[CI]

웹진단 수행계획서

2023. 07. 26.

SK shieldus

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 SK인포섹에서 작성을 하였으며, 정보보호 서약에 대한 사항을 준수 합니다.

– 목 차 –

The table of contents is empty because you aren't using the paragraph styles set to appear in it.

1.개요

1. 진단목적

본 취약점 진단은 **"JM COLLECTION"**에서 운영 중인 애플리케이션 서비스에 대하여 취약점 체크리스트를 기반으로 주요 정보의 전자적 침해 행위에 대한 취약점을 분석·평가하고, 존재하는 위협 요소에 대해 정확한 분석을 통해 보안대책을 수립 및 취약점을 제거하여 보안 위협을 최소화함으로써 사고 예방 및 안전한 운영에 기여하고자 합니다.

2. 진단대상

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

웹진단 대상 도메인의 상세 내역은 다음과 같습니다.

No	URL	비고
1	http://3.21.161.99/	쇼핑몰 홈페이지

[표 1 – 진단대상]

3. 진단일정

진단 일정은 다음과 같습니다.

업무 수행 내역	일정
사전준비 및 대상 관련 자료 수령	2023.07.28 이전
웹진단 수행	2023.08.06 ~ 2023.08.23
결과 분석 및 결과 보고서 작성	2023.08.19 ~ 2023.08.30
보고서 최종 수정 및 완료	2023.08.31 (종료)

[표 2 – 진단일정]

4. 웹진단 개요

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

(1) 취약성 분석 전용 영역인 SWAT Room에서 안전하게 진단을 수행

(2) 대상 시스템의 IP Address 정보, 관리자 계정을 획득한 상태에서 웹진단을 수행

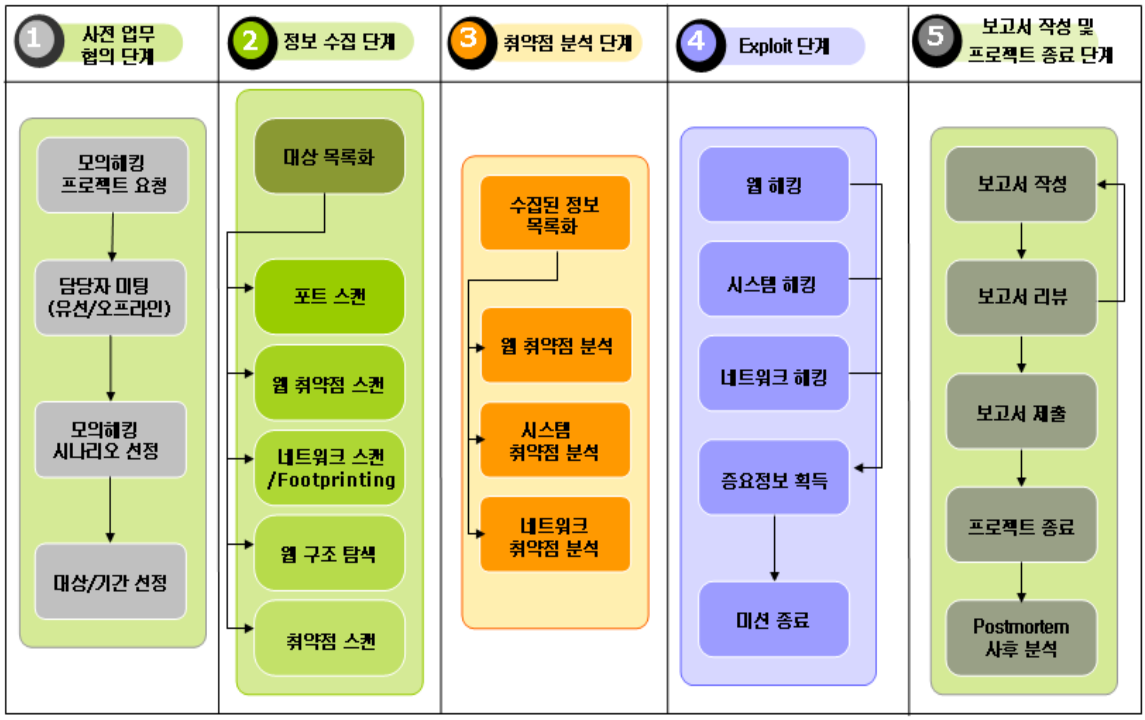
(3) 고객사의 내부 서비스용 시스템을 대상으로 수행

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

5. 웹진단 수행 방법

웹진단 수행 절차는 총 8개 분류와 28개의 항목의 체크리스트로 구성됩니다. 체크리스트는 OWASP와 NIST에서 권고하는 항목과 본 프로젝트와 연관성이 있는 보안상의 문제점을 주축으로 수립한 항목이며, 본 항목을 기반으로 수동 진단 및 점검을 수행하게 됩니다

아래 그림과 같이 기본적인 프로젝트 준비를 위한 “1) 사전 업무 협의 단계”를 거쳐 대상과 진단 항목 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 단계를 수행합니다. 마지막으로 발견된 취약점과 위협에 대한 보고서를 작성하고 검토하는 “4) 보고서 작성 및 프로젝트 종료 단계”를 수행합니다.



