Confidential

WEB 취약점진단 수행계획서

2025. 08. 13.

SK 쉴더스

Confidentiality Agreements

본 보고서는 시스템 정보와 관련한 비공개 사항이 포함되어 있으므로, 열람권한은 우선적으로 정보보안 책임자로 제한되며, 이외의 열람자격은 정보보안 책임자가 허락한 최소한의 인원으로 제한하여 주시기 바랍니다.

본 보고서는 양사간의 사전 협의 없이 어떠한 목적으로도 외부로 유출되거나 무단 복제, 무단 사용될 수 없으며, 기밀성을 유지한다는 전제하에 사용이 엄격 하게 제한됩니다.

본 보고서는 SK쉴더스에서 작성을 하였으며, 정보보호 서약에 대한 사항을 준수합니다.

- 목 차 -

1. 개요

1.1. 진단목적

본 WEB 취약점진단은 **"J.W.P. MagicShop"**의 대내외 서비스와 WEB 시스템에 대해서 취약점진단을 수행하고, 발견된 취약점이 시스템에 미치는 영향을 파악하여 보안대책을 제시함으로써, 침해사고 예방 및 서비스의 안정성을 확보하는 데 목적이 있습니다.

1.2. 진단대상

취약점진단 대상 도메인의 상세 내역은 다음과 같습니다.

No	URL	비고
1	http://43.203.87.232	홈페이지

[표 1 – 진단대상]

1.3. 진단일정

진단 일정은 다음과 같습니다.

업무 수행 내역	일정
사전준비 및 대상 관련 자료 수령	2025.08.01 ~ 2025.08.09
취약점진단 수행	2025.08.11 ~ 2025.09.05
결과 분석 및 결과 보고서 작성	2025.09.05 ~ 2025.09.17
보고서 최종 수정 및 완료	2025.09.17 (종료)

[표 2 – 진단일정]

2. WEB 취약점진단

2.1. 진단 개요

비 인가자로 인한 해킹의 위협을 테스트 하기 위하여 고객사의 내부 서비스용 시스템을 대상으로 아래와 같은 환경에서 테스트를 실시합니다.

