

明 細 書

発明の名称：

ウェブサイトの脆弱性を検査するためのシステム、方法、及びプログラム
技術分野

[0001] 本発明は、ウェブサイトの脆弱性を検査するためのシステム、方法、及びプログラムに関するものである。

背景技術

[0002] 従来、ウェブサイトの脆弱性を検査するための様々な技術が提案されている。例えば、下記特許文献1は、ウェブサイトとブラウザとの通信内容を取得し、当該通信内容に含まれるパラメータに基づいて、ウェブサイトに内在する脆弱性を分析することを開示している。こうしたパラメータに基づく脆弱性の検出は、典型的には、当該パラメータに対して、予め準備された検出パターンを適用したリクエストを送信し、当該リクエストに対するレスポンスの内容に基づいて行われる。検出パターンは、例えば、SQLインジェクションの脆弱性の場合における「'」（シングルクォート1つ）等であり、データベースへの命令文を構成する入力値等を含む。

先行技術文献

特許文献

[0003] 特許文献1：特開2004-310267号公報

発明の概要

発明が解決しようとする課題

[0004] しかしながら、上述したような従来のアプローチでは、不正な入力値に対する不具合を検出することが可能となるものの、入力値が不正でない場合の不具合を検出することはできず、例えば、仕様上、許容されない変更（例えば、商品を購入するための画面において、商品の価格を1000円から100円へと変更する等）を検出することはできなかった。

[0005] 本発明の実施形態は、ウェブサイトの様々な脆弱性の検査を支援すること

を目的の一つとする。本発明の実施形態の他の目的は、本明細書全体を参照することにより明らかとなる。

課題を解決するための手段

[0006] 本発明の一実施形態に係るシステムは、1又は複数のコンピュータプロセッサを備え、ウェブサイトの脆弱性を検査するためのシステムであって、前記1又は複数のコンピュータプロセッサは、前記ウェブサイトに含まれるウェブページのページ情報を取得するステップと、前記ページ情報に基づいて、前記ウェブサイト、前記ウェブページ、及び、前記ウェブページにおけるパラメータの少なくとも1つの種別を判定するステップと、前記少なくとも1つの種別に基づいて、前記ウェブサイトの脆弱性を検査するステップと、を実行する。

[0007] 本発明の一実施形態に係る方法は、1又は複数のコンピュータによって実行され、ウェブサイトの脆弱性を検査するための方法であって、前記ウェブサイトに含まれるウェブページのページ情報を取得するステップと、前記ページ情報に基づいて、前記ウェブサイト、前記ウェブページ、及び、前記ウェブページにおけるパラメータの少なくとも1つの種別を判定するステップと、前記少なくとも1つの種別に基づいて、前記ウェブサイトの脆弱性を検査するステップと、を備える。

[0008] 本発明の一実施形態に係るプログラムは、ウェブサイトの脆弱性を検査するためのプログラムであって、1又は複数のコンピュータに、前記ウェブサイトに含まれるウェブページのページ情報を取得するステップと、前記ページ情報に基づいて、前記ウェブサイト、前記ウェブページ、及び、前記ウェブページにおけるパラメータの少なくとも1つの種別を判定するステップと、前記少なくとも1つの種別に基づいて、前記ウェブサイトの脆弱性を検査するステップと、を実行させる。

発明の効果

[0009] 本発明の様々な実施形態は、ウェブサイトの様々な脆弱性の検査を支援する。

図面の簡単な説明

- [0010] [図1]本発明の一実施形態に係る脆弱性検査サーバ10を含むネットワークの構成を概略的に示す構成図。
- [図2]検査ルール管理テーブル152が管理する情報を例示する図。
- [図3]検査管理テーブル154が管理する情報を例示する図。
- [図4]ページ情報管理テーブル156が管理する情報を例示する図。
- [図5]ウェブサイトの脆弱性を検査する際に脆弱性検査サーバ10が実行する処理を例示するフローチャート。
- [図6]対象サイト設定画面50を例示する図。
- [図7]画面遷移を設定する際に脆弱性検査サーバ10が実行する処理を例示するフローチャート。
- [図8]検査ルールに基づく検査を行う際にサーバ10が実行する処理を例示するフローチャート。

発明を実施するための形態

- [0011] 以下、図面を参照しながら、本発明の実施形態について説明する。各図面において、同一の又は類似する構成要素に対しては同一の参照符号が付され得る。
- [0012] 図1は、本発明の一実施形態に係る脆弱性検査サーバ10を含むネットワークの構成を概略的に示す構成図である。サーバ10は、図示するように、インターネット等の通信ネットワーク20を介してユーザ端末30と通信可能に接続されている。図1においては、1つのユーザ端末30のみが図示されているが、サーバ10は、複数のユーザ端末30と通信可能に接続されている。脆弱性検査サーバ10は、ユーザ端末30を操作するユーザに対して、当該ユーザによって指定されるウェブサイト22等の脆弱性（情報セキュリティ上の欠陥）を検査する脆弱性検査サービスを提供する。脆弱性検査サーバ10は、本発明のシステムの全部又は一部を実装する装置の一例である。
- [0013] まず、脆弱性検査サーバ10のハードウェア構成について説明する。脆弱

性検査サーバ１０は、一般的なコンピュータとして構成されており、図１に示すように、コンピュータプロセッサ１１と、メインメモリ１２と、入出力Ｉ／Ｆ１３と、通信Ｉ／Ｆ１４と、ストレージ（記憶装置）１５とを備え、これらの各構成要素が図示しないバス等を介して電氣的に接続されている。

