(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년09월20일
(11) 등록번호 10-2445505
(24) 등록일자 2022년09월16일

(51) 국제특허분류(Int. Cl.)
G06F 21/57 (2013.01) *G06F 21/55* (2013.01)
H04L 51/00 (2022.01)
(52) CPC특허분류
G06F 21/577 (2013.01)
G06F 21/55 (2013.01)
(21) 출원번호 10-2021-0020231
(22) 출원일자 2021년02월16일
심사청구일자 2021년02월16일
(65) 공개번호 10-2022-0116854
(43) 공개일자 2022년08월23일
(56) 선행기술조사문헌
정천수 외 1인, '포스트 코로나19 언택트 시대 대응을 위한 AI 챗봇 구축방법에 관한 연구', 한국IT서비스학회지 제19권제4호, 2020.08, PP.31-47.
(뒷면에 계속)
전체 청구항 수 : 총 4 항

(73) 특허권자
충북대학교 산학협력단
충청북도 청주시 서원구 충대로 1 (개신동)
(72) 발명자
정재훈
충청북도 청주시 흥덕구 성봉로279번길 22-7, 306(충대빌)
김태성
충청북도 청주시 서원구 충대로 1 충북대학교
(74) 대리인
김정현

심사관 : 구대성

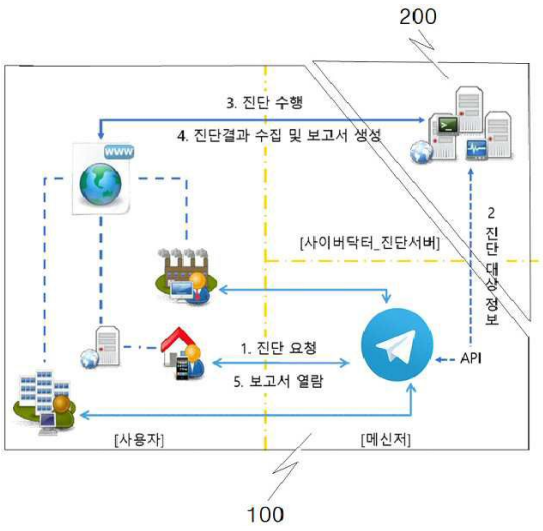
(54) 발명의 명칭 **메신저의 챗봇을 이용한 웹 애플리케이션 취약점 스캐너 시스템 및 방법**

(57) 요 약

본 발명은 메신저의 챗봇을 이용한 웹 애플리케이션 취약점 스캐너 시스템에 관한 것으로서, 메신저 프로그램을 실행할 수 있는 단말기로서, 메신저를 통해 진단 서버에 접속하고, 메신저의 챗봇 기능을 이용하여 웹 애플리케이션에 대한 진단 대상 정보를 상기 진단 서버에 전송하는 사용자 단말기 및 상기 사용자 단말기로부터 수신한 진단 대상 정보에 따라 웹 애플리케이션의 진단을 수행하고, 진단 결과 정보를 수집하여 상기 사용자 단말기에 전송하는 진단 서버를 포함한다.

본 발명에 의하면 텔레그램 등의 메신저의 챗봇을 이용한 웹 애플리케이션 취약점 스캐너 시스템 및 방법을 통하여 고액의 상용제품과 비교하여 저렴하게 구현 가능하고, 오픈소스보다 편리함을 제공할 수 있는 효과가 있다.

대 표 도 - 도1



(52) CPC특허분류
H04L 51/02 (2022.05)

(56) 선행기술조사문헌
'챗봇 기반 금융서비스의 동향 및 보안기능', 금융보안원 보안연구부 보안기술연구팀, 2016.09.20.
KR1020180127902 A
KR101840420 B1*
KR1020200114487 A*
*는 심사관에 의하여 인용된 문헌

이 발명을 지원한 국가연구개발사업

과제고유번호	1345323364
과제번호	2020-B-G016-010108
부처명	교육부
과제관리(전문)기관명	한국연구재단
연구사업명	사회맞춤형산학협력선도대학(LINC+)육성사업
연구과제명	스마트 팩토리 도입 중소기업에 적합한 취약점 진단 도구의 개발
기 여 율	1/1
과제수행기관명	충북대학교 산학협력단
연구기간	2020.07.01 ~ 2021.01.31

명 세 서

청구범위

청구항 1

메신저 프로그램을 실행할 수 있는 단말기로서, 메신저를 통해 진단 서버에 접속하고, 메신저의 챗봇 기능을 이용하여 웹 애플리케이션에 대한 진단 대상 정보를 상기 진단 서버에 전송하는 사용자 단말기; 및

상기 사용자 단말기로부터 수신한 진단 대상 정보에 따라 웹 애플리케이션의 진단을 수행하고, 진단 결과 정보를 수집하여 상기 사용자 단말기에 전송하는 진단 서버를 포함하고,

상기 진단 서버는 상기 사용자 단말기로부터 수신한 진단 대상 정보에 따라 웹 애플리케이션을 진단하는 진단 프로그램 모듈을 포함하고,

상기 진단 프로그램 모듈은 상기 사용자 단말기를 통해 전달된 IP 주소 또는 URL을 인식하여, 해당 웹 애플리케이션의 보안상 취약점을 진단하고,

상기 진단 프로그램 모듈은,

메신저의 챗봇 기능을 통해 웹 애플리케이션의 진단대상 항목을 제공하여 사용자로 하여금 선택하도록 하고, 데이터를 입력받도록 하기 위한 실행부;

상기 실행부에서 선택된 진단대상 항목의 취약점 진단을 실행하기 위한 탐지부; 및

상기 실행부에서 입력된 데이터를 해당 취약점 진단을 위한 명령어로 변환하여 상기 탐지부로 전달하기 위한 변환부

를 포함하여 이루어지는 것을 특징으로 하는 웹 애플리케이션 취약점 스캐너 시스템.

청구항 2

삭제

청구항 3

삭제

청구항 4

청구항 1에 있어서,

상기 변환부는 상기 탐지부에서 출력된 진단 결과를 메신저의 형식에 맞춰 변환하여 상기 실행부로 전달하고,

상기 실행부는 전달된 진단 결과를 메신저에서 표출되도록 하는 것을 특징으로 하는 웹 애플리케이션 취약점 스캐너 시스템.

