|  |
| --- |
| **스터디 2조 OyesMall** |
| **시나리오 기반 모의침투 결과보고서** |

|  |  |  |
| --- | --- | --- |
|  | 팀명: |  |
|  | **팀장:** |  |
|  | **팀원:** |  |
|  |  |  |
|  |  |  |
|  |  |  |

**목차**

[1. 개요 8](#_Toc191024650)

[1.1. 모의해킹 정의 8](#_Toc191024651)

[1.2. 수행일정/수행내역 8](#_Toc191024652)

[1.3. 수행 대상 (수정필요) 8](#_Toc191024653)

[1.4. 수행 단계별 방법 9](#_Toc191024654)

[1.5. 점검 항목 9](#_Toc191024655)

[1.6. 점검 도구 (수정필요) 10](#_Toc191024656)

[2. 결과 요약 12](#_Toc191024657)

[2.1. 총평 12](#_Toc191024658)

[3. 상세 수행 내역 13](#_Toc191024659)

[3.1. 환경 구성 13](#_Toc191024660)

[3.2. 정보 수집 14](#_Toc191024661)

[3.3. 계정정보 추측 및 대입 15](#_Toc191024662)

[3.3.1. 취약한 패스워드 설정 여부 15](#_Toc191024663)

[3.3.2. 어플리케이션/장비 기본 패스워드 설정 여부 17](#_Toc191024664)

[3.4. 인증 우회 19](#_Toc191024665)

[3.4.1. 쿠키 재사용 (Replay Attack) 여부 19](#_Toc191024666)

[3.4.2. 클라이언트 인증 우회 여부 (Javascript 우회) 20](#_Toc191024667)

[3.5. XSS (CSRF) 취약점 22](#_Toc191024668)

[3.5.1. 악의적인 스크립트 필터링 여부 (POST 메소드) 22](#_Toc191024669)

[3.5.2. XST, TRACE 옵션 허용 여부 23](#_Toc191024670)

[3.6. 관리자 페이지 추측 24](#_Toc191024671)

[3.6.1. 페이지 내 관리자 페이지 링크 여부 24](#_Toc191024672)

[3.6.2. 관리자 페이지 접근 여부 25](#_Toc191024673)

[3.7. 페이지 내 중요 정보 노출 25](#_Toc191024674)

[3.7.1. 중요 개인정보 노출 여부 25](#_Toc191024675)

[3.7.2. 쿠키 값 내 중요정보 유출 여부 26](#_Toc191024676)

[3.7.3. 중요정보 평문 전송 26](#_Toc191024677)

[3.8. 불필요 파일 존재 27](#_Toc191024678)

[3.8.1. 불필요한 페이지 존재 여부 27](#_Toc191024679)

[3.9. 파일 다운로드 취약점 28](#_Toc191024680)

[3.9.1. 입력 값 검증 미흡으로 파일 다운로드 공격 여부 28](#_Toc191024681)

[3.10. 파일 업로드 취약점 29](#_Toc191024682)

[3.10.1. 입력 값 검증 미흡으로 파일 업로드 공격 여부 30](#_Toc191024683)

[3.11. SQL Injection 31](#_Toc191024684)

[3.11.1. SQL Injection 허용 여부 31](#_Toc191024685)

[3.12. 최신 취약점 미패치 34](#_Toc191024686)

[3.12.1. 보안에 취약한 오래된 어플리케이션 사용 여부 34](#_Toc191024687)

[3.13. 부적절한 서버 설정 34](#_Toc191024688)

[3.13.1. 서버 보안 설정 여부 35](#_Toc191024689)

[4. 취약점 대응방안 36](#_Toc191024690)

[4.1. 계정정보 추측 및 대입 36](#_Toc191024691)

[4.1.1. 취약점 개요 36](#_Toc191024692)

[4.1.2. 권고사항 36](#_Toc191024693)

[4.1.3. 대응방안 적용 예시 37](#_Toc191024694)

**그림 목차**

[그림 1‑1 모의해킹 수행 단계 9](#_Toc191024695)

[그림 3‑1 모의해킹 환경 13](#_Toc191024696)

[그림 3‑2 모의해킹 홈페이지 (OyesMall) 14](#_Toc191024697)

[그림 3‑3 Nikto를 통한 기본적인 스캔 15](#_Toc191024698)

[그림 3‑4 취약한 패스워드 회원가입 시도 16](#_Toc191024699)

[그림 3‑5 취약한 패스워드 회원가입 성공 16](#_Toc191024700)

[그림 3‑6 SQL Injection 취약점을 이용한 데이터베이스 조사 17](#_Toc191024701)

[그림 3‑7 서버에서 사용 중인 데이터베이스 목록 17](#_Toc191024702)

[그림 3‑8 SQL Injection 취약점을 이용한 oyesmall 테이블 조사 17](#_Toc191024703)

[그림 3‑9 데이터베이스 oyesmall의 테이블 목록 18](#_Toc191024704)

[그림 3‑10 SQL Injection 취약점을 이용한 admin\_tb의 데이터 조사 18](#_Toc191024705)

[그림 3‑11 데이터베이스 oyesmall의 테이블 admin\_tb의 데이터 18](#_Toc191024706)

[그림 3‑12 로그인 전 쿠키 19](#_Toc191024707)

[그림 3‑12 로그인 후 쿠키 20](#_Toc191024708)

[그림 3‑13 회원가입 페이지 응답 소스코드 165~187 20](#_Toc191024709)

[그림 3‑14 회원가입 페이지 응답 소스코드 189~214 21](#_Toc191024710)

[그림 3‑15 회원가입 페이지 응답 소스코드 216~240 21](#_Toc191024711)

[그림 3‑16 회원가입 페이지 응답 소스코드 248~261 22](#_Toc191024712)

[그림 3‑17 그림설명을 작성해주세요 23](#_Toc191024713)

[그림 3‑18 HTTP 메서드로 TRACE 사용 23](#_Toc191024714)

[그림 3‑19 관리자 페이지 링크 위치 24](#_Toc191024715)

[그림 3‑20 OyesMall 관리자 페이지 24](#_Toc191024716)

[그림 3‑21 sqlmap을 이용하여 테이블 정보 조회 25](#_Toc191024717)

[그림 3‑22 sqlmap 결과 25](#_Toc191024718)

