculate a scan time characteristic value of the read vulnerability scan task according to the scan time data;

an update time coefficient obtaining module configured to acquire a content update time data of all the vulnerability scan tasks in the scan task pool, and calculate an update time characteristic value of the read vulnerability scan task according to the content update time data; and

a time coefficient calculation module configured to obtain the time coefficient of the read vulnerability scan task according to the scan time characteristic value and the update time characteristic value.

7. The apparatus according to claim 6, wherein the update time coefficient obtaining module comprises:

a first time acquiring module configured to acquire a first time when the latest

task content of the read vulnerability scan task being updated;

an update time interval calculation module configured to find a vulnerability scan task with the shortest task content update time interval and a vulnerability scan task with the longest task content update time interval in the scan task pool, and calculate an update time interval of the two found vulnerability scan tasks; and

an update characteristic value calculation module configured to calculate the update time characteristic value according to the first time and the update time interval.

8. A server comprising:

one or more processors, and

a memory storing computer readable instructions, which, when executed by the one or more processors cause the one or more processors to perform steps comprising:

reading a vulnerability scan task in a scan task pool;

finding a website corresponding to the vulnerability scan task, acquiring access data of the website, and obtaining a popularity coefficient of the website according to the access data;

acquiring historical vulnerability scan data and a vulnerability risk level table, and obtaining a security risk coefficient of the vulnerability scan task according to the historical vulnerability scan data and the vulnerability risk level table;

acquiring update time data of the vulnerability scan task, and calculating a time coefficient of the vulnerability scan task according to the update time data;

inputting the popularity coefficient, the security risk coefficient, and the time coefficient into a preset priority evaluation model for processing, and obtaining an execution priority weight of the vulnerability scan task; and

executing vulnerability scan tasks in the scan task pool in descending order according to the execution priority weights;

wherein the memory further comprises instructions, which, when executed by the processor, cause the processor to perform steps comprising:

acquiring a first historical vulnerability scan data of the website corresponding to the vulnerability scan task, and obtaining a task risk characteristic value of the vulnerability scan task according to the first historical vulnerability scan data and the vulnerability risk level table;

acquiring a second historical vulnerability scan data of the scan task pool, and obtaining a website risk characteristic value of the website corresponding to the vulnerability scan task according to the second historical vulnerability scan data and the vulnerability risk level table; and

calculating the security risk coefficient of the vulnerability scan task according to the task risk characteristic value and the website risk characteristic value; and

wherein a bill information comprises an enterprise identifier, a bill identifier, a bill amount, and a bill time, an account information comprises a enterprise identifier and an account amount; and the memory further comprises instructions, which, when executed by the processor, cause the processor to perform steps comprising:

acquiring a vulnerability attribute of a historical scan security vulnerability of the website corresponding to the vulnerability scan task;

finding a risk score corresponding to the vulnerability attribute in the vulnerability risk level table;

summing risk scores of the historical scan security vulnerabilities of the vulnerability scan task to obtain a risk value of the vulnerability scan task; and

summing risk scores of the historical scan security vulnerabilities of the corresponding website to obtain a risk value of the corresponding website; and

calculating the task risk characteristic value of the vulnerability scan task according to the risk value of the corresponding website and the risk value of the vulnerability scan task.

9. The server of claim 8, wherein the memory further comprises instructions, which, when executed by the processor, cause the processor to perform steps comprising:

acquiring scan time data of all the vulnerability scan tasks in the scan task pool, and calculating a scan time characteristic value of the read vulnerability scan task

according to the scan time data;

acquiring a content update time data of all the vulnerability scan tasks in the scan task pool, and calculating an update time characteristic value of the read vulnerability scan task according to the content update time data; and

obtaining the time coefficient of the read vulnerability scan task according to the scan time characteristic value and the update time characteristic value.

10. The server of claim 9, wherein the memory further comprises instructions, which, when executed by the processor, cause the processor to perform steps comprising:

acquiring a first time when the latest task content of the read vulnerability scan task being updated;

finding a vulnerability scan task with the shortest task content update time interval and a vulnerability scan task with the longest task content update time interval in the scan task pool, and calculating an update time interval of the two found vulnerability scan tasks; and

calculating the update time characteristic value according to the first time and the update time interval.

11. At least one non-transitory computer readable storage medium comprising computer readable instructions, which, when executed by one or more processors, cause the one or more processors to perform steps comprising:

reading a vulnerability scan task in a scan task pool;

finding a website corresponding to the vulnerability scan task, acquiring access data of the website, and obtaining a popularity coefficient of the website according to the access data;

acquiring historical vulnerability scan data and a vulnerability risk level table, and obtaining a security risk coefficient of the vulnerability scan task according to the historical vulnerability scan data and the vulnerability risk level table;

acquiring update time data of the vulnerability scan task, and calculating a time coefficient of the vulnerability scan task according to the update time data;

inputting the popularity coefficient, the security risk coefficient, and the time coefficient into a preset priority evaluation model for processing, and obtaining an execution priority weight of the vulnerability scan task; and

executing vulnerability scan tasks in the scan task pool in descending order according to the execution priority weights;

wherein the computer readable instructions, which, when executed by one or more processors, cause the one or more processors to perform steps comprising:

acquiring a first historical vulnerability scan data of the website corresponding to the vulnerability scan task, and obtaining a task risk characteristic value of the vulnerability scan task according to the first historical vulnerability scan data and the vulnerability risk level table;

acquiring a second historical vulnerability scan data of the scan task pool, and obtaining a website risk characteristic value of the website corresponding to the vulnerability scan task according to the second historical vulnerability scan data and the vulnerability risk level table; and

calculating the security risk coefficient of the vulnerability scan task according to the task risk characteristic value and the website risk characteristic value; and

wherein the computer readable instructions, which, when executed by one or more processors, cause the one or more processors to perform steps comprising:

acquiring a vulnerability attribute of a historical scan security vulnerability of the website corresponding to the vulnerability scan task;

finding a risk score corresponding to the vulnerability attribute in the vulnerability risk level table;

summing risk scores of the historical scan security vulnerabilities of the vulnerability scan task to obtain a risk value of the vulnerability scan task; and

summing risk scores of the historical scan security vulnerabilities of the corresponding website to obtain a risk value of the corresponding website; and

calculating the task risk characteristic value of the vulnerability scan task according to the risk value of the corresponding website and the risk value of the vulnerability scan task.

12. The storage medium of claim 11, wherein the computer readable instructions, which, when executed by one or more processors, cause the one or more processors to perform steps comprising:

- acquiring scan time data of all the vulnerability scan tasks in the scan task pool, and calculating a scan time characteristic value of the read vulnerability scan task according to the scan time data;

- acquiring a content update time data of all the vulnerability scan tasks in the scan task pool, and calculating an update time characteristic value of the read vulnerability scan task according to the content update time data; and

- obtaining the time coefficient of the read vulnerability scan task according to the scan time characteristic value and the update time characteristic value.

13. The storage medium of claim 11, wherein the computer readable instructions, which, when executed by one or more processors, cause the one or more processors to perform steps comprising:

- acquiring a first time when the latest task content of the read vulnerability scan task being updated;

- finding a vulnerability scan task with the shortest task content update time interval and a vulnerability scan task with the longest task content update time interval in the scan task pool, and calculating an update time interval of the two found vulnerability scan tasks; and

- calculating the update time characteristic value according to the first time and the update time interval.