청구항 5

웹 애플리케이션 취약점 스캐너 시스템에서의 웹 애플리케이션 취약점 스캐너 방법에서,

사용자 단말기에서 메신저를 통해 진단 서버에 접속하는 단계;

상기 사용자 단말기에서 메신저의 챗봇 기능을 통해 웹 애플리케이션에 대한 진단 대상 항목이 입력되면, 입력된 진단 대상 항목을 상기 진단 서버에 전송하는 단계;

상기 진단 서버에서 웹 애플리케이션에 대한 진단 대상 항목에 따라 진단하는 단계; 및

상기 진단 서버에서 진단 대상 항목의 진단 결과 정보를 메신저를 통해 상기 사용자 단말기에 전송하는 단계를

포함하고

상기 진단 서버는 상기 사용자 단말기로부터 수신한 진단 대상 정보에 따라 웹 애플리케이션을 진단하는 진단 프로그램 모듈을 포함하고,

상기 진단 프로그램 모듈은 상기 사용자 단말기를 통해 전달된 IP 주소 또는 URL을 인식하여, 해당 웹 애플리케이션의 보안상 취약점을 진단하고,

상기 진단 프로그램 모듈은,

메신저의 챗봇 기능을 통해 웹 애플리케이션의 진단대상 항목을 제공하여 사용자로 하여금 선택하도록 하고, 데이터를 입력받도록 하기 위한 실행부;

상기 실행부에서 선택된 진단대상 항목의 취약점 진단을 실행하기 위한 탐지부; 및

상기 실행부에서 입력된 데이터를 해당 취약점 진단을 위한 명령어로 변환하여 상기 탐지부로 전달하기 위한 변환부

를 포함하여 이루어지는 것을 특징으로 하는 웹 애플리케이션 취약점 스캐너 방법.

청구항 6

삭제

청구항 7

삭제

청구항 8

청구항 5에 있어서,

상기 변환부는 상기 탐지부에서 출력된 진단 결과를 메신저의 형식에 맞춰 변환하여 상기 실행부로 전달하고,

상기 실행부는 전달된 진단 결과를 메신저에서 표출되도록 하는 것을 특징으로 하는 웹 애플리케이션 취약점 스캐너 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 웹 애플리케이션 취약점 탐지 시스템 및 방법에 관한 것으로서, 상세하게는 텔레그램의 챗봇 기능을 이용하여 단순히 웹 애플리케이션뿐만 아니라 네트워크 전반에 걸쳐 취약점을 발견하고 해당 취약점의 대응 방안 등을 보고서로 제공하는 웹 애플리케이션 취약점 스캐너 시스템 및 방법에 관한 것이다.

[0002] 또한, 본 발명은 텔레그램의 챗봇으로 조직이나 기업이 개발과정에서 실수나 논리적 오류 등으로 인해 발생할 수 있는 보안 취약점들을 최소화할 수 있을 뿐만 아니라, 보안솔루션에 드는 비용을 줄이고 안전하게 자사 웹 애플리케이션을 운영할 수 있는 취약점 스캐너 시스템 및 방법에 관한 것이다.

배 경 기 술

[0003] 사이버 공격이 정교해지고 다양해짐에 따라 취약점으로 인한 침해사고를 예방하고, 탐지하며, 대응하는 것이 중요해지고 있다. 이러한 사이버 공격을 사전에 발견하고 대응하지 못하는 중소기업은 고객의 이탈과 기술 유출 등의 금전적 손해를 입게 된다. 이에 정부에서는 중소기업을 위한 다양한 기술 보호 지원제도를 운용하고 있다. 그러나 이러한 지원제도에도 불구하고 이용 경험은 저조하다.

[0004] 또한, 정보보호 예산편성 관련하여 국내 기업의 32.3%가 정보보호 예산을 편성하고 있으며, 기업들의 침해사고 경험률은 2.8%이고, 침해유형으로는 랜섬웨어(54.1%)가 여전히 높고 악성코드(39.5%, 8.2%p↓)는 감소하였으며, 해킹(13.7%, 9.3%p↑)이 증가하였다(한국정보보호산업협회, 2020). 그리고 ICT에 대한 의존도가 높은 국내 기업 중 대기업을 제외한 중소기업들은 사이버 보안 위협에 많이 노출되어있으나 이러한 기업의 보안에 관한 연구가

부족하며, 사이버 보안에 대한 국가적 접근방식은 위험관리보다는 비상 대응을 지향하므로 대규모 침해사고가 발생하지 않는 한 중소기업을 보호하기 위한 국가적 이니셔티브(Initiative)는 발생하지 않는다

[0005] 또한, 조직이나 기업에서 서비스를 개발하면서 상용 또는 오픈소스 취약점 점검 도구를 사용하여 사전에 문제를 발견하고 있다. 이러한 상용도구의 경우 많은 지출에 비해 비효율적으로 사용되고 있고, 오픈소스는 상용도구와 비교하면 오탐과 미탐 등의 성능의 문제가 있다.

[0006] 최근에는 스마트폰, 태블릿PC 등의 모바일 기기를 업무에 사용하는 일이 늘어나고 있다. 메신저로 일정을 확인하거나 진행 상황을 공유하기도 하고 이를 스마트폰으로 확인하고 수정까지 할 수 있을 뿐만 아니라, 심지어 모바일 기기의 연결성 확대로 사무용 PC를 가상 데스크톱 환경(VDI)으로 대체하는 스마트오피스가 본격화되고 있다.

[0007] 이렇게 모바일 기기의 성능과 휴대성 등의 이점으로 업무 공간이나 업무의 유연함을 높이지만 올해에 39%가 모바일 보안 관련 피해를 보았고, 2018년 27%, 2019년 33%에 비해 증가하고 있다. 모바일 공격으로 피해를 본 기업의 수가 증가하고 있음에도 불구하고, 보안의 취약성을 인지하고 보안 사고에 대비하지 않는 이유로는 편의성(62%), 편리성(52%), 수익 목표(46%)였으며, 예산 부족과 IT 전문가 부족은 각각 27%와 26%였다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) 대한민국 등록특허 제10-1672791호

(특허문헌 0002) 대한민국 등록특허 제10-1966193호

(특허문헌 0003) 대한민국 등록특허 제10-1875866호

(특허문헌 0004) 대한민국 등록특허 제10-2054768호

발명의 내용

해결하려는 과제

[0009] 본 발명은 상기와 같은 종래기술의 문제점을 해결하기 위해 안출된 것으로서, 텔레그램 등의 메신저 챗봇으로 조직이나 기업이 개발과정에서 실수나 논리적 오류 등으로 인해 발생할 수 있는 보안 취약점들을 최소화할 수 있을 뿐만 아니라, 보안솔루션에 드는 비용을 줄이고 안전하게 자사 웹 애플리케이션을 운영할 수 있는 취약점 스캐너 시스템 및 방법 제공을 목적으로 한다.

[0010] 본 발명의 목적은 이상에서 언급한 목적으로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0011] 이와 같은 목적을 달성하기 위한 본 발명은 메신저의 챗봇을 이용한 웹 애플리케이션 취약점 스캐너 시스템에 관한 것으로서, 메신저 프로그램을 실행할 수 있는 단말기로서, 메신저를 통해 진단 서버에 접속하고, 메신저의 챗봇 기능을 이용하여 웹 애플리케이션에 대한 진단 대상 정보를 상기 진단 서버에 전송하는 사용자 단말기 및 상기 사용자 단말기로부터 수신한 진단 대상 정보에 따라 웹 애플리케이션의 진단을 수행하고, 진단 결과 정보를 수집하여 상기 사용자 단말기에 전송하는 진단 서버를 포함한다.

