|  |
| --- |
|  |
| **[의료서비스 마이그레이션 프로젝트]** |
| **모의해킹 수행 계획서** |
| *Version 1.1* |

**2021. 11. 29**



**개 정 이 력**

| 버전 | 변경일 | 변경 사유 | 변경 내용 | 작성자 | 비고 |
| --- | --- | --- | --- | --- | --- |
| 1.0 | 2021-11-25 | 최초작성 | 보고서 최초작성 | 김민지 |  |
| 1.1 | 2021-11-29 | 항목변경 | 점검 항목 업데이트 | 김민지 |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**목차**

[1. 수행 개요 5](#_Toc89101096)

[1.1. 수행 목적 5](#_Toc89101097)

[1.2. 수행 일정 5](#_Toc89101098)

[1.3. 수행 인력 6](#_Toc89101099)

[1.4. 수행 환경 6](#_Toc89101100)

[1.5. 수행 대상 6](#_Toc89101101)

[2. 웹 모의해킹 수행 방안 7](#_Toc89101102)

[2.1. 웹 모의해킹 수행 절차 7](#_Toc89101103)

[2.2. 웹 모의해킹 시나리오 전체 개요 10](#_Toc89101104)

[2.3. 웹 취약점 점검도구 11](#_Toc89101105)

[2.4. 웹 취약점 점검항목 12](#_Toc89101106)

[2.5. 웹 취약점 위험도 산정 15](#_Toc89101107)

[3. 산출물 및 협조사항 16](#_Toc89101108)

[3.1. 프로젝트 산출물 16](#_Toc89101109)

[3.2. 협조 요청 사항 16](#_Toc89101110)

[3.3. 수행 전 협의사항 17](#_Toc89101111)

[별첨 1. 웹 모의해킹 유형 19](#_Toc89101112)

[별첨 2. OWASP Top 10 21](#_Toc89101113)

[별첨 3. 국가사이버안전센터에서 발표한 8대 취약점 23](#_Toc89101114)

[별첨 4. 주요정보통신 기반시설 기술적 취약점 분석평가 상세가이드(Web) 25](#_Toc89101115)

[별첨 5. 클라우드 모의해킹 방법론(AWS) 27](#_Toc89101116)

**표 목차**

[[표 1] 수행 일정 5](#_Toc89101117)

[[표 2] 수행 인력 6](#_Toc89101118)

[[표 3] 수행 환경 6](#_Toc89101119)

[[표 4] 웹 애플리케이션 수행 대상 6](#_Toc89101120)

[[표 5] 포트스캐닝 명령 예시 9](#_Toc89101121)

[[표 6] WAS 정보 확인 명령 실행 9](#_Toc89101122)

[[표 7] 웹 진단 시나리오 10](#_Toc89101123)

[[표 8] 웹 취약점 점검도구 목록 11](#_Toc89101124)

[[표 9] 웹 취약점 점검 항목 12](#_Toc89101125)

[[표 10] 클라우드 특화 진단 항목 14](#_Toc89101126)

[[표 11] 웹 모의해킹 위험도 등급 산정 기준 15](#_Toc89101127)

[[표 12] 결과 산출물 16](#_Toc89101128)

[[표 13] 업무 협의 리스트 17](#_Toc89101129)

[[표 14] 웹 모의해킹 테스트 유형 (Common Test Type OSSTMM 3) 상세 19](#_Toc89101130)

[[표 15] OWASP Top 10 21](#_Toc89101131)

[[표 16] 국가사이버안전센터에서 발표한 8대 취약점 23](#_Toc89101132)

[[표 17] 과학기술정보통신부의 주요 정보통신 기반시설 취약점 분석평가 상세가이드(Web) 25](#_Toc89101133)

[[표 18] EQST 클라우드 모의해킹 방법론(AWS) (클라우드 특화 진단 항목) 27](#_Toc89101134)

**그림 목차**

[[그림 1] EQST 클라우드 모의해킹 방법론의 클라우드 서비스 진단 방법론 7](#_Toc89101135)

[[그림 2] 사전 업무 협의 단계 8](#_Toc89101136)

[[그림 3] 웹 진단 시나리오 전체 개요도 10](#_Toc89101137)

1. 수행 개요
   1. 수행 목적

본 문서는 1조에서 구성한 전산 서비스 외/내부에 존재하는 다양한 보안 위협 및 침해사고 발생 가능 경로를 파악하여 위협 시나리오를 도출함. 해당 위협이 서비스에 미치는 영향을 파악하고 보안 대책을 제시하여 발견된 위협을 제거 함으로써 침해사고를 예방하고 전산 서비스의 안정성을 확보하는 것을 목적으로 함

* 1. 수행 일정

수행일정은 고객사와의 협의를 통해 11월 23일부터 12월 17일까지 03주간 진행되며 문제 발생 시 운영 시스템의 영향을 최소화 하기 위해서 시스템 운영팀의 대응이 빠른 일과 시간 (오전 9:00 ~ 오후 6:00) 중에 수행함. 시나리오 및 취약점 점검 항목에 기반한 진단을 수행하며 진단 수행 시 시스템에 영향을 줄 수 있는 해킹 시도는 진행하지 않음. 과도한 트래픽을 유발하여 서버에 부하를 줄 수 있는 진단이 필요할 경우 야간 진단(18:00 ~ 04:00)을 수행함

[표 1] 수행 일정

| 분류 | | 업무 내용 | 수행 일정 | | |
| --- | --- | --- | --- | --- | --- |
| 11. 23 ~ 11. 26 | 12. 07 ~ 12. 10 | 12. 14 ~ 12. 17 |
| 환경 및 요구 분석 | | 수행계획 수립 및 업무협의 |  |  |  |
|  |  |  |
|  |  |  |
| 과제 수행 | | 내/외부 웹 모의해킹 |  |  |  |
|  |  |  |
|  |  |  |
| 결과보고서 작성 | | 결과보고서 작성 및 종료보고 |  |  |  |
|  |  |  |
|  |  |  |
| 인력 배정 | 조상우 | 내/외부 웹 모의해킹 | 업무 협의 | 프로젝트 수행 | 결과 보고 |