[그림 1 – 웹진단 수행 방법]

(1) 사전 업무 협의 단계

웹진단 대상에 대해 담당자와 협의하여 진단 항목 선정, 진단 대상, 기간을 선정하는 단계입니다. 이 단계에서 진단 수행 시 유의사항 및 장애 대응 방안에 대한 것을 설명을 드리고 웹진단 수행계획서를 작성합니다.

(2) 정보 수집 단계

진단 대상에 대해 정보를 수집하는 단계로 기업의 전산 시스템이 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 긴밀이 협조하여 진행합니다.

(3) 취약점 분석 단계

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

(4) 보고서 작성 및 프로젝트 종료 단계

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

6. 기타 수행 방법

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

7. 웹진단 진단 도구

웹진단의 특성상 툴을 이용한 진단은 정확도가 떨어지며 상황 별 판단이 필요하므로 대부분 진단 전문 인력이 수동으로 진단합니다.

웹 취약점 진단을 수행하기 위해 사용되는 도구들을 정리하면 다음과 같습니다.

구분	진단 항목 설명
Burp Proxy	Proxy 기능을 이용한 웹 세션 조작 도구
nmap	다양한 port scan 기능과 OS Identification을 제공함. http://www.insecure.org/nmap/
기타	기타 진단자가 작성한 Exploit Code

[표 3 – 웹진단 진단 도구]

8. 주요 취약점 및 진단항목

웹진단 진단 항목은 OWASP Top 10 주요 취약점 항목과 NIST에서 권고하는 항목 및 과학기술정보통신부에서 고시한 취약점 분석•평가 기준 항목을 반영하여, 아래와 같이 진단 항목을 선정합니다.

구분	내용
OWASP TOP 10	국제 OWASP(The Open Web Application Security Project) 협회에서 발표한 웹 기반 애플리케이션의 10대 취약점을 이용하여 침투 테스트를 수행
NIST	미국 국가 표준 기술연구소 NIST(National Institute of Standards and Technolohy)에서 발표한 취약점 사례를 줄일 수 있도록 하는 권고사항을 제공하는 보고서를 참고하고 웹 진단을 수행
과학기술정보통신부	주요 정보통신 기반 시설의 안정적 운영과 중요 정보의 기밀성, 무결성, 가용성에 영향을 미칠 수 있는 위협요인을 파악하고 제거하기 위하여 국정원 및 관계 중앙행정기관과 협의를 통해 수립한 기준이며, 정보통신 기반보호법 제9조의 규정에 근거함

[표 4 – 웹진단 선정 항목 기준]

구분	진단 항목	진단 항목 설명
1	XSS / CSRF 공격 가능성	XSS / CSRF 취약점은 공격자가 웹 애플리케이션을 사용해서 다른 최종 사용자에게 악성코드를 보내 사용자 의도와 상관없이 특정 행위를 발생 시 키는 취약점
2	삽입 (Injection) 공격 가능성	해당 항목은 SQL Injection 및 Command Injection 등의 웹 애플리케이션 또는 응용프로그램에서 발생할 수 있는 모든 삽입(Injection) 공격 취약점
3	파라미터 값 및 히든 (hidden) 필드 조작 가능성	API 및 웹 애플리케이션에 전달되는 파라미터 값이나 히든 필드를 위조 /변조하여 타인의 게시물 및 개인정보 열람, 결제금액 변경, 타인의 글 수정 등을 할 수 있는 취약점
4	SSRF / File Inclusion 공격 가능성	해당 항목은 URI 구조에서 사용되는 파라미터(경로) 값의 검증 부재로 발생하는 취약점
5	검증되지 않은 리다이렉트와 포워드	검증되지 않은 URL 리다이렉트와 포워드는 악의적 목적의 사용자가 사이트에 직접적인 공격을 가하지 않고도 피싱이나 악성코드를 설치하는 악성 사이트로 리다이렉트 시키는 URL을 생성하여 불특정 다수에 스팸 메일 또는 게시글에 링크 클릭을 유도하거나 인증 토큰 발급 시 리다이렉션 도메인을 변조하여 사용자에 대한 인증 도용 및 정보 수집 등 또 다른 공격에 활용될 가능성이 있는 취약점
6	입력 값 크기 및 무결성 검증 오류	공격자가 웹 애플리케이션을 사용해서 다른 최종 사용자에게 악성코드를 보내 사용자 의도와 상관없이 특정 행위를 발생시키는 취약점