[0012] 상기 진단 서버는 상기 사용자 단말기로부터 수신한 진단 대상 정보에 따라 웹 애플리케이션을 진단하는 진단 프로그램 모듈을 포함하고, 상기 진단 프로그램 모듈은 상기 사용자 단말기를 통해 전달된 IP 주소 또는 URL을 인식하여, 해당 웹 애플리케이션의 보안상 취약점을 진단할 수 있다.

[0013] 상기 진단 프로그램 모듈은, 메신저의 챗봇 기능을 통해 웹 애플리케이션의 진단대상 항목을 제공하여 사용자로 하여금 선택하도록 하고, 데이터를 입력받도록 하기 위한 실행부, 상기 실행부에서 선택된 진단대상 항목의 취약점 진단을 실행하기 위한 탐지부 및 상기 실행부에서 입력된 데이터를 해당 취약점 진단을 위한 명령어로 변환하여 상기 탐지부로 전달하기 위한 변환부를 포함하여 이루어질 수 있다.

[0014] 상기 변환부는 상기 탐지부에서 출력된 진단 결과를 메신저의 형식에 맞춰 변환하여 상기 실행부로 전달하고, 상기 실행부는 전달된 진단 결과를 메신저에서 표출되도록 할 수 있다.

[0015] 본 발명의 웹 애플리케이션 취약점 스캐너 시스템에서의 웹 애플리케이션 취약점 스캐너 방법에서, 사용자 단말기에서 메신저를 통해 진단 서버에 접속하는 단계, 상기 사용자 단말기에서 메신저의 챗봇 기능을 통해 웹 애플리케이션에 대한 진단 대상 항목이 입력되면, 입력된 진단 대상 항목을 상기 진단 서버에 전송하는 단계, 상기 진단 서버에서 웹 애플리케이션에 대한 진단 대상 항목에 따라 진단하는 단계 및 상기 진단 서버에서 진단 대상 항목의 진단 결과 정보를 메신저를 통해 상기 사용자 단말기에 전송하는 단계를 포함한다.

[0016] 상기 진단 서버는 상기 사용자 단말기로부터 수신한 진단 대상 정보에 따라 웹 애플리케이션을 진단하는 진단 프로그램 모듈을 포함하고, 상기 진단 프로그램 모듈은 상기 사용자 단말기를 통해 전달된 IP 주소 또는 URL을 인식하여, 해당 웹 애플리케이션의 보안상 취약점을 진단할 수 있다.

[0017] 상기 진단 프로그램 모듈은, 메신저의 챗봇 기능을 통해 웹 애플리케이션의 진단대상 항목을 제공하여 사용자로 하여금 선택하도록 하고, 데이터를 입력받도록 하기 위한 실행부, 상기 실행부에서 선택된 진단대상 항목의 취약점 진단을 실행하기 위한 탐지부 및 상기 실행부에서 입력된 데이터를 해당 취약점 진단을 위한 명령어로 변환하여 상기 탐지부로 전달하기 위한 변환부를 포함하여 이루어질 수 있다.

[0018] 상기 변환부는 상기 탐지부에서 출력된 진단 결과를 메신저의 형식에 맞춰 변환하여 상기 실행부로 전달하고, 상기 실행부는 전달된 진단 결과를 메신저에서 표출되도록 할 수 있다.

발명의 효과

[0019] 본 발명에 의하면 텔레그램 등의 메신저의 챗봇을 이용한 웹 애플리케이션 취약점 스캐너 시스템 및 방법을 통하여 고액의 상용제품과 비교하여 저렴하게 구현 가능하고, 오픈소스보다 편리함을 제공할 수 있는 효과가 있다.

[0020] 또한, 본 발명에 의하면 앱 형태로 휴대폰, 태블릿, 데스크탑 등 다양한 단말에서 사용할 수 있도록 제공하고, 메신저 형태로 각종 문제를 해결할 수 있으므로, 누구나 간단하게 어디서든지 웹 애플리케이션의 취약점을 점검하고 결과를 확인할 수 있는 효과가 있다.

도면의 간단한 설명

[0021] 도 1은 본 발명의 일 실시예에 따른 텔레그램의 챗봇을 이용한 웹 애플리케이션 취약점 스캐너 시스템을 나타내는 네트워크 구성도.

도 2는 본 발명의 일 실시예에 따른 웹 애플리케이션 취약점 스캐너 방법을 나타낸 흐름도.

도 3은 본 발명의 일 실시예에 따른 텔레그램의 챗봇을 이용한 웹 애플리케이션 취약점 스캐너 방법을 구체적으로 나타낸 흐름도.

도 4는 본 발명의 일 실시예에 따른 텔레그램의 챗봇을 이용한 웹 애플리케이션 취약점 스캐너 시스템의 구성도.

도 5는 본 발명의 일 실시예에 따른 따른 텔레그램의 챗봇을 이용한 웹 애플리케이션 취약점 스캐너 시스템에서의 진단 결과 전달 과정을 나타낸 도면.

도 6은 본 발명의 일 실시예에 따른 텔레그램의 챗봇을 이용한 웹 애플리케이션 취약점 스캐너 시스템의 진단 프로그램 모듈의 탐지부의 구성도.

도 7은 본 발명의 일 실시예에 따른 텔레그램의 챗봇을 이용한 웹 애플리케이션 취약점 스캐너 시스템에서 사용자 단말기에 제공되는 메뉴를 예시한 도면.

발명을 실시하기 위한 구체적인 내용

[0022] 본 명세서에서 개시된 실시 예의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 후술되어 있는 실시 예들을 참조하면 명확해질 것이다. 그러나 본 개시에서 제안하고자 하는 실시 예는 이하에서 개시되는 실시 예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시 예들은 당해 기술분야에서 통상의 지식을 가진 자에게 실시 예들의 범주를 완전하게 알려주기 위해 제공되는 것일 뿐이다.

[0023] 본 명세서에서 사용되는 용어에 대해 간략히 설명하고, 개시된 실시 예에 대해 구체적으로 설명하기로 한다.

[0024] 본 명세서에서 사용되는 용어는 개시된 실시 예들의 기능을 고려하면서 가능한 현재 널리 사용되는 일반적인 용어들을 선택하였으나, 이는 관련 분야에 종사하는 기술자의 의도 또는 판례, 새로운 기술의 출현 등에 따라 달라질 수 있다. 또한, 특정한 경우는 출원인이 임의로 선정한 용어도 있으며, 이 경우 해당되는 명세서의 상세한 설명 부분에서 상세히 그 의미를 기재할 것이다. 따라서 본 개시에서 사용되는 용어는 단순한 용어의 명칭이 아닌, 그 용어가 가지는 의미와 본 명세서의 전반에 걸친 내용을 토대로 정의되어야 한다.

