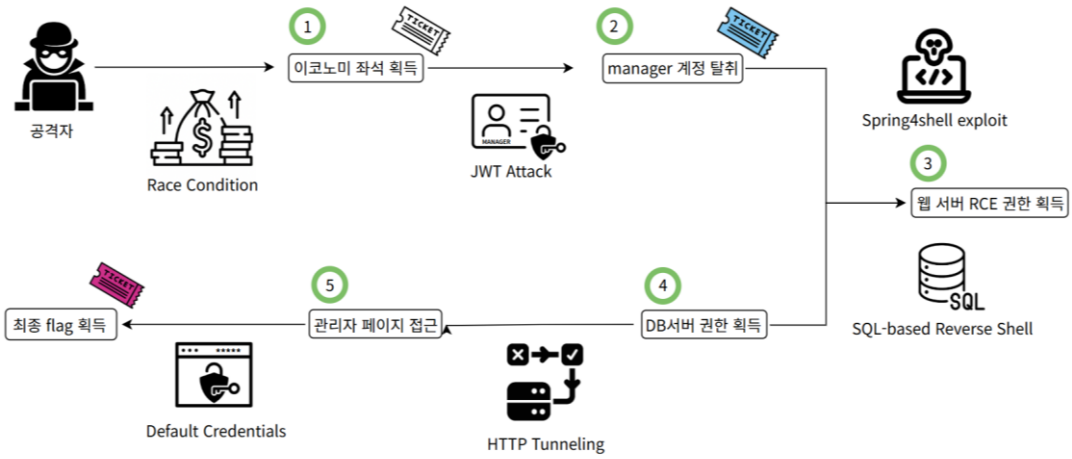
<붙임 2> 시나리오 제출양식

시나리오 제목
항공 예약 서비스 기반 최신 취약점 체이닝: 단계적 권한 상승과 Flag 탈취
시나리오 단계

1. 공격 흐름 요약



[그림 1] 시나리오 공격 흐름도

1. 일반 회원으로 회원가입하여 쿠폰을 획득한다.
2. Race Condition을 이용하여 이코노미 좌석을 예약한다.
3. JWT 우회로 매니저 페이지에 접근하여 비즈니스석으로 업그레이드한다.
4. Spring Boot 버전 확인 후 Spring4Shell 취약점을 이용해 Web 셸을 획득한다.
5. DB 계정 정보를 탈취한 후, 외부로 포트가 열려있는 DB에 접속한다.
6. 접속한 DB에서 RCE를 통해 공격자 PC와 DB 서버 간의 리버스 셸을 연결한다.
7. DB서버에서 공격자 PC와 HTTP 터널링을 수행하여 관리자 페이지에 접근한다.
8. 관리자 페이지에서 공격자의 티켓을 퍼스트석으로 업그레이드해 Flag를 획득한다.

2. 매핑된 MITRE ATT&CK for Enterprise

전술	기법	설명
Initial Access	T1078: Valid Accounts	일반 회원가입을 통해 기본 권한 획

		득
	T1190: Exploit Public-Facing Application	쿠폰 적용 API 호출을 조작해 Race Condition 발생
Privilege Escalation	T1606.003: Forge Web Credential	RS256 → HS256 알고리즘 변조, 공개키를 대칭키로 사용해 wh_manager 토큰 위조
Defense Evasion	T1649: Modify Authentication Process	변조 JWT로 기존 인증 절차를 우회하여 매니저 권한 획득
Execution	T1059.004: Command & Scripting Interpreter (Unix Shell)	(1) Spring4Shell RCE로 JSP 웹셸 생성 후 OS 명령 실행 (2) DB 서버에서 /bin/sh -i로 셸 권한 획득
Persistence	T1505.003: Server Software Component (Web Shell)	업로드된 JSP 웹셸을 통해 지속적 접근 확보
Command and Control	T1071.001: Application Layer Protocol (Web/HTTP)	4444 포트로 리버스 셸 연결, 원격 명령 채널 확보
Lateral Movement	T1210: Exploitation of Remote Services	PostgreSQL COPY ... TO PROGRAM으로 DB 서버에 리버스 셸 생성해 피벗
Impact	T1565.001: Data Manipulation (Stored Data)	관리자 페이지에서 예약 클래스를 퍼스트 클래스로 변경하고 Flag 획득

