

|  |  |
| --- | --- |
|  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |

**JM Collection**

**모듈프로젝트**

**[3조]**

**2025-05-23**

**제∙개정 이력표**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **개정번호** | **일자** | **제∙개정 내용** | **작성자** | **버전** |
| 1 | 2025.05.21 | 모듈 프로젝트 초안 작성 | 문서영 | v1.0 |
| 2 | 2025.05.21 | 리눅스 취약점 작성 | 서초빈 | v.1.1 |
| 3 | 2025.05.22 | 웹, DBMS 취약점 작성 | 한예찬 | v.1.2 |
| 4 | 2025.05.22 | 웹, DBMS 취약점 작성 | 김영찬 | v.1.3 |
| 5 | 2025.05.22 | 웹, DBMS 취약점 작성 | 정유민 | v.1.4 |
| 6 | 2025.05.22 | 윈도우 취약점 작성 | 정규환 | v1.5 |
| 7 | 2025.05.22 | 윈도우 취약점 작성 | 김지현 | v.1.6 |
| 8 | 2025.05.23 | 모듈 프로젝트 최종본 작성 | 문서영 | v.2.0 |

[1. 클라우드 아키텍처 개요 6](#_Toc198856499)

[1.1. 클라우드 아키텍처 구성 6](#_Toc198856500)

[1.2. 클라우드 용어 정리 7](#_Toc198856501)

[1.3. 시스템 환경 정보 7](#_Toc198856502)

[2. 취약점 진단 개요 8](#_Toc198856503)

[2.1. 목적 8](#_Toc198856504)

[2.2. 점검 대상 8](#_Toc198856505)

[2.3. 점검 일정 8](#_Toc198856506)

[2.4. 점검 인력 9](#_Toc198856507)

[2.4.1. 수행방안 9](#_Toc198856508)

[2.4.2. 진단방법 10](#_Toc198856509)

[2.4.3. 진단도구 11](#_Toc198856510)

[2.4.4. 진단항목 12](#_Toc198856511)

[3. 점검 결과 15](#_Toc198856512)

[3.1. 결과 요약 15](#_Toc198856513)

[4. 세부 수행내역 18](#_Toc198856514)

[4.1. 유닉스 18](#_Toc198856515)

[4.1.1. root 계정 원격 접속 제한 (U-01) 18](#_Toc198856516)

[4.1.2. root 계정 su 제한 (U-45) 20](#_Toc198856517)

[4.1.3. 패스워드 최소 길이 설정 (U-46) 22](#_Toc198856518)

[4.1.4. 패스워드 최대 사용기간 설정 (U-47) 24](#_Toc198856519)

[4.1.5. 패스워드 최소 사용기간 설정 (U-48) 26](#_Toc198856520)

[4.1.6. 불필요한 계정 제거 (U-49) 28](#_Toc198856521)

[4.1.7. /etc/shadow 파일 소유자 및 권한 설정 (U-08) 29](#_Toc198856522)

[4.1.8. /etc/hosts 파일 소유자 및 권한 설정 (U-09) 30](#_Toc198856523)

[4.1.9. /etc/syslog.conf 파일 소유자 및 권한 설정 (U-11) 31](#_Toc198856524)

[4.1.10. SUID, SGID, 설정 파일점검 (U-13) 32](#_Toc198856525)

[4.1.11. 접속 IP 및 포트 제한 (U-18) 34](#_Toc198856526)

[4.2. 윈도우 35](#_Toc198856527)

[4.2.1. Administrator 계정 이름 변경 또는 보안성 강화 (W-01) 35](#_Toc198856528)

[4.2.2. 계정 잠금 임계 값 설정 (W-04) 36](#_Toc198856529)

[4.2.3. 계정 잠금 기간 설정 (W-47) 37](#_Toc198856530)

[4.2.4. 패스워드 최소 암호 길이 (W-51) 38](#_Toc198856531)

[4.2.5. 패스워드 최소 사용 기간 (W-51) 39](#_Toc198856532)

[4.2.6. 마지막 사용자 이름 표시 안 함 (W-52) 40](#_Toc198856533)

[4.2.7. 로컬 로그온 허용 (W-53) 41](#_Toc198856534)

[4.2.8. 최근 암호 기억 (W-55) 42](#_Toc198856535)

[4.2.9. 원격터미널 접속 가능한 사용자 그룹 제한 (W-56) 43](#_Toc198856536)

[4.2.10. 하드디스크 기본 공유 제거 (W-08) 44](#_Toc198856537)

[4.2.11. 불필요한 서비스 제거 (W-14) 45](#_Toc198856538)

[4.2.12. 터미널 서비스 암호화 수준 설정 (W-58) 46](#_Toc198856539)

[4.2.13. 원격터미널 접속 타임아웃 설정 (W-67) 48](#_Toc198856540)

[4.2.14. 정책에 따른 시스템 로깅 설정 (W-69) 49](#_Toc198856541)

[4.2.15. 백신 프로그램 설치 (W-36) 50](#_Toc198856542)

[4.2.16. 화면보호기 설정 (W-38) 52](#_Toc198856543)

[4.2.17. 로그온 하지 않고 시스템 종료 허용 해제 (W-39) 54](#_Toc198856544)

[4.2.18. SAM 계정과 공유의 익명 열거 허용 안 함 (W-42) 55](#_Toc198856545)

[4.2.19. DOS 공격 방어 레지스트리 설정 (W-72) 56](#_Toc198856546)

[4.2.20. LAN Manager 인증 수준 (W-77) 58](#_Toc198856547)

[4.3. DBMS 59](#_Toc198856548)

[4.3.1. 데이터베이스의 불필요 계정을 제거하거나, 잠금 설정 후 사용 (D-02) 59](#_Toc198856549)

[4.3.2. DBA 이외의 인가되지 않은 사용자가 시스템 테이블에 접근할 수 없도록 설정 (D-06) 63](#_Toc198856550)

[4.3.3. 데이터베이스의 주요 파일 보호 등을 위해 DB 계정의 umask를 022 이상으로 설정하여 사용 (D-16) 65](#_Toc198856551)

[4.3.4. 인가되지 않은 Object Owner의 제한 (D-20) 66](#_Toc198856552)

[4.3.5. 인가되지 않은 GRANT OPTION 사용 제한 (D-21) 68](#_Toc198856553)

[4.4. 웹(Web) 69](#_Toc198856554)

[4.4.1. SQL INJECTION (SI) 69](#_Toc198856555)

[4.4.2. 정보 누출 (IL) 75](#_Toc198856556)

[4.4.3. 크로스 사이트 스크립팅 (XS) 77](#_Toc198856557)

[4.4.4. 크로스 사이트 리퀘스트 변조\_CSRF (CF) 82](#_Toc198856558)

[4.4.5. 불충분한 인가 (IN) 85](#_Toc198856559)

[4.4.6. 불충분한 세션 만료 (SC) 90](#_Toc198856560)

[4.4.7. 프로세스 검증 누락 (IA) 91](#_Toc198856561)

[4.4.8. 파일 업로드 (FU) 94](#_Toc198856562)

[4.4.9. 위치 공개 취약점 (PL) 97](#_Toc198856563)

[4.4.10. 데이터 평문 전송 (SN) 100](#_Toc198856564)

[4.4.11. 쿠키 변조 (CC) 102](#_Toc198856565)

[5. CloudWatch 105](#_Toc198856566)

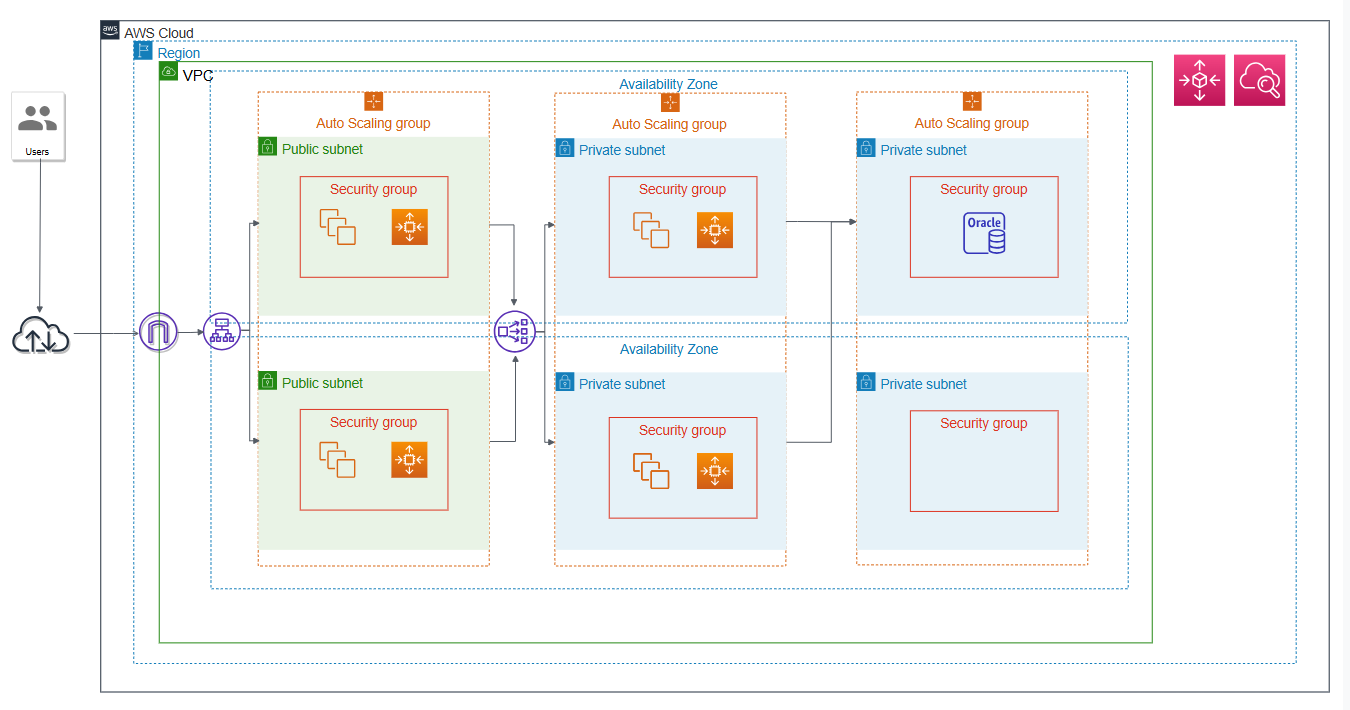
[5.1. 대시보드 생성 105](#_Toc198856567)

[6. 참고 자료 106](#_Toc198856568)

[6.1. 일반적으로 불필요한 서비스 106](#_Toc198856569)

[6.2. 감사 정책 권고 기준 108](#_Toc198856570)

1. 클라우드 아키텍처 개요
   1. 클라우드 아키텍처 구성



1

2

3

4

5

1. Web Subnet (Public Subnet)

* 서로 다른 가용 영역 2개의 각 Public Subnet에 Web 인스턴스 생성
* 인터넷 게이트웨이를 통해 외부 사용자 요청을 받을 수 있도록 설정
* ALB를 통해 웹 요청을 WAS로 전달

1. WAS Subnet (Private Subnet)

* 서로 다른 가용 영역 2개의 각 Private Subnet에 WAS 인스턴스 생성
* 외부에서는 직접 접근 불가능
* NLB를 통해 전달된 요청만 Web 서버를 통해 내부로 전달

1. RDS Subnet (Private Subnet)

* 서로 다른 가용 영역 2개 중 하나의 영역인 Private Subnet에 RDS 생성
* WAS에서만 접근 가능하도록 보안 그룹 설정
* 퍼블릭 접근 비활성화 설정

1. Auto Scaling Group

* Web 및 WAS 인스턴스에 대해 Auto Scaling Group을 설정하여 트래픽 부하에 따라 인스턴스를 자동으로 축소/확장

1. CloudWatch

* 인스턴스의 CPU 사용률과 상태를 모니터링하여 시스템 부하 및 장애 여부를 실시간으로   
  확인
  1. 클라우드 용어 정리

|  |  |
| --- | --- |
| **용어** | **설명** |
| EC2 | AWS의 가상 서버 인스턴스 |
| RDS | 데이터베이스 서버를 관리형으로 운영하기 위해 사용한  AWS의 Oracle 데이터베이스 서비스 |
| VPC | 전체 인프라를 구성하는 가상 네트워크 공간으로,  Public 및 Private Subnet으로 구성됨 |
| Public Subnet | 인터넷 게이트웨이로 연결되어 외부와 통신이 가능한 서브넷으로,  Web 서버를 배치하여 사용자의 요청을 받음 |
| Private Subnet | 외부 접근이 차단된 내부 서브넷으로 WAS나 RDS와 같은 리소스 배치 |
| ALB | Application Load Balancer의 약자.  HTTP/HTTPS 기반의 트래픽을 적절한 인스턴스로 분산 |
| NLB | Network Load Balancer의 약자.  TCP 기반의 트래픽을 적절한 인스턴스로 분산 |
| Auto Scaling Group | 서버에 부하가 발생할 때  자동적으로 서버 수를 조절하는 방식으로 서버 분산 |
| Security Group | 인스턴스 수준에서의 가상 방화벽으로,  인바운드/아웃바운드 트래픽 제어 가능 |
| 윈도우 | Web 서버의 운영체제 |
| 유닉스/리눅스 | WAS 서버의 운영체제 |

* 1. 시스템 환경 정보

|  |  |
| --- | --- |
| **인스턴스** | **버전** |
| Web | Ubuntu Server 22.04.5 LTS |
| WAS | Microsoft Windows Server 2019 Base |
| RDS(Oracle) | Version 19.16.0.0.0 |

1. 취약점 진단 개요
   1. 목적

본 프로젝트의 취약점 진단은 대상 시스템에 내재된 주요 보안 취약점을 체계적으로   
분석하고 식별함으로써, 이를 선제적으로 제거하고 보완하여 보다 안전하고 신뢰할 수 있는   
서비스 환경을 구축하는 것이 목적이다.