[0025] 본 명세서에서의 단수의 표현은 문맥상 명백하게 단수인 것으로 특정하지 않는 한, 복수의 표현을 포함한다.

[0026] 명세서 전체에서 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있음을 의미한다. 또한, 명세서에서 사용되는 "부"라는 용어는 소프트웨어, FPGA 또는 ASIC과 같은 하드웨어 구성요소를 의미하며, "부"는 어떤 역할들을 수행한다. 그렇지만 "부"는 소프트웨어 또는 하드웨어에 한정되는 의미는 아니다. "부"는 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 재생시키도록 구성될 수도 있다. 따라서, 일 예로서 "부"는 소프트웨어 구성요소들, 객체지향 소프트웨어 구성요소들, 클래스 구성요소들 및 태스크 구성요소들과 같은 구성요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로 코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들 및 변수들을 포함한다. 구성요소들과 "부"들 안에서 제공되는 기능은 더 작은 수의 구성요소들 및 "부"들로 결합되거나 추가적인 구성요소들과 "부"들로 더 분리될 수 있다.

[0027] 또한, 첨부 도면을 참조하여 설명함에 있어, 도면 부호에 관계없이 동일한 구성 요소는 동일한 참조 부호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다. 본 발명을 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

[0028] 본 발명은 메신저의 챗봇(chatbot)을 이용한 웹 애플리케이션 취약점 스캐너 시스템 및 방법에 관한 것으로서, 단순히 웹뿐만 아니라 네트워크 전반에 걸쳐 취약점을 점검할 수 있다.

[0029] 이하에서는 설명의 편의를 위하여 메신저 중에서 텔레그램의 챗봇을 이용한 웹 애플리케이션 취약점 스캐너 및 방법을 예시하여 설명하고자 한다.

[0030] 도 1은 본 발명의 일 실시예에 따른 텔레그램의 챗봇을 이용한 웹 애플리케이션 취약점 스캐너 시스템을 나타내는 네트워크 구성도이고, 도 4는 본 발명의 일 실시예에 따른 텔레그램의 챗봇을 이용한 웹 애플리케이션 취약점 스캐너 시스템의 구성도이다.

[0031] 도 1 및 도 4를 참조하면, 본 발명의 메신저의 챗봇(Chatbot)을 이용한 웹 애플리케이션 취약점 스캐너 시스템은 사용자 단말기(100) 및 진단 서버(200)를 포함한다.

[0032] 사용자 단말기(100)는 메신저 프로그램을 실행할 수 있는 단말기로서, 메신저를 통해 진단 서버에 접속하고, 메신저의 챗봇 기능을 이용하여 웹 애플리케이션에 대한 진단 대상 정보를 진단 서버(200)에 전송한다. 본 발명의 일 실시예에서 메신저 프로그램은 텔레그램(telegram)일 수 있다. 예를 들어, 사용자 단말기(100)는 핸드폰, 스마트폰, 태블시 PC를 포함하는 모바일 단말기와, 데스크탑 컴퓨터, 랩탑 컴퓨터를 포함하는 컴퓨터로 구현될 수 있다.

[0033] 진단 서버(200)는 사용자 단말기(100)로부터 수신한 진단 대상 정보에 따라 웹 애플리케이션의 진단을 수행하고, 진단 결과 정보를 수집하여 사용자 단말기(100)에 전송한다.

[0034] 진단 서버(200)는 사용자 단말기(100)로부터 수신한 진단 대상 정보에 따라 웹 애플리케이션을 진단하는 진단 프로그램 모듈(210)을 포함한다.

[0035] 진단 프로그램 모듈(210)은 사용자 단말기(100)를 통해 전달된 IP(internet protocol) 주소 또는 URL(uniform resource locator)을 인식하여, 해당 웹 애플리케이션의 보안상 취약점을 진단할 수 있다.

[0036] 진단 프로그램 모듈(100)은 실행부(21), 탐지부(22), 변환부(23), 통신부(24)를 포함하여 이루어진다.

[0037] 실행부(21)는 메신저의 챗봇 기능을 통해 웹 애플리케이션의 진단대상 항목을 제공하여 사용자로 하여금 선택하도록 하고, 데이터를 입력받도록 실행하는 역할을 한다.

[0038] 탐지부(22)는 실행부(21)에서 선택된 진단대상 항목의 취약점 진단을 수행하는 역할을 한다.

[0039] 변환부(23)는 실행부(21)에서 입력된 데이터를 해당 취약점 진단을 위한 명령어로 변환하여 탐지부(22)로 전달하는 역할을 한다.

[0040] 통신부(24)는 사용자 단말기(100)와 통신하는 역할을 한다.

[0041] 본 발명에서 변환부(23)는 탐지부(22)에서 출력된 진단 결과를 메신저의 형식에 맞춰 변환하여 실행부(21)로 전달하고, 실행부(21)는 전달된 진단 결과를 메신저에서 표출되도록 실행할 수 있다.

[0042] 도 1에 도시된 바와 같이, 본 발명에 따른 메신저 방식의 취약점 진단 장치는 텔레그램의 챗봇 환경에서의 취약점을 진단하는 시스템으로, 기밀 업무를 포함하는 보안 정보를 메신저를 통해 송수신하는 사용자 단말기(100), 사용자 단말기(100)를 통해 입력된 진단 대상 항목을 진단하는 진단 프로그램 모듈(210)을 구비한 진단 서버(200)을 포함한다.

[0043] 사용자 단말기(100)은 메신저 기능을 구비한 모바일 단말기나 컴퓨터가 될 수 있으며, 유무선 통신을 통해 진단 서버(200)에 접속할 수 있다. 모바일 단말기는 휴대전화기, 테블릿PC 및 PDA 등의 휴대용 단말기기가 될 수 있다.

[0044] 진단 서버(200)은 사용자 단말기(100)를 통해 이루어지는 다양한 업무 중에 발생할 수 있는 다양한 보안 취약점을 진단하는 서비스를 제공하기 위한 서버이다.

[0045] 진단 서버(200)에는 웹 애플리케이션의 취약점을 진단하기 위한 진단 프로그램 모듈(210)을 구비하고 있다.

[0046] 진단 프로그램 모듈(210)은 사용자 단말기를 통해 진단 서버(200)로 전달된 IP주소나 URL을 인식하고, 해당 웹 애플리케이션을 진단하여 보안 취약점을 진단하는 프로그램이다.