[표 1] 매핑된 MITRE ATT&CK for Enterprise

3. 단계적 권한 상승 구체화

1단계

단계 명: 일반 회원 가입 (Initial Access)

주요 목표: 합법적인 계정 발급을 통한 초기 접근 권한 획득

유형: 공격 – Initial Access (T1078 Valid Accounts)

주요 활동:

회원가입 페이지 접속

기본 포인트(100,000P)와 쿠폰(WELCOME90) 확보

주요 사용 도구 및 기술:

웹 브라우저, Burp Suite (요청 확인 용)

2단계

단계 명: Race Condition을 이용한 이코노미 좌석 예매

주요 목표: 결제 로직 우회 → 제한된 자산으로 이코노미 좌석 예약 확보

유형: 공격 – Exploit Public-Facing Application (T1190)

주요 활동:

쿠폰 API 중복 적용 (운임비 + 유류할증료)

Postman 등으로 동시 요청 전송

예약 API(POST /api/reservations/create) 호출

주요 사용 도구 및 기술:

Postman, 개발자 도구(F12), Burp Suite Repeater

3단계

단계 명: JWT 인증 우회 및 매니저 권한 탈취

주요 목표: wh_manager 계정 권한 탈취 → 관리자 페이지 접근

유형:

Privilege Escalation – Forge Web Credential (T1606.003)

Defense Evasion – Modify Authentication Process (T1649)

주요 활동:

JWT 토큰 알고리즘 RS256 → HS256 변조

jwks.json 공개키를 HMAC 키로 사용

sub: wh_manager 삽입 후 위조 토큰 생성

주요 사용 도구 및 기술:

JWT Decoder, Python PyJWT, Burp Suite (쿠키 삽입)

4단계

단계 명: Spring Boot 버전 확인 및 Spring4Shell 취약점 이용

주요 목표: 원격 코드 실행(RCE) → JSP 웹셸 업로드

유형: 공격 – Execution (T1059.004 Command & Scripting Interpreter)

주요 활동:

응답 헤더로 Spring Boot 2.6.5 확인

Spring4Shell 취약점(CVE-2022-22965) 익스플로잇
shell.jsp 업로드 및 명령 실행
주요 사용 도구 및 기술:
Spring4Shell POC 코드, Python Exploit Script

5단계
단계 명: DB 서버 접속
주요 목표: 환경 변수에서 DB 계정 정보 획득 → DB 서버 직접 접속
유형: 공격 – Execution (DB 접속 후 명령 실행)
주요 활동:
/etc/env 파일에서 DB 접속 정보 확인
nmap으로 포트 스캔 후 5432 포트 확인
psql 클라이언트로 DB 접속
주요 사용 도구 및 기술:
nmap, psql, Burp Suite

6단계
단계 명: DB 권한 악용 → 리버스 셸 획득
주요 목표: DB 서버에서 공격자 서버로 셸 연결
유형: 공격 – Lateral Movement (T1210 Exploitation of Remote Services)
주요 활동:
PostgreSQL COPY TO PROGRAM 기능 악용
Python one-liner 코드로 리버스 셸 생성
nc -lvnp 4444 대기 후 연결 확보
주요 사용 도구 및 기술:
netcat (nc), PostgreSQL COPY TO PROGRAM

7단계
단계 명: 내부망 관리자 서버 접근 (C2 & Pivoting)
주요 목표: DB 서버 → admin-server 내부망 우회 접속
유형:
Command & Control – Application Layer Protocol (T1071.001)
Lateral Movement – Internal Pivoting
주요 활동:
DB 서버에서 chisel 다운로드 및 실행
공격자 PC에 리버스 프록시 연결