* 1. 점검 대상

|  |  |  |
| --- | --- | --- |
| **번호** | **대상** | **서버 URL** |
| 1 | JM COLLECTION | web-as-alb-1392225615.us-west-2.elb.amazonaws.com |

* 1. 점검 일정

**대상선정**

**및**

**시스템현황 파악**

**취약점**

**진단 진행**

**결과 분석**

**대응방안**

**및**

**보고서**

* 2025년 05월 20일 ~ 2025년 05월 23일

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **단계** | **일정** | | | |
| **05/20** | **05/21** | **05/22** | **05/23** |
| 대상선정 및 시스템 현황 파악 | 시스템 아키텍처 파악 | 시스템 분석 | - | - |
| 취약점 진단 진행 | - | 유닉스/윈도우/웹/데이터베이스 진단 | 유닉스/윈도우/웹/데이터베이스 진단 |  |
| 결과분석 | - | - | 1차 결과 취합 | 최종 결과 분석 |
| 대응방안 및 보고서 작성 | - | - | 대응방안 작성 | 최종 보고서 작성 및 발표  자료 정리 |

* 1. 점검 인력

|  |  |  |
| --- | --- | --- |
| **번호** | **이름** | **파트** |
| 1 | 김영찬 | 웹, 데이터베이스 |
| 2 | 김지현 | 윈도우 |
| 3 | 문서영 | 발표, 유닉스, 보고서 취합 |
| 4 | 서초빈 | 조장, 유닉스, 보고서 취합 |
| 5 | 정규환 | 아키텍처 구성, 윈도우 |
| 6 | 정유민 | 웹, 데이터베이스 |
| 7 | 한예찬 | 웹, 데이터베이스 |

* + 1. 수행방안

1. 유닉스 서버 점검

* 계정 및 권한 설정, 패스워드 정책 등 리눅스 보안 기준에 따라 점검을 진행하였다.
* 불필요한 SUID/SGID 파일, root 원격접속 제한 설정을 확인하고, 보안 패치 적용 여부를 점검하였다.
* SSH 설정 및 로깅 설정 등을 통해 시스템 보안 수준을 확인하였다.

1. 윈도우 서버 점검

* 윈도우 서버의 보안 강화를 위해 계정, 서비스, 패치, 로그, 전반적인 보안 설정 전반을   
  아우르는 취약점 점검을 수행하였다.
* 서버에 등록된 모든 계정의 권한 및 잠금 정책이 적절히 설정되어 있는지 확인하고,   
  불필요한 공유 폴더 및 서비스가 비활성화되어 있는지 검토하였다.
* 또한 이벤트 로그의 수집·보존 정책과 감사 항목이 적절히 구성되어 이상 징후를 신속히 포착할 수 있는지 평가하였고, 백신 설치, 화면보호기 설정, DoS 방어용 레지스트리   
  구성 등 핵심 보안 항목을 종합적으로 진단하였다.

1. 웹(Web) 취약점 점검

* 주요기반시설 웹 보안 가이드를 기반으로 진단을 수행하였다.
* Burp Suite, 파이썬 등을 활용하여 자동화 스캔을 실시하고, 수동으로 XSS, SQLi, CSRF 등 취약점을 검증하였다.
* 입력 값 검증, 세션 관리, 접근제어, 에러 메시지 노출 등 주요 항목을 점검하였다.

1. DBMS (Oracle) 점검

* DB 접근 제어 및 권한 관리 기준에 따라 Oracle DB의 설정을 점검하였다.
* SQL Plus, ubuntu 등으로 계정 및 권한 조회를 수행하고, PUBLIC 권한 접근 설정 및   
  계정 관리 여부를 확인하였다.
* 비밀번호 정책, 계정 접근 제한/권한 설정 등 주요 항목을 중점적으로 점검하였다.
  + 1. 진단방법

과학기술정보통신부에서 제시한 「주요정보통신기반시설 기술적 취약점 점검 가이드라인」의   
항목을 기준으로, 시스템별 구성과 운영 환경에 맞춰 정밀하고 체계적인 방식으로 보안 진단을   
수행하였다.

* 리눅스: Xshell7.0을 이용하여 SSH로 웹 서버 공인 IP에 접속, ubuntu 계정으로   
  로그인했다. CLI 환경에서 패스워드 정책, 불필요한 계정, root 원격 접속, su/sudo 권한, 파일 시스템 권한 등을 cat, vim, ls -l, grep 명령어를 이용하여 점검하였다.
* 윈도우: RDP 원격 데스크톱을 통해 WAS EC2 인스턴스의 임시 공인 IP에 Administrator 계정으로 접속한 후, 보안 정책, 서비스 상태 확인, 보안 패치 적용 현황, 이벤트 로그   
  점검, 방화벽 규칙 등을 일괄 점검하였다. 점검이 완료되면 즉시 해당 인스턴스를   
  Private Subnet으로 재배치하여 외부 노출을 최소화하였다.
* DBMS: Xshell 7.0을 이용해 Oracle 19.0.0.0이 설치된 서버에 원격 접속한 후, 최고 권한을 가진 CHMAINADMIN 계정으로 SQL\*Plus에 접속하여 해당 환경에서 데이터베이스 계정 및 권한 설정, 패스워드 정책, 감사(AUDIT) 설정 등의 주요 보안 항목을 점검하여   
  데이터베이스 보안 설정을 진단했다.
* 웹(Web): Kali Linux 2025.1a 환경에서 Burp Suite Professional 2025.4.23, Gobuster v3.6, sqlmap 1.7.3 등의 도구를 활용하여 웹 애플리케이션에 대한 자동화 스캔과 수동 점검을 병행하였고, XSS, SQL INJECTION, CSRF 등 주요 취약점에 대해 실제 공격과 유사한   
  방식으로 정밀하게 진단하였다.
  + 1. 진단도구

|  |  |
| --- | --- |
| **점검 도구** | **내용** |
| Burp Suite | 로컬 프록시 서버, 파라미터 변경 |
| Sqlmap | 쿼리 문 자동 삽입 도구 |
| Gobuster | 웹 서버의 숨겨진 디렉토리나 파일을 찾아주는 도구 |

* + 1. 진단항목

진단 항목은 **「기술적 취약점 분석 · 평가 가이드」**를 기준으로 선정했다.

이 중 실제로 취약점이 발견된 항목만을 선별하여 관련 코드 및 위험도와 함께 작성했다.

※ 취약점이 발견되지 않은 항목은 보고서에서 제외하였음.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **유닉스** | | | | |
| **번호** | **코드** | **항목** | **항목** | **위험도** |
| 1 | U-01 | 계정 관리 | root 계정 원격 접속 제한 | 상 |
| 2 | U-02 | 패스워드 복잡성 설정 | 상 |
| 3 | U-03 | 패스워드 잠금 임계 값 설정 | 상 |
| 4 | U-45 | root 계정 su 제한 | 하 |
| 5 | U-46 | 패스워드 최소 길이 미흡설정 | 중 |
| 6 | U-47 | 패스워드 최대 사용기간 설정 | 중 |
| 7 | U-48 | 패스워드 최소 사용기간 설정 | 중 |
| 8 | U-49 | 불필요한 계정확인 | 하 |
| 9 | U-08 | 파일 및  디렉터리 관리 | /etc/shadow 파일 소유자 및 권한 설정 | 상 |
| 10 | U-09 | /etc/hosts 파일 소유자 및 권한 설정 | 상 |
| 11 | U-11 | /etc/syslog.conf 파일 소유자 및 권한 설정 | 상 |
| 12 | U-13 | SUID, SGID, 설정 파일점검 | 상 |
| 13 | U-18 | 접속 IP 및 포트 제한 | 상 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **윈도우** | | | | |
| **번호** | **코드** | **항목** | **위험도** | **위험도** |
| 1 | W-01 | 계정 관리 | Administrator 계정 이름 변경 또는 보안성 강화 | 상 |
| 2 | W-04 | 계정 잠금 임계 값 설정 | 상 |
| 3 | W-47 | 계정 잠금 기간 설정 | 중 |
| 4 | W-49 | 패스워드 최소 암호 길이 | 중 |
| 5 | W-51 | 패스워드 최소 사용 기간 | 중 |
| 6 | W-52 | 마지막 사용자 이름 표시 안함 | 중 |
| 7 | W-53 | 로컬 로그온 허용 | 중 |
| 8 | W-55 | 최근 암호 기억 | 중 |
| 9 | W-56 | 원격터미널 접속 가능한 사용자 그룹 제한 | 중 |
| 10 | W-08 | 서비스 관리 | 하드디스크 기본 공유 제거 | 상 |
| 11 | W-14 | 불필요한 서비스 제거 | 상 |
| 12 | W-58 | 터미널 서비스 암호화 수준 설정 | 중 |
| 13 | W-67 | 원격터미널 접속 타임아웃 설정 | 중 |
| 14 | W-69 | 패치 관리 | 정책에 따른 시스템 로깅 설정 | 중 |
| 15 | W-36 | 보안 관리 | 백신 프로그램 설치 | 상 |
| 16 | W-38 | 화면보호기 설정 | 상 |
| 17 | W-39 | 로그온 하지 않고 시스템 종료 허용 해제 | 상 |
| 18 | W-42 | SAM 계정과 공유의 익명 열거 허용 안함 | 상 |
| 19 | W-72 | DoS 공격 방어 레지스트리 설정 | 중 |
| 20 | W-77 | LAN Manager 인증 수준 | 중 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **DBMS** | | | | |
| **번호** | **코드** | **분류** | **항목** | **위험도** |
| 1 | D-02 | 계정관리 | 데이터베이스의 불필요 계정을 제거하거나,  잠금 설정 후 사용 | 상 |
| 2 | D-03 | 패스워드의 사용기간 및 복잡도를 기관 정책에  맞도록 설정 | 상 |
| 3 | D-06 | 접근관리 | DBA 이외의 인가되지 않은 사용자가 시스템  테이블에 접근할 수 없도록 설정 | 상 |
| 4 | D-16 | 데이터베이스의 주요 파일 보호 등을 위해  DB계정의 umask를 022 이상으로 설정하여 사용 | 하 |
| 5 | D-20 | 옵션관리 | 인가되지 않은 Object Owner의 제한 | 하 |
| 6 | D-21 | 인가되지 않은 GRANT OPTION 사용 제한 | 중 |

|  |  |  |  |
| --- | --- | --- | --- |
| **웹** | | | |
| **번호** | **코드** | **항목** | **위험도** |
| 1 | SI | SQL 인젝션 | 상 |
| 2 | IL | 정보 누출 | 상 |
| 3 | XS | 크로스 사이트 스크립팅 | 상 |
| 4 | CF | 크로스 사이트 리퀘스트 변조(CSRF) | 상 |
| 5 | IN | 불충분한 인가 | 상 |
| 6 | SC | 불충분한 세션 만료 | 상 |
| 7 | IA | 프로세스 검증 누락 | 상 |
| 8 | FU | 파일 업로드 | 상 |
| 9 | PL | 위치 공개 | 상 |
| 10 | SN | 데이터 평문 전송 | 상 |
| 11 | CC | 쿠키 변조 | 상 |

1. 점검 결과
   1. 결과 요약

* 현재 웹 사이트에 대한 취약점 결과 유닉스에서 11개, 윈도우에서 20개, DBMS에서 5개,   
  웹에서 11개로 총 47개를 발견했다.
* 유닉스 시스템에 대한 취약점 분석 결과, root 계정 su 제한 설정 부재, 시스템 패스워드 설정 정책 미흡, 관리자 파일 권한 설정 오류 등 보안 설정 미흡이 발견되었다.
* 윈도우 서버에 대한 취약점 분석 결과, 계정 및 패스워드 정책, 불필요한 접속, 감사 정책,   
  시스템 보안 방어 미흡 등 정책 및 보안 설정에 대해 미흡한 부분들이 발견되었다.
* 데이터베이스 취약점 분석 결과, 불필요한 계정과 미흡한 잠금 설정, 일반 사용자에 대한   
  시스템 테이블 접근 허용, 부적절한 umask 설정, 인가되지 않은 GRANT OPTION 사용 등   
  권한 관리와 보안 설정에 다수의 취약점이 발견되었다.
* 웹 취약점 분석 결과 SQL INJECTION, 크로스 사이트, 불충분한 인가, 쿠키 변조, 파일 업로드, 정보 누출 등 여러 웹 취약점들이 발견되었다.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **유닉스** | | | | |
| **번호** | **분야** | **취약항목** | **공격영향** | **취약점 개수** |
| 1 | 계정관리 | root 계정 | 무작위 대입 공격 및  사전 대입 공격 | 2개 |
| 2 | 패스워드 설정 | 무작위 대입 공격,  사전 대입공격, 계정탈취 | 4개 |
| 3 | 파일, 디렉토리 관리 | 특정 파일의  소유자 및 권한 설정 | 크래킹, 파밍, 시스템 과부화 | 3개 |
| 4 | 파일 및 디렉토리 관리 | 악의적 권한 상승,  시스템 침해사고 | 2개 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **윈도우** | | | | |
| **번호** | **분야** | **취약항목** | **공격영향** | **취약점 개수** |
| 1 | 계정 관리 | 계정 및  패스워드 정책 | 패스워드 추측 공격,  무작위 대입 공격 | 5개 |
| 2 | 로컬 정책 | 비인가자 접근,  암호 유일성 취약 | 3개 |
| 3 | 원격 접속 | 비인가자 접근 | 1개 |
| 4 | 서비스 관리 | 불필요한 접속 | 악성 트래픽 유입  바이러스 침투 | 2개 |
| 5 | 원격 접속 | 비인가자 접근 | 2개 |
| 6 | 패치 관리 | 감사 정책 | 원인 파악 문제 | 1개 |
| 7 | 보안 관리 | 세션 및 화면 보호 설정 미흡 | 중요 정보 열람 및 탈취  서버 강제 종료 | 1개 |
| 8 | 시스템 보안 방어 미흡 | 악성코드 감염  시스템 자원 고갈 | 2개 |
| 9 | 계정 및 인증 정보 보호 미흡 | 패스워드 크래킹 공격  비인가 시스템 종료 | 3개 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **DBMS** | | | | |
| **번호** | **분야** | **취약항목** | **공격영향** | **취약점 개수** |
| 1 | 계정 관리 | 데이터베이스의 불필요 계정을 제거하거나, 잠금 설정 후 사용 | 권한 오·남용, 내부침해, 보안 사고 위험 | 1개 |
| 2 | 접근 관리 | DBA 이외의 인가되지 않은 사용자가 시스템 테이블에 접근 할 수 없도록 설정 | 비인가자 접근 차단으로 데이터 보안 강화 | 2개 |
| 3 | 데이터베이스의 주요 파일 보호 등을 위해 DB 계정의 umask를 022 이상으로 설정하여 사용 | 파일 권한 강화로 데이터 유출 및 변조 위험 감소 |
| 4 | 옵션 관리 | 인가되지 않은 Object Owner의 제한 | 데이터 무단 변경 및 권한 남용 방지 | 2개 |
| 5 | 인가되지 않은 GRANT OPTION 사용 제한 | 권한 부적절 부여로 보안 위협 발생 |