(1) 취약성분석 전용영역인 SWAT Room 에서 안전하게 진단을 수행

(2) 대상시스템의 IP Address 정보만을 획득한 상태에서 취약점진단을 수행

(3) 고객사의 내부 서비스용 시스템을 대상으로 수행

(4) 대상 시스템의 특권을 획득하여 특권소유의 파일 또는 디렉터리 표시를 남김

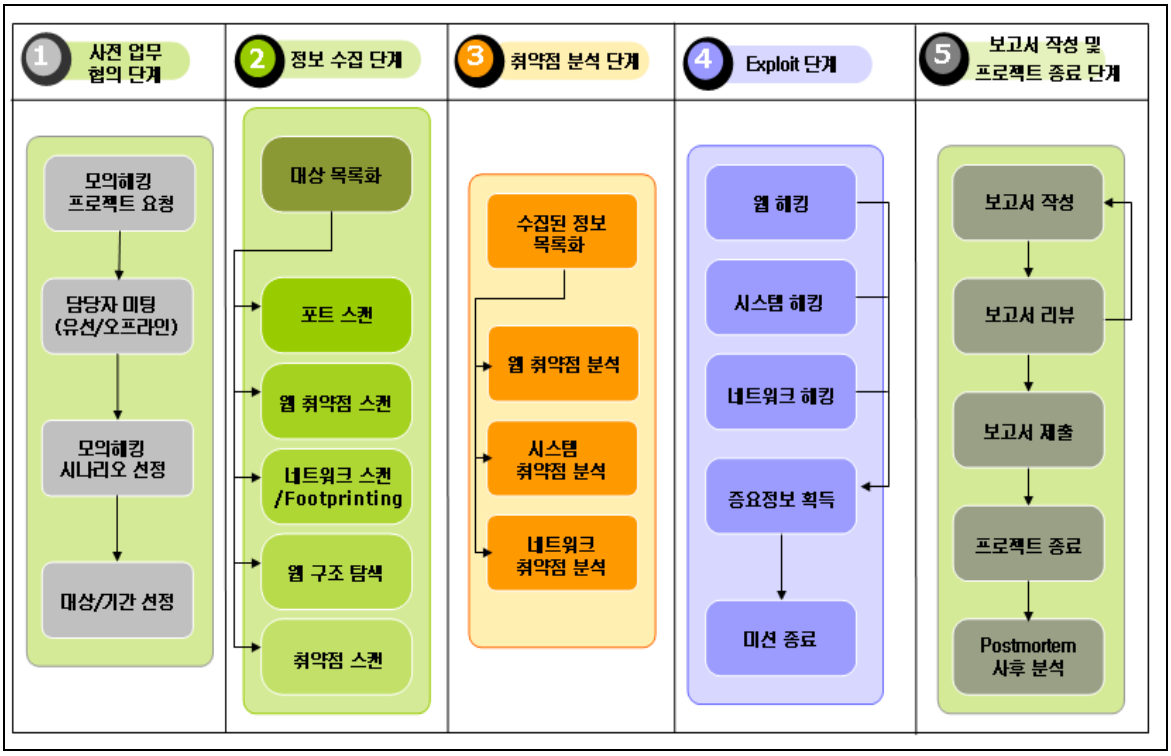
(UNIX 계열 : /infosec, Windows 계열 : C:₩infosec)

(5) 대상 시스템 주변의 시스템을 이용한 공격이 가능할 경우 주변 시스템을 경유한 공격

2.2. 진단 수행 방법

웹 취약점진단 수행 절차는 SK 쉴더스에서 자체 연구 개발한 방법론인 TMoIPT(The Methodology of Infosec Penetration Test)를 통해서 수행됩니다.

아래 그림과 같이 기본적인 프로젝트 준비를 위한 "1) 사전 업무 협의 단계"를 거쳐 대상과 시나리오 및 기간을 정한 후 정보 수집을 위한 "2) 정보 수집 단계"를 진행합니다. 이 단계에서 수집된 정보를 바탕으로 하여 "3) 취약점 분석 단계"를 진행하며 상세 취약점 분석 단계 후에 실제 공격을 위한 "4) Exploit 단계"를 수행합니다. 마지막으로 발견된 취약점과 위협에 대한 보고서를 작성하고 검토하는 "5) 보고서 작성 및 프로젝트 종료 단계"를 수행합니다.



[그림 1 – 취약점진단 수행 방법]

(1) 사전 업무 협의 단계

취약점진단 대상에 대해 담당자와 협의하여 취약점진단 시나리오 선정, 취약점진단 대상, 기간을 선정하는 단계입니다. 이 단계에서 취약점진단 수행 시 유의사항 및 장애 대응방안에 대한 것을 설명을 드리고 취약점진단 수행계획서를 작성합니다.

(2) 정보 수집 단계

취약점진단 대상에 대해 정보를 수집하는 단계로 기업의 전산시스템이 속한 네트워크 구간에 대한 정보 수집을 통해서 사용하고 있는 IP 대역을 조사하며, 수집된 대상 IP 구역 내 시스템에 대해서 포트스캔, 웹 취약점 스캔, 네트워크 스캔 등을 수행하여 공격을 위한 정보를 수집합니다.

이 단계에서 자동화된 스캐닝 툴을 이용하기 때문에 장애가 발생하지 않도록 사전에 고객 측 담당자와 긴밀히 협조하여 진행합니다.