[0014] コンピュータプロセッサ１１は、ＣＰＵ又はＧＰＵ等として構成され、ストレージ１５等に記憶されている様々なプログラムをメインメモリ１２に読み込んで、当該プログラムに含まれる各種の命令を実行する。メインメモリ１２は、例えば、ＤＲＡＭ等によって構成される。

[0015] 入出力Ｉ／Ｆ１３は、操作者等との間で情報をやり取りするための各種の入出力装置を含む。入出力Ｉ／Ｆ１３は、例えば、キーボード、ポインティングデバイス（例えば、マウス、タッチパネル等）等の情報入力装置、マイクロフォン等の音声入力装置、カメラ等の画像入力装置を含む。また、入出力Ｉ／Ｆ１３は、ディスプレイ等の画像出力装置、スピーカー等の音声出力装置を含む。

[0016] 通信Ｉ／Ｆ１４は、ネットワークアダプタ等のハードウェア、各種の通信用ソフトウェア、又はこれらの組み合わせとして実装され、通信ネットワーク２０等を介した有線又は無線の通信を実現できるように構成されている。

[0017] ストレージ１５は、例えば、磁気ディスク又はフラッシュメモリ等によって構成される。ストレージ１５は、オペレーティングシステムを含む様々なプログラム及び各種データ等を記憶する。例えば、ストレージ１５は、図１に示すように、脆弱性の検査に用いられる検査ルールに関する情報を管理する検査ルール管理テーブル１５２と、検査に関する情報を管理する検査管理テーブル１５４と、検査対象のウェブサイトに含まれるウェブページに関するページ情報を管理するページ情報管理テーブル１５６と、を有する。これらのテーブルは、その一部が１つのテーブルに統合されてもよいし、複数のテーブルに分割されてもよい。

[0018] また、例えば、ストレージ１５は、本発明の一実施形態に係るサーバ側プログラム４０を記憶する。当該プログラム４０は、サーバ１０を、脆弱性検

査サービスを提供するためのシステムの全部又は一部として機能させるためのプログラムである。サーバ側プログラム40の少なくとも一部は、後述する端末側プログラム42を介して、ユーザ端末30側において実行されるように構成され得る。

[0019] 本実施形態において、脆弱性検査サーバ10は、それぞれが上述したハードウェア構成を有する複数のコンピュータを用いて構成され得る。例えば、サーバ10は、複数のサーバ装置によって構成される。

[0020] このように構成された脆弱性検査サーバ10は、ウェブサーバ及びアプリケーションサーバとしての機能を有するように構成することができ、ユーザ端末30からの要求に応答して各種の処理を実行し、当該処理の結果に応じた画面データ（例えば、HTMLデータ）及び制御データ等をユーザ端末30に対して送信する。ユーザ端末30では、受信したデータに基づくウェブページ又はその他の画面が出力される。

[0021] 次に、ユーザ端末30のハードウェア構成について説明する。ユーザ端末30は、一般的なコンピュータとして構成されており、図1に示すように、コンピュータプロセッサ31と、メインメモリ32と、入出力I/F33と、通信I/F34と、ストレージ（記憶装置）35とを備え、これらの各構成要素が図示しないバス等を介して電氣的に接続されている。

[0022] コンピュータプロセッサ31は、CPU又はGPU等として構成され、ストレージ35等に記憶されている様々なプログラムをメインメモリ32に読み込んで、当該プログラムに含まれる各種の命令を実行する。メインメモリ32は、例えば、DRAM等によって構成される。

[0023] 入出力I/F33は、操作者等との間で情報をやり取りするための各種の入出力装置を含む。入出力I/F33は、例えば、キーボード、ポインティングデバイス（例えば、マウス、タッチパネル等）等の情報入力装置、マイクロフォン等の音声入力装置、カメラ等の画像入力装置を含む。また、入出力I/F33は、ディスプレイ等の画像出力装置、スピーカー等の音声出力装置を含む。

- [0024] 通信 I / F 3 4 は、ネットワークアダプタ等のハードウェア、各種の通信ソフトウェア、及びこれらの組み合わせとして実装され、通信ネットワーク 2 0 等を介した有線又は無線の通信を実現できるように構成されている。
- [0025] ストレージ 3 5 は、例えば、磁気ディスク又はフラッシュメモリ等によって構成される。ストレージ 3 5 は、オペレーティングシステムを含む様々なプログラム及び各種データ等を記憶する。ストレージ 3 5 が記憶するプログラムは、アプリケーションマーケット等からダウンロードされてインストールされ得る。また、ストレージ 3 5 は、上述した端末側プログラム 4 2 を記憶する。当該プログラム 4 2 は、ウェブブラウザ、又は、その他のアプリケーション（例えば、本実施形態の脆弱性検査サービス用の端末側アプリケーション等）として構成され、上述したように、サーバ側プログラム 4 0 の少なくとも一部を実行するように構成され得る。
- [0026] 本実施形態において、ユーザ端末 3 0 は、スマートフォン、タブレット端末、又はパーソナルコンピュータ等として構成され得る。
- [0027] このように構成されたユーザ端末 3 0 を操作するユーザは、ストレージ 3 5 等にインストールされている端末側プログラム 4 2 を介したサーバ 1 0 との通信を実行することによって、当該サーバ 1 0 が提供する脆弱性検査サービスを利用することができる。
- [0028] 次に、このように構成された脆弱性検査サーバ 1 0 が有する機能について説明する。サーバ 1 0 のコンピュータプロセッサ 1 1 は、図 1 に示すように、メインメモリ 1 2 に読み込まれたプログラム（例えば、サーバ側プログラム 4 0 の少なくとも一部）に含まれる命令を実行することによって、管理機能制御部 1 1 2、ページ情報取得部 1 1 4、ページ情報解析部 1 1 6、及び、検査制御部 1 1 8 として機能するように構成されている。
- [0029] 管理機能制御部 1 1 2 は、脆弱性検査サービスの管理機能の制御に関する様々な処理を実行するように構成されている。例えば、管理機能制御部 1 1 2 は、当該管理機能に関する様々な画面の画面データ及び制御データ等をユーザ端末 3 0 に対して送信し、ユーザ端末 3 0 において出力される当該画面