|  |  |  |  |
| --- | --- | --- | --- |
| **웹** | | | |
| **번호** | **취약항목** | **공격영향** | **취약점 개수** |
| 1 | SQL INJECTION (SI) | 악의적인 SQL 코드 삽입 가능 및 데이터 탈취/조작/삭제 가능 | 2개 |
| 2 | 정보 누출 (IL) | 시스템 내부 정보나 민감한 데이터가 노출 | 1개 |
| 3 | 크로스 사이트 스크립팅 (XS) | **세션 탈취, 피싱, 사용자 정보 유출** 등 | 2개 |
| 4 | 크로스 사이트 리퀘스트 변조\_CSRF (CF) | 의도하지 않은 요청 자동 전송 및 계정 탈취, 설정 변경, 금전 이체 등 | 1개 |
| 5 | 불충분한 인가 (IN) | 권한 없는 접근 허용 | 1개 |
| 6 | 불충분한 세션 만료 (SC) | 세션이 만료돼도 접근이 계속 가능 | 1개 |
| 7 | 프로세스 검증 누락 (IA) | 비정상 요청도 처리되어 악용 가능 | 1개 |
| 8 | 파일 업로드 (FU) | 악성 파일 업로드로 시스템 침해 및 서비스 중단이 발생 | 1개 |
| 9 | 위치 공개 취약점 (PL) | 사생활 침해 및 위치 악용 가능 | 1개 |
| 10 | 데이터 평문 전송 (SN) | 암호화가 되어있지 않아 중간에서 탈취/조작 위험 | 1개 |
| 11 | 쿠키 변조 (CC) | 세션 탈취, 권한 상승 등 보안 위협 | 1개 |

1. 세부 수행내역
   1. 유닉스
      1. root 계정 원격 접속 제한 (U-01)

**취약점 개요**

* 시스템 정책에 root 계정의 원격 터미널 접속 차단 설정이 적용되어 있는지 점검한다.   
  이는 관리자 계정 탈취로 인한 시스템 장악을 방지하고 외부 비인가자의 root 계정 접근 시도를 원천적으로 차단하기 위함이다.
* root 계정은 운영 체제의 모든 기능 설정 및 변경이 가능한 최고 수준의 권한을 가지며   
  공격자가 이를 탈취할 경우 원격 접속을 통해 시스템을 완전히 장악하거나, 무작위 대입공격,   
  사전 대입공격 등 악의적인 시도로 인해 root 계정 자체가 사용 불가능해질 위험이 존재한다.

**취약점 설명**

Step 1) root 계정 접근 제한 확인

**sshd\_config** 파일을 확인했을 때, 제한 설정이 존재하지 않는다.

|  |
| --- |
| cat /etc/ssh/sshd\_config | grep -I permitrootlogin |
|  |

Step 2) 접속 확인

root 계정으로 접속했을 때, 비밀번호 없이 접근이 가능하다.

|  |
| --- |
| sudo su - |
|  |

**취약점 대응방안**

Step 1) 파일 변경

sshd\_config 파일 내에서 **#PermitRootLogin prohibit-password**를 **PermitRootLogin No**로  
 바꾼다.

|  |
| --- |
| vi /etc/ssh/sshd\_config |
|  |

* + 1. root 계정 su 제한 (U-45)

**취약점 개요**

* su 명령어 사용을 허락하는 사용자를 지정하는 그룹이 설정되어 있는지 점검하여  
   su 그룹에 포함되지 않은 일반인 사용자의 su 명령 사용을 원천적으로 차단하는지 확인한다.
* 무분별한 사용자 변경으로 타사용자 소유의 파일을 변경할 수 있으며 root 계정으로   
  변경하는 경우 관리자 권한 획득이 가능하다.
* 현재 사이트에 설정은 리눅스 배포판에 기본 설정과 같은데, 보안을 위해서는   
  **pam\_wheel.so**설정을 활성해서 su 사용 제한하는 것이 좋다.

**취약점 설명**

Step 1) su 계정 그룹 확인

su 명령어 사용을 특정 그룹에 속한 사용자에게 허용/차단을 하는 설정이 주석처리 되어있다.

|  |
| --- |
| cat /etc/pam.d/su |
|  |

**취약점 대응방안**

Step 1) 파일 설정

“**/etc/pam.d/su**”파일의 주석 설정을 해제한다.

|  |
| --- |
| vim /etc/pam.d/su |
|  |

* + 1. 패스워드 최소 길이 설정 (U-46)

**취약점 개요**

* 시스템 설정에 의해 패스워드 최소 길이 설정이 적용되어 있는지 점검하여 짧은 패스워드 길이로 발생하는 취약점을 이용한 공격들을 예방하기 위해 시스템 정책에 패스워드 최소 길이 설정이 되어있는지 점검한다.
* 패스워드 문자열이 짧은 경우 유추가 가능할 수 있으며 패스워드 해시 값을 무작위 대입공격,  
  사전 대입 공격 등으로 단시간에 패스워드 크랙이 가능해지므로, 설정 값을 관리해야 한다.

**취약점 설명**

Step 1) PASS\_MIN\_LEN 8 설정 파일 적용 여부확인  
확인결과 **PASS\_MIN\_LEN, PASS\_MAX\_LEN** 설정이 되어있지 않다.

|  |
| --- |
| cat /etc/login.defs |
|  |

**취약점 대응방안**

Step 1) 설정 변경

**login.def** 파일 내에서 **PASS\_MIN\_LEN**, **PASS\_MAX\_LEN** 설정을 바꿔준다.

|  |
| --- |
| vim /etc/login.defs |
|  |

* + 1. 패스워드 최대 사용기간 설정 (U-47)

**취약점 개요**

* 패스워드 최대 사용기간(90일)이 설정이 되어 있는지 점검하여 시스템 정책에서 사용자 계정의 장기간 패스워드 사용을 방지하고 있는지 확인한다.
* 패스워드 최대 사용 기간을 설정하지 않은 경우 비인가자의 각종 공격을 시도할 수 있는 기간 제한이 없음으로 공격자 입장에서는 장기적인 공격을 시행할 수 있어 시행기간에 비례하여 사용자 패스워드가 유출될 수 있는 확률이 증가한다.

**취약점 설명**

Step 1) **login.defs** 파일 확인

**/etc/login.defs** 파일 내에서 **PASS\_MAX\_DAYS** 값이 **90**인지 확인한다.

|  |
| --- |
| vim /etc/login,defs |
|  |

**취약점 대응방안**

Step 1) 설정 변경

**login.defs** 파일 내에서 **PASS\_MAX\_DAYS** 설정을 바꿔준다.

|  |
| --- |
| vim /etc/login,defs |
|  |

* + 1. 패스워드 최소 사용기간 설정 (U-48)

**취약점 개요**

* 패스워드를 변경할 수 없도록 하고 관련 설정(최근 암호 기억)과 함께 시스템에 적용하여 패스워드 변경 전에 사용했던 패스워드를 재 사용할 수 없도록 방지하는지 확인하기 위해 점검한다.
* 패스워드 최대 사용 기간을 설정하지 않은 경우 즉시 이전 사용한 비밀번호로 변경이 가능하여 보안상 취약하다.

**취약점 설명**

Step 1) 파일 확인

**/etc/login.defs** 파일 내에서 **PASS\_MIN\_DAYS** 값을 확인한다.

|  |
| --- |
| vim /etc/login,defs |
|  |

**취약점 대응방안**

Step 1) 파일 설정 변경

**login.defs** 파일 내에서 **PASS\_MIN\_DAYS** 설정을 **1**로 바꿔준다.

|  |
| --- |
| vim /etc/login,defs |
|  |

* + 1. 불필요한 계정 제거 (U-49)

**취약점 개요**

* 불필요한 계정이 존재하는지 점검하여 관리되지 않은 계정에 의한 침입에 대비하는지 확인하기 위해 불필요한 계정이 존재하는지 점검한다.

**취약점 설명**

Step 1) 사용하지 않는 Default 계정 점검

점검결과 Default 계정인 **uucp**가 있는 것을 알 수 있다.

|  |
| --- |
| cat /etc/passwd | egrep “lp|uucp|nuucp” |
|  |

**취약점 대응방안**

Step 1) **userdel** 명령으로 아래 형식을 지켜 불필요한 사용자 계정 삭제

|  |
| --- |
| userdel <user\_name> |

* + 1. /etc/shadow 파일 소유자 및 권한 설정 (U-08)

**취약점 개요**

* **/etc/shadow** 파일의 경우 관리자만 제어할 수 있게 하여 비인가자들의 접근을 파일소유자 및   
  권한을 설정해야 한다.

**취약점 설명**

Step 1) “**/etc/shadow**” 파일의 소유자 및 권한 확인

|  |
| --- |
| ls -l /etc/shadow |
|  |

**취약점 대응방안**

Step 1) “**/etc/shadow**” 파일의 소유자 및 권한 변경 (소유자 root, 권한 400)

|  |
| --- |
| #chown root /etc/shadow  #chmod 400 /etc/shadow |

* + 1. /etc/hosts 파일 소유자 및 권한 설정 (U-09)

**취약점 개요**

* **/etc/hosts** 파일의 경우 관리자만 제어할 수 있게 하여 비인가자들의 파일 변조를 방지하기 위해 hosts 파일의 권한 적정성을 점검한다.
* 소유자 외 비인가자들에게 쓰기 권한이 주어진 경우 파밍 공격 등에 악용될 수 있다.

**취약점 설명**

Step 1) “**/etc/hosts**”파일의 소유자 및 권한 확인

|  |
| --- |
| ls -l /etc/hosts |
|  |

**취약점 대응방안**

Step 1) “**/etc/hosts**”파일의 소유자 및 권한 변경 (소유자 root, 권한 600)

|  |
| --- |
| #chown root /etc/hosts  #chmod 600 /etc/hosts |

* + 1. /etc/syslog.conf 파일 소유자 및 권한 설정 (U-11)

**취약점 개요**

* **/etc/rsyslog.conf** 파일의 경우 관리자만 제어할 수 있게 하여 비인가자들의 파일 변조를 방지하기 위해 host 파일의 권한 적정성을 점검한다.
* **/etc/rsyslog.conf** 파일에 로그 저장위치가 노출되며 그 기록을 이용하여 시스템 과부하를 유도할 수 있는 위험성이 존재한다.

**취약점 설명**

Step 1) “**/etc/rsyslog.conf** ”파일의 소유자 및 권한 확인

|  |
| --- |
| ls -l /etc/rsyslog.conf |
|  |

**취약점 대응방안**

Step 1) “**/etc/rsyslog.conf** ” 파일의 소유자 및 권한 변경 (소유자 root, 권한 640)

|  |
| --- |
| #chown root /etc/rsyslog.conf  #chmod 640 /etc/rsyslog.conf |

* + 1. SUID, SGID, 설정 파일점검 (U-13)

**취약점 개요**

* 불필요한 SUID, SGID 설정 제거로 악의적인 사용자의 권한상승을 방지하기 위해 SUID, SGID 설정 여부 점검을 진행한다.
* SUID, SGID 파일에 대한 접근권한이 적절하지 않을 경우 SUID, SGID 설정된 파일로  
   특정 명령어를 실행하여 root 권한 획득이 가능하다.

**취약점 설명**

Step 1) OS별 주요 실행파일에 대한 SUID/SGID 설정 여부 확인

|  |
| --- |
| find / -type f \( -perm -4000 -o -perm -2000 \) -exec ls -l {} \; 2>/dev/null |
|  |

**취약점 대응방안**

Step 1) 제거 방법

|  |
| --- |
| #chmod -s |

Step 2) 주기적인 감사 방법

|  |
| --- |
| #find / -user root -type f \( -perm -04000 -o -perm -02000 \) -xdev -exec ls –al {} \; |

Step 3) 반드시 사용이 필요한 경우 특정 그룹에서만 사용하도록 제한하는 방법

|  |
| --- |
| #/usr/bin/chgrp <group\_name> <setuid\_file\_name >  #/usr/bin/chmod 4750 <setuid\_file\_name> |

* + 1. 접속 IP 및 포트 제한 (U-18)

**취약점 개요**

* 허용되지 않은 IP나 포트에서 접근이 가능하도록 설정되어 있을 경우, 공격자는 Telnet, FTP 등의 취약한 서비스에 접근하여 시스템 침해나 정보 유출을 일으킬 수 있다.

