1-4. 안전한 코딩방법

증적

■ 웹 취약점 점검 (1/2)

Description

- 서비스보안팀에서는 사내 모든 서비스에 대해 연1회 이상 웹 취약점 및 안전한 코딩 점검을 수행하며, 발견된 취약점은 일정 기간 내 조치하도록 관리하고 있음
- 웹 취약점 점검은 두레이 프로젝트를 통해 수행주체, 수행시기, 점검 결과, 조치내역에 관한 사항을 확인할 수 있음

1-4. 안전한 코딩방법

증적

■ 웹 취약점 점검 (2/2)

(보안검수)-정기/1221

☆[웹-공공 토스트클라우드 TCA-Member (CAB)] 정기 보안검수 결과 공유

태그 1.년도: 2021 2.법인: NHN 3.유형: 정기 4.검수현황: 이행완료

등록자 지종선 (2021.08.18 16:20)
담당자 지종선
참조 강성진, 신우진, 심소영, 이예송, 조병걸, 진혜진, 홍영기

› 본문/댓글 이미지 4 (294.7 KB)

[웹-공공 토스트클라우드 TCA-Member (CAB)] 정기

서비스 URL / API 리스트

- https://alpha-gov-tca.toast.com/iframe/TCA%20Menu/Operations/Member(CAB)

검수 기간

- 2021-8-12 ~ 2021-8-13

발견 취약점 (취약 2건, 권고 0건)

※ 취약점 제목을 클릭하면 상세 설명을 확인할 수 있습니다.

(Minor) 3-3 계정 정보 노출 취약점
1. 프로젝트 상세 정보 조회시 마스킹 되지 않은 id, 휴대폰번호, email 정보 노출

(Minor) 7-2 서버 정보 노출 취약점
1. 부적절한 파라미터 입력 시 서버 개발 환경 정보 노출 에러 발생

기타 사항

- 개발 보안 가이드: 웹/모바일웹 개발 보안 가이드
- 결과 회신이 없거나 조치가 완료되지 않은 경우, 인증심사 진행 시 결함사항으로 확인되어 대응에

(공유)개발보안가이드

★웹/모바일웹 개발 보안 가이드 점검 체크리스트

가이드 항목

대상	항목	세부항목	Risk level
웹/모바일웹	입력값 검증	[웹/모바일웹] 1.1 SQL Injection 허용 취약점	Major
웹/모바일웹		[웹/모바일웹] 1.2 Command Injection 허용 취약점	Major
웹/모바일웹		[웹/모바일웹] 1.3 CSV Injection 허용 취약점	Major
웹/모바일웹		[웹/모바일웹] 1.4 XSS/CSRF 허용 취약점	Major
웹/모바일웹		[웹/모바일웹] 1.5 요청 및 응답 값 위/변조 취약점	Major
웹/모바일웹		[웹/모바일웹] 1.6 검증되지 않은 리다이렉트 및 포워드 취약점	Minor
웹/모바일웹	파일 관리 및 처리	[웹/모바일웹] 2.1 악성 파일 실행 취약점	Critical
웹/모바일웹		[웹/모바일웹] 2.2 악성 파일 업로드 취약점	Major
웹/모바일웹		[웹/모바일웹] 2.3 임의 파일 다운로드 취약점	Major
웹/모바일웹	중요 정보 전송/저장	[웹/모바일웹] 3.1 요청 및 응답 값 내 중요 정보 노출 취약점	Major
웹/모바일웹		[웹/모바일웹] 3.2 소스코드 내 중요 정보 노출 취약점	Minor
웹/모바일웹		[웹/모바일웹] 3.3 계정 정보 노출 취약점	Minor
웹/모바일웹	인증 및 권한 관리	[웹/모바일웹] 4.1 미흡한 인증 처리 취약점	Major
웹/모바일웹		[웹/모바일웹] 4.2 부적절한 인증 방식 사용 취약점	Major
웹/모바일웹		[웹/모바일웹] 4.3 쿠키/세션 재사용 취약점	Minor
웹/모바일웹		[웹/모바일웹] 4.4 중요 정보 캐시 허용 취약점	Minor