を介したユーザによる操作入力に応答して様々な処理を実行し、当該処理の結果に応じた画面データ及び制御データ等をユーザ端末30に対して送信する。管理機能制御部112によって制御される管理機能は、例えば、ログイン処理（ユーザ認証）、課金制御、及び、ユーザアカウントの管理等を含む。

[0030] ページ情報取得部114は、検査対象のウェブサイト22に含まれる各ウェブページに関するページ情報を取得するように構成されている。例えば、ページ情報取得部114は、これらの複数のウェブページを巡回してページ情報を取得する。当該巡回は、ページ情報取得部114によって自動的に行われ、又は、ユーザ端末30のユーザによる手動操作を伴って行われる。取得したページ情報は、例えば、ページ情報管理テーブル154において管理される。ページ情報は、ウェブページに関する様々な情報を含み、例えば、HTMLデータ、及び、リクエストパラメータの名称及び値等を含む。

[0031] ページ情報解析部116は、ページ情報の解析に関する様々な処理を実行するように構成されている。例えば、ページ情報解析部116は、各ウェブページのページ情報に基づいて、ウェブサイト22、各ウェブページ、及び、当該ウェブページにおけるパラメータの少なくとも1つの種別（例えば、意味、用途、又は、機能等と言うこともできる。）を判定するように構成されている。こうした種別は、例えば、ルールベース、又は、機械学習によるモデル（例えば、ストレージ15等に格納される。）を介して判定される。例えば、機械学習によって生成される学習済みモデルは、ページ情報が入力されると、上述した種別を判定するための情報を出力するように構成される。学習済みモデルは、大規模言語モデルを含む。

[0032] 検査制御部118は、ウェブサイト22の脆弱性の検査を制御するための様々な処理を実行するように構成されている。例えば、検査制御部118は、ウェブサイト22、各ウェブページ、及び、当該ウェブページにおけるパラメータの少なくとも1つの種別に基づいて、ウェブサイト22の脆弱性を検査するように構成されている。例えば、検査制御部118は、こうした種

別に対応する検査ルールに従って、ウェブサイト22の脆弱性を検査する（例えば、検査ルールとして設定されている検査パターンが適用されたHTTPリクエストをウェブサイト22に対して送信し、当該ウェブサイト22から受信したHTTPレスポンスの内容に基づいて、対応する検査項目についての脆弱性を判定する。）。例えば、検査制御部118は、ウェブサイト22の種別、及び、各ウェブページの種別の組合せに対応する検査ルールに従って、ウェブサイト22の脆弱性を検査する。

[0033] このように、本実施形態における脆弱性検査サーバ10は、ウェブサイト22に含まれる複数のウェブページの各々のページ情報に基づいて、ウェブサイト22、各ウェブページ、及び／又は、各ウェブページにおけるパラメータの種別を判定し、こうした種別に基づいてウェブサイト22の脆弱性を検査するから、単なる不正な入力値に対する不具合のほか、ウェブサイト、ウェブページ、又は、パラメータの意味、用途、及び、機能等に応じた適切な検査を行うことが可能となる。つまり、サーバ10は、ウェブサイトの様々な脆弱性の検査を支援する。

[0034] また、検査制御部118は、ウェブサイト22に含まれる複数のウェブページの中から所定種別のウェブページを特定し、当該ウェブページに対する所定操作を介して、ウェブサイト22の脆弱性を検査するように構成され得る。所定操作は、脆弱性を検査するための様々な操作を含み、典型的には、HTTPリクエストの送信を伴う。こうした構成は、特定の種別のウェブページに対する所定操作を介した脆弱性の検査を可能とする。

[0035] この場合、検査制御部118は、予め定められた複数の検査ルールの中から、ウェブサイト22の種別に対応する検査ルールを特定し、ウェブサイト22に含まれる複数のウェブページの中から、特定された検査ルールに対応する所定種別のウェブページを特定するように構成され得る。各検査ルールに対応するウェブサイト22の種別は、例えば、検査ルール管理テーブル152において管理される。こうした構成は、ウェブサイト22の種別に基づく検査ルールに対応する種別のウェブページに対する所定操作を介した脆弱

性の検査を可能とする。

[0036] 本実施形態において、検査制御部 118 は、各ウェブページにおける複数のパラメータの中から所定種別のパラメータを特定し、当該ウェブページに対する所定操作であって、特定したパラメータの値の変更を伴う当該所定操作を介して、ウェブサイト 22 の脆弱性を検査するように構成され得る。こうした構成は、所定種別のパラメータの値の変更を伴う所定操作を介した脆弱性の検査を可能とする。