**취약점 설명**

Step 1) 명령어 확인

현재 우분투에서 사용하는 **iptables**를 확인했을 때, 외부에서 들어오는 모든 트래픽을 기본으로 허용하고 있다.

|  |
| --- |
| sudo iptables -L |
|  |

**취약점 대응방안**

Step 1) **iptables** 명령어를 통해 접속할 IP 및 포트 정책 추가

|  |
| --- |
| #iptables –A INPUT –p tcp –s 192.168.1.0/24 —dport 22 –j ACCEPT  #iptables -A INPUT -p tcp --dport 22 -j DROP |

Step 2) **iptables** 설정 저장

|  |
| --- |
| #/etc/rc.d/init.d/iptables save |

* 1. 윈도우
     1. Administrator 계정 이름 변경 또는 보안성 강화 (W-01)

**취약점 개요**

* 일반적으로 관리자 계정으로 잘 알려진 “**Administrator**”라는 이름을 변경하지 않은 경우, 악의적인 사용자의 패스워드 추측 공격을 통해 사용 권한 상승의 위험이 있으며, 관리자를 유인하여 침입자의 액세스를 허용하는 악성코드를 실행할 가능성이 있어 위험하다.

**취약점 설명**

Step 1) 관리자 계정 이름 확인

관리자 계정인 “**Administrator**” 계정을 확인했다.

|  |
| --- |
|  |

**취약점 대응방안**

Step 1) **제어판 > 관리도구 > 로컬 보안 정책**으로 이동 후, **로컬 정책 > 보안 옵션** 클릭

“**계정: Administrator 계정 이름 바꾸기**”를 더블 클릭 후, 유추하기 어려운 계정 이름으로

변경한다.

* + 1. 계정 잠금 임계 값 설정 (W-04)

**취약점 개요**

* 시스템의 “**계정 잠금 임계 값**”이 설정되지 않거나 “**6**” 이상의 값으로 설정되어 있는 경우, 공격자는 자동화된 방법을 이용하여 모든 사용자 계정에 대해 암호조합 공격을 자유롭게 시도할 수 있으므로 사용자 계정 정보가 노출될 수 있어 위험하다.

**취약점 설명**

Step 1) **제어판 > 시스템 및 보안 > 관리 도구 > 로컬 보안 정책**으로 이동 후,   
**계정 정책 > 계정 잠금 정책** 클릭

“**계정 잠금 임계 값**”이 설정되어 있지 않는 것을 확인했다.

|  |
| --- |
|  |

**취약점 대응방안**

Step 1) **제어판 > 시스템 및 보안 > 관리 도구 > 로컬 보안 정책**으로 이동 후,  
 **계정 정책 > 계정 잠금 정책** 클릭

“**계정 잠금 임계 값**”을 더블 클릭 후, “**5**“ 이하의 값으로 설정한다.

* + 1. 계정 잠금 기간 설정 (W-47)

**취약점 개요**

* “**시스템의 계정 잠금 기간**”과 “**잠금 수를 원래대로 설정**”이 설정되어 있지 않은 경우, 로그인   
  실패 시 공격자의 자동화된 암호 추측 공격이 가능해지며 사용자 계정의 패스워드 정보가 유출될 수 있어 위험하다.

**취약점 설명**

Step 1) **제어판 > 시스템 및 보안 > 관리 도구 > 로컬 보안 정책**으로 이동 후,   
**계정 정책 > 계정 잠금 정책** 클릭

“**계정 잠금 기간**”과 “**다음 시간 후 계정 잠금 수를 원래대로 설정**”이 “**해당 없음**”인 것을  
 확인했다.

|  |
| --- |
|  |

**취약점 대응방안**

Step 1) **제어판 > 시스템 및 보안 > 관리 도구 > 로컬 보안 정책**으로 이동 후,   
**계정 정책 > 계정 잠금 정책** 클릭

“**계정 잠금 기간**”과 “**다음 시간 후 계정 잠금 수를 원래대로 설정**”을 더블 클릭 후,  
 “**60분**” 이상으로 설정한다.

* + 1. 패스워드 최소 암호 길이 (W-51)

**취약점 개요**

* “**최소 암호 길이**”가 설정되어 있지 않거나 “**8문자**” 미만으로 설정되어 있는 경우, 짧은 패스워드 및 일반적인 단어와 일반적인 어구를 허용해 공격자에게 사전 공격이나 가능한 모든 문자의 조합을 시도하는 무작위 공격을 통해 패스워드가 도용될 수 있어 위험하다.

**취약점 설명**

Step 1) **제어판 > 시스템 및 보안 > 관리 도구 > 로컬 보안 정책**으로 이동 후,   
**계정 정책 > 암호 정책** 클릭

“**최소 암호 길이**”가 설정되어 있지 않는 것을 확인했다.

|  |
| --- |
|  |

**취약점 대응방안**

Step 1) **제어판 > 시스템 및 보안 > 관리 도구 > 로컬 보안 정책**으로 이동 후,   
**계정 정책 > 암호 정책** 클릭

“**최소 암호 길이**”를 더블 클릭 후, “**최소**”를 “**8문자**”로 설정한다.

* + 1. 패스워드 최소 사용 기간 (W-51)

**취약점 개요**

* 패스워드 변경 후 “**최소 사용 기간**”이 “**0일**”로 설정되어 있는 경우, 사용자에게 익숙한 패스워드로 즉시 변동이 가능하여 재사용함으로써 원래 암호를 같은 날 다시 사용할 수 있어 보안적으로 위험하다.

**취약점 설명**

Step 1) **제어판 > 시스템 및 보안 > 관리 도구 > 로컬 보안 정책**으로 이동 후,  
 **계정 정책 > 암호 정책**

“**최소 암호 사용 기간**”이 “**0일**”로 설정되어 있는 것을 확인했다.

|  |
| --- |
|  |

**취약점 대응방안**

Step 1) **제어판 > 시스템 및 보안 > 관리 도구 > 로컬 보안 정책**으로 이동 후,  
 **계정 정책 > 암호 정책**

“**최소 암호 사용 기간**”을 더블 클릭 후, “**0**”보다 큰 값으로 설정한다.

* + 1. 마지막 사용자 이름 표시 안 함 (W-52)

**취약점 개요**

* “**마지막 로그인 사용자 이름 표시 안 함**” 이 “**사용 안 함**”으로 설정되어 있는 경우, 마지막으로 로그온한 사용자의 이름이 로그온 대화 상자에 표시되어 공격자는 이를 획득해서 암호를 추측하거나 무작위 공격을 시도할 가능성이 있어 위험하다.

**취약점 설명**

Step 1) **제어판 > 시스템 및 보안 > 관리 도구 > 로컬 보안 정책**으로 이동 후,  
 **로컬 정책 > 보안 옵션** 클릭

“**마지막 로그인 사용자 이름 표시 안 함**” 이 “**사용 안 함**”으로 설정되어 있는 것을 확인했다.

|  |
| --- |
|  |

**취약점 대응방안**

Step 1) **제어판 > 시스템 및 보안 > 관리 도구 > 로컬 보안 정책**으로 이동 후,  
 **로컬 정책 > 보안 옵션** 클릭

“**마지막 로그인 사용자 이름 표시 안 함**”을 더블 클릭 후, “**사용**”으로 변경한다.

* + 1. 로컬 로그온 허용 (W-53)

**취약점 개요**

* 로컬 로그온 허용 정책에 “**Administrators**” 나 “**IUSR\_**” 계정을 제외하고 불필요한 다른 사용자 계정이나 그룹이 포함되어 있는 경우, 해당 계정을 악용한 비인가자의 시스템 접근 가능성이 높아지며, 이를 통해 악성 코드가 실행되어 권한 상승이나 내부 정보 유출 등의 보안 사고로 이어질 수 있어 위험하다.

**취약점 설명**

Step 1) **제어판 > 시스템 및 보안 > 관리 도구 > 로컬 보안 정책**으로 이동 후,  
 **로컬 정책 > 사용자 권한 할당** 클릭

“**로컬 로그온 허용**”에서 “**Administrators**” 외에 불필요한 사용자인 “**Backup Operators**”,  
 “**Users**” 계정이 존재하는 것을 확인했다.

|  |
| --- |
|  |

**취약점 대응방안**

Step 1) **제어판 > 시스템 및 보안 > 관리 도구 > 로컬 보안 정책**으로 이동 후,  
 **로컬 정책 > 사용자 권한 할당** 클릭

“**로컬 로그온 허용 정책**”을 더블 클릭 후, “**Administrators**”외에 불필요한 사용자인  
 “**Backup Operators**”, “**Users**” 계정을 제거한다.

* + 1. 최근 암호 기억 (W-55)

**취약점 개요**

* 사용자가 현재 암호 또는 최근에 사용했던 암호와 동일한 새 암호를 만들 수 있게 “**최근 암호 기억**” 이 설정되지 않은 경우, 특정 계정에 동일한 암호를 오랫동안 사용하는 것이 가능하여 공격자가 무작위 공격을 통해 패스워드 정보 노출 가능성이 커질 수 있어 위험하다.

**취약점 설명**

Step 1) **제어판 > 시스템 및 보안 > 관리 도구 > 로컬 보안 정책**으로 이동 후,  
 **계정 정책 > 암호 정책**

“**최근 암호 기억**” 이 “**0개**” 로, 설정되어 있지 않은 것을 확인했다.

|  |
| --- |
|  |

**취약점 대응방안**

Step 1) **제어판 > 시스템 및 보안 > 관리 도구 > 로컬 보안 정책**으로 이동 후,  
 **계정 정책 > 암호 정책**

“**최근 암호 기억**”을 “**4개**” 이상으로 설정한다.

* + 1. 원격터미널 접속 가능한 사용자 그룹 제한 (W-56)

**취약점 개요**

* 관리자 권한을 가진 “**Administrators**” 계정을 제외하고 원격 접속이 가능한 별도의 사용자 계정이 존재하지 않은 경우, 일반 사용자나 외부의 임의의 사용자가 인증 절차를 우회하여 원격으로 시스템에 접근할 가능성이 존재하며, 이로 인해 서버 내의 중요 설정을 변경하거나 민감한 정보가 외부로 유출될 수 있는 보안 위협이 발생할 수 있어 위험하다.

**취약점 설명**

Step 1) **제어판 > 시스템 및 보안 > 시스템 > 원격 설정 > [사용자 선택]** 클릭

관리자 계정인 “**Administrators**”를 제외한 원격 접속이 가능한 별도의 계정이 존재하지  
 않는 것을 확인했다.

|  |
| --- |
|  |

**취약점 대응방안**

Step 1) **제어판 > 시스템 및 보안 > 시스템 > 원격 설정 > [사용자 선택]** 클릭

비어 있는 해당 목록에 원격 사용자를 지정해준다.

* + 1. 하드디스크 기본 공유 제거 (W-08)

**취약점 개요**

* 윈도우는 프로그램 및 서비스를 네트워크나 컴퓨터 환경에서 관리하기 위해 시스템 기본 공유 항목을 자동으로 생성하는데 이를 제거하지 않은 경우, 비인가자가 모든 시스템 자원에 접근할 수 있는 위험한 상황이 발생할 수 있으며, 이러한 공유 기능의 경로를 이용하여 바이러스가 침투될 수 있어 위험하다.

**취약점 설명**

Step 1) **제어판 > 시스템 및 보안 > 관리 도구 > 컴퓨터 관리**로 이동 후,  
 **시스템 도구 > 공유 폴더 > 공유** 클릭

“**C 드라이브**”가 “**기본 공유**”되어 있는 것을 확인했다.

|  |
| --- |
|  |

**취약점 대응방안**

Step 1) **제어판 > 시스템 및 보안 > 관리 도구 > 컴퓨터 관리**로 이동 후,  
 **시스템 도구 > 공유 폴더 > 공유** 클릭

해당하는 목록 클릭 후, 마우스 오른쪽 버튼 클릭 후, “**공유 중지**”를 클릭해준다.

Step 2) 레지스트리 편집기 이동

“**\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareWks**” 해당 경로로 계속해서 이동해준 뒤, “**AutoShareServer**” 키 값을 “**0**”으로 설정하고 없으면 새롭게 생성하여 설정한다.

* + 1. 불필요한 서비스 제거 (W-14)

**취약점 개요**

* 일반적으로 시스템 내에서 불필요한 서비스들이 계속해서 구동 중인 경우, 이를 악용한 공격자가 시스템에 침투할 가능성이 존재하며, 특히 네트워크와 관련된 서비스의 경우에는 해당 서비스가 사용하는 포트가 외부에 열려 있을 수 있어, 이를 통해 외부로부터의 비인가 접근이나 악성 트래픽 유입 등의 침입 시도가 발생할 수 있어 위험하다.

**취약점 설명**

Step 1) **제어판 > 시스템 및 보안 > 관리 도구 > 서비스**로 이동

**일반적으로 불필요한 서비스 목록(6.1 참조)** 중 “DHCP Client”,   
 “Distributed Link Tracking Client”, “DNS Client”, “Print Spooler”이 실행 중인 것을 확인했다.

|  |
| --- |
|  |

**취약점 대응방안**

Step 1) **제어판 > 시스템 및 보안 > 관리 도구 > 서비스**로 이동

실행 중인 “**DHCP Client**”, “**Distributed Link Tracking Client**”, “**DNS Client**”, “**Print Spooler**” 서비스들을 각각 마우스 오른쪽 버튼 클릭해서 “**중지**”를 클릭한다.