* 1. 수행 인력

모의해킹을 수행할 인력은 다음과 같음

[표 2] 수행 인력

| 담당업무 | 수행원 | 직급 | 연락처 | 이메일 |
| --- | --- | --- | --- | --- |
| 내/외부 웹 모의해킹 | 조상우 |  | 010-9934-6348 |  |

* 1. 수행 환경

모의해킹을 수행할 환경은 다음과 같음

[표 3] 수행 환경

| 구분 | 점검자 | IP | 점검 장소 |
| --- | --- | --- | --- |
| 내/외부자 관점 | 조상우 | 223.38.22.161 XXX.XXX.XXX.XXX | 재택 동국대학교 |

* 1. 수행 대상

모의해킹을 수행할 진단대상은 다음과 같음

* + 1. 웹 애플리케이션 대상

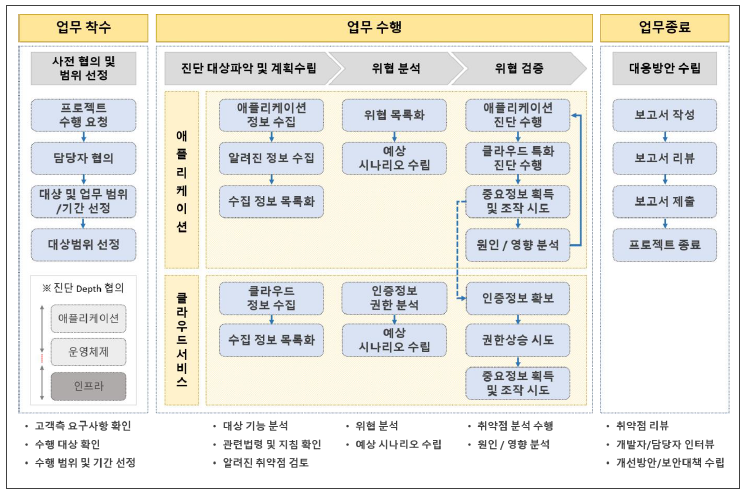
[표 4] 웹 애플리케이션 수행 대상

| No, | 구분 | 대상명 | URL | IP | 담당자 | 비고 |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 대외 | 의료서비스 홈페이지 | http://www.skhealers.com | 3.35.57.37  3.35.129.21 | 조상우 | - |

1. 웹 모의해킹 수행 방안
   1. 웹 모의해킹 수행 절차

EQST 클라우드 모의해킹 방법론의 클라우드 서비스 진단 방법론을 이용하여 진단을 수행함

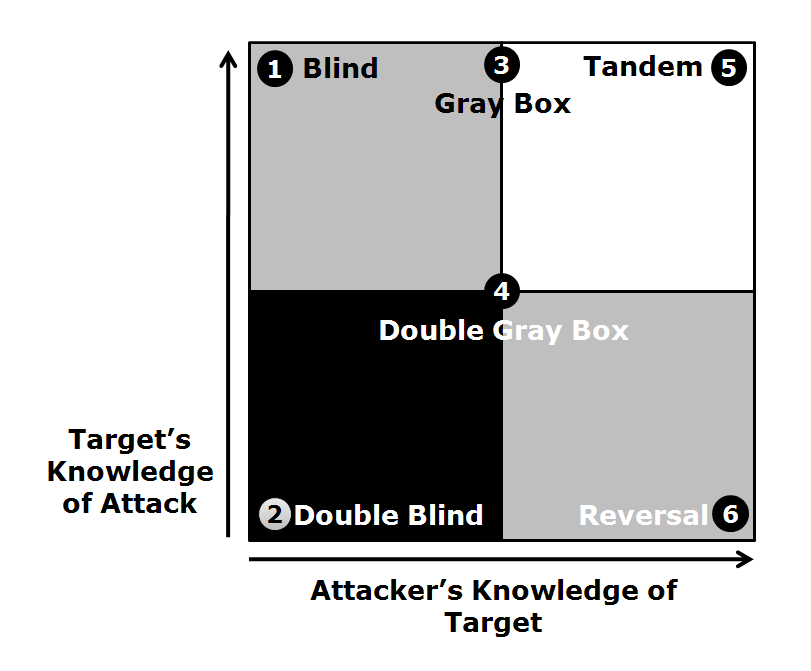
[그림 1] EQST 클라우드 모의해킹 방법론의 클라우드 서비스 진단 방법론



* + 1. 사전업무협의 단계

모의해킹을 시작하기에 앞서 고객사 및 담당자와 회의를 통해 요구사항을 반영한 구체적인 모의해킹 시나리오, 진단대상, 기간을 선정하는 단계이며 공통 테스트 타입을 기준으로 시스템 구성, 서비스 영향도 등을 파악 후 상세 시나리오와 기간을 선정함. 일반적인 웹 모의해킹의 경우, Blind 테스트 형태로 진행하나 취약점 탐지의 효율성을 높이기 위해 Tandem 타입의 테스트 방법을 선호함. (※ 테스트 유형별 상세 설명은 별첨1.모의해킹 유형을 참조)

[그림 2] 사전 업무 협의 단계



* + 1. 현황분석 단계

사전업무협의 단계에서 선정된 모의해킹 시나리오를 기준으로 공격할 대상 목록을 만들고, 공격 대상에 대해 포트스캔, 웹 구조 파악, 웹 취약점 스캔을 수행하여 모의해킹 대상이 되는 시스템에 대한 정보를 수집함. 포트 스캐닝 도구인 NMAP을 사용하여 공격 대상 시스템의 열려있는 포트에 대한 스캐닝을 수행함. 공격 대상 시스템의 WAS 정보를 확인하기 위하여 HTTP Request 요청 시 서버로부터 돌아오는 응답 값을 통해 WAS 배너 정보를 확인함

[표 5] 포트스캐닝 명령 예시

|  |
| --- |
| #nmap -v -sS –P0 –O xxx.xxx.xxx.xxx |

[표 6] WAS 정보 확인 명령 실행

|  |
| --- |
| C:\>telnet www.test.com 80  OPTIONS / HTTP/1.0  HTTP/1.1 302 Found  Date: Mon, 10 Jan 2013 13:10:53 GMT  Server: Apache  Location: http://www.test.com/error/error403.html  Content-Length: 226  Connection: close  Content-Type: text/html; charset=iso-8859-1 |