[그림 3‑23 그림설명을 작성해주세요 26](#_Toc191024719)

[그림 3‑24 그림설명을 작성해주세요 26](#_Toc191024720)

[그림 3‑25 중요정보 평문 전송 27](#_Toc191024721)

[그림 3‑26 그림설명을 작성해주세요 28](#_Toc191024722)

[그림 3‑27 사용자가 업로드한 파일 28](#_Toc191024723)

[그림 3‑28 다운로드 시 입력 값 29](#_Toc191024724)

[그림 3‑29 시스템 파일 다운로드 시도 29](#_Toc191024725)

[그림 3‑30 시스템 파일 다운로드 성공 29](#_Toc191024726)

[그림 3‑31 악성 파일 업로드 시도 30](#_Toc191024727)

[그림 3‑32 업로드 시 입력 값 31](#_Toc191024728)

[그림 3‑33 파일 확장자 변경 31](#_Toc191024729)

[그림 3‑34 악성 파일 업로드 성공 31](#_Toc191024730)

[그림 3‑6 SQL Injection 취약점을 이용한 데이터베이스 조사 32](#_Toc191024731)

[그림 3‑7 서버에서 사용 중인 데이터베이스 목록 32](#_Toc191024732)

[그림 3‑8 SQL Injection 취약점을 이용한 oyesmall 테이블 조사 32](#_Toc191024733)

[그림 3‑9 데이터베이스 oyesmall의 테이블 목록 33](#_Toc191024734)

[그림 3‑10 SQL Injection 취약점을 이용한 admin\_tb의 데이터 조사 33](#_Toc191024735)

[그림 3‑11 데이터베이스 oyesmall의 테이블 admin\_tb의 데이터 33](#_Toc191024736)

[그림 3‑36 취약한 웹 서버 소프트웨어 사용 34](#_Toc191024737)

[그림 3‑37 서버 보안 설정 미흡 35](#_Toc191024738)

[그림 4‑1 계정정보 추측 및 대입 점검 방법 36](#_Toc191024739)

[그림 4‑2 계정정보 추측 및 대입 보안 설정 방법 37](#_Toc191024740)

[그림 4‑3 비밀번호 검증 스크립트 37](#_Toc191024741)

[그림 4‑4 입력 값 검증(거짓) 38](#_Toc191024742)

[그림 4‑5 입력 값 검증(참) 39](#_Toc191024743)

**표 목차**

[표 1‑1 모의해킹 진단 일정 8](#_Toc191024744)

[표 1‑2 모의해킹 수행 범위 8](#_Toc191024745)

[표 1‑3 수행 단계 설명 9](#_Toc191024746)

[표 1‑4 점검 항목 10](#_Toc191024747)

[표 1‑5 점검 도구 11](#_Toc191024748)

[표 2‑1 모의해킹 진단 내역 12](#_Toc191024749)

[표 3‑1 계정정보 추측 및 대입 점검 항목 15](#_Toc191024750)

[표 3‑2 인증 우회 점검 항목 19](#_Toc191024751)

[표 3‑3 XSS (CSRF) 취약점 점검 항목 22](#_Toc191024752)

[표 3‑4 관리자 페이지 추측 점검 항목 24](#_Toc191024753)

[표 3‑5 페이지내 중요 정보 노출 점검 항목 25](#_Toc191024754)

[표 3‑6 불필요 파일 존재 점검 항목 27](#_Toc191024755)

[표 3‑7 파일 다운로드 취약점 점검 항목 28](#_Toc191024756)

[표 3‑8 파일 업로드 취약점 점검 항목 30](#_Toc191024757)

[표 3‑9 SQL Injection 점검 항목 31](#_Toc191024758)

[표 3‑10 최신 취약점 미패치 점검 항목 34](#_Toc191024759)

[표 3‑11 부적절한 서버 설정 점검 항목 35](#_Toc191024760)

# 개요

## 모의해킹 정의

본 모의해킹 진단은 웹 서비스의 관련된 모든 정보 자산에 대해 취약점을 도출/분석 하여 대책을 수립하기 위한 것이다. 시나리오 기반으로 해커와 동일한 환경과 조건, 기술을 가지고 모의 침투를 실행하여 취약점을 발견하고, 발견된 취약점을 점검하여 사전 예방을 통한 보안 현황 확인과 대응 방안 확립을 목적으로 한다.

## 수행일정/수행내역

본 모의해킹은 2025년 02월 20일부터 ~ 2025년 02월 21일까지 2일간 진행이 되었다. Task 별 자세한 일정은 표 1‑1과 같다.

|  |  |
| --- | --- |
| 02월 20일(목) | 02월 21일(금) |
| 환경분석  모의해킹 수행 | 모의해킹 수행  보고서 작성 |

표 ‑ 모의해킹 진단 일정

## 수행 대상 (수정필요)

본 모의해킹은 아래 표 1‑2의 OyesMall 웹 서비스를 대상으로 점검을 진행했다.

|  |  |  |
| --- | --- | --- |
| 대상 도메인 | 대상 IP 정보 | 서비스 |
| http://210.95.67.235:8183/ | 210.95.67.235 | ASP 웹 서비스 |
|  |  |  |

표 ‑ 모의해킹 수행 범위

## 수행 단계별 방법

본 모의해킹은 단계별로 정보 수집부터 보고서 작성까지 아래 그림 1‑1의 과정을 통해 진행된다.



그림 ‑ 모의해킹 수행 단계

각 수행 단계별 요약 설명은 아래 표 1‑3과 같다.

|  |  |
| --- | --- |
| 수행 단계 | 설명 |
| 정보 수집 | 대상에 대한 서버/네트워크/서비스에 대한 불필요한 서비스 접근 가능성, 외부에서 파악할 수 있는 정보들을 수집하는 단계 |
| 취약점 분석 | 각 네트워크 구간별로 적합한 취약점 스캔 도구를 이용하여 발생할 수 있는 취약점에 대한 정보를 수집하는 단계 (단, 네트워크 장비/서비스에 장애를 유발할 수 있는 경우에는 제외) |
| 침투 테스트 | 취약점 정보 수집 및 분석 단계를 통해 획득한 정보를 기반으로 수동 점검하여 시스템 내부까지 침투할 수 있는지 시나리오 기반으로 접근하는 단계 |
| 실제 공격 | 취약점이 확인되었을 때 공격에 의한 시스템 보안 위협이 시스템 및 비지니스 측면에서 어느 정도의 영향을 미칠 수 있는지 분석하는 단계 |
| 보고서 작성 | 도출된 취약점에 대한 총평/영향도/상세분석/보안가이드가 포함된 보고서를 작성하는 단계 |

