**[SKdevsec]**

**취약점 진단 수행계획서**

**2021. 05.** **10**

**- 목 차 -**

[1. 개요 3](#_Toc3284973)

[1.1. 진단목적 3](#_Toc3284974)

[1.2. 진단대상 3](#_Toc3284975)

[1.3. 진단일정 3](#_Toc3284976)

[2. 취약점 진단 시나리오 3](#_Toc3284977)

[2.1. 취약점 진단 개요 4](#_Toc3284978)

[2.2. 취약점 진단 수행 방법 4](#_Toc3284979)

[2.3. 취약점 진단 진단 도구 5](#_Toc3284981)

[2.4. 주요 취약점 및 진단항목 6](#_Toc3284982)

[2.5. 수행 산출물 8](#_Toc3284983)

개요

* 1. 진단목적

SKdevsec의 홈쇼핑 서비스와 시스템에 대하여 비 인가자의 관점에서 취약점 진단을 수행하고, 발견된 취약점이 시스템에 미치는 영향을 파악하여 보안대책을 제시함으로써, 침해사고 예방 및 서비스의 안정성을 확보하는데 그 목적이 있습니다.

* 1. 진단대상

해당 도메인에 대하여 점검을 수행하며, 외부망에서 내부망 침투 가능 테스트 및 침투 과정에서 일반 및 관리자 권한을 획득하여 최종적으로 고객정보의 획득을 목적으로 합니다.

취약점 진단 대상 도메인의 상세 내역은 다음과 같습니다.

|  |  |  |
| --- | --- | --- |
| **No** | **URL** | **비고** |
| 1 | http://www.kilhyomin.com/ | 메인페이지 |

[표 1 – 진단대상]

* 1. 진단일정

진단 일정은 다음과 같습니다.

|  |  |
| --- | --- |
| **업무 수행 내역** | **일정** |
| 사전준비 및 대상 관련 자료 수령 | 2021.05.10 이전 |
| 1차 취약점 진단 수행 | 2021.05.11 ~ 2021.05.18 |
| 결과 분석 및 결과 보고서 작성 | 2021.05.19 ~ 2021.05.22 |
| 2차 취약점 진단 수행 | 2021.06.04 ~ 2021.06.09 |
| 결과 분석 및 결과 보고서 작성 | 2021.06.10 ~ 2021.06.13 |
| 보고서 최종 수정 및 완료 | 2021.06.13 (종료) |

[표 2 – 진단일정]

# 취약점 진단 시나리오

* 1. 취약점 진단 개요

(1) 고객사 사이트의 취약점 진단 의뢰 가정(사이트 개발)