* + 1. 취약점 분석 및 해결방안 산출

정보 수집 단계에서 수집된 정보를 기준으로 취약점을 분석하고 비인가 접근, 데이터베이스 정보 획득, 웹 페이지 변조 등의 공격을 시도함. 사용되는 공격 기법은 OWASP TOP 10, 국가 사이버안전센터에서 발표한 8대 취약점, 주요 정보통신 기반시설 취약점 분석평가 기준, 금융분야 취약점 분석평가 기준 중 중요 항목을 선별하여 EQST 클라우드 모의해킹 방법론의 클라우드 서비스 진단 방법론을 기반으로 모의해킹을 수행함

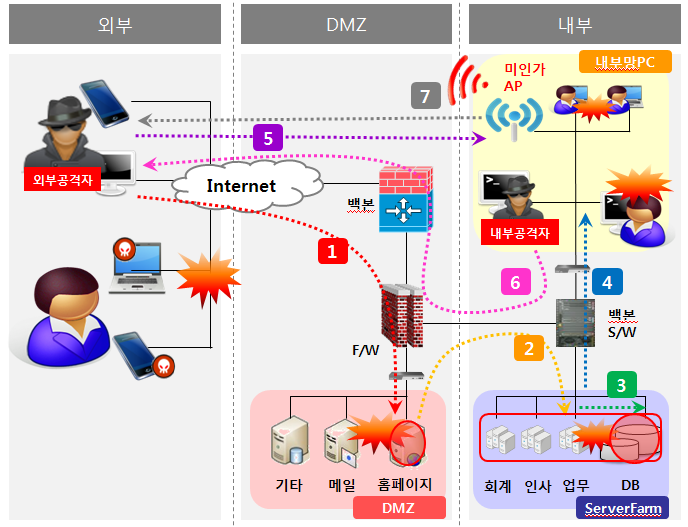
* + 1. 보고서작성 및 프로젝트 종료

공격대상 시스템 별로 발견된 취약점 및 공격 결과의 상세한 내용과 보안대책 및 권고사항을 정리하여 고객사 담당자에게 보고하며 담당자의 최종 승인을 받은 후 프로젝트를 종료함

* 1. 웹 모의해킹 시나리오 전체 개요

웹 모의해킹 시나리오의 전체적인 개요는 아래와 같음

[그림 3] 웹 진단 시나리오 전체 개요도



[표 7] 웹 진단 시나리오

| 시나리오 | 세부 시나리오 |
| --- | --- |
| 시나리오 1 | 홈페이지 및 기타 웹사이트의 소스 취약점을 이용한 가입자 정보 조회, 유출 및 웹 소스 다운로드 가능성 여부 점검 |
| 시나리오 2 | 네트워크 접근제어 취약점을 이용한 Server Farm 내 서버 비인가 접근 가능성 여부 점검 |
| 시나리오 3 | Server Farm 내 취약한 서버(개발서버 등)을 이용한 비인가 접근 및 중요정보 유출 가능성 여부 점검 |

* 1. 웹 취약점 점검도구

웹 모의해킹에 사용할 주요 점검도구는 다음과 같음

[표 8] 웹 취약점 점검도구 목록

| 구분 | 진단 도구 | 설명 |
| --- | --- | --- |
| SQL인젝션 | Sqlmap | 데이터베이스 정보를 추출하기 위해 사용 |
| 프록시 | BurpSuite | 서버로 전송되는 파라미터 값을 확인하고 수정하기 위해 사용 |
| 네트워크 | Wireshark | 네트워크 패킷을 분석하기 위해 사용 |
| netcat | Reverse shell 을 맺기 위해 사용 |
| 스캐너 | Nmap | 개방된 포트 및 제공중인 서비스를 스캔하기 위해 사용 |
| Nikto | 웹 서버를 대상으로 취약한 파일/프로그램과 취약한 설정 등을 탐지하기 위해 사용 |
| ZAP | 자동 웹 취약점 스캐너로 사용 (부가적으로 프록시, 퍼저 등 사용 가능) |

* 1. 웹 취약점 점검항목

점검 항목은 OWASP TOP 10, 국가 사이버안전센터에서 발표한 8대 취약점, 과학기술정보통신부 주요 정보통신 기반시설 기술적 취약점 분석평가 방법 상세 가이드, EQST 클라우드 모의해킹 방법론(AWS) 항목을 기준으로 점검함

