별첨 #6. 취약점 분석 및 모의침투 지침

제 1 장 총칙

제 1 조(목적)

본 지침은 「밥세권 서비스 보안정책서」 제 12 조(취약점 분석 및 모의 침투)에 따라 정보시스템의 취약점을 체계적으로 식별·평가하고, 모의침투를 통해 보안수준을 검증하기 위한 절차 및 기준을 규정함을 목적으로 한다.

제 2 조(적용 범위)

본 지침은 다음 시스템 전체에 적용한다.

1. 웹·API·백엔드·관리자 페이지
2. 관리자 페이지 및 내부 운영페이지
3. 프론트엔드 및 공개된 웹서비스 전 구간
4. DB·캐시·로그 서버 등 인프라 서버
5. 네트워크 장비 및 보안장비(WAF/UTM/IPS 등)
6. 결제 시스템 및 PG 연동 구간
7. 클라우드 리소스(IAM, Security Group, VPC, Storage 등)

제 3 조(책임과 역할)

1. 정보보호책임자(CISO)
   - 취약점 평가 계획 승인
   - 심각한 취약점 발생 시 조치 우선순위 결정
2. 정보보안담당자
   - 정기 취약점 점검 수행
   - 모의침투 관리·통제
   - 위험도 산정 및 보고
3. 시스템관리자·개발팀
   - 취약점 조치 및 패치 적용
   - 구조 개선 및 보안 코딩 반영

제 2 장 취약점 분석 절차

제 4 조(취약점 분석 주기)

1. 정기 취약점 점검은 연 1 회 이상 실시한다.
2. 다음 경우에는 추가 점검을 수행한다.

- 주요 서비스 기능 변경
- 신규 인프라 구축(서버, 네트워크, 보안장비 등)
- 보안 사고 또는 의심행위 발생
- 결제 모듈 또는 PG 연동 로직 변경

제 5 조(취약점 분석 항목)

1. 웹 취약점 (OWASP Top 10 기반)
    - Injection(SQLi, Command Injection 등)
    - 인증 및 세션관리 취약점
    - 접근통제 우회
    - XSS
    - 파일 업로드 우회
    - 취약한 구성(Misconfiguration)
    - 민감정보 노출
    - SSRF, CSRF
    - 브루트포싱 가능 여부
2. 시스템/OS 취약점
    - 패치 미적용
    - 불필요 서비스 실행
    - 권한 설정 취약
    - Root 권한 관리 취약
    - SSH 보안 설정 부족
    - 환경파일 및 설정파일 노출
3. 네트워크 취약점
    - 방화벽/ACL 오개방 여부
    - 포트 스캔 및 서비스 노출
    - 위험국가 IP 정책 준수 여부
    - 내부망/DMZ 간 이동 경로 검증
4. 보안장비(WAF/UTM/IPS) 구성 점검
    - 시그니처 최신화 여부
    - 정책 미흡 여부
    - 탐지·차단 로그 검증
5. 결제 보안 취약점
    - Webhook 서명 검증 부재
    - Transaction 파라미터 변조 가능성
    - 민감정보 저장 여부
    - PG 연동 IP 화이트리스트 미적용
    - TLS 미적용 구간 존재 여부
6. 클라우드 취약점

- IAM 권한 과도 여부
- 루트 계정 MFA 미적용
- Security Group 과다 개방
- 공개된 Storage(S3 등) 존재 여부
- CloudTrail/Config 등 로깅 비활성화
- 메타데이터 서비스 접근 통제 여부

제 6 조(취약점 분석 도구)

취약점 분석은 다음 도구 또는 동등한 기능을 제공하는 도구를 활용할 수 있다.

1. OS/미들웨어 스캐너: Nessus, Qualys, OpenVAS 등
2. 웹 취약점 도구: OWASP ZAP, Burp Suite
3. 클라우드 보안 진단 도구: ScoutSuite, Prowler
4. 소스코드 분석 도구(SAST): SonarQube 등

제 7 조(위험도 분류 기준)

취약점은 다음 기준으로 분류한다.