(2) 대상시스템의 IP Address 정보와 코드를 제공받아 취약점 진단을 수행

(3) 고객사의 내부 서비스용 시스템을 대상으로 수행

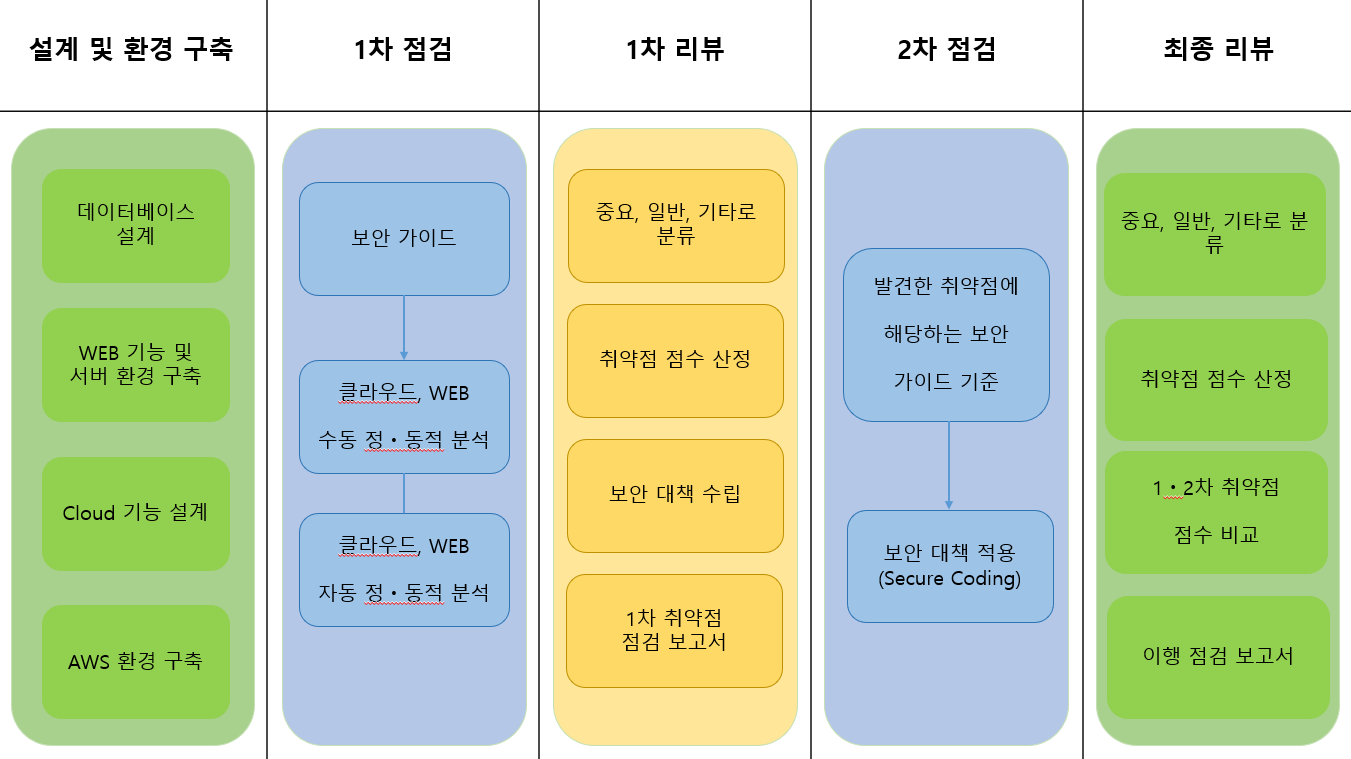
(4) 가이드 라인을 바탕으로 취약점 진단 수행

(5) 자동화 툴과 병행하여 다양한 방법의 취약점 진단 수행

* 1. 취약점 진단 수행 방법

아래 그림과 같이 기본적인 프로젝트 준비와 실제 구축을 진행하는 (1) 설계 및 환경 구축를 거쳐 수동 및 자동 점검을 실시하는 (2) 1차 점검를 진행합니다. 이 단계에서 수집된 정보를 바탕으로 하여 (3) 1차 리뷰를 진행하며 발생한 취약점을 보완하여 시큐어 코딩이 적용되는 (4) 2차 점검를 수행합니다. 마지막으로 개선전과 개선후의 비교를 통한 보고서 작성과 미흡한 부분에 대해서 검토하는 (5) 최종 리뷰를 수행합니다.

[그림 1 – 취약점 진단 수행 방법]



* + 1. 설계 및 환경 구축

가정한 고객사의 웹페이지를 개발하는 단계입니다. 데이터 베이스 설계, 웹의 기능 및 서버 환경을 구축하고 프론트엔드와 백엔드의 서버를 위한 클라우드 기능 설계과 AWS환경 구축을 진행합니다.

* + 1. 1차 점검

보안 가이드를 바탕으로 동적 분석을 진행합니다. 동적 분석은 수동과 자동을 병행합니다. 수동 점검은 보안 가이드에 있는 XSS / CSRF 공격 가능성, SQL / Command Injection 공격 가능성 등 26항목을 주요항목과 일반항목으로 나누고, 시스템의 직접적인 접근 및 침입, DB 획득 등 서버 시스템 장악이 가능한 취약점을 주는 주요항목을 중점으로 공격을 진행합니다. 이와 더불어 자동화 툴을 이용하여 수동점검과 비교하여 미진한 부분을 보충하여 점검을 실시합니다.