[0037] この場合、検査制御部 118 は、ウェブページに対する所定操作に応じて遷移する遷移先のウェブページのページ情報に基づいて、ウェブサイト 22 の脆弱性を検査するように構成され得る。例えば、検査制御部 118 は、遷移先のウェブページのページ情報に基づいて、所定操作の操作結果（例えば、正常終了か否か）を判定し、当該判定結果に基づいて、当該所定操作に関する脆弱性を判定するように構成される。こうした構成は、所定操作に応じた遷移先のウェブページのページ情報に基づく脆弱性の検査を可能とする。

[0038] また、検査制御部 118 は、各ウェブページのページ情報を所定の学習済みモデルに入力し、当該所定の学習済みモデルから出力されるウェブサイト 22 の脆弱性を示す脆弱性スコアを取得するように構成され得る。当該学習済みモデルは、例えば、多量の訓練データを用いた機械学習を介して生成され、ページ情報が入力されると、対応するウェブサイト 22 の脆弱性スコアが出力されるように構成される。当該学習済みモデルは、例えば、ストレージ 15 等に格納される。こうした構成は、ページ情報及び学習済みモデルを用いた脆弱性スコアの取得を可能とする。

[0039] この場合、検査制御部 118 は、取得した脆弱性スコアが閾値未満である場合、当該スコアを検査結果とする一方、当該脆弱性スコアが閾値以上である場合、ウェブページに対する所定操作を介して、ウェブサイト 22 の脆弱性を検査するように構成され得る。こうした構成は、脆弱性スコアが小さい（脆弱性の深刻度が低い）場合に、ウェブページに対する所定操作を介した検査を回避することを可能とする。

- [0040] 次に、このような機能を有する本実施形態の脆弱性検査サーバ 10 の一態様としての具体例について説明する。まず、この例において、各テーブルが管理する情報について説明する。図 2 は、この例において、検査ルール管理テーブル 152 が管理する情報を例示する。この例における検査ルール管理テーブル 152 は、脆弱性の検査に適用される検査ルールに関する情報を管理し、図示するように、個別の検査ルールを識別する「検査ルール ID」に対応付けて、この検査ルールが適用されるウェブサイトの種別を示す「サイト種別」、この検査ルールが適用されるウェブページの機能（種別）を示す「ページ機能」、この検査ルールが適用されるパラメータの種別を示す「パラメータ種別」、検査方法に関する情報である「検査方法情報」、検査結果の判定方法に関する情報である「結果判定方法情報」等の情報を管理する。これらの情報は、脆弱性検査サービスの提供者によって、予め設定される。
- [0041] 図 3 は、この例において、検査管理テーブル 154 が管理する情報を例示する。この例における検査管理テーブル 154 は、検査の案件に関する情報を管理し、図示するように、個別の検査（案件）を識別する「検査 ID」に対応付けて、検査対象のウェブサイトの検査の起点となるトップ画面（トップページ）の URL である「トップ画面 URL」、検査の実行日時である「検査実行日時」等の情報を管理する。
- [0042] 図 4 は、この例において、ページ情報管理テーブル 156 が管理する情報を例示する。この例におけるページ情報管理テーブル 156 は、検査対象のウェブサイトにおける複数の画面（ウェブページ）のうち、検査の際の画面遷移に含まれる各画面に関する情報を管理し、図示するように、個別の検査を識別する「検査 ID」及び検査対象のウェブサイトにおいて個別の画面を識別する「画面 ID」の組合せに対応付けて、当該画面の URL である「画面 URL」、当該画面の「HTML データ」、当該画面において送信されるリクエストパラメータに関する情報（名称及び値）である「パラメータ情報」、画面遷移における当該画面の遷移元に関する情報（遷移元の画面の画面 ID、及び、遷移元の画面要素の要素 ID 等）である「遷移元情報」、当該

画面の検査結果に関する情報である「検査結果情報」等の情報を管理する。
この例において、検査の際の画面遷移は、詳しくは後述するが、サーバ１０によって自動的に設定される。

[0043] 以上、この例において、各テーブルが管理する情報について説明した。次に、この例において、脆弱性検査サーバ１０が実行する処理、及び、ユーザ端末３０において出力される画面等について説明する。

[0044] 図５は、この例において、ウェブサイトの脆弱性を検査する際に脆弱性検査サーバ１０が実行する処理を例示するフローチャートである。サーバ１０は、まず、図示するように、脆弱性を検査する対象のウェブサイトの設定を受け付ける（ステップＳ１００）。こうした設定の受付は、ユーザ端末３０において出力される画面を介して行われる。

[0045] 図６は、ユーザ端末３０において出力される、検査対象のウェブサイトの設定を受け付けるための対象サイト設定画面５０を例示する。当該画面５０は、図示するように、検査対象のウェブサイトのトップ画面（トップページ）のＵＲＬを入力するためのＵＲＬ入力領域５２と、当該ウェブサイトへのログインに用いられるログインＩＤを入力するためのログインＩＤ入力領域５４と、当該ウェブサイトへのログインに用いられるパスワードを入力するためのパスワード入力領域５６と、「巡回・検査開始」というテキストが付加された続行ボタン５８とを有する。このように、この例では、検査対象のウェブサイトの設定情報として、トップ画面のＵＲＬ、ログインＩＤ、及び、パスワードが受け付けられる。

[0046] 続行ボタン５８は、検査対象のウェブサイトの巡回（画面遷移の設定）及び検査を指示するためのオブジェクトである。図５のフローチャートに戻り、続行ボタン５８が選択されると、サーバ１０は、次に、検査対象のウェブサイトを巡回し、検査の際の画面遷移を設定する（ステップＳ１１０）。