Firefox 브라우저 + SOCKS5 프록시 설정

주요 사용 도구 및 기술:

chisel, SOCKS5 Proxy, Firefox

8단계

단계 번호: 8

단계 명: 관리자 페이지 접근 및 예약 변경

주요 목표: 좌석 등급을 비즈니스/퍼스트 클래스로 업그레이드

유형: 공격 – Impact (T1565.001 Data Manipulation)

주요 활동:

관리자 페이지 로그인 (admin/admin)

예약 관리 기능에서 공격자 좌석을 업그레이드

주요 사용 도구 및 기술:

브라우저, Burp Suite

9단계

단계 명: Flag 획득

주요 목표: 최종 목표 달성 – 관리자 페이지에서 Flag 획득

유형: 공격 – Impact (데이터 조작, 권한 남용)

주요 활동:

마이페이지 접속 → First Class 예약 내역 확인

Flag 획득 및 시나리오 종료

주요 사용 도구 및 기술:

브라우저

시나리오 목적

최신 취약점 체이닝을 통한 웹 보안 공격 이해도를 향상시키고, 내부망 침투·권한 상승 과정을 MITRE ATT&CK 기반으로 학습하여 실전 보안 사고 대응 역량을 습득한다.

시나리오 줄거리

1. 제안 배경

대다수의 웹 보안 실습 환경은 게시판, 로그인, 파일 업로드 등의 기능을 개별적으로 분리하고, 특정 취약점 하나를 학습하는 구조로 설계되어 있다. 이러한 환경은 단일 기술을 익히기에는 유용하지만, 현실의 복잡한 서비스 구조 혹은 연계 공격 흐름을 체감하기에는 한계가 있다. 특히 권한 상승, 인증 우회, 내부망 침투와 같이 여러 요소가 유기적으로 연결되는 과정은 단편적인 문제 풀이만으로 실전과 유사한 위협 흐름을 이해하고 대응하는 데 한계가 있다.

본 시나리오는 위와 같은 교육적 한계를 극복하고자, '항공권 예매'라는 현실적인 도메인을 기반으로 설계되었다. 결제, 인증, 예약, 관리자 기능 등 다양한 요소가 하나의 서비스 흐름 안에 통합되어 있다. 실습자는 단순히 개별 취약점을 찾는 것을 넘어, 실제 서비스 로직을 악용해 금전적 이득을 취하거나, 인증 구조를 우회하여 관리자 권한을 탈취하는 등 공격자의 관점에서 최종 목표를 달성하는 전 과정을 직접 체험하게 된다.

이러한 시나리오 기반 학습은 개별 기술의 숙련도를 넘어, 전략적 공격 경로를 설계하고 시스템의 허점을 파고드는 종합적인 보안 사고를 요구한다. 본 시나리오는 이를 통해 실습자가 현실의 복합적인 보안 위협을 이해하고, 단일 취약점 중심의 학습을 넘어선 시나리오 기반 실습의 필요성과 효과를 체감할 수 있도록 구성된 교육용 환경이다.

1. 시나리오 개요

본 시나리오는 항공권 예매라는 실제 서비스 환경을 기반으로, 일반 사용자 권한에서 내부망 관리자 권한까지 단계적으로 접근 권한을 확대해 나가는 침투 과정을 체험할 수 있도록 구성되었다.

공격자는 일반 회원으로 가입해 초기 포인트와 쿠폰을 지급받지만, 해당 자산만으로는 항공권을 확보할 수 없다. 이때 결제 로직의 허점을 이용해 하나의 쿠폰을 두 항목에 중복 적용하는 Race Condition을 유발하여, 제한된 자산으로 이코노미 좌석을 확보한다. 이어서 JWT 서명 알고리즘 우회 취약점을 악용해 관리자 권한으로 위조한 토큰을 생성하고, 이를 통해 관리자 페이지에 접근한다.