* + 1. 터미널 서비스 암호화 수준 설정 (W-58)

**취약점 개요**

* 원격 연결을 허용하고 있는 상태에서 “**클라이언트와의 연결에 대한 암호화 수준**” 이 설정되어 있지 않거나 설정된 암호화 수준이 낮은 경우, 데이터가 평문으로 전송되거나 암호화가 충분하지 않아 통신 중간에 제3자가 이를 가로채거나 변조할 수 있는 가능성이 존재하며 이로 인해 계정 정보, 인증 토큰, 중요 시스템 명령어 등 민감한 정보가 외부에 노출될 우려가 있어 위험하다.

**취약점 설명**

Step 1) **제어판 > 시스템 및 보안 > 시스템 > 원격 설정**으로 이동 후, **[원격]** 탭 클릭

“**이 컴퓨터에 대한 원격 연결 허용**”이 선택되어 있는 것을 확인했다.

|  |
| --- |
|  |

Step 2) 로컬 그룹 정책 편집기(gpedit.msc)로 이동 후, **컴퓨터 구성 > 관리 템플릿 > Windows 구성 요소 > 터미널 서비스 > 원격 데스크톱 세션 호스트 > 보안** 클릭

“**클라이언트 연결 암호화 수준 설정**”이 구성되어 있지 않은 것도 확인했다.

|  |
| --- |
|  |

**취약점 대응방안**

Step 1) **제어판 > 시스템 및 보안 > 시스템 > 원격 설정**으로 이동 후, **[원격] 탭** 클릭

“**이 컴퓨터에 대한 원격 연결 허용 안 함**”으로 선택한다.

Step 2) 로컬 그룹 정책 편집기(gpedit.msc) 로 이동 후, **컴퓨터 구성 > 관리 템플릿 > Windows 구성 요소 > 터미널 서비스 > 원격 데스크톱 세션 호스트 > 보안** 클릭

허용한 경우에는 “**클라이언트 연결 암호화 수준 설정**”을 더블 클릭 후, “**중간**” 이상으로 설정해준다.

* + 1. 원격터미널 접속 타임아웃 설정 (W-67)

**취약점 개요**

* 불필요한 명령어나 파일 등 주기적인 예약 작업의 존재 여부를 주기적으로 점검하지 않거나 해당 작업을 제거하지 않은 경우, 시작프로그램과 더불어 해킹과 트로이 목마, 백도어를 설치하여 공격하기 좋은 루트로 사용될 수 있어 위험하다.

**취약점 설명**

Step 1) 로컬 그룹 정책 편집기 (gpedit.msc) 로 이동 후, **컴퓨터 구성 > 관리 템플릿 > Windows 구성 요소 > 터미널 서비스 > 원격 데스크톱 세션 호스트 > 세션 시간 제한** 클릭

“**원격 데스크톱 서비스 세션에 대한 시간 제한 설정**”이 구성되어 있지 않은 것을 확인한다.

|  |
| --- |
|  |

**취약점 대응방안**

Step 1) 로컬 그룹 정책 편집기 (gpedit.msc) 로 이동 후, **컴퓨터 구성 > 관리 템플릿 > Windows 구성 요소 > 터미널 서비스 > 원격 데스크톱 세션 호스트 > 세션 시간 제한** 클릭

“**원격 데스크톱 서비스 세션에 대한 시간 제한 설정**”을 더블 클릭 후, “**사용**”을 선택해준 뒤   
“**활성 세션 제한**”을 설정한다.

* + 1. 정책에 따른 시스템 로깅 설정 (W-69)

**취약점 개요**

* 감사 정책 권고 기준에 따라 감사 설정이 되어 있지 않거나 감사 설정 수준이 너무 낮은 경우, 보안 관련 문제 발생 시 원인을 파악하기 어려우며 법적 대응을 위한 충분한 증거 확보가 어려울 수 있어 위험하다.

**취약점 설명**

Step 1) **제어판 > 시스템 및 보안 > 관리 도구 > 로컬 보안 정책**으로 이동 후,   
**로컬 정책 > 감사정책** 클릭

**감사 정책 권고 기준(**6.2 **참조)**에 따른 “**계정 관리 감사**”와 “**계정 로그온 이벤트 감사**”,   
“**디렉터리 서비스 액세스 감사**”, “**로그온 이벤트 감사**”, “**시스템 이벤트 감사**”, “**정책 변경 감사**” 가 “**감사 안 함**”으로 설정되어 있는 것을 확인한다.

|  |
| --- |
|  |

**취약점 대응방안**

Step 1) **제어판 > 시스템 및 보안 > 관리 도구 > 로컬 보안 정책**으로 이동 후,   
**로컬 정책 > 감사정책** 클릭

“**계정 관리 감사**”, “**디렉터리 서비스 액세스 감사**”, “**로그온 이벤트 감사**”, “**정책 변경 감사**”를  
 각각 더블 클릭 후, “**성공**”으로 설정해주고, “**계정 로그온 이벤트 감사**”, “**시스템 이벤트 감사**”를 “**성공**”, “**실패**” 로 설정한다.

* + 1. 백신 프로그램 설치 (W-36)



* 윈도우에 백신 프로그램이 설치되어 있지 않은 경우 시스템이 실시간으로 악성코드를   
  탐지할 수 없다.
* 웜이나 트로이목마 같은 악성코드는 네트워크 공유, 이메일 등을 통해 빠르게 전파되는데,   
  백신 부재 시에는 이러한 침투 경로를 사전에 차단하거나 감염 이후 치료할 수 있는 수단이 없기에 시스템 가용성 및 데이터 무결성에 문제가 발생할 수 있다.



Step 1) 윈도우에서 바이러스백신 프로그램이 설치되어 있지 않음.

|  |
| --- |
| 윈도우 프로그램 추가/제거 화면 |
|  |



* AhnLab, 트렌드 마이크로, 알약 등 신뢰할 수 있는 백신을 설치한다.
* 최소 일일 1회 정기 검사 스케줄을 구성하여 시스템 전반을 점검한다.
* 백신 프로그램과 바이러스 정의(시그니처) 파일을 자동 업데이트로 설정한다.
  + 1. 화면보호기 설정 (W-38)



* 윈도우에 화면 보호기 설정이 없거나 비활성화되어 있으면, 사용자가 일정 시간 자리를   
  비웠을 때 워크스테이션이 잠기지 않는다.
* 이로 인해 무단 사용자가 해당 서버에 접근하여 화면을 조작하거나 중요 정보를 열람/탈취할 위험이 있다.
* 특히 관리자 권한으로 로그인 된 상태가 유지되면 시스템 설정 변경, 계정 추가/삭제 등 치명적인 보안 사고로 이어질 수 있다.



  Step 1) 윈도우에서 화면 보호기 설정 확인

|  |
| --- |
| 윈도우 화면 보호기 설정 화면 |
| |  | | --- | |  | |



* 화면 보호기를 설정하고, 대기 시간을 10분 이하로 지정한다.
* 화면 보호기 해제 시 반드시 암호 입력을 요구하도록 구성한다.
* 화면 보호기 비활성 상태가 감지될 경우 보안 담당자에게 알림이 전송되도록 한다.
  + 1. 로그온 하지 않고 시스템 종료 허용 해제 (W-39)



* 윈도우 로그인 화면에서 “시스템 종료” 버튼이 활성화되어 있으면, 사용자 인증 없이도 서버를 종료할 수 있는 취약점이 발생한다.
* 인증되지 않은 사용자가 의도치 않게 또는 악의적으로 시스템을 종료하면, 정상 서비스가 종료되고 데이터 처리 중단/손실의 우려가 있다.
* 따라서 비로그온 상태에서 시스템 종료 기능을 반드시 비활성화 시켜야 한다.



  Step 1) “시스템 종료: 로그온 하지 않고 시스템 종료 허용”이 사용으로 설정됨.

|  |
| --- |
| 윈도우 로컬 정책의 보안 옵션 화면 |
|  |



* 로컬 정책의 보안 옵션에 있는 **“로그온 하지 않고 시스템 종료 허용**”을

“**사용 안함**”으로 설정한다.

* + 1. SAM 계정과 공유의 익명 열거 허용 안 함 (W-42)



* 윈도우에서 “**SAM 계정과 공유의 익명 열거 허용**”이 활성화되어 있으면, 네트워크에 연결된 누구나 로그인 없이 도메인 사용자, 컴퓨터, 그룹 계정 목록과 공유 이름을 확인할 수 있습니다.
* 도메인 환경에서는 계정 정보가 곧 권한과 연결되므로, 익명 사용자에게 계정 열람을 허용하는 것은 심각한 보안 위협이 됩니다.



Step 1) “**네트워크 액세스 : SAM 계정과 공유의 익명 열거**”가 ‘**사용 안함**’으로 설정됨.

|  |
| --- |
| 윈도우 로컬 정책의 보안 옵션 화면 |
|  |



* “네트워크 액세스 : SAM 계정과 공유의 익명 열거”를 “사용”으로 설정한다.
  + 1. DOS 공격 방어 레지스트리 설정 (W-72)



* 윈도우에서 TCP/IP 스택의 DoS 방어용 레지스트리 설정이 되어 있지 않으면, 대량의 SYN 패킷이나 비정상적인 네트워크 요청으로 시스템 자원이 과도하게 소비되어 서비스 거부(DoS) 상태에   
  빠질 수 있다.
* 설정된 대기 시간과 재전송 횟수가 길 경우, 공격을 빠르게 막하기에 중요한 서비스가   
  중단될 수 있다.
* “SynAttackProject” 레지스트리는 SYN 플러딩 공격에 대응하기 위해 대기 시간과 재전송 전략을 조정한다.
* “EnableDeadGWDetect” 레지스트리는 불량 게이트웨이를 감지하는 기능을

활성화하는 레지스트리 값이다.

* “KeepAliveTime” 레지스트리는 유휴 연결에 Keep-alive 패킷을 전송하는 주기를 설정하는 값이다.
* “NoNameReleaseOnDeamnd” 레지스트리는 NetBIOS 이름 해제 요청을 차단하여

이름 해제 공격을 방어하기 위한 값이다.



Step 1) 설정 확인

명시된 레지스트리 값이 추가 또는 변경하여 적용되어 있지 않다.

|  |
| --- |
| 윈도우 레지스트리 화면 |
|  |



* “**SynAttackProject**”은 윈도우 2008 이후 서버 버전 기본 활성화되어 있기에 해당 레지스트리를   
  제외한 레지스트리 값을 모두 추가한다.
* “**EnableDeadGWDetect**”을 “**0(False)**”으로 설정한다.
* “**KeepAliveTime**”을 “**300,000(5분)**”으로 설정한다.
* “**NoNameReleaseOnDemand**”를 “**1(True)**”로 설정한다.
  + 1. LAN Manager 인증 수준 (W-77)



* 윈도우에서 기본적으로 LAN Manager(LM) 또는 NTLM 인증을 허용하면, 네트워크 로그인 과정에서 사용자의 암호 해시가 약한 프로토콜을 통해 전송됩니다.
* 이 경우 공격자는 패킷을 가로채거나 크래킹을 통해 실제 암호를 유추할 수 있습니다.
* 특히 LM 해시는 쉽게 풀 수 있도록 설계되어 있어, 강력한 암호를 사용해도 취약점이 존재합니다.
* 따라서 보안 강화를 위해 NTLMv2 수준의 인증만 허용해야 합니다.
* NTLMv2은 윈도우 경에서 사용하는 로그인 인증 프로토콜로, 서버-클라이언트가 주고받는 메시지를 매번 달라지는 난수와 타임스탬프(시간 정보)를 바탕으로 암호화해, 실제 비밀번호를 네트워크로 전송하지 않는다.



Step 1) 설정 확인

“**네트워크 보안: LAN Manager 인증 수준**” 정책에 설정이 되어 있지 않다.

|  |
| --- |
| 윈도우 로컬 정책의 보안 옵션 화면 |
|  |



1. 로컬 정책의 보안 옵션에서 “네트워크 보안: LAN Manager 인증 수준” 정책에

“NTLMv2 응답만 보내기”로 설정한다.

1. 위 조치를 통해 윈도우환경에서 안전한 NTLMv2 인증만 사용하도록 강제하여,

네트워크 로그인 보안을 크게 강화할 수 있습니다.

* 1. DBMS
     1. 데이터베이스의 불필요 계정을 제거하거나, 잠금 설정 후 사용 (D-02)

**취약점 개요**

* 기관 정책에 맞게 패스워드 사용기간 및 복잡도 설정이 적용되어 있지 않고 설정이 적용되어 있는지 점검한다.