표 ‑ 수행 단계 설명

## 점검 항목

점검 항목은 OWASP TOP 10, SANS TOP 25, KISA 48대 취약점 항목 등을 기반으로 제작된 자사의 취약점 점검 방법론을 이용하여 진행된다.

|  |  |  |  |
| --- | --- | --- | --- |
| **순번** | **분류** | **코드** | **점검 항목** |
| 1 | 계정정보 추측 및 대입 | BP-001 | 취약한 패스워드 설정 여부 |
| BP-002 | 어플리케이션/장비 기본 패스워드 설정 여부 |
| 2 | 인증 우회 | BP-003 | 쿠키 재사용 (Replay Attack) 여부 |
| BP-004 | 중요페이지 세션/인증/접근 체크 여부 |
| BP-005 | 클라이언트 인증 우회 여부 (Javascript 우회) |
| 3 | 파라미터 조작 | BP-006 | URL 정보 내 파라미터 위/변조 여부 |
| BP-007 | 필드 값 조작에 따른 검증 여부 |
| 4 | XSS (CSRF) 취약점 | BP-008 | 악의적인 스크립트 필터링 여부 (POST 메소드) |
| BP-009 | URL 파라미터 필터링 여부 (GET 메소드) |
| BP-010 | XST, TRACE 옵션 허용 여부 |
| BP-011 | CSRF 취약점 허용 여부 |
| 5 | 에러 메시지 처리 | BP-012 | 에러 메시지를 통한 중요/불필요한 정보 유출 |
| 6 | 디렉터리 리스팅 취약점 | BP-013 | 디렉터리 리스팅 여부 |
| 7 | 관리자 페이지 추측 | BP-014 | 페이지 내 관리자 페이지 링크 여부 |
| BP-015 | 관리자 페이지 접근 여부 |
| 8 | 페이지내 중요 정보 노출 | BP-016 | 중요 개인정보 노출 여부 |
| BP-017 | 쿠키 값 내 중요정보 유출 여부 |
| BP-018 | 데이터베이스 관련 정보 유출 여부 |
| BP-019 | 중요정보 평문전송 |
| 9 | 불필요 파일 존재 | BP-020 | 불필요한 페이지 존재 여부 |
| BP-021 | 백업, 압축 등 불필요 파일 존재 여부 |
| BP-022 | 테스트 페이지, 데모 페이지 삭제 여부 |
| 10 | 파일 다운로드 취약점 | BP-023 | 입력 값 검증 미흡으로 파일 다운로드 공격 여부 |
| 11 | 파일 업로드 취약점 | BP-024 | 입력 값 검증 미흡으로 파일 업로드 공격 여부 |
| 12 | 부적절한 Include 취약점 | BP-025 | 부적절한 Include 허용 여부 |
| 13 | URL 강제 호출 | BP-026 | 비인가 페이지 강제 호출 여부 |
| 14 | SQL Injection | BP-027 | SQL Injection 허용 여부 |
| 15 | 최신 취약점 미패치 | BP-028 | 보안에 취약한 오래된 어플리케이션 사용 여부 |
| 16 | 부적절한 서버 설정 | BP-029 | 서버 보안 설정 여부 |
| 17 | 법적 요구사항 검토 | BP-030 | 개인정보보호법에 의한 적절성 여부 |

표 ‑ 점검 항목

## 점검 도구 (수정필요)

본 모의해킹을 수행하면서 사용된 도구는 아래 표 1‑5와 같다.

|  |  |  |
| --- | --- | --- |
| 도구 이름 | 용도 | 사이트 |
| Nmap | 취약점 분석 | http://nmap.org/ |
| DirBuster | 디렉터리 스캔 | http://sourceforge.net/projects/dirbuster/ |
| Nikto | 취약점 분석 | https://cirt.net/Nikto2 |
| BeEF | 침투 테스트 | http://BeEFproject.com/ |
| Wireshark | 네트워크 패킷 분석 | https://www.wireshark.org/ |
| SQLMap | SQL Injection 테스트 | www.sqlmap.org/ |
| BurpSuite | 프록시 | http://portswigger.net/Burp/ |
| Metasploit | 침투 테스트 | www.metasploit.com |
| Volatility | 메모리 분석 | http://www.volatilityfoundation.org/ |
| Nessus | 취약점 스캔 | http://www.tenable.com/products/nessus |
| Cain & Abel | 패스워드 크랙 | http://www.oxid.it/cain.html |
| SQLGate | 데이터베이스 원격 접속 | http://www.sqlgate.com/kr/ |
| Paros | 프록시 | http://sourceforge.net/projects/paros/ |

표 ‑ 점검 도구

# 결과 요약

## 총평

본 모의해킹 진단 결과 총 00개의 취약점이 발견되었다. 취약점은 영향도 평가 기준에 따라 High (H) : 53개, Medium (M) : 27개, Low (L) : 92개 총 172개의 취약점이 도출되었다. 주요 취약점은 아래 표 2‑1과 같다.