[0047] 특히 진단 프로그램 모듈(210)을 구성하는 변환부(23)는 탐지부(22)에서 출력된 결과를 메신저의 형식에 맞춰 실행부로 전달한다.

[0048] 물론, 실행부(21)로 전달된 진단 결과는 메신저를 통해 사용자 단말기(100)로 전달된다.

[0049] 또한, 텔레그램을 통해 진단 결과를 송부하는 과정에서 Q&A는 챗봇(chatbot) 등을 사용하여 흔히 발생하는 질문에 대해서는 자동으로 응답할 수 있게 구현할 수 있다.

[0050] 탐지부(22)는 사용자 단말기(100)로부터 전송된 진단대상 항목의 취약성을 진단하는 기능을 하는 것으로, 진단 대상 항목은 해당 사용자 단말기에 설치된 앱이나 웹페이지들 및 송수신되는 데이터 파일이 될 수 있고, 진단 방법은 바이러스나 파일의 오류를 진단하되 통상적으로 사용되는 진단 기술이 사용될 수 있다.

[0051] 도 6은 본 발명의 일 실시예에 따른 텔레그램의 챗봇을 이용한 웹 애플리케이션 취약점 스캐너 시스템의 진단 프로그램 모듈의 탐지부의 구성도이다.

[0052] 도 6을 참조하면, 탐지부(22)는 취약점 진단부(61)와 대응부(62)로 구성될 수 있다. 예를 들어, 취약점 진단부(61)는 OWASP Top 10, 주요 정보통신 기반 시설의 기술적 취약점 등의 내용을 진단할 수 있고, 대응부(62)는 취약점 대응방안 리포트를 PDF, XHTML 등의 형식으로 생성할 수 있다.

[0053] 도 6에 도시된 바와 같이, 탐지부(22)는 취약점을 진단하고, 진단된 정보에 대한 대응 방법을 찾아낼 수 있다. 여기서, 대응 방법 정보 또한 바이러스나 파일 오류에 통상적으로 되는 기술이 사용될 수 있고, 이는 진단 서버(200)에 구비된 데이터베이스에 이미 저장 내지는 설정될 수 있고, 진단 결과 새로운 취약점이 발생하였을 때는 진단 서버의 관리자가 이를 인지하여 전문가의 도움을 받아 해당하는 신규 취약점에 대한 해결 방법을 제공할 수 있다.

[0054] 도 2는 본 발명의 일 실시예에 따른 웹 애플리케이션 취약점 스캐너 방법을 나타낸 흐름도이다.

[0055] 도 2를 참조하면, 웹 애플리케이션 취약점 스캐너 시스템에서의 웹 애플리케이션 취약점 스캐너 방법에서, 사용자 단말기(100)에서 메신저를 통해 진단 서버(200)에 접속을 시도한다(S201).

[0056] 접속에 성공하면, 사용자 단말기(100)에서 메신저의 챗봇 기능을 통해 웹 애플리케이션에 대한 진단 대상 항목이 입력되면, 입력된 진단 대상 항목을 진단 서버(200)에 전송한다(S203).

[0057] 그리고, 사용자 단말기(100)에서 메신저의 챗봇 기능을 통해 진단 항목 유형이 선택되면, 선택된 진단 항목 유형을 진단 서버(200)에 전송한다(S205).

[0058] 진단 서버(200)에서는 진단 대상 항목 및 진단 항목 유형에 따라 웹 애플리케이션에 대한 진단을 실시한다

(S207).

[0059] 그리고, 진단 서버(200)는 진단 결과를 기반으로 사용 목적에 따른 보고서를 생성하고(S209), 진단 대상 항목의 진단 결과 정보를 메신저를 통해 사용자 단말기(100)에 전송한다(S211).

[0060] 진단 서버(200)는 사용자 단말기(100)로부터 수신한 진단 대상 정보에 따라 웹 애플리케이션을 진단하는 진단 프로그램 모듈(210)을 포함한다.

[0061] S201 단계는 사용자 단말기를 통해 진단 서버에 접속하는 단계로서, 이 단계에서는 해당 사용자의 고유 식별 ID가 감지된다.

[0062] 이렇게 감지된 정보는 진단 대상 항목에 포함될 수 있고, 진단 대상 항목은 사용자 단말기(100)를 통해 진단 서버에 전송될 수 있다.

[0063] 도 5는 본 발명의 일 실시예에 따른 따른 텔레그램의 챗봇을 이용한 웹 애플리케이션 취약점 스캐너 시스템에서의 진단 결과 전달 과정을 나타낸 도면이다.

[0064] 도 5에 도시한 바와 같이, 사용자 단말기(100)가 최초 접속 이후 진행되는 접속에서는 기존에 점검된 취약점 정보에 대한 최신 취약점을 업데이트할 수 있다. 즉, 사용자 단말기(100)에서 진단 대상의 IP 또는 URL이 입력되면, 진단 서버(200)에서는 IP 또는 URL을 확인하고, 진단 유형을 확인하고, 사용 목적에 따라 보고서 양식을 변경하고, 취약점별 대응방안 리포트를 생성하여 사용자에게 진단 결과를 제공할 수 있다. 이 과정에서 문의사항(질의 및 답변, Q & A 등)과 광고 등이 포함될 수 있다. 이처럼 본 발명에서 메신저에 의해 전송되는 정보는 진단 결과 정보는 물론 Q&A(질의&답변), 광고가 포함될 수 있다.

[0065] 본 발명에서 진단하는 단계(S207)는 통상적으로 보안을 진단하는 진단 방법에 따라 이루어질 수 있고, 진단 결과를 전송하는 단계에서는 전달 결과 정보를 메신저를 통해 전달할 수 있다.

[0066] 진단 결과를 전송하는 단계(S211)에서 진단 결과 정보는 파일 또는 문자 형식으로 전송될 수 있으며, 진단 결과 정보의 일측에 광고나 문의사항에 대한 답변 정보가 더 추가될 수 있다.

[0067] 도 3은 본 발명의 일 실시예에 따른 텔레그램의 챗봇을 이용한 웹 애플리케이션 취약점 스캐너 방법을 구체적으로 나타낸 흐름도이다.

[0068] 도 3을 참조하면, 사용자가 사용자 단말기(100)에서 텔레그램의 챗봇을 통해 스타트 버튼을 클릭하면(S301, S303), 메인 메뉴가 출력된다(S305). 도 7은 본 발명의 일 실시예에 따른 텔레그램의 챗봇을 이용한 웹 애플리케이션 취약점 스캐너 시스템에서 사용자 단말기에 제공되는 메뉴를 예시한 도면으로서, 도 7을 참조하면, '진단하기', '결과보기', '문의하기', '업데이트', '공지사항', '회사소개'의 메인 메뉴가 예시되어 있다.