[0047] 図７は、画面遷移を設定する際にサーバ１０が実行する処理を例示するフローチャートである。サーバ１０は、まず、図示するように、検査対象のウェブサイトのトップ画面にアクセスし、当該トップ画面を画面遷移に追加す

る（ステップS 2 0 0）。具体的には、ウェブブラウザが起動され、対象サイト設定画面5 0を介して入力されたURLによって特定されるトップ画面へのアクセスが行われる。また、ページ情報管理テーブル1 5 6において、当該トップ画面に関する情報が登録され、具体的には、検査ID、画面ID、画面URL、HTMLデータ、及び、パラメータ情報が設定される。

[0048] 続いて、サーバ1 0は、トップ画面に含まれる複数の遷移対象要素を特定する（ステップS 2 1 0）。具体的には、リンク又はスクリプト等が設定された画面構成要素（ボタン、画像、及び、テキスト等）が、遷移対象要素として特定される。

[0049] 次に、サーバ1 0は、特定された要素をクリックし（ステップS 2 2 0）、クリックに応じた遷移先の画面が、画面遷移への追加対象の画面である場合には（ステップS 2 3 0においてYES）、当該遷移先の画面への遷移を画面遷移に追加する（ステップS 2 4 0）。具体的には、ページ情報管理テーブル1 5 6において、遷移先の画面に関する情報が登録され、つまり、検査ID、画面ID、画面URL、HTMLデータ、パラメータ情報、及び、遷移元情報が設定される。なお、遷移元情報には、遷移元であるトップ画面を識別する画面ID、及び、クリックされた要素を識別する要素IDが設定される。

[0050] また、この例では、遷移対象要素をクリックする際に、必須入力項目が存在する場合には、予め準備されている入力値（対象サイト設定画面5 0を介して入力されたログインID及びパスワードの組合せを含む。）が自動的に設定される。

[0051] 一方、クリックに応じた遷移先の画面が、画面遷移への追加対象外の画面である場合には（ステップS 2 3 0においてNO）、当該画面への遷移は画面遷移に追加されない。

[0052] ここで、この例では、以下の2つの画面は、画面遷移への追加対象外の画面と判断される。

（1）検査対象のウェブサイトの外部のサイトの画面

(2) 既に画面遷移に含まれる画面と重複する画面

[0053] (2) に関して、2つの画面間の重複は、この例では、これらの画面間の類似度に基づいて判断され、具体的には、当該類似度が閾値以上である場合に、2つの画面が重複すると判断される。類似度は、様々な基準を用いて算出することができ、例えば、画面（ページ）の内容、URL、及び、URLパラメータの比較に基づいて算出することができる。

[0054] そして、トップ画面に含まれる複数の遷移対象要素の全てについて、クリックに応じた遷移先画面への遷移の画面遷移への追加の有無が判定されると（ステップS260においてNO）、次に、サーバ10は、画面遷移に追加された各画面について、トップ画面と同様に、当該画面に含まれる複数の遷移対象要素の特定（ステップS280）、及び、各要素のクリックに応じた遷移の画面遷移への追加の有無の判定（ステップS220～S260）を行う。こうした処理は、画面遷移への新たな画面の追加がなくなるまでの間（ステップS270においてNO）、繰り返し行われる。

[0055] 図5のフローチャートに戻り、こうして画面遷移が設定されると、続いて、サーバ10は、設定された画面遷移に従って、脆弱性の検査を実行する（ステップS120）。具体的には、ウェブブラウザを起動し、ページ情報管理テーブル156において管理されている情報に従って、画面遷移に含まれる各画面を順に訪れて、予め定められた脆弱性の検査項目の検査を行う。脆弱性の検査項目は、例えば、OWASP Top10において規定されている項目を含む。検査結果は、ページ情報管理テーブル156の検査結果情報に登録される。

[0056] また、この例では、予め定められた上述した検査項目について、その検査の性質に応じて、検査ルールに基づく検査が実行される。検査ルールは、検査ルール管理テーブル152において管理されており、例えば、以下のような検査ルールを含む。

(ルール1)

サイト種別 : ECサイト
ページ機能 : 商品購入画面
パラメータ種別 : 商品価格
検査方法 : 数値変更 (0.5倍)
結果判定方法 : 完了画面上の価格情報

(ルール2)

サイト種別 : SNSサイト
ページ機能 : 非公開メッセージ画面
パラメータ種別 : メッセージID
検査方法 : 数値変更 (-1)
結果判定方法 : 同画面上の自ユーザのメッセージ情報

(ルール3)

サイト種別 : SNSサイト
ページ機能 : 投稿内容編集画面
パラメータ種別 : 投稿ID
検査方法 : 数値変更 (-1)
結果判定方法 : 投稿内容閲覧画面上の投稿情報

(ルール4)

サイト種別 : 全て
ページ機能 : パスワード変更画面
パラメータ種別 : パスワード値
検査方法 : 学習済みモデルによる脆弱性スコアの使用

(ルール5)