|  |  |  |
| --- | --- | --- |
| 취약점 | 요약 | 영향도 |
| 계정정보 추측 및 대입 | 단순한 패스워드 설정으로 계정정보 추측 가능 |  |
| 인증 우회 | CAMEL 웹 서비스는 세션 토큰을 영구적으로 사용하고 있으며, 쿠키 재사용 공격에 취약한 것으로 확인 |  |
| 파라미터 조작 | 해당 취약점은 발견되지 않음 | N / 0 |
| XSS 취약점 | 게시판 서비스에 악성 스크립트 삽입 및 다른 사용자 권한 획득이 가능하며, 바이러스 배포가 가능 |  |
| 에러 메시지 처리 | 해당 취약점은 발견되지 않음 | N / 0 |
| 디렉터리 리스팅 | 해당 취약점은 발견되지 않음 | N / 0 |
| 관리자 페이지 추측 | 메인 페이지내 관리자 로그인 페이지 링크 여부 확인 |  |
| 페이지내 중요 정보 노출 | 개인정보수정 페이지에 불필요한 중요 개인정보가 노출 |  |
| 불필요한 파일 존재 | 서비스 개발 이후에 불필요한 백업 파일 존재로 소스 파일 일부 노출 |  |
| 파일 다운로드 | 입력 경로를 체크하지 않는 파일 다운로드 스크립트를 이용하여 웹 사이트 주요 파일 다운로드 |  |
| 파일 업로드 | 벼룩시장 게시판에 별도의 검증 절차가 없이 웹셸 업로드 확인 |  |
| 부적절한 Include 취약점 | 해당 취약점은 발견되지 않음 | N / 0 |
| URL 강제 호출 | 해당 취약점은 발견되지 않음 | N / 0 |
| SQL Injection | 관리자 페이지, 상품관리, 게시판내 검색 페이지에서 SQL Injection 취약점 발견 |  |
| 최신 취약점 미패치 | 취약점 점검 도구인 네서스(Nessus)를 이용하여 점검한 결과 총 19개의 웹 취약점이 발견 |  |
| 부적절한 서버 설정 | 잘못된 서버 설정으로 인한 디렉토리 리스팅 등이 가능 |  |
| 법적 요구사항 검토 | 해당 취약점은 발견되지 않음 | N / 0 |

표 ‑ 모의해킹 진단 내역

# 상세 수행 내역

## 환경 구성

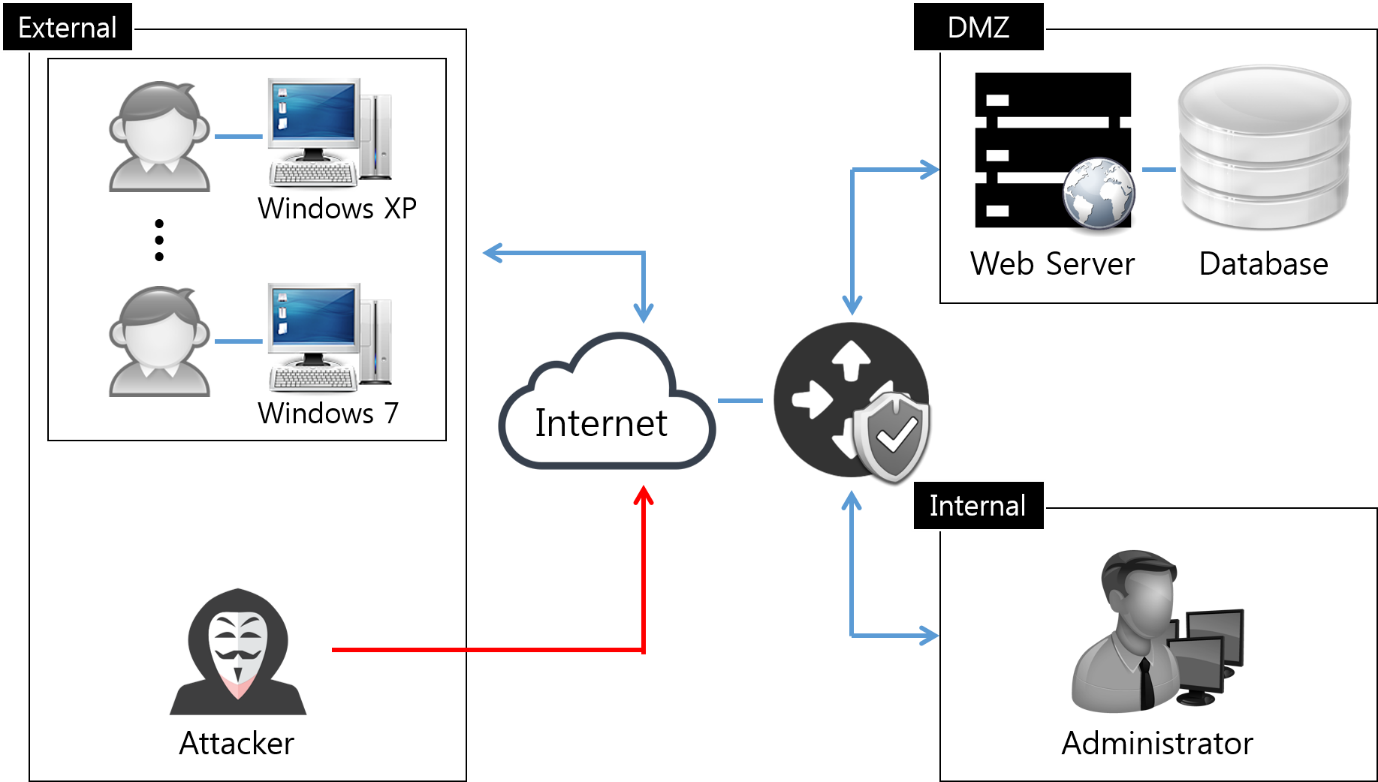


그림 ‑ 모의해킹 환경

위 그림 3‑1은 본 모의해킹 보고서의 환경 구성이다. 공격 대상서버는 ASP로 구성된 쇼핑몰이며, MSSQL을 사용한다. 공격자는 OyesMall ASP 쇼핑몰을 대상으로 다양한 시나리오 공격을 통해 모의해킹을 수행하며, 도출된 취약점을 바탕으로 대응 방안을 적용해본다.

* 환경은 시나리오 따라 달라질 수 있음

## 정보 수집

텍스트, 스크린샷, 소프트웨어, 웹 페이지이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 모의해킹 홈페이지 (OyesMall)

위 그림 3‑2는 시나리오 기반 모의해킹을 수행할 ASP로 구성된 OyesMall 쇼핑몰이다.

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

그림 ‑ Nikto를 통한 기본적인 스캔

위 그림 3‑3은 nikto는 웹 서비스 취약점을 자동 점검해주는 Perl로 작성된 오픈 소스 도구이다. nikto의 스캔 결과로 보안에 취약한 오래된 어플리케이션을 사용하고 있는 점, 보안 헤더가 설정되지 않은 점, HTTP에서 TRACE메서드가 사용 가능한 점을 발견했다.