[0069] 사용자 메인 메뉴 중에서 '진단하기' 버튼을 클릭하면(S307), 사용자의 저장 폴더가 있는지 확인한다(S309). 사용자의 저장폴더가 없으면 새로 폴더를 생성하고(S311), 점검대상 IP 또는 URL을 입력한다(S313).

[0070] 그리고, 진단 유형을 선택한다(S315). 예를 들어, 진단 유형은 OWASP Top 10 주요정보통신기반시설 기술적 취약점 분석평가 가이드 웹 기타 등이 있을 수 있다.

[0071] 그리고, 진단 서버(200)에서 진단을 수행하고(S317), 사용 목적이 기술적 문제 해결인 경우 전문가용 양식을 사용하고, 그렇지 않으면 간단한 양식을 사용한다(S319, S321, S323).

[0072] 그리고, 결과 보고서를 생성하여 사용자의 저장폴더에 저장한다(S325).

[0073] '결과 보기' 버튼을 클릭하면(S327), 사용자의 진단 결과 보고서 파일이 있는 경우, 사용자의 저장폴더에서 진단 결과 보고서 파일 리스트를 다운로드하여 열람한다(S331, S333).

[0074] '문의하기' 버튼을 클릭하면(S335), FAQ, Q/A 질문하기, Q/A 답장하기 메뉴를 제공한다(S337, S339, S341).

[0075] '업데이트' 버튼을 클릭하면(S343), 업데이트를 진행한다(S345).

[0076] '공지사항' 버튼을 클릭하면(S347), 업데이트 및 최신 취약점 정보를 출력한다(S349).

[0077] '사이버닥터 기업소개' 버튼을 클릭하면(S351), 사이버닥터 기업소개 관련 연락처, 이메일 주소 등을 제공한다.

[0078] 이러한 과정은 사용자의 사용 종료에 의해 종료된다(S355).

[0079] 이상 본 발명을 몇 가지 바람직한 실시 예를 사용하여 설명하였으나, 이들 실시 예는 예시적인 것이며 한정적인

것이 아니다. 본 발명이 속하는 기술분야에서 통상의 지식을 지닌 자라면 본 발명의 사상과 첨부된 특허청구범위에 제시된 권리범위에서 벗어나지 않으면서 다양한 변화와 수정을 가할 수 있음을 이해할 것이다.