サイト種別 : 全て

ページ機能 : データ削除画面

パラメータ種別 : データ I D

検査方法 : 学習済みモデルによる脆弱性スコアの使用

[0057] 図8は、検査ルールに基づく検査を行う際にサーバ10が実行する処理を例示するフローチャートである。サーバ10は、まず、図示するように、対象のウェブサイトのサイト種別を判定する（ステップS300）。この例では、ウェブサイトのサイト種別を判定するための学習済みモデルを用いて、当該サイト種別が判定される。当該学習済みモデルは、多量の訓練データを用いた機械学習によって生成され、ウェブサイトに含まれる複数のウェブページの各々のページ情報（HTMLデータ及びパラメータ情報）が入力されると、予め定められた複数のサイト種別（例えば、ECサイト、及び、SNSサイト等）の各々の確率を示すスコアを出力するように構成されている。サーバ10は、対象のウェブサイト（検査）において設定されている画面遷移に含まれる各画面のページ情報（HTMLデータ及びパラメータ情報）を学習済みモデルに入力し、当該学習済みモデルから出力されるスコアが最も高いサイト種別を、対象のウェブサイトのサイト種別であると判定する。各画面のページ情報は、ページ情報管理テーブル156において管理されている。

[0058] 続いて、判定されたサイト種別が、対象の検査ルール（複数の検査ルールの中から所定の順序に従って、対象の検査ルールが特定される。）において設定されているサイト種別と一致する場合には（ステップS305においてYES）、サーバ10は、画面遷移に含まれる複数の画面の中から、検査ルールに設定されている機能に対応する画面を特定する（ステップS310）。一方、判定されたサイト種別が検査ルールにおいて設定されているサイト種別と一致しない場合には（ステップS305においてNO）、当該検査ルールの対象外のウェブサイトであるから、当該検査ルールに基づく検査はスキップされる。

[0059] この例では、上述したサイト種別と同様に、画面の機能を判定するための学習済みモデルを用いて、当該機能が判定される。当該学習済みモデルは、多量の訓練データを用いた機械学習によって生成され、各画面のページ情報が入力されると、複数の機能（例えば、商品購入画面、非公開メッセージ画面、投稿内容編集画面、パスワード変更画面、及び、データ削除画面等）の各々の確率を示すスコアを出力するように構成されている。サーバ10は、これらの複数の機能のうち、当該学習済みモデルから出力されるスコアが最も高い機能を、各画面の機能であると判定する。そして、複数の画面のうち、検査ルールにおいて設定されている機能の画面が特定される。

[0060] そして、対象の検査ルールに対応する画面（当該検査ルールに設定されている機能の画面）が存在する場合（ステップS315においてYES）、サーバ10は、当該画面における複数のパラメータのうち、検査ルールに含まれる所定種別のパラメータを特定する（ステップS320）。一方、検査ルールに対応する画面が存在しない場合には（ステップS315においてNO）、当該検査ルールの対象外のウェブサイトであるから、当該検査ルールに基づく検査はスキップされる。

[0061] この例では、所定種別（例えば、商品価格、メッセージID、投稿ID、パスワード値、及び、データID等）のパラメータを判定するための学習済みモデルを用いて、当該パラメータが特定される。当該学習済みモデルは、多量の訓練データを用いた機械学習によって生成され、各画面のページ情報及び当該画面に含まれるパラメータの名称（例えば、`item_price`、`message_id`、`post_id`、`password`、又は、`data_id`等）が入力されると、当該名称を入力されたパラメータが所定種別のパラメータである確率を示すスコアを出力するように構成されている。サーバ10は、各画面に含まれる複数のパラメータのうち、当該学習済みモデルから出力されるスコアが閾値以上であるパラメータを、所定種別のパラメータであると判定する。

[0062] そして、検査ルールに対応する所定種別のパラメータが存在する場合には

(ステップS 3 2 5においてYES)、サーバ10は、学習済みモデルを介して脆弱性スコアを取得する(ステップS 3 3 0)。当該学習済みモデルは、多量の訓練データを用いた機械学習によって生成され、各画面のページ情報が入力されると、当該画面の脆弱性のスコアを出力するように構成されている。

[0063] 一方、所定種別のパラメータが存在しない場合には(ステップS 3 2 5においてNO)、当該検査ルールの対象外のウェブサイトであるから、当該検査ルールに基づく検査はスキップされる。

[0064] 学習済みモデルを介して脆弱性スコアを取得すると、次に、サーバ10は、検査ルールにおいて設定されている検査方法がパラメータ値の変更でない場合(ステップS 3 3 5においてNO)、又は、当該検査方法がパラメータ値の変更であっても(ステップS 3 3 5においてYES)、取得した脆弱性スコアの値が閾値未満である場合(ステップS 3 4 0においてNO)には、検査結果としての脆弱性スコアを記録する(ステップS 3 6 0)。具体的には、ページ情報管理テーブル156において、対応する画面の検査結果情報に対して、脆弱性スコアが登録される。なお、上述した検査ルールの例のルール1～5のうち、設定されている検査方法がパラメータ値の変更でない場合は、ルール4、5が該当する(つまり、この例において、「検査方法がパラメータ値の変更でない場合」とは「検査方法が学習済みモデルによる脆弱性スコアの使用である場合」と言える。))。

[0065] 一方、検査ルールにおいて設定されている検査方法がパラメータ値の変更であって(ステップS 3 3 5においてYES)、且つ、取得した脆弱性スコアの値が閾値以上である場合(ステップS 3 4 0においてYES)には、サーバ10は、パラメータ値を変更してリクエストを送信する(ステップS 3 4 5)。具体的には、パラメータ値の変更内容は、検査ルールの検査方法情報に設定されており、例えば、上述した例のルール1では、所定種別のパラメータが「商品価格」である場合に、「0.5倍」という数値変更が設定されている。この場合、例えば、対応する画面のページ情報における「100