* + 1. 1차 리뷰

1차 점검에서 나온 결과를 기반으로 하여 중요, 일반, 기타를 내부적으로 분류합니다. 주요항목과 일반항목의 개수를 종합하여 100점 만점을 기준으로 취약점 점수를 산정합니다. 이후 해당 고객사의 맞는 보안 대책을 수립하고, 취약점 점검 보고서를 작성합니다.

* + 1. 2차 점검

점검에서 포착된 보안상 취약한 부분을 보안 가이드를 기준으로 시큐어 코딩을 조사하고 적용합니다. 그 다음, 1차 점검과 동일한 방식으로 2차 점검을 실시합니다.

* + 1. 최종 리뷰

개선되지 못한부분에 대하여 중요, 일반, 기타를 재분류 취약점 점수를 재산정하여 개선의 정도를 비교합니다. 이후 적용한 보안대책에대한 보고서를 작성합니다.

* 1. 취약점 진단 진단 도구

보다 정확한 취약점 점검을 위해 수동과 도구를 병행하여 진행합니다.

취약점 진단을 수행하기 위해 사용되는 도구들을 정리하면 다음과 같습니다.

|  |  |
| --- | --- |
| **구분** | **진단 항목 설명** |
| Burpproxy | Proxy 기능을 이용한 웹 세션 및 파라미터 조작 도구 |
| Wireshark | 네트워크 패킷 점검 도구  http://www.wireshark.com/ |
| arachni | Ruby언어 기반의 무료 웹사이트 취약점 점검 도구 |

[표 3 – 취약점 진단 진단 도구]

* 1. 주요 취약점 및 진단항목

취약점 진단 진단 항목은 OWASP Top 10 주요 취약점 항목과 과학기술정보통신부에서 고시한 취약점 분석•평가 기준 항목을 반영하여, 아래와 같이 진단항목을 선정합니다.

|  |  |
| --- | --- |
| **구분** | **내용** |
| OWASP TOP 10 | 국제 OWASP(The Open Web Application Security Project) 협회에서 발표한 웹 기반 어플리케이션의 10대 취약점을 이용하여 침투 테스트를 수행 |
| 과학기술정보통신부 | 주요정보통신기반시설의 안정적 운영과 중요정보의 기밀성, 무결성, 가용성에 영향을 미칠 수 있는 위협요인을 파악하고 제거하기 위하여 국정원 및 관계 중앙행정기관과 협의를 통해 수립한 기준이며, 정보통신기반보호법 제9조의 규정에 근거함 |

[표 4 – 취약점 진단 선정 항목 기준]