[표 9] 웹 취약점 점검 항목

| NO | 취약유형 | 코드 | 세부 진단 항목 | 진단 내용 |
| --- | --- | --- | --- | --- |
| 1 | 입력 값 검증 부재 | SI | SQL 인젝션 | 웹페이지 내 SQL 인젝션 취약점 존재 여부 점검 |
| 2 | XI | XPath 인젝션 | 웹페이지 내 조작된 XPath 쿼리 공격 가능성 점검 |
| 3 | OC | 운영체제 명령 실행 | 웹 사이트 내 운영체제 명령 실행 취약점 존재 여부 점검 |
| 4 | XS | 크로스 사이트 스크립팅 | 웹 사이트 내 크로스사이트 스크립팅 취약점 존재 여부 점검 |
| 5 | BO | 버퍼 오버 플로우 | 사용자가 입력한 파라미터 값의 문자열 길이 제한 확인 |
| 6 | FS | 포맷 스트링 | 웹 애플리케이션에 포맷 스트링 취약점 존재 여부 점검 |
| 7 | LI | LDAP 인젝션 | 웹페이지 내 LDAP 인젝션 취약점 점검 |
| 8 | SS | SSI 인젝션 | 웹페이지 내 SSI 인젝션 공격 가능성 점검 |
| 9 | 취약한 파일처리 | FU | 파일 업로드 | 웹 사이트의 게시판, 자료실 등에 조작된 Server Side Script 파일 업로드 및 실행 가능 여부 점검 |
| 10 | FD | 파일 다운로드 | 웹 사이트에서 파일 다운로드 시 허용된 경로 외 다른 경로의 파일 접근이 가능한지 여부 점검 |
| 11 | PT | 경로 추적 | 웹 서버와 웹 애플리케이션의 파일 또는 디렉터리의 접근 통제 여부 점검 |
| 12 | PL | 위치 공개 | 예측 가능한 폴더의 위치 사용 여부 및 불필요한 파일의 존재 여부 점검 |
| 13 | 취약한 인증 및 세션 관리 | CF | 크로스 사이트 리퀘스트 변조(CSRF) | 사용자의 신뢰(인증) 정보의 변조 여부 점검 |
| 14 | PV | 프로세스 검증 누락 | 인증이 필요한 웹 사이트의 중요(관리자 페이지, 회원변경 페이지 등) 페이지에 대한 접근제어 설정 여부 확인 |
| 15 | AU | 자동화 공격 | 웹 애플리케이션의 특정 프로세스(로그인 시도, 게시글 등록, SMS 발송 등)에 대한 반복적인 요청 시 통제 여부 확인 |
| 16 | IA | 불충분한 인증 | 중요 페이지 접근 시 추가 인증 요구 여부 점검 |
| 17 | IN | 불충분한 인가 | 민감한 데이터 또는 기능에 접근 및 수정 시 통제 여부 점검 |
| 18 | CC | 쿠키 변조 | 쿠키 사용 여부 및 사용하는 경우 안전한 알고리즘으로 암호화 여부 점검 |
| 19 | PR | 취약한 패스워드 복구 | 웹 사이트 내 패스워드 복구 절차의 적절성 점검 |
| 20 | SC | 불충분한 세션만료 | 세션의 만료 기간 설정 여부 점검 |
| 21 | SE | 세션 예측 | 단순한 방법(연속된 숫자 할당 등)으로 생성되는 세션 ID를 예측하여 세션 탈취 여부 점검 |
| 22 | SF | 세션 고정 | 사용자 로그인 시 항상 일정하게 고정된 세션 ID 값을 발행하는지 여부 확인 |
| 23 | 중요 정보 처리미흡 | IL | 정보 누출 | 웹 서비스 시 불필요한 정보가 노출되는지 여부 점검 |
| 24 | SN | 데이터 평문 전송 | 서버와 클라이언트 간 통신 시 데이터의 암호화 여부 점검 |
| 25 | 취약한 접근통제 관리 | AE | 관리자 페이지 노출 | 유추하기 쉬운 URL로 관리자 페이지 및 메뉴 접근의 가능 여부 점검 |
| 26 | BF | 약한 문자열 강도 | 웹페이지 내 로그인 폼 등에 약한 강도의 문자열 사용 여부 점검 |
| 27 | 부적절한  환경 설정 | DI | 디렉토리 인덱싱 | 웹 서버 내 디렉터리 인덱싱 취약점 존재 여부 점검 |
| 28 | 기타 | CS | 악성 콘텐츠 | 게시판 등에 악성 콘텐츠 삽입 및 실행 여부 점검 |

[표 10] 클라우드 특화 진단 항목

| NO | 세부 진단 항목 | 항목 설명 |
| --- | --- | --- |
| 1 | Lambda: 서버 사이드 요청 위조 (SSRF) | 애플리케이션 서버에서 요청을 보내 메타데이터/내부 자원을 탈취할 수 있는 취약점 |
| 2 | Lambda: SQL Injection | 검증되지 않은 사용자 입력값이 SQL 쿼리 실행에 영향을 주어 개발자가 의도하지 않은 기능을 실행시키는 취약점 |
| 3 | Lambda: 운영체제 명령실행 | 검증되지 않은 사용자 입력값이 OS 명령어 실행에 영향을 주어 개발자가 의도하지 않은 기능을 실행시키는 취약점 |
| 4 | Lambda: XML 외부객체 공격 (XXE) | XML 문서에서 동적으로 외부 URI의 리소스를 포함시킬 수 있는 External Entity를 사용하여서버의 로컬파일 접근, 서비스 거부 등을 유발할 수 있는 취약점 |
| 5 | DynamoDB: NoSQL Injection | 검증되지 않은 사용자 입력 값이 NoSQL 쿼리실행에 영향을 주어 개발자가 의도하지 않은 기능을 실행시키는 취약점 |
| 6 | S3: 파일 업로드 | 정적 페이지 및 바이너리파일을 업로드하여 2차 악성 행위(피싱, 악성코드 유포 등)가 가능한 취약점 |
| 7 | S3: 불필요한 Public 설정 | 불필요한 public 설정으로 노출될 경우 공격자가 중요 파일에 접근하거나 비공개 서비스에 대해 접근할 수 있는 취약점 |
| 8 | S3: 불필요 기능 및 클라우드 리소스 | 임시파일, 백업파일, 관리자페이지 등에 접근이 가능하여 민감한 정보 노출 및 기능을 이용할 수 있는 취약점 |

* 1. 웹 취약점 위험도 산정

점검 결과 발견된 취약점의 위험도를 “상”,”중”,”하” 취약점으로 분류함

[표 11] 웹 모의해킹 위험도 등급 산정 기준

| 분류 | 중요 취약점 | 취약점 예시 |
| --- | --- | --- |
| 상 | - 관련 취약점을 통한 직접적인 위협이 존재할 경우  - 서버 측 중요 자원에 직접접근 및 수정 가능할 경우  - DB에 직접 접근이 가능하거나 개인정보 열람 및 유출 가능할 경우 | - 파일업로드에 의한 서버 시스템 제어  - 서버 명령 원격지 실행  - DB정보 유출 가능한 SQL Injection  - 관리자 세션 획득이 가능한 XSS  - 파라미터 값을 변조함으로 금전적인 손실이나 관리자 획득이 가능  - 시스템 관리자/ 웹 사이트 계정의 유출 및 획득  - 악성 코드 업로드 및 삭제 가능 |
| 중 | - 해당 취약점을 통한 2차 공격 위협이 존재하는 경우  - '위험도 상' 공격에 악용 가능한 정보 및 수단을 제공하는 경우  - 서버 프로그램 로직의 취약점 등을 이용한 간접적 방식으로 서버 측 정보 변경 및 DB정보 접근 가능 여부 | - 취약한 실명인증 우회  - 시스템 파일 다운로드 가능한 경우  - 파라미터 변조에 의한 인증우회  - 외부 사용자 또는 관리자 접근이 많은  사이트의 XSS 취약점  - 디렉토리 리스팅, 추측 가능한 관리자 페이지, 쿠키변조 등 |
| 하 | - 직접적인 위협은 낮으나 보안기준에 위반되므로 변경이 필요한 사항이 존재할 경우  - 관련 취약점에 대한 보안진단 평가가 대체로 양호한 경우 | - 중요정보가 포함되지 않은 오류 메시지  - GET 방식의 XSS 취약점  - 기본 파일 또는 설치 시 생성된 파일 |