(3) 취약점 분석 단계

정보수집단계에서 수집된 정보를 기반으로 하여 대상 시스템에 대한 취약점을 분석합니다. 이 단계에서 High Risk, Middle Risk, Low Risk 를 내부적으로 분류하여 이 중 High Risk 부분을 중점적으로 공격을 진행합니다.
취약점진단 성격상 내부 망에 침투하여 대상 전산 시스템의 중요한 기밀 정보를 추출할 수 있는 가능성 여부를 확인하는 단계이기 때문에 Low Risk 와 같은 취약점보다 High Risk 취약점을 중점으로 분석을 진행합니다.

(4) Exploit 단계

취약점 분석단계에서 정리된 Risk Level 별 취약점 항목에 대해서 실제 시스템에 공격을 진행하는 단계입니다. 이 단계에서 웹 해킹, 시스템 해킹, 네트워크 해킹을 수행하게 되며 웹 서버의 권한 획득, 시스템 권한획득을 시도합니다.
다양한 공격을 통해 내부 망에 중요한 정보나 중요 DB 시스템에 접속하여 Top Secret 를 추출하면 미션을 종료합니다.

(5) 보고서 작성 및 프로젝트 종료 단계

취약점진단 진행 시 발견된 취약점과 위협에 대한 설명과 그에 대한 보안대책을 제시하기 위해 보고서를 작성하는 단계입니다. 최종적으로 작성된 보고서는 고객에게 전달합니다.

2.3. 기타 수행 방법

대상시스템의 서비스에 영향을 주는 테스트(예:DoS 공격)는 안전을 위하여 테스트 항목에서 제외합니다. 대상시스템의 서비스에 장애 발생 시에는 비상연락망을 통하여 긴급조치를 취하여 복구될 수 있도록 합니다.

2.4. 진단 도구

WEB 취약점진단의 특성상 툴을 이용한 진단은 정확도가 떨어지며 상황 별 판단이 필요하므로 대부분 취약점진단 전문인력이 수동으로 진단합니다.

WEB 취약점진단을 수행하기 위해 사용되는 도구들을 정리하면 다음과 같습니다.

구분	진단 항목 설명
Burp Suite / Burpproxy	Proxy 기능을 이용한 웹 세션 조작 도구
dirbuster	브루트포싱 방식의 디렉터리·파일 점검 도구
wireshark	네트워크 패킷 점검 도구 http://www.wireshark.com/
기타	기타 진단자가 작성한 Exploit Code

[표 3 – WEB 취약점진단 도구]

2.5. 주요 취약점 및 진단항목

구분	진단 항목	진단 항목 설명
1	버퍼 오버플로우	사용자가 입력한 파라미터 값의 문자열 길이 제한 점검
2	포맷스트링	포맷스트링과 이것을 사용하는 printf() 함수의 취약점을 이용하여 RET의 위치에 셸 코드의 주소를 읽어 셸을 획득하는 공격
3	LDAP 인젝션	웹 애플리케이션을 악용하여 민감한 사용자 정보를 노출하거나 LDAP (Lightweight Directory Access Protocol) 데이터 저장소에 표시된 정보를 수정할 수 있는 코드 주입 공격
4	운영체제 명령 실행	웹에서 시스템 명령어인 system(), exec() 등을 실행시킬 수 있는 환경을 제공한 대상에게 실행되는 공격
5	SQL 인젝션	응용 프로그램 보안 상의 허점을 의도적으로 이용해, 악의적인 SQL문을 실행되게 함으로써 데이터베이스를 비정상적으로 조작하는 코드 인젝션 공격
6	SSI 인젝션	시스템 권한을 가지지 못한 일반 사용자도 시스템 명령을 삽입할 수 있는 공격
7	XPath 인젝션	웹 애플리케이션의 보안 취약점을 이용하여 공격자가 악의적인 XPath 쿼리를 주입하고 실행할 수 있는 공격
8	디렉터리 인덱싱	WEB 서버 구조 노출뿐만 아니라 백업 파일이나 소스파일, 공개되어서는 안되는 파일 등에 대해 목록 점검
9	정보 누출	웹/앱에서 사용자와 관련되거나 서버에 관련된 정보를 노출 점검
10	악성 콘텐츠	게시판 등에 악성 콘텐츠 삽입 및 실행 여부 점검
11	크로스사이트 스크립팅	악의적인 사용자가 공격하려는 사이트에 스크립트를 넣는 공격
12	약한 문자열 강도	웹페이지 내 로그인 폼 등에 약한 강도의 문자열 사용 여부 점검

