

의료기관 웹(홈페이지) 취약점 점검이란?

외부에서 접근성이 용이한 홈페이지의 취약점을 사전 점검·예방함으로써
진료정보, 개인정보 유출에 대한 사전 위협요인 최소화 및
신뢰성 향상을 위한 예방 서비스

점검 대상

- 의료기관 대표 홈페이지
- 신규 개발 홈페이지
- 중요정보 보유 웹 페이지 등

점검 항목

- SQL 인젝션, XSS 등 28개 항목
- 파일 업로드 등 9개 항목 수동점검
- 센터에서 원격점검 수행

점검 기간

- 약 2~5일 소요
- 1~3일(자동 및 수동점검 수행)
- 1~2일(결과보고서 작성)

사전준비

환경조사 및 일정 협의 등

점검 및 결과보고

취약점 점검 및 결과리뷰

보완조치

(의료기관) 조치 및 회신

정기점검

차년도 정기점검 수행

웹 취약점 점검 절차

점검 방법

표준화된 주요정보통신기반시설 점검항목에 따라 웹 취약점 분석 시스템을 이용한 원격점검 및 분석
파일업로드, 불충분한 인증 등 홈페이지 영향 및 자동점검 불가 9개 항목은 수동점검 수행

점검 결과

의료기관은 점검결과 보고서 수신 후 검출 된 취약점 항목을 조치하여 웹 보안수준 강화
센터는 의료기관에 대한 체계적인 지원을 위해 차년도 정기점검 계획수립

기타 사항

점검비용 : 의료기관 대상 무상 서비스

관련문의 : 02-6360-6500 / cert@hisc.or.kr

서비스 신청하기(hisc.or.kr)