**취약점 설명**

Step 1) SQL\*Plus 쿼리문으로 확인

|  |
| --- |
| SQL > SELECT \* FROM DBA\_PROFILES WHERE RESOURCE\_TYPE = 'PASSWORD'; |

Step 2) 결과 확인

1. 비밀번호를 영원히 바꾸지 않아도 된다고 설정 되어있다.

|  |
| --- |
|  |

1. 비밀번호 만료 기간이 설정되어 있지 않다.

|  |
| --- |
|  |

1. 재사용 제한이 없다고 설정되어 있다.

|  |
| --- |
|  |

1. 비밀번호 복잡성이 체크 되어있지 않다.

|  |
| --- |
|  |

1. 오래된 계정이 비활성화되어 있지 않다.

|  |
| --- |
|  |

**취약점 대응방안**

1. 비밀변호 변경 주기를 설정한다. (평균 변경 주기 : 90일)

|  |
| --- |
| SQL > ALTER PROFILE DEFAULT LIMIT PASSWORD\_LIFE\_TIME 90; |

1. 비밀번호 만료 후 유예기간을 설정한다. (평균 유예기간 : 7일)

|  |
| --- |
| SQL > ALTER PROFILE DEFAULT LIMIT PASSWORD\_GRACE\_TIME 7; |

1. 비밀번호 재사용을 방지하기 위해 제한을 해준다.

|  |
| --- |
| SQL > ALTER PROFILE DEFAULT LIMIT PASSWORD\_REUSE\_MAX 10;  (최근 10개로 사용했던 비밀번호를 기억)  또는  ALTER PROFILE DEFAULT LIMIT PASSWORD\_REUSE\_TIME 365;  (365일 이내에 같은 비밀번호 사용 불가) |

1. 비밀번호가 단순하게 설정 가능하지 못하게 복잡성 함수를 적용한다.

|  |
| --- |
| SQL > ALTER PROFILE DEFAULT LIMIT PASSWORD\_VERIFY\_FUNCTION VERIFY\_FUNCTION;   * 최소 8자 * 대/소문자, 숫자 포함 * 사용자 이름 포함 금지 * 사전 비밀번호 거부 |

1. 1년 이상 사용하지 않은 계정을 조회하고 계정을 잠근다.

|  |
| --- |
| 오래된 계정 조회  SQL > SELECT username, account\_status, last\_login  2 FROM dba\_users  3 WHERE last\_login < SYSDATE - 365;  계정 잠금  SQL > ALTER USER <사용자이름> ACCOUNT LOCK; |

* + 1. DBA 이외의 인가되지 않은 사용자가 시스템 테이블에 접근할 수 없도록 설정   
       (D-06)

**취약점 개요**

* 시스템 테이블에 일반 사용자 계정이 접근할 수 없도록 설정되어 있는지 점검한다. 시스템 테이블의 일반 사용자 계정 접근 제한 설정 적용 여부를 점검하여 일반 사용자 계정 유출 시 발생할 수 있는 비인가자의 시스템 테이블 접근 위험을 차단하기 위함이다.
* 시스템 테이블의 일반 사용자 계정 접근 제한 설정이 되어 있지 않을 경우 객체, 사용자, 테이블 및 뷰, 작업 내역 등의 시스템 테이블에 저장된 정보가 누출될 수 있다.

**취약점 설명**

Step 1) DBA만 접근 가능한 테이블의 권한 확인

|  |
| --- |
| SQL> select grantee, privilege, owner, table\_name from dba\_tab\_privs where (owner='SYS' or table\_name like 'DBA\_%') and privilege <> 'EXECUTE' and grantee not in ('PUBLIC', 'AQ\_ADMINISTRATOR\_ROLE', 'AQ\_USER\_ROLE', 'AURORA$JIS$UTILITY$', 'OSE$HTTP$ADMIN', 'TRACESVR', 'CTXSYS', 'DBA', 'DELETE\_CATALOG\_ROLE', 'EXECUTE\_CATALOG\_ROLE', 'EXP\_FULL\_DATABASE', 'GATHER\_SYSTEM\_STATISTICS', 'HS\_ADMIN\_ROLE', 'IMP\_FULL\_DATABASE', 'LOGSTDBY\_ADMINISTRATOR', 'MDSYS','ODM', 'OEM\_MONITOR', 'OLAPSYS', 'ORDSYS', 'OUTLN', 'RECOVERY\_CATALOG\_OWNER', 'SELECT\_CATALOG\_ROLE', 'SNMPAGENT', 'SYSTEM', 'WKSYS', 'WKUSER', 'WMSYS', 'WM\_ADMIN\_ROLE', 'XDB', 'LBACSYS', 'PERFSTAT', 'XDBADMIN') and grantee not in (select grantee from dba\_role\_privs where granted\_role='DBA') order by grantee; |
|  |

Step 2) 결과 확인

1217개의 결과값이 나온 것을 확인할 수 있다.

|  |
| --- |
|  |

**취약점 대응방안**

필요하게 테이블 접근 권한이 사용자 계정에 할당된 경우, 어떤 계정이나 role이   
나타나지 않게 설정한다.

|  |
| --- |
| SQL> REVOKE 권한 on 객체 FROM User; |

* + 1. 데이터베이스의 주요 파일 보호 등을 위해 DB 계정의 umask를 022 이상으로  
        설정하여 사용 (D-16)

**취약점 개요**

* 사용자 계정의 umask 설정이 022 이상으로 설정되어 있는지 점검한다. 소프트웨어 설치 때 생성되는 파일에 관리자를 제외한 일반 사용자의 파일 수정 권한을 제거함으로써 비인가자에 의한 데이터베이스 주요 파일 변경이나 삭제로부터 보호하기 위함이다.
* umask를 “022” 이상으로 설정하지 않을 경우, 비인가자에 의한 데이터베이스의 주요 파일 변경, 삭제 등으로 데이터베이스 시스템 장애가 발생할 수 있다.

**취약점 설명**

Step 1) umask를 통해 umask 값 확인

해당 환경은 022보다 이하의 값으로 취약하다.

|  |
| --- |
| $ umask |
|  |

**취약점 대응방안**

umask 값을 022 이상으로 설정을 권장한다.

|  |
| --- |
| $ umask 022 |

* + 1. 인가되지 않은 Object Owner의 제한 (D-20)

**취약점 개요**

* Oracle DB 내 시스템 및 DBA 계정 외 오브젝트를 보유한 계정(APPQOSSYS 등)이 존재하여, 불필요한 계정 또는 점검이 필요한 계정일 가능성이 있음. 해당 계정의 사용 여부 및 접근 권한을 점검하고, 필요 시 접근 제한 또는 삭제 등의 조치를 권고한다.

**취약점 설명**

Step 1) 설정 확인(SQL\*Plus)

DBA가 아닌 사용자 중 시스템 계정이 아닌 스키마(OWNER)만 조회하는

Oracle SQL 문 입력한다.

|  |
| --- |
| SQL> Select distinct owner from dba\_objects where owner not in  ('SYS','SYSTEM', 'MDSYS','CTXSYS',‘ORDSYS','ORDPLUGINS',  'AURORA$JIS$UTILITY$','HR','ODM','ODM\_ MTR','OE','OLAPDBA','OLA  PSYS','OSE$HTTP$ADMIN','OUTLN','LBACSYS','MTSYS','PM',  'PUBLIC','QS','QS\_ADM',’QS\_CB','QS\_CBADM',‘DBSNMP','QS\_CS','QS\_ES','QS\_OS',  'QS\_WS','RMAN', 'SH', 'WKSYS', 'WMSYS','XDB') and owner not in (select  grantee from dba\_role\_privs where granted\_role='DBA'); |

Step 2) 결과 확인(SQL\*Plus)

DBA 권한이 없는 계정에 오브젝트(owner)가 존재한다.

|  |
| --- |
|  |

**취약점 대응방안**

Step 1) 권한 취소(SQL\*Plus)

특정 사용자(User)에게 부여된 객체(Object)에 대한 권한을 회수(REVOKE)하는

명령어를 입력한다.

|  |
| --- |
| SQL> REVOKE 권한 on 객체 FROM User; |

|  |
| --- |
| [참고 자료] |
|  |

* + 1. 인가되지 않은 GRANT OPTION 사용 제한 (D-21)

**취약점 개요**

* PUBLIC 사용자에게 XDB 스키마 객체에 대한 재부여(Grantable='YES') 권한이 다수 부여되어 있어, 권한 확산 가능성이 존재한다. 해당 권한의 사용 여부를 검토하고, 불필요한 경우 회수(REVOCATION)를 권고한다.

**취약점 설명**

Step 1) 설정 확인(SQL\*Plus)

DBA가 아닌 사용자(grantee) 중에서 시스템 계정이 아닌 소유자(owner)의 객체(table)에

대해 권한 위임이 가능한(grantable='YES') 권한을 가진 사용자 목록을 조회하는 SQL 문을

입력한다.

|  |
| --- |
| SQL> Select grantee||':'||owner||'.'||table\_name from dba\_tab\_privs where  grantable='YES' and owner not in  ('SYS','MDSYS','ORDPLUGINS','ORDSYS','SYSTEM', 'WMSYS','SDB', 'LBACSYS') and  grantee not in (select grantee from dba\_role\_privs where granted\_role= 'DBA')  order by grantee; |

Step 2) 결과 확인(SQL\*Plus)

계정이 나오는 경우, 취약하다고 볼 수 있다.

|  |
| --- |
|  |

**취약점 대응방안**

Step 1) 권한 취소, 재부여(SQL\*Plus)

지정된 사용자(User)로부터 특정 역할(Role)을 회수(REVOKE)하는 명령어 입력한다.

|  |
| --- |
| SQL> REVOKE Role FROM User; |

* 1. 웹(Web)
     1. SQL INJECTION (SI)

**취약점 개요**

* 자유게시판에서 메인 페이지에 있는 검색창에 SQL 쿼리문을 입력하여 참, 거짓 결과를 비교하며 사용자의 입력 값으로 웹 사이트 SQL 쿼리가 완성되는 약점을 이용하며,   
  입력 값을 변조하여 정상적인 SQL 쿼리를 조합하거나 실행하는 공격이다.
* 개발자가 생각하지 못한 SQL문을 실행되게 함으로써 데이터베이스를 비정상적으로   
  조작 가능하다.

|  |  |  |
| --- | --- | --- |
| **번호** | **URL** | **파라미터** |
| 1 | http://web-as-alb-1392225615.us-west-2.elb.amazonaws.com/main.do | keyword |
| 2 | http://web-as-alb-1392225615.us-west-2.elb.amazonaws.com/adminCouponList.do | - |

**취약점 설명**

|  |  |
| --- | --- |
| **Case 1** | 전체 상품 검색 (Blind SQL) |

Step 1) 메인 페이지 > 전체 검색 입력 칸

|  |
| --- |
|  |

Step 2) SQL 쿼리 문을 입력하여 결과 화면 확인

쿼리 문 결과 값이 참 일 때 결과 화면이다.

|  |
| --- |
| 쿼리 문 **'AND '1' = '1' --** |
|  |

쿼리 문 결과 값이 거짓 일 때 결과 화면이다.

|  |
| --- |
| 쿼리 문 **'AND '1' = '2' --** |
|  |

Step 3) 파이썬 자동화 코드를 이용하여 중요 데이터 추출

USER 데이터 추출이 가능하다.

|  |
| --- |
| 쿼리 예시) 가디건' AND SUBSTR(USER,1, 1) = 'C' -- |
|  |

같은 방법으로 데이터 베이스 내의 테이블 이름 추출이 가능하다.

|  |
| --- |
|  |

|  |  |
| --- | --- |
| **Case 2** | 관리자 페이지 |

Step 1) 관리자 페이지 > 쿠폰관리 > 쿠폰 목록/수정

URL을 통해 별도의 인증 없이 관리자 페이지 접속이 가능하다.

|  |
| --- |
|  |

Step 2) 검색어 입력 칸에 SQL 쿼리 문 입력

참 쿼리 문을 입력했을 때 결과이다.

|  |
| --- |
| 쿼리 문: test' or 1 = 1 — |
|  |

거짓 쿼리문을 입력했을 때 결과이다.

|  |
| --- |
| 쿼리 문: test' or 1 = 0 — |
|  |

Step 3) SQL NAP 도구를 이용하여 쿼리 문 자동 삽입

쿠폰 관리 페이지를 대상으로 명령어를 실행한다.

|  |
| --- |
| 링크: http://web-as-alb-1392225615.us-west-2.elb.amazonaws.com/adminCouponList.do |
|  |

Step 4) 중요한 정보 추출 결과를 확인

|  |
| --- |
|  |

**취약점 대응방안**

* SQL 쿼리에 사용되는 문자열의 유효성을 검증하는 로직 구현한다.
* 아래와 같은 특수문자를 사용자 입력 값으로 지정하지 않는다.

(아래 문자들은 해당 데이터베이스에 따라 달라질 수 있음)

|  |
| --- |
|  |

* Dynamic SQL 구문 사용을 지양하며 파라미터에 문자열 검사 필수로 적용한다.
* 시스템에서 제공하는 에러 메시지 및 데이터베이스에서 제공하는 에러 코드가 노출되지 않도록 예외처리를 해준다.
* 웹 방화벽에 인젝션 공격 관련 (JSP)

- 문자열 유효성 검증 로직 구현

(예) 특정 문자열 필터링 적용 (※ 예로 제시한 것으로, 구현 시 다를 수 있음)

request로 입력 값을 가져오는 경우 입력 값에서 특수문자를 제거하여 바인딩하는 소스 삽입

replaceAll() 메소드를 사용하여 구현한다.

|  |
| --- |
|  |

* + 1. 정보 누출 (IL)

**취약점 개요**

* 웹 서비스 시 불필요한 정보가 노출되는지 여부를 점검한다. 웹 서비스 시 불필요한 정보가 노출되는 것을 방지함으로써 2차 공격에 활용될 수 있는 정보 노출을 차단하기 위함이다.
* 웹 사이트에 중요정보(개인정보, 계정정보, 금융정보 등)가 노출되거나 에러 발생 시 과도한 정보(애플리케이션 정보, DB 정보, 웹 서버 구성 정보, 개발 과정의 코멘트 등)가 노출될 경우 공격자들의 2차 공격을 위한 정보로 활용될 수 있다.

|  |  |  |
| --- | --- | --- |
| **번호** | **URL** | **파라미터** |
| 1 | http://web-as-alb-1392225615.us-west-2.elb.amazonaws.com/ manager/ | - |
| 2 | http://web-as-alb-1392225615.us-west-2.elb.amazonaws.com/ manager/html/ | - |
| 3 | http://web-as-alb-1392225615.us-west-2.elb.amazonaws.com/ manager/html/upload/ | 업로드 파일 |
| 4 | http://web-as-alb-1392225615.us-west-2.elb.amazonaws.com/ docs/ | - |

**취약점 설명**

|  |  |
| --- | --- |
| **Case 1** | 경로 접근 오류 |

Step 1) 특정 경로 URL 입력 시 과도한 정보 노출

관리자 페이지로 추정되는 URL에 접근 시 뜨는 에러 메시지에서 과도한 정보가 노출된다.

|  |
| --- |
|  |

|  |  |
| --- | --- |
| **Case 2** | 불필요한 페이지 동작 |

Step 1) 특정 경로 URL 입력 시 불필요한 페이지로 이동

/docs/ 입력 시 Apache Tomcat으로 이동한다.

|  |
| --- |
|  |

**취약점 대응방안**

Step 1) 400, 500번대의 에러 코드에 대해 별도의 에러 페이지로 Redirect 하거나 적절한   
에러처리 루틴을 설정하여 처리되도록 한다. 이 설정은 **httpd.conf**의 전역 설정에 추가한다.