13	불충분한 인증	중요 페이지 접근 시 추가 인증 요구 여부 점검
14	취약한 패스워드 복구	웹 사이트 내 패스워드 복구 절차의 적절성 점검
15	크로스사이트 리퀘스트 변조(CSRF)	사용자가 자신의 의지와 무관하게 공격자가 의도한 요청을 웹 서버에 전송하도록 만드는 공격
16	세션 예측	단순한 방법(연속된 숫자 할당 등)으로 생성되는 세션 ID를 예측하여 세션 탈취 여부 점검
17	불충분한 인가	민감한 데이터 또는 기능에 접근 및 수정 시 통제 여부 점검
18	불충분한 세션 만료	세션의 만료 기간 설정 여부 점검
19	세션 고정	사용자 로그인 시 항상 일정하게 고정된 세션 ID 값을 발행하는지 여부 점검
20	자동화 공격	웹 애플리케이션의 특정 프로세스(로그인 시도, 게시글 등록, SMS 발송 등)에 대한 반복적인 요청 시 통제 여부 점검
21	프로세스 검증 누락	인증이 필요한 웹 사이트의 중요(관리자 페이지, 회원변경 페이지 등) 페이지에 대한 접근제어 설정 여부 점검
22	파일 업로드	웹 사이트의 게시판, 자료실 등에 조작된 Server Side Script 파일 업로드 및 실행 가능 여부 점검
23	파일 다운로드	웹 사이트에서 파일 다운로드 시 허용된 경로 외 다른 경로의 파일 접근이 가능한지 여부 점검
24	관리자 페이지 노출	유추하기 쉬운 URL로 관리자 페이지 및 메뉴 접근의 가능 여부 점검
25	경로 추적	서버와 웹 애플리케이션의 파일 또는 디렉터리의 접근 통제 여부 점검
26	위치 공개	예측 가능한 폴더의 위치 사용 여부 및 불필요한 파일의 존재 여부 점검
27	데이터 평문 전송	서버와 클라이언트 간 통신 시 데이터의 암호화 여부 점검

28	쿠키 변조	쿠키 사용 여부 및 사용하는 경우 안전한 알고리즘으로 암호화 여부 점검

[표 4– 주요 진단 항목]

2.6. 수행 산출물

산출물	제출 시기	비고
취약점진단 수행계획서	진단 수행 전	본 문서
취약점진단 결과보고서	진단 수행 후	대상 정보시스템의 취약점진단 진단과정, 결과에 대한 개선안의 설명서
취약점 이행점검 결과보고서	조치 이행 후	대상 정보시스템의 점검 결과에 대한 설명서

[표 5 – 수행 산출물]

3. 협조사항

비인가자로 인한 해킹의 위협을 테스트 하기 위하여 고객사의 내부 서비스용 시스템을 대상으로 아래와 같은 환경에서 테스트를 실시합니다.

3.1. 진단 수행 간의 협조 사항

(1) 대상 도메인의 URL 정보

(2) 진단 수행간의 발생한 흔적 삭제

(3) 대상 시스템의 정상 작동 확인

3.2. 담당자에게 협조를 구하는 사항

(1) 담당하고 있는 대상에 대한 취약점진단 일정 숙지

(2) 비상 사태에 대비하여 주요 데이터에 대한 백업 수행

(3) 취약점진단 수행기간 동안 특이사항 발생에 대비한 담당자 대기