7	악성코드파일 업로드	악성코드 파일 업로드 가능성 취약점은 웹 서버의 잘못된 설정을 이용하여 웹 서버 내에서 악성코드를 실행하는 취약점
8	중요 정보 파일 다운로드 가능성	특정 디렉터리 내에 있는 디렉터리나 파일에 접근하기 위해 외부 입력 값으로 접근 경로명을 구성할 경우 지정된 디렉터리 외 경로로 접근할 수 있는 특수문자(“..”, “/” 등)를 경로명에 포함하여 시스템 내의 파일을 다운로드할 수 있는 취약점
9	패스워드 정책 유무 및 반영 여부	패스워드 생성/재생성 시 안전한 패스워드 규칙이 적용되지 않아 제3자 또는 공격자가 쉽게 추측할 수 있으며 무차별 대입 공격 등을 통하여 짧은 시간 내 패스워드를 획득할 수 있는 취약점
10	인증 실패 횟수 제한	아이디/패스워드 기반의 인증 또는 휴대폰 SMS, E-Mail 인증 등을 통한 인증 시도 시 실패 횟수 제한이 존재하지 않을 경우, 인증 시도를 무한 반복할 수 있어 Brute Force Attack이나 Dictionary Attack에 취약
11	계정 정보 파악 가능성	일반적으로 게시물의 작성자, 댓글 작성자, 이벤트 당첨자 등에 사용자의 계정 정보를 노출할 경우 패스워드 추측이나 접근 시도의 중요한 정보를 제공 또한 관리자 로그인 시 디폴트 계정 또는 추측 가능한 계정(예: admin, manager, administrator, system 등)을 사용할 경우에도 무작위 대입 공격에 노출
12	관리자 페이지 분리 여부	일반 사용자와 관리자의 로그인 페이지가 동일할 경우, 관리자로의 접근 시도가 발생할 수 있는 취약점
13	검색엔진 정보 노출 가능성	검색 엔진 기능에 의해 웹 서비스 공격에 필요한 정보(시스템, 개인정보 등)가 검색되어 해킹의 빌미를 제공할 수 있는 취약점
14	백업 파일 및 테스트 파일 존재 여부	시스템 설치 시 생성되는 디폴트 페이지 및 개발, 운영상에 생성되는 백업 파일 또는 테스트 파일을 작성하는 경우가 많지만, 이를 잊어버리고, 방치했을 경우 공격자는 이런 파일에 접근하거나, 구글과 같은 검색 엔진을 통해 각종 시스템과 애플리케이션에 대한 정보를 획득할 수 있으며 이러한 정보를 통해 웹 서버 침투, 자료 유출, 시스템을 제어 등의 2차 공격에 악용될 수 있는 취약점 또한, 웹 에디터 모듈의 디폴트/샘플 페이지 등이 그대로 존재할 경우 이를 통하여 악성코드 파일의 업로드에 활용될 수 있으며 특히 FCKeditor의 샘플 페이지를 통해 디렉터리 탐색 등 서버의 추가 정보를 얻는데 활용될 수 있는 취약점
15	쿠키(Cookie) 및 웹 스토리지(Web Storage) 조작 가능성	쿠키(Cookie)는 클라이언트와 서버 간의 정보 유지를 위해서 사용하는 기술로 HTTP 프로토콜의 단점을 보완하고자 만든 기술이지만, 별도의 암호화나 안전성을 확보하지 못해, 네트워크 패킷을 캡처 하거나 간단한 툴을 사용하는 것만으로도 해당 값을 알아낼 수 있는 취약점