## 계정정보 추측 및 대입

|  |  |  |
| --- | --- | --- |
| 분류 | 코드 | 점검 항목 |
| 계정정보  추측 및 대입 | BP-001 | 취약한 패스워드 설정 여부 |
| BP-002 | 어플리케이션/장비 기본 패스워드 설정 여부 |

표 ‑ 계정정보 추측 및 대입 점검 항목

### 취약한 패스워드 설정 여부

계정과 동일한 패스워드 생성 또는 단순 패스워드가 생성 가능하도록 웹 로직이 구현되어 있을 경우에 발생할 수 있는 취약점이다. 공격자가 무차별 대입 공격을 실행하면 사용자의 계정 및 패스워드가 노출될 수 있으며, 테스트 용도로 사용된 계정 또한 삭제되지 않을 경우 침해사고가 발생할 수 있다.

텍스트, 스크린샷, 번호, 폰트이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 취약한 패스워드 회원가입 시도

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 취약한 패스워드 회원가입 성공

위 그림 3‑4, 그림 3‑5를 보면 test 라는 취약한 패스워드를 넣어도 아무런 검증 없이 그냥 넘어간다. 사전에 있는 단어나 아이디에 포함된 단어 등 유추하기 쉬운 패스워드는 자동화된 툴을 사용하면 간단하게 찾을 수 있다.

### 어플리케이션/장비 기본 패스워드 설정 여부

초기 설치 시 제공하는 기본 계정과 패스워드를 그대로 사용할 경우 발생할 수 있는 취약점이다. 기본 패스워드는 자동 스캔 도구를 통해 쉽게 노출될 위험이 있으며, 공격자가 이를 악용하면 중요 정보가 탈취될 가능성이 높다.

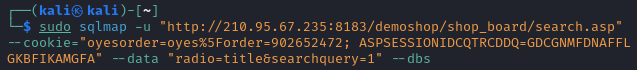


그림 ‑ SQL Injection 취약점을 이용한 데이터베이스 조사

텍스트, 스크린샷, 폰트, 디자인이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 서버에서 사용 중인 데이터베이스 목록

위 그림 3‑6, 그림 3‑7은 sqlmap을 활용하여 서버에서 사용 중인 데이터베이스 목록을 조회한 모습이다.

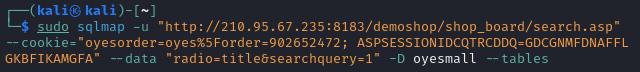


그림 ‑ SQL Injection 취약점을 이용한 oyesmall 테이블 조사

텍스트, 스크린샷, 메뉴, 폰트이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 데이터베이스 oyesmall의 테이블 목록

위 그림 3‑8, 그림 3‑9은 sqlmap을 이용해 데이터베이스 oyesmall 내 테이블 목록을 확인한 모습이다.

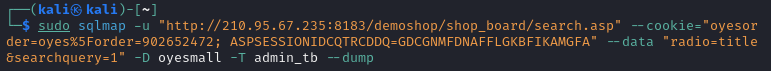


그림 ‑ SQL Injection 취약점을 이용한 admin\_tb의 데이터 조사

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 데이터베이스 oyesmall의 테이블 admin\_tb의 데이터

위 그림 3‑10, 그림 3‑11은 sqlmap을 사용하여 데이터베이스 oyesmall 내 테이블 admin\_tb의 데이터를 확인한 모습이다. 이를 통해 ID가 admin, PW가 admin인 관리자 계정 정보를 확인했다. SQL이 취약할 경우, 공격자가 SQL Injection 탐지 도구를 활용하면 정보가 쉽게 유출될 수 있다.

## 인증 우회

|  |  |  |
| --- | --- | --- |
| 분류 | 코드 | 점검 항목 |
| 인증 우회 | BP-003 | 쿠키 재사용 (Replay Attack) 여부 |
| BP-005 | 클라이언트 인증 우회 여부 (Javascript 우회) |

표 ‑ 인증 우회 점검 항목

### 쿠키 재사용 (Replay Attack) 여부

여러 세션에서 동일한 쿠키를 재사용할 수 있도록 웹 로직이 구현되어 있을 경우 발생할 수 있는 취약점이다. 공격자는 탈취한 쿠키를 활용해 사용자의 인증 세션을 이용할 수 있으며, 추가적인 인증 절차 없이 정상 사용자로 가장할 수 있다. 이로 인해 계정 탈취, 권한 상승, 민감한 정보 접근 등의 보안 사고가 발생할 위험이 크다.

텍스트, 폰트, 소프트웨어, 스크린샷이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 로그인 전 쿠키

텍스트, 소프트웨어, 웹 페이지, 웹사이트이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 로그인 후 쿠키

위 그림 3‑12, 그림 3‑13을 보면 F12 개발자 도구로 확인한 로그인 전, 후 쿠키가 동일하다. 이는 세션 관리가 적절하게 이루어지지 않았다는 의미이며, 보안 취약점을 초래할 수 있다.

### 클라이언트 인증 우회 여부 (Javascript 우회)

설명설명.

텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 회원가입 페이지 응답 소스코드 165~187

텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 회원가입 페이지 응답 소스코드 189~214

텍스트, 소프트웨어, 폰트, 스크린샷이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 회원가입 페이지 응답 소스코드 216~240

텍스트, 폰트, 번호, 스크린샷이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 회원가입 페이지 응답 소스코드 248~261

위 그림 3‑14, 그림 3‑15, 그림 3‑16, 그림 3‑17과 같이 OyesMall의 회원가입 페이지는 클라이언트 인증만 존재한다. Burp Suite를 이용해 회원가입 응답 페이지를 수정할 경우 클라이언트 인증을 우회하여 주소, 전화번호, 핸드폰번호, 직업, 이메일 필드를 인증 없이 회원가입이 가능하다.

## XSS (CSRF) 취약점

|  |  |  |
| --- | --- | --- |
| 분류 | 코드 | 점검 항목 |
| 인증 우회 | BP-008 | 악의적인 스크립트 필터링 여부 (POST 메소드) |
| BP-010 | XST, TRACE 옵션 허용 여부 |

표 ‑ XSS (CSRF) 취약점 점검 항목

### 악의적인 스크립트 필터링 여부 (POST 메소드)

사용자가 입력하는 데이터를 검증하지 않아 악의적인 스크립트가 포함된 입력값이 그대로 처리될 경우 발생할 수 있는 취약점이다. 공격자는 악성 스크립트를 삽입하여 사용자의 세션 탈취, 피싱, 권한 없는 요청 수행 등을 유도할 수 있다. 이를 악용하여 사용자의 개인 정보가 유출되거나, 관리자가 의도하지 않은 명령을 실행하게 되어 시스템에 장애를 일으킬 위험이 있다.