1. 산출물 및 협조사항
   1. 프로젝트 산출물

[표 12] 결과 산출물

| 산출물 | 제출 시기 | 주요 내용 |
| --- | --- | --- |
| 수행 계획서 | 수행 전 | 수행 목적 및 범위  수행 일정 및 인력투입 계획  수행방안 및 산출물 목록  사업추진에 필요한 협조 요청사항 및 선결 사항 등 |
| 결과 보고서 | 종료 시 | 모의해킹 진단 결과 보고서  모의해킹 보안 가이드 |

* 1. 협조 요청 사항

모의해킹 작업 시 시스템에 영향을 줄 수 있는 해킹시도를 수행하지 않으나, 부득이한 경우 시스템에 문제가 발생할 가능성에 대비하여 담당자와 시스템 영향력에 대한 사전 협조 및 동의를 구함. 문제 발생 시 담당자에게 연락을 하여 긴급히 정상화 시킬 수 있도록 담당자가 항시 모니터링 수행을 하도록 권장함

* 1. 수행 전 협의사항

모의해킹 수행 중 발생 가능한 안전사고를 예방하며 효율적인 프로젝트를 진행하기 위해 필요함. 프로젝트 수행 전, 고객사와 협의를 통해 진단대상 및 진단환경과 요구사항을 전달받고 진단 전 진단대상 요청 목록과 협조 사항을 전달함

[표 13] 업무 협의 리스트

| 구분 | 항목 | 예시 |
| --- | --- | --- |
| 진단 대상 | URL 또는 IP | 협의된 대상만 진단을 수행하는지 또는 대상 외 추가 대상 포함 여부 확인 (링크, IP 대역 또는 서브도메인으로 확인) |
| 대상별 용도 | 대국민, 인터넷 뱅킹, WTS, 웹 서비스, 과금 서비스 등 |
| 진단 위치 | 진단 위치 및 담당자 연락처 방문 가능 일정 등 회신 |
| 대상 구분 | 공공, 금융, 민간 기업 등  (공공/금융 진단시 비 인가된 AP 허용을 불가함) |
| 진단 방법 | 테스트 타입 | Blind , Double Blind , Gray Box , Double Gray Box , Tandem , Reversal |
| 모의해킹 시나리오 선정 | 웹서버 공격, 거점을 활용한 내부망 연계 공격 |
| 수행 위치 | 내부/외부 |
| 수행 장소 | 실제 수행 장소 |
| 방화벽 적용 여부 | 적용/미적용 |
| 사용 툴 사전 고지 및 협의 | 자동화 툴 사용 및 트래픽 발생 가능 툴 사용 여부 고지 |
| 무선 네트워크 모의해킹 시나리오 선정 | AP 탐지, 취약 AP를 활용한 연계 공격 시도 허용 여부 |
| 진단 시간  계획 및  일정 | 일정 및 계획 | 일정 및 대상별 진단 계획 |
| 진단 수행 시간 | 기간 : 2014.01.06 ~ 20.14.02.07  시간 : AM 09:00 ~ PM 06:00 |
| 보고 주기 및 방식 | 주간 보고, 모의해킹 종료 시점 보고 등 |
| 진단 일정 및 계획 | 일정 및 대상별 진단 계획 및 무선 네트워크 모의해킹 종료 시점 협의 |
| 고객사  사전 협조  요청 사항 | 관련 문서 요청 | 수행 대상 리스트, 네트워크 구성도, 개발 사양서, 참고 자료 등 |
| IP 할당 요청 | 내부 진단 시 |
| 계정 요청 | 테스트 계정 필요 시 계정요청 |
| 주요 데이터 백업 권고 | 주요 데이터 베이스 백업 권고 |
| 서버 환경 특이 사항 및  주의사항 | 과금 발생, 동시 접속자 수가 많은 서버의 서비스 지연 가능성, 저사양의 네트워크 관리 서버의 시스템 다운 가능성, 로드 밸런싱을 통한 진단 대상 외 분산 서버 접근 가능성 |
| 서버 및 네트워크 운영  담당자 연락망 | 시스템 장애 혹은 서비스 지연사고 발생 시 대응 방안 |
| 방문 허용 요청 | 방문 허용 요청 필요 시 |
| 고객사 특이사항 | 고객사에서 요청한 특이사항 | 특정 시간 내에만 진단, 외부에서만 진단, 관제 대응 현황 체크 등 |
| 산출물 | 최종 제출 산출물 리스트 | 수행계획서, 결과보고서 등 |

별첨 1. 웹 모의해킹 유형

일반적인 웹 모의해킹 테스트의 경우, Blind 테스트 형태로 진행하나 취약점 탐지의 효율성을 높이기 위해서는 Tandem 유형의 해킹 타입을 선호함 (공격자에게 제공하는 정보가 많아 탐지하기 좋음).