등급	설명	조치 기한
High	시스템 장악 가능, 개인정보 유출 가능, 인증 우회 등	즉시(24~72 시간 내)
Medium	일부 공격 가능, 보안 우회 가능	2 주 이내
Low	정보노출·구성 취약 등 영향 제한적	1 개월 이내
Info	정보 수준의 권고사항	차기 점검 시까지

제 8 조(취약점 조치 절차)

1. 취약점 발견 → 등급 분류 → 조치 요청 → 조치 후 재검증
2. High 취약점은 즉시 임시 차단 또는 우회정책(WAF Rule 등) 적용한다.
3. 조치 결과는 문서화하여 1 년 이상 보관한다.
4. 패치는 변경관리 절차에 따라 진행한다.

제 3 장 모의침투

제 9 조(모의침투 실시 기준)

1. 중요 서비스는 반기 1 회 이상 모의침투를 수행한다.
2. 다음 경우 즉시 추가 모의침투를 수행한다.
    - 새로운 결제 기능 또는 API 적용
    - 대규모 구조 변경
    - 보안 사고 또는 공격 시도 감지
    - WAF/IPS 정책 완전 변경

제 10 조(모의침투 범위)

1. 웹·API·관리자 페이지
2. 인증·세션·권한 관리 로직
3. 결제 트랜잭션 변조 가능성
4. 서버 OS·네트워크 경로 우회
5. WAF/UTM 회피 공격
6. 클라우드 IAM/보안그룹 취약점
7. 내부망 침투(필요 시)

제 11 조(모의침투 방법)

1. Black Box
    - 외부 공격자 관점
    - 공개된 웹/결제/API 기반 테스트
2. Gray Box
    - 개발 문서·API 명세 기반
    - 관리자 페이지 점검
    - 내부 API 호출 검증
3. White Box(선택)
    - 소스코드 리뷰
    - 구성파일·Secret 값 검증
    - DevSecOps 파이프라인 확인

제 12 조(금지된 공격)

서비스 안정성을 위해 다음 공격은 사전 승인 없이는 금지한다.

1. 대량 트래픽(DoS/DDoS)
2. 데이터 삭제·변조 공격
3. 실제 결제 시도(모의결제 환경만 사용)
4. 운영데이터에 대한 직접 SQL Injection 조작
5. 클라우드 IAM 에 대한 파괴적 테스트

제 13 조(모의침투 결과 보고)

보고서에는 다음 항목을 반드시 포함한다.

1. 취약점 목록 및 등급
2. 영향 범위
3. 재현 절차
4. 개선 권고사항
5. 조치 완료 여부

보고서는 정보보호책임자(CISO)에게 제출하고 관련 부서와 공유한다.

제 4 장 자동화 보안 점검

제 14 조(SAST—정적 분석)

1. 주요 릴리즈마다 수행
2. 확인 항목:
    - 인증/인가 로직
    - 민감정보 로그 출력
    - 입력값 검증 누락
    - 암호화 미적용

제 15 조(DAST—동적 분석)

1. 분기 1 회 이상 수행
2. 웹 기반 서비스 전체 URL 크롤링
3. 공격 벡터: SQLi, XSS, CSRF, SSRF 등

제 5 장 취약점 조치 검증

제 16 조(재검증)

1. 조치 완료 후 반드시 재검증 필요
2. 동일 취약점이 재발하는 경우 근본 원인 분석(RCA) 실시

제 17 조(추적 관리)

1. 취약점 조치 현황은 관리대장에 기록
2. Closed 까지 진행하며 뒤로 미루기 금지
3. High/Medium 은 매주 점검 회의에서 진행 상황 공유

제 6 장 예외관리

제 18 조(예외 승인)

1. 기술적 한계로 즉시 조치 불가한 취약점은 예외 신청 가능
2. 필수 포함 항목
    - 사유
    - 위험 분석

- 대체 통제(WAF Rule 등)
- 적용 기간

3. CISO 승인 후 적용
4. 만료 즉시 원복 및 재점검

제 7 장 부칙

제 19 조(시행일)

본 지침은 2025 년 12 월 29 일부터 시행한다.

제 20 조(개정)

본 지침은 정보보호책임자의 검토 후 개정한다.