<그림을 삽입하려면 여기서부터

텍스트, 스크린샷, 폰트, 그래픽이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 그림설명을 작성해주세요

여기까지 복사해서 사용하세요>

### XST, TRACE 옵션 허용 여부

웹 서버에서 TRACE 메소드가 활성화되어 있어 XST(Cross-Site Tracing) 공격이 가능할 경우 발생할 수 있는 취약점이다. 공격자는 XSS과 결합하여 피해자의 브라우저에서 실행되는 악성 스크립트를 이용해 쿠키 값을 추출한다. 이를 통해 세션 하이재킹이나 CSRF 공격을 수행하여 계정 탈취, 정보 유출 등 보안 사고가 발생할 위험이 높아진다.

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

그림 ‑ HTTP 메서드로 TRACE 사용

위 그림 3‑19를 보면 HTTP 메서드로 TRACE가 사용되고 있다.

## 관리자 페이지 추측

|  |  |  |
| --- | --- | --- |
| 분류 | 코드 | 점검 항목 |
| 관리자 페이지  추측 | BP-014 | 페이지 내 관리자 페이지 링크 여부 |
| BP-015 | 관리자 페이지 접근 여부 |

표 ‑ 관리자 페이지 추측 점검 항목

### 페이지 내 관리자 페이지 링크 여부

관리자 페이지로 이동할 수 있는 링크가 일반 사용자 페이지에 노출되어 있을 경우 발생할 수 있는 취약점이다. 공격자가 별도의 인증 절차 없이 관리자 페이지에 접근이 가능하거나, 약한 인증 방식이 적용되면 쉽게 접속하여 중요 설정 변경 등의 보안 사고로 이어질 수 있다.

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 관리자 페이지 링크 위치

위 그림 3‑20를 보면 좌측 상단에 위치한 Red를 통해 관리자 페이지로 접근할 수 있다. 관리자 계정 정보는 3.3.2에서 획득했기 때문에 인증에 성공하여 관리자 페이지 내부로 접속할 수 있다.

스크린샷, 텍스트, 디자인이(가) 표시된 사진

자동 생성된 설명

그림 ‑ OyesMall 관리자 페이지

위 그림 3‑21은 Red를 통해 접근한 관리자 페이지 로그인 화면이다.

### 관리자 페이지 접근 여부

웹 어플리케이션에서 별도의 보안 조치 없이 관리자 페이지에 직접 접근할 수 있을 경우 발생할 수 있는 취약점이다. 공격자가 자동화된 스캔 도구를 활용하여 관리자 페이지를 통한 주요 정보 접근이 가능해진다.

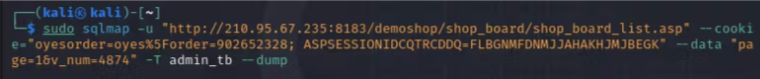


그림 ‑ sqlmap을 이용하여 테이블 정보 조회

텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

그림 ‑ sqlmap 결과

위 그림 3‑22, 그림 3‑23을 보면 관리자 ID, PW가 admin, admin인 것이 확인된다. 이렇게 취득한 계정 정보로 쉽게 관리자 페이지에 접속하여 관리자 권한을 획득할 수 있다.

## 페이지 내 중요 정보 노출

|  |  |  |
| --- | --- | --- |
| 분류 | 코드 | 점검 항목 |
| 페이지 내 중요  정보 노출 | BP-016 | 중요 개인정보 노출 여부 |
| BP-017 | 쿠키 값 내 중요정보 유출 여부 |
| BP-019 | 중요정보 평문 전송 |

표 ‑ 페이지내 중요 정보 노출 점검 항목

### 중요 개인정보 노출 여부

사용자의 개인정보가 암호화되지 않은 상태로 노출될 경우 발생할 수 있는 취약점이다. 공격자는 단순한 웹 크롤링이나 브라우저 개발자 도구를 이용해 노출된 개인정보를 쉽게 획득할 수 있으며, 이를 통해 피싱 공격, 금융 사기 등의 보안 사고로 이어질 가능성이 높다. 특히, 로그 파일이나 HTML 소스코드 내에 개인정보가 포함된 경우, 검색 엔진을 통해 무단으로 수집될 위험도 존재한다.

<그림을 삽입하려면 여기서부터

텍스트, 스크린샷, 폰트, 그래픽이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 그림설명을 작성해주세요

여기까지 복사해서 사용하세요>

### 쿠키 값 내 중요정보 유출 여부

쿠키 값에 민감한 정보(사용자 인증 토큰, 세션 ID 등)가 암호화되지 않은 채 저장되거나 전송될 경우 발생할 수 있는 취약점이다. 공격자가 네트워크를 가로채거나 XSS 공격을 통해 탈취한 쿠키 값으로 정보 유출, 계정 탈취 등이 발생할 수 있다.

<그림을 삽입하려면 여기서부터

텍스트, 스크린샷, 폰트, 그래픽이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 그림설명을 작성해주세요

여기까지 복사해서 사용하세요>

### 중요정보 평문 전송

중요한 정보가 암호화 없이 평문으로 전송될 경우 발생할 수 있는 취약점이다. 공격자는 중간자 공격을 통해 사용자의 로그인 정보, 결제 정보 등을 탈취할 수 있다. HTTPS 대신 HTTP를 사용하는 경우, 데이터가 암호화되지 않아서 네트워크를 통해 전송되는 동안 노출될 위험이 크다.

텍스트, 폰트, 스크린샷, 라인이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 중요정보 평문 전송

위 그림 3‑26은 로그인 요청 시 비밀번호 및 개인정보를 평문으로 전송하는 모습이다. 암호화 없이 그대로 전송되므로 중간자 공격에 취약하다. 민감한 정보 및 개인 정보는 암호화하여 전송하고, 데이터베이스 저장 시에도 해싱 또는 암호화 기법을 적용하는 것이 필요하다.