[표 14] 웹 모의해킹 테스트 유형 (Common Test Type OSSTMM 3) 상세

| Type | | Description | 공격자 제공 정보(예) | 타겟 제공 정보(예) | 취약점 탐지 효율성 |
| --- | --- | --- | --- | --- | --- |
| 1 | Blind  Test | 공격자는 타겟에 대한 사전 정보가 없는 상태로 모의해킹을 수행하지만 타겟은 공격자가 수행할 테스트에 대한 모든 내용을 인지한 상태로 테스트 수행함. 주로 공격자의 스킬을 테스트하기 위한 목적으로 사용되며 War Gaming에서 사용되는 테스트 방식이 이 분류에 속함 | 공격자 IP  진단 항목  공격시간  진단 도구 | 타겟 URL or IP | 하 |
| 2 | Double Blind | 공격자는 타겟에 대한 사전 정보를 갖고 있지 않으며 타겟도 공격에 대한 아무 정보를 갖지 않은 상태로 수행됨. 해당 테스트를 통해 타겟이 얼마나 공격에 잘 대비하고 있는가를 알 수 있음. Double Blind Test는 블랙박스테스트 혹은 침투 테스트 (모의해킹) 라고 함 | 없음 | 타겟 URL | 하 |
| 3 | Gray Box | 공격자는 타겟에 대해 제한된 정보만 알고 있으며 타겟은 공격에 대한 모든 정보를 사전에 알고 준비된 상태에서 수행함. 이 방식은 테스트의 효율성을 고려한 방식이며 공격자가 갖고 있는 정보에 따라 더 깊은 레벨의 테스트를 수행 할 수 있음. 이 테스트는 취약점 테스트 라고도 하며, 자체 점검을 위해 사용함 | 공격자 IP  진단 항목  공격시간  진단 도구 | 타겟 일반사용자 계정 (최소 2개)  타겟 OS 정보  타겟 WAS 정보  타겟 DB 정보  타겟 URL | 중 |
| 4 | Double Gray Box | 공격자는 타겟에 대해 제한된 정보만 알고 있으며 타겟은 공격에 대해 사전 통보는 받지만 공격에 대한 구체적인 내용은 알고 있지 않은 상태로 수행되며 공격자의 스킬과 타겟의 대응 정도를 평가할 수 있음 | 공격시간 | 타겟 일반사용자 계정 (최소 2개)  타겟 OS 정보  타겟 WAS 정보  타겟 DB 정보  타겟 URL | 중 |
| 5 | Tandem | 공격자와 타겟 모두 공격에 대한 정보를 알고 있으며, 공격자가 대상 시스템에 대한 모든 정보를 알고 모든 권한을 갖고 있는 상태로 수행되므로 발생 가능한 보안 위협에 대해 철저한 검증을 하는 것이 가능함. 단 테스트를 위해 대상 시스템에 대한 모든 정보, 권한을 공격자에게 미리 알려줘야 하므로 내부 인력이 자체 점검을 위해 진행 하는 경우가 많음 | 공격자 IP  진단 항목  공격시간  진단 도구 | 타겟 관리자 계정  타겟 관리자 접속 URL  타겟 일반사용자 계정 (최소 2개)  타겟 시스템 계정  타겟 OS 정보  타겟 WAS 정보  타겟 DB 정보  타겟 웹 소스  타겟 URL | 상 |
| 6 | Reversal | 공격자가 타겟에 대한 모든 정보를 알고 있으나 타겟은 공격에 대해서 언제 어떻게 수행될 지에 대한 아무런 정보를 갖고 있지 않은 상태로 수행함. 이 테스트의 목적은 타겟이 언제 있을지 모르는 공격에 제대로 대응 하고 있는지를 점검하기 위해 수행되며, 공격자가 갖고 있는 정보에 따라 더 깊은 레벨의 테스트를 수행할 수 있음 | 없음 | 타겟 관리자 계정  타겟 관리자 접속 URL  타겟 일반사용자 계정 (최소 2개)  타겟 시스템 계정  타겟 OS 정보  타겟 WAS 정보  타겟 DB 정보  타겟 웹 소스  타겟 URL | 상 |

별첨 2. OWASP Top 10

[표 15] OWASP Top 10

| NO | 항목 | 내용 |
| --- | --- | --- |
| 1 | Broken Access Control (접근 권한 취약점) | 엑세스 제어는 사용자가 권한을 벗어나 행동할 수 없도록 정책을 시행함. 만약 엑세스 제어가 취약하면 사용자는 주어진 권한을 벗어나 모든 데이터를 무단으로 열람, 수정 혹은 삭제 등의 행위로 이어질 수 있음. |
| 2 | Cryptographic Failures (암호화 오류) | Sensitive Data Exposure(민감 데이터 노출)의 명칭이 2021년 Cryptographic Failures(암호화 오류)로 변경되었음. 적절한 암호화가 이루어지지 않으면 민감 데이터가 노출될 수 있음. |
| 3 | Injection (인젝션) | SQL, NoSQL, OS 명령, ORM(Object Relational Mapping), LDAP, EL(Expression Language) 또는 OGNL(Object Graph Navigation Library) 인젝션 취약점은 신뢰할 수 없는 데이터가 명령어나 쿼리문의 일부분으로써, 인터프리터로 보내질 때 취약점이 발생함. |
| 4 | Insecure Design (안전하지 않은 설계) | Insecure Design(안전하지 않은 설계)는 누락되거나 비효율적인 제어 설계로 표현되는 다양한 취약점을 나타내는 카테고리임. 안전하지 않은 설계와 안전하지 않은 구현에는 차이가 있지만, 안전하지 않은 설계에서 취약점으로 이어지는 구현 결함이 있을 수 있음. |
| 5 | Security Misconfiguration (보안설정오류) | 애플리케이션 스택의 적절한 보안 강화가 누락되었거나 클라우드 서비스에 대한 권한이 적절하지 않게 구성되었을 때, 불필요한 기능이 활성화 되거나 설치되었을 때, 기본계정 및 암호화가 변경되지 않았을 때, 지나치게 상세한 오류 메세지를 노출할 때, 최신 보안기능이 비활성화 되거나 안전하지 않게 구성되었을 때 발생함. |
| 6 | Vulnerable and Outdated Components (취약하고 오래된 요소) | 취약하고 오래된 요소는 지원이 종료되었거나 오래된 버전을 사용할 때 발생함. 이는 애플리케이션 뿐만 아니라, DBMS, API 및 모든 구성요소 들이 포함됨. |
| 7 | Identification and Authentication Failures (식별 및 인증 오류) | Broken Authentication(취약한 인증)으로 알려졌던 해당 취약점은 identification failures(식별 실패)까지 포함하여 더 넓은 범위를 포함할 수 있도록 변경되었음. 사용자의 신원확인, 인증 및 세션관리가 적절히 되지 않을 때 취약점이 발생할 수 있음. |
| 8 | Software and Data Integrity Failures(소프트웨어 및 데이터 무결성 오류) | 2021년 새로 등장한 카테고리로 무결성을 확인하지 않고 소프트웨어 업데이트, 중요 데이터 및 CI/CD 파이프라인과 관련된 가정을 하는데 중점을 둠. |
| 9 | Security Logging and Monitoring Failures (보안 로깅 및 모니터링 실패) | Insufficient Logging & Monitoring(불충분한 로깅 및 모니터링) 명칭이었던 카테고리가 Security Logging and Monitoring Failures (보안 로깅 및 모니터링 실패)로 변경되었음. 로깅 및 모니터링 없이는 공격활동을 인지할 수 없음. 이 카테고리는 진행중인 공격을 감지 및 대응하는데 도움이 됨. |
| 10 | Server-Side Request Forgery (서버 측 요청 위조) | 2021년 새롭게 등장하였습니다. SSRF 결함은 웹 애플리케이션이 사용자가 제공한 URL의 유효성을 검사하지 않고 원격 리소스를 가져올 때마다 발생함. 이를 통해 공격자는 방화벽, VPN 또는 다른 유형의 네트워크 ACL(액세스 제어 목록)에 의해 보호되는 경우에도 응용 프로그램이 조작된 요청을 예기치 않은 대상으로 보내도록 강제할 수 있음. |