0円」の商品価格が「500円」に変更されたリクエストが送信される。当該リクエストの送信は、商品購入処理の実行とすることができる。また、例えば、上述した例のルール2では、所定種別のパラメータが「メッセージID」である場合に、「-1」という数値変更が設定されている。この場合、例えば、対応する画面のページ情報における「12345」のメッセージIDが「12344」に変更されたリクエストが送信される。当該リクエストの送信は、メッセージ送信処理の実行とすることができる。また、例えば、上述した例のルール3では、所定種別のパラメータが「投稿ID」である場合に、「-1」という数値変更が設定されている。この場合、例えば、対応する画面のページ情報における「987」の投稿IDが「986」に変更されたリクエストが送信される。当該リクエストの送信は、投稿内容編集処理の実行とすることができる。

[0066] 続いて、サーバ10は、ウェブサイトからのレスポンスに基づいて脆弱性を判定し、判定結果を登録する（ステップS350）。脆弱性の判定は、検査ルールにおける結果判定方法情報に基づいて行われ、例えば、上述した例のルール1では、レスポンスに基づく遷移先の商品購入完了画面において、変更後の商品価格での正常処理が確認された場合に、脆弱性が有ると判定される。また、例えば、上述した例のルール2では、レスポンスに基づく遷移先の非公開メッセージ画面において、変更後のメッセージ（他のユーザのメッセージ）での正常処理が確認された場合に、脆弱性が有ると判定される。また、例えば、上述した例のルール3では、レスポンスに基づく遷移先の投稿内容閲覧画面において、変更後の投稿（他のユーザの投稿）での正常処理が確認された場合に、脆弱性が有ると判定される。こうした判定結果は、ページ情報管理テーブル156において、対応する画面の検査結果情報に対して登録される。

[0067] このように、この例では、検査ルールにおいて設定されている検査方法がパラメータ値の変更でない場合（検査方法が学習済みモデルによる脆弱性スコアの使用である場合）には、学習済みモデルを介して取得された脆弱性ス

コアが検査結果として用いられる。こうした脆弱性スコアの取得は、パラメータ値を変更してリクエストを送信する検査と比較して、本番環境や他の開発環境等への影響を抑制することができると共に、検査時間が短縮される。例えば、本番環境等への影響が想定される検査ルールについては、パラメータ値の変更でない検査方法が予め設定される。

[0068] 例えば、上述したルール4では、パスワード変更画面において、パスワード値のパラメータ値に対して「' or 1=1 --」等を設定してリクエストを送信する検査（SQL Injectionの検査）を行うと、他のユーザのパスワードが変更される等の影響が想定される。また、例えば、上述したルール5では、データ削除画面において、データIDのパラメータ値を変更（例えば、-1）してリクエストを送信する検査を行うと、テスト以外の用途で利用されているデータ、又は、他のユーザの実データ等が削除される等の影響が想定される。

[0069] また、この例では、検査ルールにおいて設定されている検査方法がパラメータ値の変更である場合であっても、学習済みモデルを介して取得された脆弱性スコアが閾値未満である場合には、当該脆弱性スコアが検査結果として用いられる。この結果、パラメータ値を変更してリクエストを送信する検査の実施を、脆弱性の深刻度が高い（スコアが比較的大きい）と想定されるケースに限定することができる。

[0070] こうして脆弱性スコアを記録し（ステップS360）、又は、脆弱性の判定結果を登録すると（ステップS350）、次に、サーバ10は、未処理の検査ルールがある場合（ステップS355においてNO）、ステップS305へと戻り、次の検査ルールを対象として、サイト種別、画面の機能、及び、パラメータの種別に基づく検査を行う。こうした検査は、最後の検査ルールとなる（ステップS355においてYES）までの間、繰り返される。

[0071] 上述した例において、検査ルールが、自然言語（例えば「ECサイトの商品購入画面では、商品の価格が含まれるリクエストパラメータを特定し、この値を改ざんしたリクエストを送信する。改ざんした価格で商品が購入でき

た場合、脆弱性として報告する」という文章）で設定されるようにしてもよい。この場合、自然言語で設定された検査ルールを、大規模言語モデル（LLM）等を介して解析すればよい。

[0072] 上述した例では、学習済みモデルを介して、サイト種別、画面の機能、及び、パラメータ種別を判定するようにしたが、こうした種別を、大規模言語モデル（LLM）を介して判定するようにしてもよい。

[0073] 上述した例では、学習済みモデルを介して脆弱性スコアを取得するようにしたが、脆弱性スコアに加えて、当該スコアを算出した根拠（「但し、 $\times \times \times$ の場合を除く」というような制約条件など）を出力可能な大規模言語モデル（LLM）を用いるようにしてもよい。

[0074] 以上説明した本実施形態に係る脆弱性検査サーバ10は、ウェブサイト22に含まれる複数のウェブページの各々のページ情報に基づいて、ウェブサイト22、各ウェブページ、及び／又は、各ウェブページにおけるパラメータの種別を判定し、こうした種別に基づいてウェブサイト22の脆弱性を検査するから、単なる不正な入力値に対する不具合のほか、ウェブサイト、ウェブページ、又は、パラメータの意味、用途、及び、機能等に応じた適切な検査を行うことが可能となる。つまり、サーバ10は、ウェブサイトの様々な脆弱性の検査を支援する。