## 불필요 파일 존재

|  |  |  |
| --- | --- | --- |
| 분류 | 코드 | 점검 항목 |
| 불필요 파일  존재 | BP-020 | 불필요한 페이지 존재 여부 |

표 ‑ 불필요 파일 존재 점검 항목

### 불필요한 페이지 존재 여부

실제로 사용되지 않거나 불필요한 페이지가 남아 있을 경우 발생할 수 있는 취약점이다. 공격자는 이러한 페이지를 통해 내부 시스템의 구조나 설정 정보를 파악할 수 있으며, 미처 삭제되지 않은 테스트 페이지나 디버깅 도구를 통해 중요한 정보에 접근할 수 있게 된다.

<그림을 삽입하려면 여기서부터

텍스트, 스크린샷, 폰트, 그래픽이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 그림설명을 작성해주세요

여기까지 복사해서 사용하세요>

## 파일 다운로드 취약점

|  |  |  |
| --- | --- | --- |
| 분류 | 코드 | 점검 항목 |
| 파일 다운로드  취약점 | BP-023 | 입력 값 검증 미흡으로 파일 다운로드 공격 여부 |

표 ‑ 파일 다운로드 취약점 점검 항목

### 입력 값 검증 미흡으로 파일 다운로드 공격 여부

파일 다운로드 기능에서 입력 값에 대한 검증이 제대로 이루어지지 않을 경우 발생할 수 있는 취약점이다. 공격자가 서버에 저장된 시스템 관련 파일을 다운로드 받을 수 있다. 이로 인해 원격 코드 실행, 시스템 침해, 서버 손상 등의 피해가 발생할 수 있다.

텍스트, 폰트, 소프트웨어, 라인이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 사용자가 업로드한 파일

Burp Suite에서 Intercept on 상태로 위 그림 3‑28에 보이는 shell(1).cer 파일을 다운로드 시도한다.

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 다운로드 시 입력 값

Burp Suite에서 그림 3‑29과 같이 다운로드 시 입력값을 확인할 수 있다.

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 시스템 파일 다운로드 시도

시스템 파일 shop\_download.asp을 다운로드 받기 위하여 Burp Suite에서 입력값을 그림 3‑30처럼 변경한다.

텍스트, 라인, 폰트, 스크린샷이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 시스템 파일 다운로드 성공

Intercept off하면 그림 3‑31와 같이 시스템 파일이 다운로드된다.

## 파일 업로드 취약점

|  |  |  |
| --- | --- | --- |
| 분류 | 코드 | 점검 항목 |
| 파일 업로드  취약점 | BP-024 | 입력 값 검증 미흡으로 파일 업로드 공격 여부 |

표 ‑ 파일 업로드 취약점 점검 항목

### 입력 값 검증 미흡으로 파일 업로드 공격 여부

파일 업로드 기능에서 입력 값에 대한 검증이 제대로 이루어지지 않을 경우 발생할 수 있는 취약점이다. 공격자가 업로드할 파일의 형식이나 확장자를 조작하여 악성 파일을 업로드할 수 있다. 이후 이를 다운로드하고 실행시키면 원격 코드 실행, 시스템 침해, 서버 손상 등으로 이어질 수 있다.

텍스트, 스크린샷, 디스플레이, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 악성 파일 업로드 시도

위 그림 3‑32을 보면 악성 파일의 확장자를 업로드가 가능한 jpg로 변경하여 정상 파일로 위장했다. Burp Suite에서 Intercept on 상태로 Submit을 시도한다.

텍스트, 폰트, 스크린샷, 라인이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 업로드 시 입력 값

Burp Suite에서 그림 3‑33과 같이 업로드 시 입력값을 확인할 수 있다.

텍스트, 폰트, 스크린샷, 라인이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 파일 확장자 변경

Burp Suite에서 입력값을 그림 3‑34처럼 변경하여 정상파일로 위장한 악성 파일을 원래 확장자로 복구한다.

텍스트, 소프트웨어, 폰트, 아쿠아이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 악성 파일 업로드 성공

Intercept off하면 그림 3‑35와 같이 시스템 파일이 다운로드된다

## SQL Injection

|  |  |  |
| --- | --- | --- |
| 분류 | 코드 | 점검 항목 |
| SQL Injection | BP-027 | SQL Injection 허용 여부 |

표 ‑ SQL Injection 점검 항목

### SQL Injection 허용 여부

사용자가 입력한 값이 직접 SQL 쿼리문에 포함될 경우 발생할 수 있는 취약점이다. 공격자가 이를 조작하여 원래 의도된 커리 외의 다른 명령을 실행할 수 있다. 데이터베이스에서 민감한 정보를 탈취하거나, 데이터베이스의 내용을 변경하는 등의 피해가 발생할 가능성이 높다.

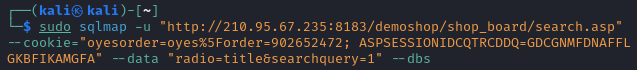


그림 ‑ SQL Injection 취약점을 이용한 데이터베이스 조사

텍스트, 스크린샷, 폰트, 디자인이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 서버에서 사용 중인 데이터베이스 목록

위 그림 3‑36, 그림 3‑37은 sqlmap을 활용하여 서버에서 사용 중인 데이터베이스 목록을 조회한 모습이다.

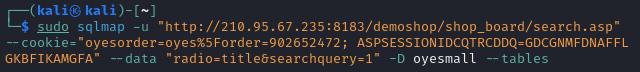


그림 ‑ SQL Injection 취약점을 이용한 oyesmall 테이블 조사

텍스트, 스크린샷, 메뉴, 폰트이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 데이터베이스 oyesmall의 테이블 목록

위 그림 3‑38, 그림 3‑39은 sqlmap을 이용해 데이터베이스 oyesmall 내 테이블 목록을 확인한 모습이다.

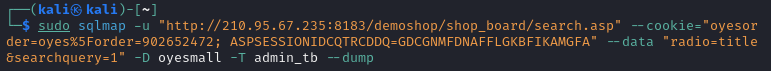


그림 ‑ SQL Injection 취약점을 이용한 admin\_tb의 데이터 조사

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 데이터베이스 oyesmall의 테이블 admin\_tb의 데이터

위 그림 3‑40, 그림 3‑41은 sqlmap을 사용하여 데이터베이스 oyesmall 내 테이블 admin\_tb의 데이터를 확인한 모습이다. 이를 통해 ID가 admin, PW가 admin인 관리자 계정 정보를 확인했다. SQL이 취약할 경우, 공격자가 SQL Injection 탐지 도구를 활용하면 정보가 쉽게 유출될 수 있다.