Step 2) 특정 에러 코드에 대해 에러 메시지를 출력한다.

|  |
| --- |
| Apache 구문  ErrorDocument 500 “Error Message”  ErrorDocument 404 “/your web root/error.html”  ErrorDocument 404 “/your web root/error.html”  ErrorDocument 402 http:/xxx.com/error.html |

* + 1. 크로스 사이트 스크립팅 (XSS)

**취약점 개요**

* QnA 게시판에서 사용자의 입력 데이터를 출력할 때 특수문자를 필터링에 등록하거나 이스케이프 처리하지 않아 공격자가 등록한 악성 스크립트가 게시물을 열람하는 관리자의   
  웹 브라우저에서 실행 가능하다.
* 검색창에서 악성스크립트 입력 시 서버에 저장되지 않고 바로 실행 가능하다.

|  |  |  |
| --- | --- | --- |
| **번호** | **URL** | **파라미터** |
| 1 | http://web-as-alb-1392225615.us-west-2.elb.amazonaws.com/shop/goodsList/outer/NewItem.do | - |
| 2 | http://web-as-alb-1392225615.us-west-2.elb.amazonaws.com/qna/openQnaList.do | - |

**취약점 설명**

|  |  |
| --- | --- |
| **Case 1** | 카테고리 검색란 (Reflected XSS) |

Step 1) “**메인 페이지 > 카테고리 선택**”에서 “**검색란**”

|  |
| --- |
|  |

Step 2) 검색란에 악성 스크립트 삽입

|  |
| --- |
| 스크립트 구문 "><script>alert(1)</script> |
|  |

Step 3) 스크립트 실행 결과 확인

|  |
| --- |
|  |

|  |  |
| --- | --- |
| **Case 2** | QNA 게시판 작성 (Stored XSS) |

Step 1) “**메인 페이지 > 고객 센터 > QNA 게시판”에서 “글쓰기**” 클릭

|  |
| --- |
|  |

Step 2) 게시글 작성 페이지에서 스크립트 작성

|  |
| --- |
| 스크립트 구문1: 제목 <script>alert(”제목 XSS”);</script> |
| 스크립트 구문2: 내용 <script>alert(”내용 XSS”);</script> |
|  |

Step 3) 게시글 작성 후 스크립트 실행 결과

제목 입력 부분에서 취약점이 있는 것을 확인할 수 있다.

|  |
| --- |
|  |

내용 입력 부분에서 취약점이 있는 것을 확인할 수 있다.

|  |
| --- |
|  |

**취약점 대응방안**

* 웹 사이트에 사용자 입력 값이 저장되는 페이지는 공격자가 웹 브라우저를 통해 실행되는 스크립트 언어(HTML, JavaScript, VBScript 등)를 사용하여 공격하므로 해당되는 태그 사용을 사전에 제한하고, 사용자 입력 값에 대한 필터링 작업이 필요하다.
* 게시물의 본문 외에도 제목, 댓글, 검색어 입력 창, 그 외 사용자 측에서 넘어오는 값을 신뢰하는 모든 form과 파라미터 값에 대해서 필터링을 수행한다.
* 입력 값에 대한 필터링 로직 구현 시 공백 문자를 제거하는 trim, replace 함수를 사용하여 반드시 서버 측에서 구현되어야 한다.
* URLDecoder 클래스에 존재하는 decode 메소드를 통해 URL 인코딩이 적용된 사용자 입력 값을 디코딩함으로써 우회 공격을 차단한다.
* 웹 방화벽에 모든 사용자 입력 폼(회원정보 변경, 게시판, 댓글, 자료실, 검색, URL 등)을 대상으로 특수문자, 특수 구문 필터링하도록 룰셋을 적용시킨다.

※ 필터링 조치 대상 입력 값

• 스크립트 정의어 : <SCRIPT>, <OBJECT>, <APPLET>, <EMBED>, <FORM>, <IFRAME> 등

• 특수문자 : <, >, ", ', &, %, %00(null) 등

* + 1. 크로스 사이트 리퀘스트 변조\_CSRF (CF)

**취약점 개요**

* 사용자의 신뢰(인증) 정보 내에서 사용자의 요청(Request)을 변조함으로써 XSS 취약점이 발견된 곳에서 악성 스크립트를 통해 등록, 수정, 삭제 등의 기능을 사용하여 해당 사용자의 권한으로 악의적인 공격을 수행할 수 있다.

|  |  |  |
| --- | --- | --- |
| **번호** | **URL** | **파라미터** |
| 1 | <http://web-as-alb-1392225615.us-west-2.elb.amazonaws.com/qna/openQnaList.do> | - |

**취약점 설명**

Step 1) “**메인 페이지 > QnA 게시판 > 글쓰기**”에 XXS 취약점이 존재하는지 확인

|  |
| --- |
|  |

Step 2) 등록 및 변경 등의 데이터 수정 기능의 페이지가 있는지 조사 후 스크립트 작성

POST 요청을 보내 글을 자동으로 작성해주는 스크립트 작성한다.

|  |
| --- |
|  |

Step 3) 다른 계정이나 관리자 계정으로 해당 게시물 열람

해당 게시물을 읽게 되면 스크립트가 실행되어 자동으로 게시물 작성한다.

|  |
| --- |
|  |

Step 4) 결과 확인

로그인 된 계정으로 자동으로 게시물 작성된다.

|  |
| --- |
|  |

**취약점 대응방안**

* 웹 사이트에 사용자 입력 값이 저장되는 페이지는 요청이 일회성이 될 수 있도록 설계한다.
* 사용 중인 프레임워크에 기본적으로 제공되는 CSRF 보호 기능 사용한다.
* 사용자가 정상적인 프로세스를 통해 요청하였는지 HTTP 헤더의 Referer 검증 로직 구현한다.
* 정상적인 요청(Request)과 비정상적인 요청(Request)를 구분할 수 있도록 Hidden Form을 사용하여 임의의 암호화된 토큰(세션 ID, Timestamp, nonce 등)을 추가하고 이 토큰을 검증하도록 설계한다.
* HTML이나 자바스크립트에 해당되는 태그 사용을 사전에 제한하고, 서버 단에서 사용자   
  입력 값에 대한 필터링 구현한다.
* HTML Editor 사용으로 인한 상기사항 조치 불가 시,

서버 사이드/서블릿/DAO(Data Access Object) 영역에서 조치하도록 설계한다.

* XSS 조치 방안 참조
  + 1. 불충분한 인가 (IN)

**취약점 개요**

* 민감한 데이터 또는 기능에 접근 및 수정 시 통제 여부를 점검한다. 접근 권한에 대한 검증 로직을 구현하여 비인가자의 악의적인 접근을 차단하기 위함이다.
* 접근제어가 필요한 중요 페이지의 통제수단이 미흡한 경우, 비인가자가 URL 파라미터 값 변경 등의 방법으로 중요 페이지에 접근하여 민감한 정보 열람 및 변조 가능하다.

|  |  |  |
| --- | --- | --- |
| **번호** | **URL** | **파라미터** |
| 1 | http://web-as-alb-1392225615.us-west-2.elb.amazonaws.com/order/basketAllOrderWrite.do | ORDER\_TOTAL\_PAY\_PRICE |
| 2 | http://web-as-alb-1392225615.us-west-2.elb.amazonaws.com/qna/openQnaDetail.do | - |

**취약점 설명**

|  |  |
| --- | --- |
| **Case 1** | 결제 값 변조 |

Step 1) 상품 결제

구매하고자 하는 상품의 결제 화면이다.

|  |
| --- |
|  |

Step 2) 결제 시도 패킷 캡처

결제 버튼을 클릭할 때 패킷을 잡는다.

|  |
| --- |
|  |

Step 3) 결제할 상품의 값 변조

**ORDER\_TOTAL\_PAY\_PRICE** 값을 변조한다.

|  |
| --- |
|  |

Step 4) 주문 완료 페이지

주문이 완료되었다.

|  |
| --- |
|  |

Step 5) 결제 내역 확인

주문 배송 내역 확인 시 변조한 가격으로 결제되었다.

|  |
| --- |
|  |

|  |  |
| --- | --- |
| **Case 2** | 다른 유저 글 접근 |

Step 1) QNA 글 작성 후 접근 시도

글 작성 후 본인 글에 접근을 시도한다.

|  |
| --- |
|  |

Step 2) 접근 시도 패킷 캡처

접근 시도의 첫 패킷이다. Forward를 한 번 눌러 넘긴다.

|  |
| --- |
|  |

Step 3) QNA\_NO 값 변조

게시글의 인덱스 역할을 하는 QNA\_NO 값을 변조한다.

|  |
| --- |
|  |

Step 4) 다른 유저의 글 접근 가능

다른 유저의 글을 비밀번호 없이 접근 가능하다.

|  |
| --- |
|  |

**취약점 대응방안**

* + 접근제어가 필요한 중요 페이지는 세션을 통한 인증 등 통제수단을 구현하여 인가된 사용자 여부를 검증 후 해당 페이지에 접근할 수 있도록 한다.
  + 페이지별 권한 매트릭스를 작성하여 접근제어가 필요한 모든 페이지에서 권한 체크가 이뤄지도록 구현하여야 한다.
    1. 불충분한 세션 만료 (SC)

**취약점 개요**

* 세션의 만료 기간 설정 여부를 점검한다. 세션 타임아웃 기능을 구현하여 공격자가 만료되지 않은 세션 활용을 방지하기 위함이다.
* 시스템 테이블의 일반 사용자 계정 접근 제한 설정이 되어 있지 않을 경우 객체, 사용자, 테이블 및 뷰, 작업 내역 등의 시스템 테이블에 저장된 정보가 누출될 수 있다.

|  |  |  |
| --- | --- | --- |
| **번호** | **URL** | **파라미터** |
| 1 | http://web-as-alb-1392225615.us-west-2.elb.amazonaws.com | - |

**취약점 설명**

Step 1) 일정 시간 이후 세션 유지

인증 후 시간이 오래 경과하여도 세션이 유지된다.

|  |
| --- |
|  |

**취약점 대응방안**

* 세션 타임아웃 구현 시 타임아웃 시간은 10분으로 설정할 것을 권고한다.
  + 1. 프로세스 검증 누락 (IA)

**취약점 개요**

* 인증이 필요한 웹 사이트의 중요(관리자 페이지, 회원변경 페이지 등) 페이지에 대한 접근제어 설정 여부를 확인한다. 인증이 필요한 모든 페이지에 대해 유효 세션임을 확인하는 프로세스 및 주요 정보 페이지에 접근 요청자의 권한 검증 로직을 적용하여, 비인가자가 하위 URL 직접 접근, 스크립트 조작 등의 방법으로 중요한 페이지에 접근을 시도하는 것을 차단하기 위함이다.
* 인증이 필요한 웹 사이트의 중요(관리자 페이지, 회원변경 페이지 등) 페이지에 대한 접근 제어가 미흡할 경우 하위 URL 직접 접근, 스크립트 조작 등의 방법으로 중요한 페이지에 대한 접근이 가능하다.

|  |  |  |
| --- | --- | --- |
| **번호** | **URL** | **파라미터** |
| 1 | http://web-as-alb-1392225615.us-west-2.elb.amazonaws.com/ qna/openQnaWrite.do | - |
| 2 | http://web-as-alb-1392225615.us-west-2.elb.amazonaws.com/ notice/openNoticeWrite.do | - |
| 3 | http://web-as-alb-1392225615.us-west-2.elb.amazonaws.com/ faq/openFaqWrite.do | - |

**취약점 설명**

Step 1) QNA 글 작성 URL을 통한 경로 유추

문의글 작성 URL을 통해 공지사항 및 FAQ와 같이 관리자만 작성할 수 있는 곳의 경로를   
유추한다.

|  |
| --- |
|  |

Step 2) 공지사항 작성 URL 접근

URL에 유추한 경로를 입력하면 공지사항 글을 작성할 수 있다.

|  |
| --- |
|  |

Step 3) 일반 유저의 공지사항 글 작성

일반 유저가 공지사항 게시판에 글을 작성할 수 있다.

|  |
| --- |
|  |

Step 4) 관리자 검증 과정 부재

작성자에 대한 검증이 없어 작성자가 관리자로 표시된다.

|  |
| --- |
|  |

**취약점 대응방안**

1. 우회될 수 플로우를 차단하여야 하며, 페이지별 권한 매트릭스를 작성하여 페이지에   
   부여된 권한의 타당성을 체크한 후 권한 매트릭스를 기준으로 전 페이지에서 권한 체크가  
   이뤄지도록 구현하여야 한다.
2. 인증이 필요한 모든 페이지에 대해 유효 세션임을 확인하는 프로세스 및 주요 정보   
   페이지에 접근 요청자의 권한 검증 로직을 적용한다.
3. 유효 세션의 검증 및 페이지에 대한 접근 권한을 Client Side Script에 의존할 경우   
   사용자가 임의로 수정할 수 있으므로 Server Side Script로 구현된 프로세스를 사용한다.
   * 1. 파일 업로드 (FU)