별첨 3. 국가사이버안전센터에서 발표한 8대 취약점

[표 16] 국가사이버안전센터에서 발표한 8대 취약점

| NO | 항목 | 내용 |
| --- | --- | --- |
| 1 | 디렉토리 리스팅 | 인터넷 사용자에게 모든 디렉토리 및 파일 목록이 보여지게 되고, 파일의 열람 및 저장도 가능하게 되어 비공개 자료가 유출될 수 있음 |
| 2 | 파일 다운로드 | 게시판 등에 저장된 자료에 대해 ‘다운로드 스크립트’를 이용하여 다운로드 기능을 제공하면서, 대상 자료파일의 위치 지정에 제한조건을 부여하지 않았을 경우에 URL칸의 다운로드 스크립트의 인수 값에 ‘../’문자열 등을 입력하여 시스템 디렉토리 등에 있는 /etc/passwd와 같은 비공개 자료들이 유출될 수 있음 |
| 3 | XSS | 게시판에 새 게시물을 작성하여 등록할 때와 같이 사용자의 입력을 받아 처리하는 웹 응용프로그램에서 입력 내용에 대해 실행코드인 스크립트의 태그를 적절히 필터링 하지 않을 경우에 악의적인 스크립트가 포함된 게시물을 등록할 수 있어 해당 게시물을 열람하는 일반 사용자의 PC로부터 개인정보인 쿠키를 유출할 수 있는 등의 피해를 초래할 수 있음 |
| 4 | 파일 업로드 | 첨부파일 업로드를 허용하는 홈페이지 게시판에서 .php, .j네 등의 확장자 이름의 스크립트 파일의 업로드를 허용할 경우에 해커가 악성 실행 프로그램을 업로드한 후에 홈페이지 접속 방식으로 원격에서 서버컴퓨터의 시스템 운영 명령어를 실행시킬 수 있음. |
| 5 | WebDAV | 윈도우 서버 컴퓨터에서 기본으로 설치되는 원격관리기능인 WebDAV가 계속 사용가능 하도록 설정되어 있고, WebDAV 라이브러리 파일의 속성 및 홈페이지 디렉토리에 쓰기 권한이 모두 허용되어 있는 경우에 해커가 WebDAV 도구를 사용, 원격에서 홈페이지 디렉토리에 임의의 파일을 삽입하여 화면을 변조할 수 있음 |
| 6 | 테크노트 취약점 | 국내에서 개발되어 무료 배포중인 게시판 제작 프로그램 ‘테크노트’의 일부 CGI프로그램들에서 인수 값 처리시에‘|’문자 이후에 나오는 컴퓨터 운영 명령어가 실행될 수 있는 결함이 있어 해커는 홈페이지 접속 방식으로 컴퓨터 명령어를 실행하여 화면을 변조 하거나 컴퓨터를 조작할 수 있음 |
| 7 | 제로보드 취약점 | 국내에서 개발되어 무료 배포중인 게시판 제작 프로그램‘제로보드’의 일부 PHP프로그램이 원격에 있는 PHP파일을 실행할 수 있는 결함이 있어 해커는 홈페이지 접속 방식으로 컴퓨터 명령어를 실행하여 화면을 변조하거나 컴퓨터를 조작할 수 있음 |
| 8 | SQL Injection | 웹 브라우저 주소(URL)창 또는 사용자 ID 및 패스워드 입력화면 등에 데이터베이스 SQL문에 사용되는 문자기호( ‘ ) 및 ( “ )의 입력을 적절히 필터링 하지 않은 경우에 해커가 SQL문으로 해석될 수 있도록 조작한 입력으로 데이터베이스를 인증절차 없이 접근, 자료를 무단 유출하거나 변조할 수 있음 |

별첨 4. 주요정보통신 기반시설 기술적 취약점 분석평가 상세가이드(Web)