Description

- 수행 방법은 수동 진단으로 '웹/모바일웹 개발 보안 가이드' 내 보안 체크리스트 기반으로 점검함
- 수행 시 점검 도구는 웹 취약점 스캐너(Appscan)과 웹 프락시 툴(burp suite), 모바일 점검 툴(frida, magisk hide), 바이너리 위변조 툴(IDA pro) 외 다수
- 웹 취약점 스캐너(Appscan) 경우 "주요정보통신기반시설, OWASP, 전자금융" 체크리스트 항목을 참고해서 룰을 만들어 사용

1-4. 안전한 코딩방법

증적

보 완 조 치 내 역 서			
신청기관	NHN		
평가구분	☐ 최초평가	■ 사후평가(4 차)	☐ 갱신평가
서비스 구분	■ IaaS (표준등급)	☐ SaaS (☐ 표준등급 / ☐ 간편등급)	
보완구분	☐ 서면/현장평가	■ 취약점	☐ 기타
서비스명칭	NHN Cloud(공공기관)		
해당부서	IT보안실/서비스보안팀		

관련조항	모의침투 테스트 결과
보완내용	☐ 모의침투 테스트 점검 결과 웹 페이지 취약점 8개, 콘솔 페이지 취약점 7개로 총 취약점 15개가 발견되었으며, 조치 11개, 예외 4개 대응 함
보완내역 및 재발방지 대책	☐ 취약점 조치 내역 - 예외 4건 취약점 항목

번호	보안약점 명	예외
1	4-20-1) 전송 값 재사용 가능 (취약)	1
2	4-10-1) exe 파일 업로드 가능 (취약)	1
3	4-21-1) 권한 삭제 가능 (취약)	1
4	5-1-1) 불필요한 서비스 존재 (취약)	1

- 조치 11건 취약점 항목
이행 결과보고서 엑셀 참고

취약 항목			대응	내용
1) 정보수집	발견된 취약 항목 없음			
2) 네트워크 취약점 점검 결과	발견된 취약 항목 없음			
3) 시스템 취약점 점검 결과	발견된 취약 항목 없음			
4) 웹 취약점 점검 결과	4-9) 정보 누출	4-9-1) HTTP 404 에러 페이지 노출 (취약)	완료	사용자 정의 페이지 출력
		4-9-2) HTTP 405 에러 페이지 노출 (취약)	완료	사용자 정의 페이지 출력
	4-10) 악성 콘텐츠	4-10-1) exe 파일 업로드 가능 (취약)	예외	이행점검 시 별도 소명을 통해서 예외처리 요청
	4-12) 약한 문자열 강도	4-12-1) 회원 추가 시 단순 비밀번호 설정 (취약)	완료	
	4-21) 프로세스 검증 누락	4-21-1) 권한 삭제 가능 (취약)	예외	권한없는 사용자는 [멤버 관리]탭 노출이 안되서 해당 페이지 접근 불가 [그림 192] 권한이 없는 계정에서는 해당 기능 disabled된 "권한 삭제" 버튼으로도 노출이 안됨
	4-29) 파라미터 변조	4-29-1) 타 사용자 계정의 프로젝트 생성 (취약)	완료	12월 7일 배포 예정
	4-30) 불필요한 Method 사용	4-30-1) 불필요한 Method 활성화 (취약)	완료	OPTIONS, HEAD 등 불필요한 메소드 사용 시, 에러페이지로 이동
5) 공통 취약점	5-1) 불필요한 서비스 제거	5-1-1) 불필요한 서비스 존재 (취약)	예외	지속적으로 생성/삭제되는 인스턴스(사설IP)라 지금 해당 IP를 찾기 어려움 이행점검때도 여전히 존재하는 서비스면 용도 설명

관련문서 또는 시스템	※ 2021_NHN(Iaas 클라우드)_모의침투_이행_결과보고					
보완조치 결과제출	작성자	추연수	확인자	성동진	작성일	2021년 12월 8일

Description

- **KISA의 클라우드 보안인증 사후 심사 시 모의침투 점검을 수행하며, 관련된 사항에 대해 조치 완료함**