[0075] 本発明の他の実施形態において、上述した実施形態における脆弱性検査サーバ10が有する機能の一部又は全部は、脆弱性検査サーバ10及びユーザ端末30が協働することによって実現され、又は、ユーザ端末30によって実現され得る。

[0076] 本明細書で説明された処理及び手順は、明示的に説明されたもの以外にも、ソフトウェア、ハードウェアまたはこれらの任意の組み合わせによって実現される。例えば、本明細書で説明される処理及び手順は、集積回路、揮発性メモリ、不揮発性メモリ、磁気ディスク等の媒体に、当該処理及び手順に相当するロジックを実装することによって実現される。また、本明細書で説明された処理及び手順は、当該処理・手順に相当するコンピュータプログラ

ムとして実装し、各種のコンピュータに実行させることが可能である。

[0077] 本明細書中で説明された処理及び手順が単一の装置、ソフトウェア、コンポーネント、モジュールによって実行される旨が説明されたとしても、そのような処理または手順は複数の装置、複数のソフトウェア、複数のコンポーネント、及び／又は複数のモジュールによって実行され得る。また、本明細書において説明されたソフトウェアおよびハードウェアの要素は、それらをより少ない構成要素に統合して、またはより多い構成要素に分解することによって実現することも可能である。

[0078] 本明細書において、発明の構成要素が単数もしくは複数のいずれか一方として説明された場合、又は、単数もしくは複数のいずれとも限定せずに説明された場合であっても、文脈上別に解すべき場合を除き、当該構成要素は単数又は複数のいずれであってもよい。

請求の範囲

- [請求項1] 1 又は複数のコンピュータプロセッサを備え、ウェブサイトの脆弱性を検査するためのシステムであって、前記 1 又は複数のコンピュータプロセッサは、
- 前記ウェブサイトに含まれるウェブページのページ情報を取得するステップと、
- 前記ページ情報に基づいて、前記ウェブサイト、前記ウェブページ、及び、前記ウェブページにおけるパラメータの少なくとも 1 つの種別を判定するステップと、
- 前記少なくとも 1 つの種別に基づいて、前記ウェブサイトの脆弱性を検査するステップと、を実行する、
- システム。
- [請求項2] 前記判定するステップは、前記ページ情報が入力されると、前記少なくとも 1 つの種別を判定するための情報を出力するように構成された第 1 学習済みモデルを用いて、前記少なくとも 1 つの種別を判定する、
- 請求項 1 のシステム。
- [請求項3] 前記判定するステップは、前記ウェブページの種別を少なくとも判定し、
- 前記検査するステップは、前記ウェブサイトに含まれる複数のウェブページの中から所定種別の前記ウェブページを特定し、前記ウェブページに対する所定操作を介して、前記ウェブサイトの脆弱性を検査する、
- 請求項 1 のシステム。
- [請求項4] 前記判定するステップは、前記ウェブサイト、及び、前記ウェブページの種別を少なくとも判定し、
- 前記 1 又は複数のコンピュータプロセッサは、さらに、予め定められた複数の検査ルールの中から、前記ウェブサイトの種別に対応する

第1検査ルールを特定するステップを実行し、

前記検査するステップは、前記複数のウェブページの中から、前記第1検査ルールに対応する前記所定種別の前記ウェブページを特定することを含む、

請求項3のシステム。

[請求項5] 前記判定するステップは、前記パラメータの種別を少なくとも判定し、

前記検査するステップは、前記ウェブサイトに含まれる第1ウェブページにおける複数のパラメータの中から所定種別の第1パラメータを特定し、前記第1ウェブページに対する所定操作であって、前記第1パラメータの値の変更を伴う前記所定操作を介して、前記ウェブサイトの脆弱性を検査する、

請求項1のシステム。

[請求項6] 前記検査するステップは、前記第1ウェブページに対する前記所定操作に応じて遷移する第2ウェブページの前記ページ情報に基づいて、前記ウェブサイトの脆弱性を検査する、

請求項5のシステム。

[請求項7] 前記1又は複数のコンピュータプロセッサは、さらに、前記ページ情報を第2学習済みモデルに入力し、前記第2学習済みモデルから出力される前記ウェブサイトの脆弱性を示すスコアを取得するステップを実行する、

請求項1のシステム。

[請求項8] 前記検査するステップは、前記スコアが閾値未満である場合、前記スコアを検査結果とする一方、前記スコアが前記閾値以上である場合、前記ウェブページに対する所定操作を介して、前記ウェブサイトの脆弱性を検査する、

請求項7のシステム。

[請求項9] 1又は複数のコンピュータによって実行され、ウェブサイトの脆弱

性を検査するための方法であって、

前記ウェブサイトに含まれるウェブページのページ情報を取得するステップと、

前記ページ情報に基づいて、前記ウェブサイト、前記ウェブページ、及び、前記ウェブページにおけるパラメータの少なくとも1つの種別を判定するステップと、

前記少なくとも1つの種別に基づいて、前記ウェブサイトの脆弱性を検査するステップと、を備える、

方法。

[請求項10]

ウェブサイトの脆弱性を検査するためのプログラムであって、1又は複数のコンピュータに、

前記ウェブサイトに含まれるウェブページのページ情報を取得するステップと、

前記ページ情報に基づいて、前記ウェブサイト、前記ウェブページ、及び、前記ウェブページにおけるパラメータの少なくとも1つの種別を判定するステップと、

前記少なくとも1つの種別に基づいて、前記ウェブサイトの脆弱性を検査するステップと、を実行させる、

プログラム。