16	인증(세션 및 토큰) 값 안전성 설정 여부	해당 항목은 웹 애플리케이션 및 응용프로그램 이용 시 사용되는 사용자, 단말 등의 인증(세션 및 토큰) 값에 대한 안전성 설정 및 적용 여부를 확인하는 취약점
17	접근제어 우회 가능성 확인	접근 제어 및 권한 체크, 필요 프로그램 설치, 파일 업로드, 실명인증 등 인증, 권한, 제어, 확인 등의 과정을 처리하는 부분에서 Client Side Script(Javascript, VBScript 등)를 사용하여 제어하는 경우 사용자가 임의로 수정하여 쉽게 우회하여 접근할 수 있는 취약점 또한 중요 정보를 보여주는 화면에 no-cache를 설정하지 않은 경우, 로그아웃 후에도 브라우저의 뒤로 가기 기능을 통해 해당 중요 정보를 열람할 수 있는 취약점
18	비인증 상태로 중요 page 접근 가능성	로그인을 확인하는 모듈이 존재하는 않는 관리자 페이지나 기타 페이지가 존재한다면 로그인을 하지 않고 직접적인 접근이 가능하게 되는 문제가 발생할 수 있는 취약점
19	일반 계정 권한 상승 가능성	사용자 계정으로 로그인 된 상태에서 관리자 page나 권한 검증 부재로 인해 권한이 낮은 계정으로 접근이 허가되지 않은 상위 권한 page에 접속이 가능하거나, 동일한 권한의 사용자 계정이지만 그룹, 팀, 파트너사 등으로 구분되어 있는 경우 접근제어 부재로 인해 허가되지 않은 기능에 접근 가능한 경우가 존재합니다. 이는 접근제어 통제(ACL)가 설정이 미흡하여 발생하는 취약점
20	소스코드 내 주요 정보 노출 여부	웹 페이지 소스에 인증 정보를 하드 코딩하여 내부 인증에 사용하거나 외부 컴포넌트와 통신하는 것은 정보가 노출될 수 있어 취약점
21	요청 및 응답 값 내 주요 정보 포함여부 확인	애플리케이션이 사용하는 파라미터 값은 언제든지 사용자가 확인할 수 있는 값이기 때문에 파라미터 값에 디렉터리, 파일구조, 개인정보, 사용자 식별 값, 결제정보 등과 같은 중요한 값이 포함되어 있으면 개인고객 정보 또는 서버 설정 정보 등이 노출될 가능성 또한, 개인고객 정보를 입력받는 페이지에서 평문으로 전송 시 네트워크 스니핑과 같은 방법으로 사용자의 개인정보를 쉽게 얻거나 변조할 수 있으며 노출된 정보는 또 다른 공격에 이용될 수 있는 취약점
22	오류페이지를 통한 정보 노출 여부	데이터베이스 에러가 발생할 경우 에러 정보를 이용하여 해당 사이트가 가진 잠재적 취약점을 유추할 수 있는 취약점
23	일괄적인 오류 처리 페이지 존재 여부	로그인 페이지에서 잘못된 계정 정보를 입력하였을 때 계정의 존재 유무를 파악할 수 있는 메시지나 상이한 오류 코드 등을 출력하는 경우, 유효한 계정 정보를 파악할 수 있으며 이러한 정보는 무작위 대입 공격에 활용될 수 있습니다.

24	Client Request Method	PUT, DELETE 등 불필요한 메서드가 활성화되어 있을 경우 공격자가 악성파일을 업로드하거나 중요 파일의 삭제가 가능해지는 등 웹 사이트를 변조할 수 있는 취약점
25	파일 목록화 가능성	웹 서버의 설정 미흡으로 디렉터리 검색 기능이 활성화되어 있는 경우 해당 디렉터리에 존재하는 모든 파일의 리스트를 출력하므로 Web 서버 구조 노출 및 주요 설정 파일의 내용이 유출될 가능성
26	서버 헤더 정보 노출	응답 헤더를 통해 웹 서버 또는 웹 애플리케이션 서버의 종류 및 버전 정보가 노출될 경우 또 다른 공격에 이용될 수 있는 취약점
27	취약한 보안설정	보안상 취약한 서버 설정, 패치 및 라이브러리, 모듈, 알고리즘, 프레임워크 등의 사용은 공격자에게 대상 시스템 및 기능 등에 접근이 가능하도록 하며 이로 인해 시스템 상의 권한 및 정보 등을 획득할 수 있는 취약점 또한 SSL 통신 시 인증서 관리가 미흡(신뢰 되지 않은 인증서 사용, 인증서 Chain 검증 부재 등) 할 경우 공격자가 MITM을 통한 SSL 통신 스니핑 및 패킷 조작이 가능하며 다른 연계 공격 등에 이용될 가능성
28	취약점 진단 항목에 정의되지 않은 취약점	27개 항목에 포함되지 않는 새로운 Zero-Day 공격을 포함한 기타 취약점이 존재할 경우

[표 5 – 주요 진단 항목]

9. 수행 산출물

산출물	제출 시기	비고
웹진단 수행계획서	진단 수행 전	본 문서
웹진단 결과보고서	진단 수행 후	대상 정보시스템의 웹 취약점 진단 과정, 결과에 대한 개선안의 설명서

[표 6 – 수행 산출물]

2.협조사항

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

10.진단 수행 간의 협조 사항

(1) 대상 도메인의 URL 정보

(2) 진단 수행 간의 발생한 흔적 삭제

(3) 대상 시스템의 정상 작동 확인

2. 담당자에게 협조를 구하는 사항

(1) 담당하고 있는 대상에 대한 웹진단 일정 숙지

(2) 비상사태에 대비하여 주요 데이터에 대한 백업 수행

(3) 진단 수행 기간 동안 특이사항 발생에 대비한 담당자 대기

.