[표 17] 과학기술정보통신부의 주요 정보통신 기반시설 취약점 분석평가 상세가이드(Web)

| NO | 취약유형 | 코드 | 세부 진단 항목 | 진단 내용 |
| --- | --- | --- | --- | --- |
| 1 | 입력 값 검증 부재 | SI | SQL 인젝션 | 웹페이지 내 SQL 인젝션 취약점 존재 여부 점검 |
| 2 | XI | XPath 인젝션 | 웹페이지 내 조작된 XPath 쿼리 공격 가능성 점검 |
| 3 | OC | 운영체제 명령 실행 | 웹 사이트 내 운영체제 명령 실행 취약점 존재 여부 점검 |
| 4 | XS | 크로스 사이트 스크립팅 | 웹 사이트 내 크로스사이트 스크립팅 취약점 존재 여부 점검 |
| 5 | BO | 버퍼 오버 플로우 | 사용자가 입력한 파라미터 값의 문자열 길이 제한 확인 |
| 6 | FS | 포맷 스트링 | 웹 애플리케이션에 포맷 스트링 취약점 존재 여부 점검 |
| 7 | LI | LDAP 인젝션 | 웹페이지 내 LDAP 인젝션 취약점 점검 |
| 8 | SS | SSI 인젝션 | 웹페이지 내 SSI 인젝션 공격 가능성 점검 |
| 9 | 취약한 파일처리 | FU | 파일 업로드 | 웹 사이트의 게시판, 자료실 등에 조작된 Server Side Script 파일 업로드 및 실행 가능 여부 점검 |
| 10 | FD | 파일 다운로드 | 웹 사이트에서 파일 다운로드 시 허용된 경로 외 다른 경로의 파일 접근이 가능한지 여부 점검 |
| 11 | PT | 경로 추적 | 웹 서버와 웹 애플리케이션의 파일 또는 디렉터리의 접근 통제 여부 점검 |
| 12 | PL | 위치 공개 | 예측 가능한 폴더의 위치 사용 여부 및 불필요한 파일의 존재 여부 점검 |
| 13 | 취약한 인증 및 세션 관리 | CF | 크로스 사이트 리퀘스트 변조(CSRF) | 사용자의 신뢰(인증) 정보의 변조 여부 점검 |
| 14 | PV | 프로세스 검증 누락 | 인증이 필요한 웹 사이트의 중요(관리자 페이지, 회원변경 페이지 등) 페이지에 대한 접근제어 설정 여부 확인 |
| 15 | AU | 자동화 공격 | 웹 애플리케이션의 특정 프로세스(로그인 시도, 게시글 등록, SMS 발송 등)에 대한 반복적인 요청 시 통제 여부 확인 |
| 16 | IA | 불충분한 인증 | 중요 페이지 접근 시 추가 인증 요구 여부 점검 |
| 17 | IN | 불충분한 인가 | 민감한 데이터 또는 기능에 접근 및 수정 시 통제 여부 점검 |
| 18 | CC | 쿠키 변조 | 쿠키 사용 여부 및 사용하는 경우 안전한 알고리즘으로 암호화 여부 점검 |
| 19 | PR | 취약한 패스워드 복구 | 웹 사이트 내 패스워드 복구 절차의 적절성 점검 |
| 20 | SC | 불충분한 세션만료 | 세션의 만료 기간 설정 여부 점검 |
| 21 | SE | 세션 예측 | 단순한 방법(연속된 숫자 할당 등)으로 생성되는 세션 ID를 예측하여 세션 탈취 여부 점검 |
| 22 | SF | 세션 고정 | 사용자 로그인 시 항상 일정하게 고정된 세션 ID 값을 발행하는지 여부 확인 |
| 23 | 중요 정보 처리미흡 | IL | 정보 누출 | 웹 서비스 시 불필요한 정보가 노출되는지 여부 점검 |
| 24 | SN | 데이터 평문 전송 | 서버와 클라이언트 간 통신 시 데이터의 암호화 여부 점검 |
| 25 | 취약한 접근통제 관리 | AE | 관리자 페이지 노출 | 유추하기 쉬운 URL로 관리자 페이지 및 메뉴 접근의 가능 여부 점검 |
| 26 | BF | 약한 문자열 강도 | 웹페이지 내 로그인 폼 등에 약한 강도의 문자열 사용 여부 점검 |
| 27 | 부적절한  환경 설정 | DI | 디렉토리 인덱싱 | 웹 서버 내 디렉터리 인덱싱 취약점 존재 여부 점검 |
| 28 | 기타 | CS | 악성 콘텐츠 | 게시판 등에 악성 콘텐츠 삽입 및 실행 여부 점검 |

별첨 5. 클라우드 모의해킹 방법론(AWS)

[표 18] EQST 클라우드 모의해킹 방법론(AWS) (클라우드 특화 진단 항목)

| NO | 세부 진단 항목 | 항목 설명 |
| --- | --- | --- |
| 1 | Lambda: 서버 사이드 요청 위조 (SSRF) | 애플리케이션 서버에서 요청을 보내 메타데이터/내부 자원을 탈취할 수 있는 취약점 |
| 2 | Lambda: SQL Injection | 검증되지 않은 사용자 입력값이 SQL 쿼리 실행에 영향을 주어 개발자가 의도하지 않은 기능을 실행시키는 취약점 |
| 3 | Lambda: 운영체제 명령실행 | 검증되지 않은 사용자 입력값이 OS 명령어 실행에 영향을 주어 개발자가 의도하지 않은 기능을 실행시키는 취약점 |
| 4 | Lambda: XML 외부객체 공격 (XXE) | XML 문서에서 동적으로 외부 URI의 리소스를 포함시킬 수 있는 External Entity를 사용하여서버의 로컬파일 접근, 서비스 거부 등을 유발할 수 있는 취약점 |
| 5 | DynamoDB: NoSQL Injection | 검증되지 않은 사용자 입력 값이 NoSQL 쿼리실행에 영향을 주어 개발자가 의도하지 않은 기능을 실행시키는 취약점 |
| 6 | S3: 파일 업로드 | 정적 페이지 및 바이너리파일을 업로드하여 2차 악성 행위(피싱, 악성코드 유포 등)가 가능한 취약점 |
| 7 | S3: 불필요한 Public 설정 | 불필요한 public 설정으로 노출될 경우 공격자가 중요 파일에 접근하거나 비공개 서비스에 대해 접근할 수 있는 취약점 |
| 8 | S3: 불필요 기능 및 클라우드 리소스 | 임시파일, 백업파일, 관리자페이지 등에 접근이 가능하여 민감한 정보 노출 및 기능을 이용할 수 있는 취약점 |