**취약점 개요**

* 웹 사이트의 게시판, 자료실 등에 조작된 Server Side Script 파일이 업로드 되는 파일에 대한 확장자 검증이 이루어졌는지 확인 여부 점검한다.

|  |  |  |
| --- | --- | --- |
| **번호** | **URL** | **파라미터** |
| 1 | http://web-as-alb-1392225615.us-west-2.elb.amazonaws.com/shop/openGoodsWrite.do | - |

**취약점 설명**

Step 1) 관리자 페이지 > 상품등록

|  |
| --- |
|  |

Step 2) php 파일을 이용 > 업로드 > 파일 선택 > 파일 등록

|  |
| --- |
| php 파일  <?php  system($\_GET[cmd=http://web-as-alb-1392225615.us-west-2.elb.amazonaws.com/shop/openGoodsWrite.do]);  ?> |
|  |

Step 3) 이미지 정보 > 확인 후 작성하기 클릭

|  |
| --- |
|  |

Step 4) png, jpg 등 이미지 파일 외 다른 파일 업로드 되는지 확인

|  |
| --- |
|  |

**취약점 대응방안**

* 사용자가 파일을 업로드할 수 있는 모든 모듈에 적용이 필요하다.
* 화이트 리스트 방식으로 허용된 확장자만 업로드 가능하도록 서버 측 통제를 적용한다.
* 업로드 되는 파일을 디렉터리에 저장할 때 파일명과 확장자를 외부 사용자가 추측할 수 없는 문자열로 변경하여 저장한다.(파일 이름은 DB에 저장)
* 업로드 파일을 위한 전용 디렉터리를 별도로 생성하여 웹 서버 데몬 설정 파일(httpd.conf 등)에서 실행 설정을 제거함으로써, Server Side Script가 업로드 되더라도 웹 엔진이 실행하지 않는 환경을 설정한다.
* 파일 업로드 필드를 대상으로 특수 문자를 필터링하도록 웹 방화벽 룰셋을 적용한다.
  + 1. 위치 공개 취약점 (PL)

**취약점 개요**

* 웹 URL에서 불필요한 파일이 존재하거나, 샘플 페이지가 존재하는지 확인 여부 점검한다.

|  |  |  |
| --- | --- | --- |
| **번호** | **URL** | **파라미터** |
| 1 | http://web-as-alb-1392225615.us-west-2.elb.amazonaws.com/main.do | - |
| 2 | http://web-as-alb-1392225615.us-west-2.elb.amazonaws.com/docs/ | - |
| 3 | http://web-as-alb-1392225615.us-west-2.elb.amazonaws.com/server-status/ | - |
| 4 | http://web-as-alb-1392225615.us-west-2.elb.amazonaws.com/manager/ | - |

**취약점 설명**

Step 1) 메인 홈페이지 > URL 창

|  |
| --- |
|  |

Step 2) Gobuster 활용

|  |
| --- |
| gobuster dir -u http://web-as-alb-1392225615.us-west-2.elb.amazonaws.com/ -w /usr/share/wordlists/dirb/common.txt |
|  |

Step 3) 각각의 URL 마다 하나씩 입력

|  |
| --- |
|  |

|  |
| --- |
|  |

|  |
| --- |
|  |

**취약점 대응방안**

* robots.txt 파일 작성을 통해 검색 차단할 디렉터리, 확장자, 페이지 등을 지정할 수 있으며 HTML의 HEAD 태그 내에 META 태그를 추가하여 검색엔진의 인덱싱을 차단한다.
* 웹 디렉터리를 조사하여 아래의 삭제해야 할 파일 확장자에 포함된 백업 파일을 모두 삭제하고, \*.txt 확장자와 같이 작업 중 생성된 일반 텍스트 파일이나 이미지 파일 등도 제거한다.
* 백업 파일은 백업 계획을 수립하여 안전한 곳에 정기적으로 백업해야 하며 웹 서버에서는 운영에 필요한 최소한의 파일만을 생성하여야 한다.
* 웹 서버 설정 후 디폴트 페이지와 디폴트 디렉터리 및 Banner를 삭제하여 Banner Grab에 의한 시스템 정보 유출을 차단한다.
* Apache, IIS, Tomcat 등 각 웹 서버 설정 시 함께 제공되는 샘플 디렉터리 및 매뉴얼 디렉터리, 샘플 애플리케이션을 삭제하여 보안 위험을 최소화한다.
  + 1. 데이터 평문 전송 (SN)

**취약점 개요**

* 서버와 클라이언트 간 통신 시 데이터의 암호화 여부를 점검한다. 서버와 클라이언트 간 통신 시 데이터의 암호화 전송 미흡으로 정보 유출의 위험을 방지하고자 한다.
* 웹 상의 데이터 통신은 대부분 텍스트 기반으로 이루어지기 때문에 서버와 클라이언트 간에 암호화 프로세스를 구현하지 않으면 간단한 도청(Sniffing)을 통해 정보를 탈취 및 도용할 수 있다.

|  |  |  |
| --- | --- | --- |
| **번호** | **URL** | **파라미터** |
| 1 | http://web-as-alb-1392225615.us-west-2.elb.amazonaws.com/ joinForm.do | MEMBER\_ID,  MEMBER\_PASSWD |
| 2 | http://web-as-alb-1392225615.us-west-2.elb.amazonaws.com/ loginAction.do | MEMBER\_ID,  MEMBER\_PASSWD |

**취약점 설명**

Step 1) 중요정보 송신 페이지 확인

로그인 및 회원가입 페이지에서 아이디와 패스워드를 입력한다.

|  |
| --- |
|  |

Step 2) 중요정보 암호화 통신 확인

로그인 페이지에서 중요정보가 암호화 없이 평문으로 서버에 전송된다.

|  |
| --- |
|  |

**취약점 대응방안**

* + 암호화 전송 시 프로토콜 설계의 결함이 있는 SSLv2, SSLv3, TLSv1.0, TLSv1.1은   
     비활성화가 필수이며, TLSv1.2 이상 사용을 권장한다.
  + httpd-ssl.conf의 SSL 관련 VirtualHost 설정에 아래를 추가한다.

|  |
| --- |
| SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1 |

* + 1. 쿠키 변조 (CC)

**취약점 개요**

* 쿠키 사용 여부 및 사용하는 경우 안전한 알고리즘으로 암호화 여부를 점검한다. 쿠키를 사용하는 경우 안전한 알고리즘으로 암호화하여 공격자가 쿠키 인젝션 등과 같은 쿠키 값 변조를 통한 다른 사용자로의 위장 및 권한 변경을 방지하고자 한다.
* 클라이언트에 전달되는 쿠키에 사용자 식별 값이 평문으로 노출될 경우 쿠키 변조를 통해 다른 사용자의 유효한 세션을 취득할 수 있으며, 기타 중요정보의 유출 및 변조가 가능하다.

|  |  |  |
| --- | --- | --- |
| **번호** | **URL** | **파라미터** |
| 1 | http://web-as-alb-1392225615.us-west-2.elb.amazonaws.com | Cookie |

**취약점 설명**

Step 1) 계정 로그인

본인 계정으로 로그인을 한다.

|  |
| --- |
|  |

Step 2) 쿠키 값 변조

본인의 쿠키 값을 다른 유저의 쿠키 값으로 변조한다.

|  |
| --- |
|  |

Step 3) 다른 유저로 로그인

본인의 정보가 다른 유저로 바뀐 것을 확인할 수 있다.

|  |
| --- |
|  |

**취약점 대응방안**

* 쿠키 대신 보안성이 강한 Server Side Session 방식을 사용한다.
* 쿠키(또는 Session)를 사용해서 중요정보나 인증을 구현해야 할 경우엔 안전한 알고리즘 (SEED, 3DES, AES 등)을 적용한다.
* HTTP 헤더에 아래와 같이 설정하여 세션 ID 값은 HTTPS를 통해서만 전송되도록   
  설정하고, 자바스크립트를 통해 세션 ID 값 등 쿠키 정보가 유출되지 않도록 보호한다.

|  |
| --- |
| Set-Cookie : secure, HttpOnly  Set-Cookie : domain=app.mysite.com |

1. CloudWatch
   1. 대시보드 생성

**Web | WAS**

|  |  |
| --- | --- |
|  | |
| **설명** | **CPU Utilization - AutoScaling 그룹별 대시보드**  서버의 전체 CPU 자원이 얼마나 사용되고 있는지 백분율로 나타내는 지표 |
|  | |
| **설명** | **HealthyHostCount - 대상 그룹별 대시보드**  로드 밸런서에 등록된 인스턴스 중 정상 상태를 만족하는 인스턴스의 개수를 나타내는 지표 |

|  |  |
| --- | --- |
|  | |
| **설명** | **StatusCheckFailed - AutoScaling 그룹별 대시보드**  AWS 환경에서 인스턴스의 시스템 검사 또는 상태 검사를 통과하지 못했는지 알려주는 지표 (0 : 통과, 1 : 실패) |

1. 참고 자료
   1. 일반적으로 불필요한 서비스

[참고 표 1]

|  |  |
| --- | --- |
| **서비스명** | **기능 및 설명** |
| Alerter | 네트워크상에서 사용자와 컴퓨터에 관리용 경고메시지를 전송하는 기능 |
| Automatic Updates | 중요한 윈도우 업데이트를 다운로드하고 설치할 수 있도록 하는  애플리케이션. 수동 패치를 적용하거나, MS패치 관리 서버로 패치를  일괄적으로 관 리하는 경우 불필요한 서비스 |
| Clipbook | 서버 내 Clipbook을 다른 클라이언트와 공유 |
| Computer Browser | 네트워크에 있는 모든 컴퓨터의 목록을 업데이트 하고 관리하는 기능 |
| Cryptographic Services | 윈도우 파일의 서명을 확인하는 카탈로그 데이터베이스 서비스를 총괄 |
| DHCP Client | IP 주소와 DNS 이름을 DHCP 서버에 등록하거나 DHCP 서버로부터 동적으로 IP주소를 가져오는 기능을 수행. 단독으로 시스템을 수행하며  고정IP를 사용하는 경우 불필요한 서비스 |
| Distributed Link Tracking Client, Server | 네트워크 도메인의 여러 컴퓨터나 일반컴퓨터에서 NTFS 파일간의  연결을 관리하는 도구. Active Directory가 구성되어 있지 않은 서버에서는 불필요한 서비스. |
| DNS Client | 컴퓨터에 대한 도메인 이름 시스템(DNS)이름을 확인하고 캐시에  보관하는 기능. DNS 서버가 아닌 시스템에서는 유명무실하나, IPSEC을  사용하는 경우 필요한 경우 있음 |
| Error reporting Service | 프로그램 오류가 시 응용프로그램의 오류를 MS에 보고한다는 내용을 표시하는 기능 |
| Human Interface Device Access | 키보드 또는 기타 멀티미디어 장치에 사전 정의된 버튼들을 사용하는 HID 장치들을 위한 서비스 |
| IMAPI CD-Burning COM Service | 서버에 CD-RW 또는 DVD-RW가 장착되어 보조 백업장치 역할을 하기  위해서 자체 레코딩 백업을 할 수 있음 |
| Messenger | 클라이언트와 서버 사이에 netsend 및 경고서비스 메시지를 전송하는 기능 |
| NetMeeting Remote Desktop Sharing | 윈도우9X 운영체제부터 인증된 사용자가 넷미팅을 사용해서 원격으로  컴퓨터에 접근할 수 있도록 하는 기능 |
| Portable Media Serial Number | 컴퓨터에 연결된 이동성 음악연주기(미디기기)의 등록번호를 복원하는  기능 |
| Print Spooler | 인쇄 과정에 있는 스풀링을 관리하는 서비스. 프린터가 있는 경우 필수  서비스이나, 프린터가 연결되지 않은 시스템에서는 불필요함 |
| Remote Registry | 원격 사용자가 이 컴퓨터에서 레지스트리 설정을 수정할 수 있도록  설정하는 애플리케이션 |
| Simple TCP/IP Services | Echo, Discard, Character Generator, Daytime, Quote of the Day 지원 |
| Wireless Zero Configuration | 802.11 어댑터에 대해 자동 구성을 공급하는 기본적인 도구 |

* 1. 감사 정책 권고 기준

[참고 표 2]

|  |  |  |  |
| --- | --- | --- | --- |
| **감사 정책** | **설정** | **고급 감사 정책** | **설정** |
| 개체 액세스 감사 | 감사 안 함 | - | 감사 안 함 |
| 계정 관리 감사 | 성공 | 사용자 계정 관리  컴퓨터 계정 관리  보안 그룹 관리 | 성공  성공  성공 |
| 계정 로그온 이벤트 감사 | 성공 | 자격 증명 유효성 검사  Kerberos 서비스 티켓 작업  Kerberos 인증서비스 | 성공  성공  성공 |
| 권한 사용 감사 | 감사 안 함 | - | 감사 안 함 |
| 디렉토리 서비스 액세스 감사 | 성공 | 디렉토리 서비스 액세스 | 성공 |
| 로그온 이벤트 감사 | 성공/실패 | 로그온  로그오프  계정 잠금  특수 로그온  네트워크 정책 서버 | 성공/실패  성공  성공  성공  성공, 실패 |
| 시스템 이벤트 감사 | 성공/실패 | 보안 상태 변경  시스템 무결성  기타 시스템 이벤트 | 성공  성공/실패  성공/실패 |
| 정책 변경 감사 | 성공 | 감사 정책 변경  인증 정책 변경 | 성공  성공 |
| 프로세스 추적 감사 | 감사 안 함 | - | 감사 안 함 |