부호의 설명

[0081] 100 사용자 단말기 200 진단 서버

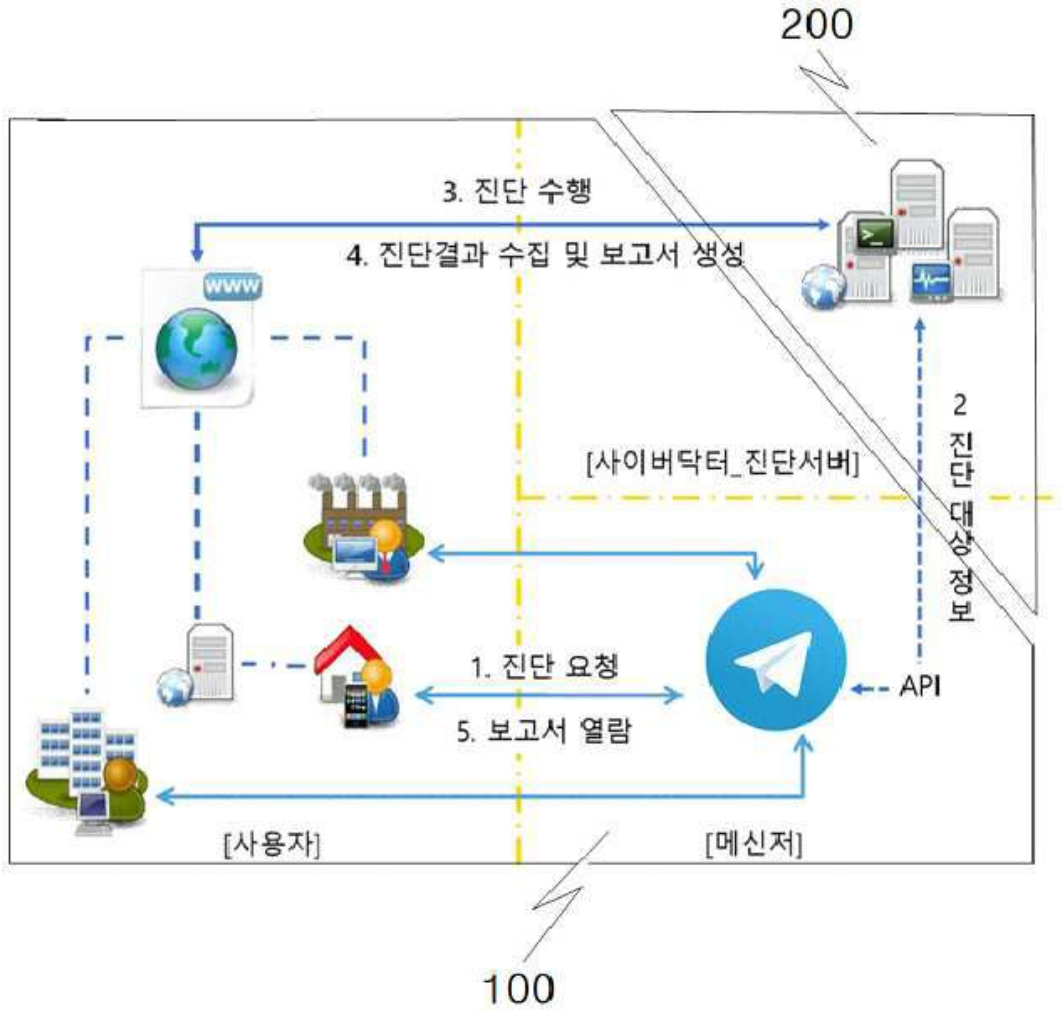
210 진단 프로그램 모듈 21 실행부

22 탐지부 23 변환부

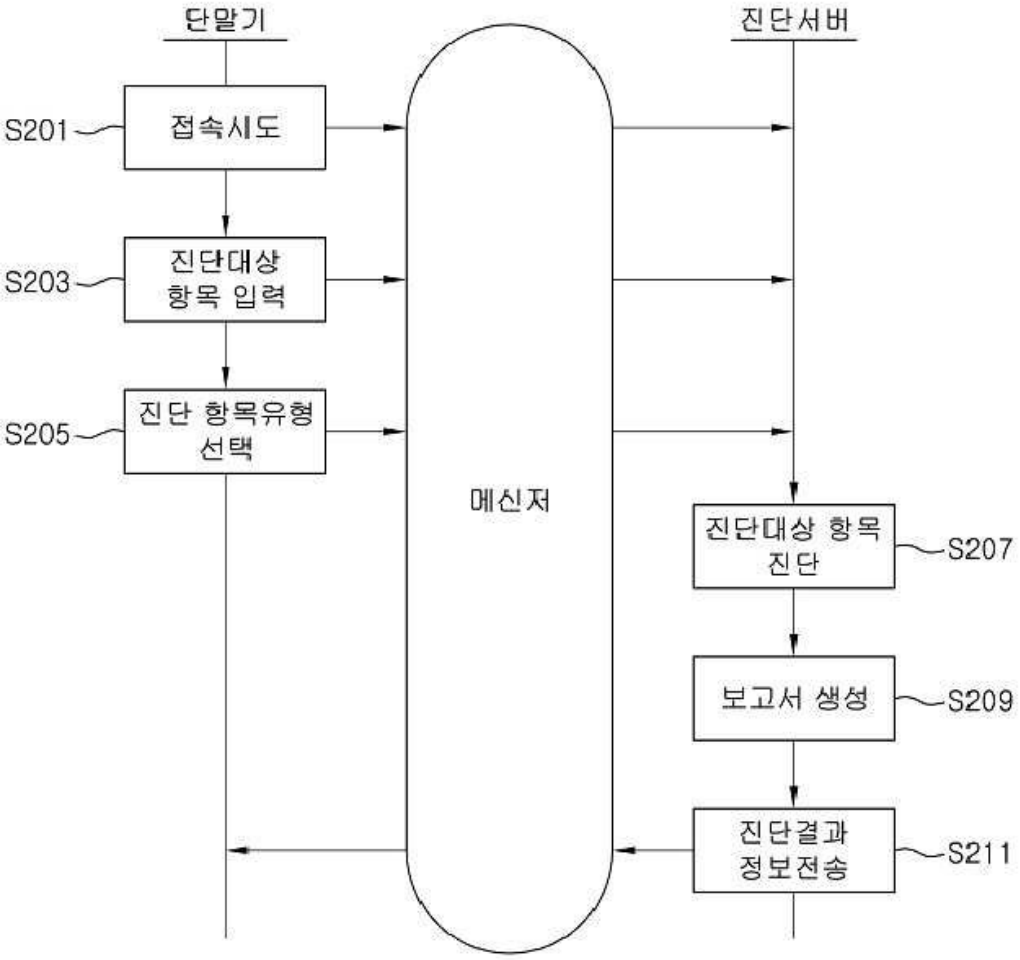
24 통신부

도면

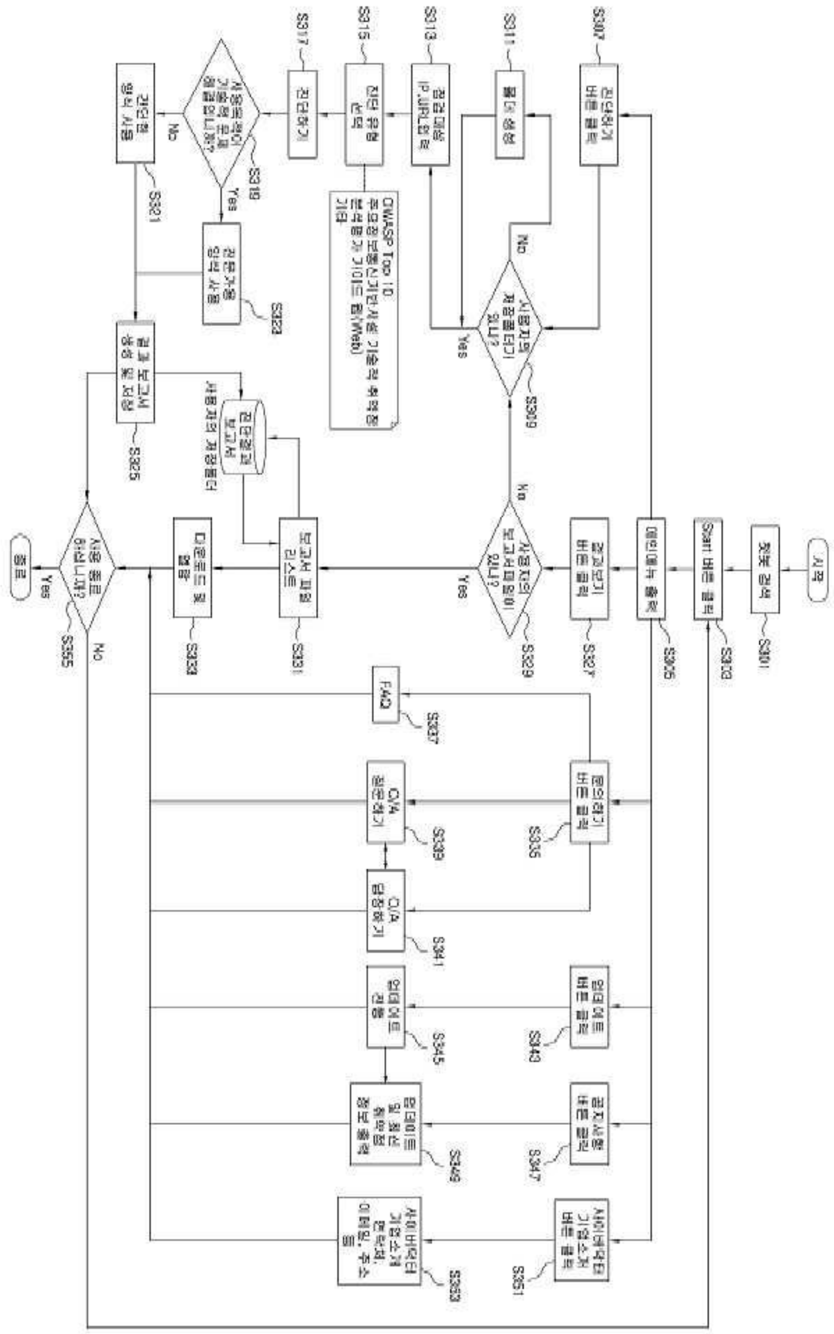
도면1



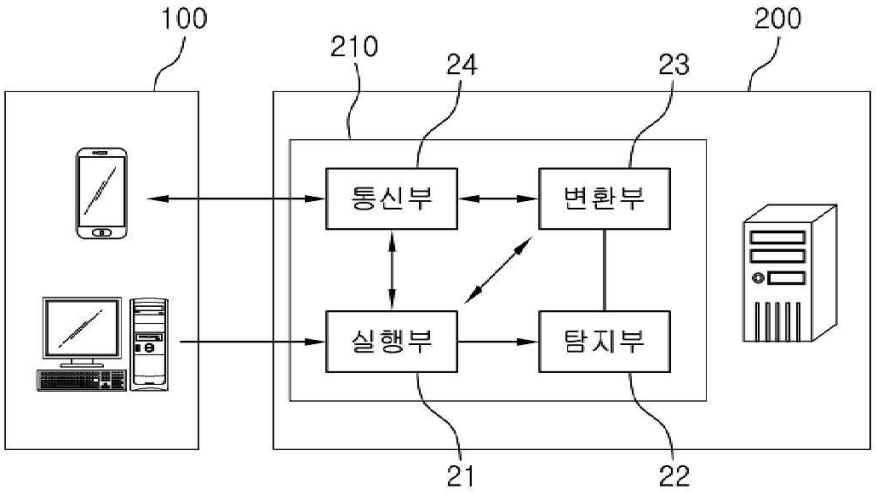
도면2


단말기
진단서버
S201
접속시도
S203
진단대상
항목 입력
S205
진단 항목유형
선택
메신저
진단대상 항목
진단
S207
보고서 생성
S209
진단결과
정보전송
S211