## 최신 취약점 미패치

|  |  |  |
| --- | --- | --- |
| 분류 | 코드 | 점검 항목 |
| 최신 취약점  미패치 | BP-028 | 보안에 취약한 오래된 어플리케이션 사용 여부 |

표 ‑ 최신 취약점 미패치 점검 항목

### 보안에 취약한 오래된 어플리케이션 사용 여부

오래된 어플리케이션이나 시스템에서 최신 보안 패치가 적용되지 않을 경우 발생할 수 있는 취약점이다. 보안 패치가 미적용된 시스템은 기존에 발견된 취약점들이 여전히 존재하기 때문에 공격자가 이를 활용할 수 있다.

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 취약한 웹 서버 소프트웨어 사용

위 그림 3‑42을 보면 보안에 취약한 Microsoft-IIS/6.0을 사용하고 있다. 지원이 종료되어 보안 업데이트가 제공되지 않기 때문에, 새로운 취약점이 발견되어도 패치가 불가능하다.

## 부적절한 서버 설정

|  |  |  |
| --- | --- | --- |
| 분류 | 코드 | 점검 항목 |
| 부적절한  서버 설정 | BP-029 | 서버 보안 설정 여부 |

표 ‑ 부적절한 서버 설정 점검 항목

### 서버 보안 설정 여부

서버 보안 설정이 약하거나 불필요한 서비스가 활성화되어 있는 경우 발생할 수 있는 취약점이다. 공격자가 서버에 대한 불법적인 접근을 시도하거나 시스템을 악용할 수 있다.

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

그림 ‑ 서버 보안 설정 미흡

위 그림 3‑43를 보면 X-Frame-Option 헤더와 X-Content-Type-Options 헤더가 설정되지 않았다. X-Frame-Option 헤더가 설정되지 않으면 iframe을 삽입하여 클릭재킹 공격이 가능해진다. X-Content-Type-Options 헤더가 설정되지 않으면 MIME 타입을 자동으로 결정하여 실행할 수 없어 XSS 공격이 가능해진다.

# 취약점 대응방안

취약점 대응방안은 안전행정부와 한국인터넷진흥원에서 발행한 주요정보통신기반시설 기술적 취약점 분석 평가 방법 상세가이드를 기반으로 작성했다. 대응방안은 상세 수행 내역에서 도출된 취약점과 순서는 동일하며, 관리적, 기술적, 물리적 그리고 소스코드 관점의 보안을 설명한다.

## 계정정보 추측 및 대입

### 취약점 개요

계정이나 패스워드, 암호화 키 등을 유추하기 위해 반복적으로 값을 입력하여 해당 값을 발견해 내는 취약점으로 유추가 용이한 계정 및 패스워드의 사용을 방지하기 위해 계정 및 패스워드 값의 적절성 및 복잡성을 검증하는 체크 로직을 구현해야 한다.

### 권고사항

* 점검 방법

인증 값에 단순 조합의 값을 삽입하여 정상적인 인증을 취득하는지 확인한다.

|  |
| --- |
| * 취약한 계정: admin, administrator, manager, guest, test, scott, tomcat, root, user, operator, anonymous 등 * 취약한 패스워드: Abcd, aaaa, 1234, 1111, test, password, public, blank 패스워드, ID와 동일한 패스워드 등 |

그림 ‑ 계정정보 추측 및 대입 점검 방법

* 보안 설정 방법

취약한 계정 및 패스워드를 삭제하고, 그림 4‑2와 같이 사용자가 취약한 계정이나 패스워드를 등록하지 못하도록 패스워드 규정이 반영된 체크 로직을 구현하여야 한다.

|  |
| --- |
| * 다음 각 목의 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성   + 영문 대문자(26개)   + 영문 소문자(26개)   + 숫자(10개)   + 특수문자(32개) * 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고 * 비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경 |

그림 ‑ 계정정보 추측 및 대입 보안 설정 방법

### 대응방안 적용 예시

자바스크립트를 이용하여 사용자가 입력한 패스워드를 검증하는 스크립트를 구현한다.

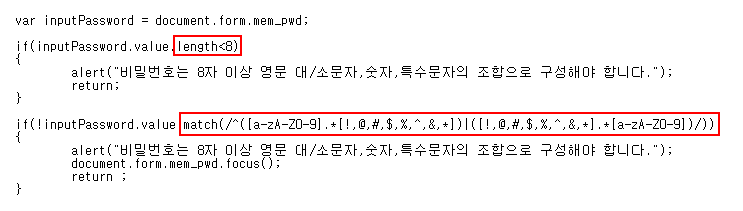


그림 ‑ 비밀번호 검증 스크립트

비밀번호 검증을 위해 먼저 비밀번호의 길이를 점검한다. 입력된 비밀번호가 8자 이하인 경우 경고 창을 출력하도록 하였다. 다음으로 입력된 값이 정해진 규칙에 맞추어 제대로 조합 되었는지 확인하기 위해 정규표현식을 이용하여 입력된 비밀번호를 검증하도록 하였다. 위 그림 4‑3에 포함된 정규표현식을 보면 입력 받은 값에는 영문 대문자, 영문 소문자, 숫자, 특수문자(!,@,#,$,%,^,&,\*)가 포함 되어야 한다. 여기에 조건문을 이용하여 입력된 값과 정규표현식을 비교하여 거짓이면 경고 메시지를 출력하도록 하였고, 참이라면 다음 단계로 넘어가도록 하였다.



그림 ‑ 입력 값 검증(거짓)

비밀번호 검증 스크립트가 제대로 구성되었는지 확인하기 위해 대상이 되었던 회원가입 페이지에 테스트를 진행하였다. 비밀번호 입력란에 영문 대문자, 소문자, 숫자, 특수문자를 포함하였고, 대신 7자리 까지만 입력하여 회원가입을 진행하였다. 위 그림 4‑4은 그 결과로 에러메시지가 출력되는 것을 확인할 수 있다.



그림 ‑ 입력 값 검증(참)

위에서 진행했던 것과 다르게 이번에는 비밀번호 값을 8자리 입력하여 회원가입을 시도 하였다. 위 그림 4‑5은 그 결과를 보여주고 있으며, 정상적으로 회원가입과 로그인이 진행된 것을 볼 수 있다.