|  |  |  |
| --- | --- | --- |
| **구분** | **진단 항목** | **진단 항목 설명** |
| **1** | XSS / CSRF 공격 | 게시판 및 URL인자 값에 특정 자바스크립트 를 입력하여 클라이언트 측에 실행하는 공격 |
| **2** | SQL / Command Injection 공격 | 로그인 폼 및 변수 값에 SQL 쿼리문을 입력하여 로그인 우회, DB 열람 및 조작을 하는 공격 |
| **3** | 검증되지 않은 리다이렉트와 포워드 | 변수 값을 조작하여 피싱이나 악성코드를 설치하는 악성 사이트로 리다이렉트 시키는 URL을 생성하는 공격 |
| **4** | 파라미터 값 및 히든(hidden) 필드 조작 | 파라미터나 히든 필드 조작을 통하여 인증이 없는 페이지에 접속하거나 서버 측에 전송하는 과정에서 조작하는 공격 |
| **5** | 악성코드파일 업로드 | asp, php, jsp 와 같이 파일을 업로드하여 시스템 권한을 획득하는 공격 |
| **6** | 파라미터 값 위조/변조를 통한 서버 데이터 활용 | 파라미터 값이나 URL을 위/변조하여 권한이 없는 게시물의 내용을 보거나 타인의 정보를 열람 및 유출 가능성 점검 |
| **7** | 중요 정보 파일 다운로드 | 파일을 다운로드하는 애플리케이션 인자 값을 조작하여 시스템 내 파일을 다운로드 하는 공격 |
| **8** | 패스워드 정책 유무 및  반영 여부 | 패스워드 재/생성시 안전한 패스워드 규칙 적용 여부 확인 |
| **9** | 인증 실패 횟수 제한 | 로그인 및 인증실패 제한 여부 점검 |
| **10** | 계정 정보 파악 | 웹 페이지에서 계정 정보가 노출될 여부 점검 |
| **11** | 관리자 페이지 분리 여부 | 일반 사용자와 관리자 로그인 페이지의 분리 여부 확인 |
| **12** | 검색엔진 정보 노출 가능성 | 웹 서비스 공격에 필요한 정보가 검색되는지 여부 확인 |
| **13** | 백업 파일 및 테스트 파일 존재 여부 | 서버 내 백업파일, 디폴트 페이지, 샘플 파일 등을 통하여 중요 정보를 획득하는 공격 |
| **14** | 쿠키 조작 가능성 | 쿠키 조작 및 도용으로 타사용자처럼 위장하는 공격 |
| **15** | 세션 재사용 가능성 및 타임아웃 설정 여부 | 동일한 세션 정보를 이용해 사용자의 세션 정보를 탈취 및 도용하는 공격 여부 확인 및 타임하웃 설정 확인 |
| **16** | 접근제어 우회 가능성 확인 | 우회가 가능한 부분에서 인증 / 권한 처리 존재 여부 확인 |
| **17** | 비인증 상태로 중요 page접근 가능성 | 로그인이 필요한 페이지에 비 로그인시 이동되는지에 대한 여부 확인 |
| **18** | 일반계정 권한 상승 가능성 | 접근제어통제(ACL)의 설정 여부 확인 |
| **19** | 소스코드 내 주요정보 노출 여부 | 하드 코딩내용중 주요 정보가 포함되어있는지 여부 확인 |
| **20** | 요청 및 응답 값 내 주요정보 포함여부 확인 | 용청 및 응답간에 주요한 값이 포함되어 있는지 여부 확인 |
| **21** | 오류페이지를 통한 정보 노출 여부 | 에러 페이지에서 노출되는 시스템의 정보 노출 여부 확인 |
| **22** | 일괄적인 오류 처리 페이지 존재 여부 | 계정 존재 유무를 유추할 수 있는 오류메세지 노출 여부 확인 |
| **23** | Client Request Method | PUT, DELETE 등 메소드로 악성파일 업로드, 중요파일의 삭제 등 웹 사이트를 변조할 수 있는 취약점 |
| **24** | 파일 목록화 가능성 | 디렉토리 검색 기능이 활성화 되어있는지 여부 확인 |
| **25** | 서버 헤더정보 노출 | 응답 헤어를 통해 웹 서버 또는 웹 애플리케이션 서버의 종류 및 버전 정보가 노출되는지 여부 확인 |
| **26** | 취약한 보안설정 | 보안상 취약한 서버 설정, 패치 및 라이브러리, 모듈, 알고리즘, 프레임 워크 등의 사용이 있는지 확인 |
| **27** | 취약점 진단 항목에 정의되지 않은 취약점 | 서비스 상에 존재하는 기타 취약점 |

[표 5 – 주요 진단 항목]

* 1. 수행 산출물

|  |  |  |
| --- | --- | --- |
| **산출물** | **제출 시기** | **비고** |
| **취약점 진단 수행계획서** | 진단 수행 전 | 본 문서 |
| **취약점 진단 결과보고서** | 진단 수행 후 | 결과 보고서, 이행 점검 보고서 작성 |

[표 6 – 수행 산출물]