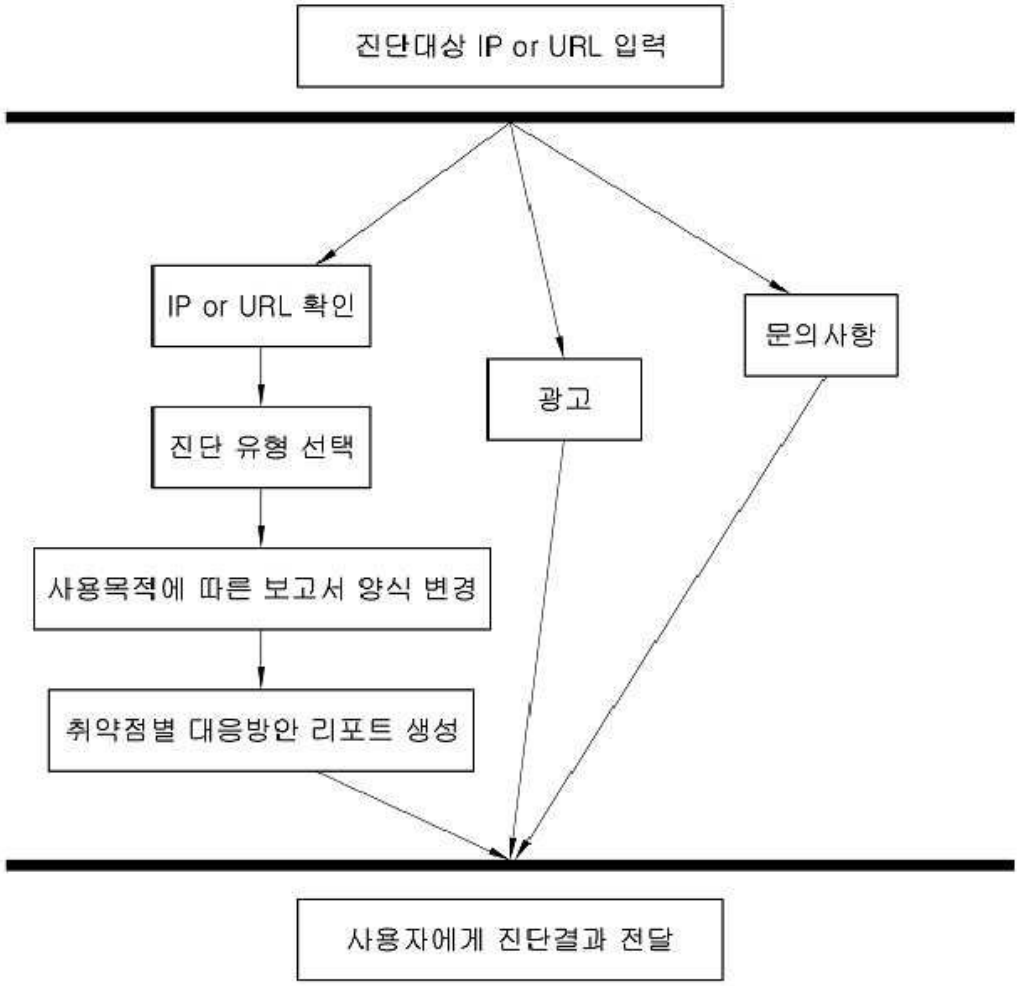
도면3



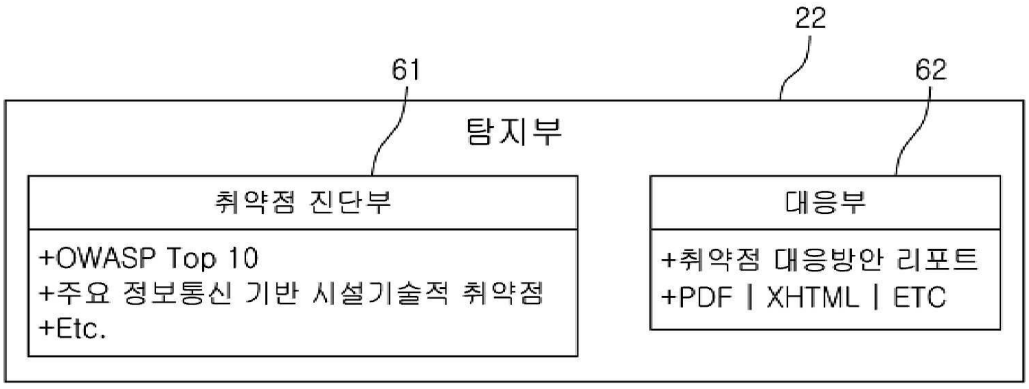
도면4


100
210
24
23
200
통신부
변환부
실행부
탐지부
21
22

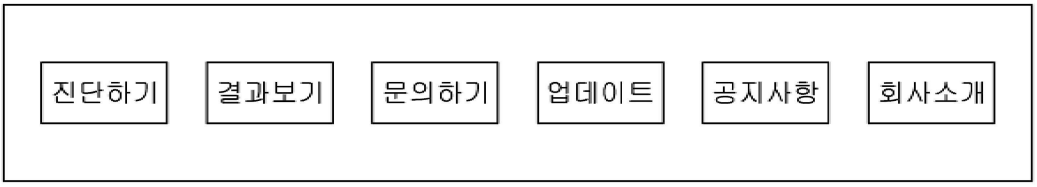
도면5


진단대상 IP or URL 입력
IP or URL 확인
진단 유형 선택
사용목적에 따른 보고서 양식 변경
취약점별 대응방안 리포트 생성
광고
문의사항
사용자에게 진단결과 전달

도면6


22
61
62
탐지부
취약점 진단부
+OWASP Top 10
+주요 정보통신 기반 시설기술적 취약점
+Etc.
대응부
+취약점 대응방안 리포트
+PDF | XHTML | ETC

도면7


진단하기
결과보기
문의하기
업데이트
공지사항
회사소개