공격자는 해당 페이지의 응답 헤더에 노출된 Spring Boot 버전을 기반으로 Spring4Shell 취약점을 식별한다. 이후 웹셸을 업로드하여 시스템 내부 설정 파일에 접

근하고, DB 계정 정보를 획득한다. 이를 바탕으로 DB 서버에 접속하여 리버스 셸을 획득하고, 내부 설정 파일을 통해 admin 서버의 존재를 확인한다. 직접 접근이 차단된 환경이기 때문에, chisel을 활용해 리버스 터널링을 구성하고 브라우저를 통해 관리자 페이지에 접속한다. 최종적으로 공격자는 좌석 업그레이드 기능을 활용해 자신의 티켓을 퍼스트 클래스로 변경하고, 마이페이지에서 플래그를 확인하며 시나리오를 마무리한다.

2. 시나리오 컨셉

본 시나리오는 항공권 예약 서비스를 제공하는 가상의 항공사로, 실제 항공사 웹사이트와 유사한 기능을 갖춘 웹 애플리케이션을 운영한다. 본 시나리오는 해당 웹 페이지에 침투한다고 가정하여, 일련의 취약점 체이닝을 통해 최종적으로 내부망 관리자 서버를 장악하는 것을 최종 목표로 한다.

서비스는 항공편 검색, 예매, 예약 내역 확인 등 일반적인 항공사에서 제공하는 기능으로 구성되어 있다. 사용자의 권한은 일반회원, 관리자로 구분된다. 공격자는 일반회원부터 시작하여 이코노미 클래스 항공권을 확보한 뒤, 권한 상승 과정을 거쳐 내부망 관리자 권한을 획득하고, 자신의 좌석을 퍼스트 클래스 좌석으로 업그레이드하는 것을 목표로 한다.

시나리오 전반에 걸쳐 다양한 웹 취약점이 포함되어 있으며, 각 단계는 서비스 로직에 숨어 있는 보안 허점을 파악하고 이를 활용하는 방식으로 진행된다. 이를 통해 실습자는 실전 침투 흐름에서의 권한 상승 및 시스템 장악 과정을 종합적으로로 실습할 수 있다.

3. 시나리오 필요성

본 시나리오를 통해 실습자는 Race Condition, JWT 알고리즘 우회, Spring4Shell, 웹셸 업로드, 리버스 터널링 등 다양한 공격 기법을 체이닝함으로써, 단순한 기술 숙련을 넘어 실제 침투 시나리오를 설계하고 수행하는 역량을 기를 수 있다. 특히 도메인 특화 비즈니스 로직의 취약점부터 내부망 침투, 터널링 등 인프라 보안 요소까지 포함하고 있어, 개발·운영·보안 각 부서가 실제 서비스 운영 시 간과하기 쉬운 보안 지점을 통합적으로 학습할 수 있으며, 다음과 같은 실전 역량 향상에 기여한다.

3.1 실전 중심의 보안 교육을 위한 구성

단순한 취약점 나열이 아닌, 여러 취약점들의 체이닝을 통한 침투 과정을 보여준다. Race Condition → JWT 알고리즘 우회 → Spring4Shell → 웹셸 → 리버스 터널링으로 이어지는 다단계 체이닝 공격 흐름을 따라가며 실전 모의해킹 환경을 경험하도록 한다.

3.2 비즈니스 로직·인프라까지 아우르는 전방위 보안 감각 강화

항공권 결제, 쿠폰 처리와 같은 도메인 기반 로직부터, 웹 프레임워크 RCE 및 내부망 터널링에 이르는 계층별 보안 요소를 함께 다루어, 개발·운영·보안팀 모두 놓치기 쉬운 지점을 통합적으로 파악하도록 돕는다.

3.3 권한 상승과 접근 제어의 중요성 체험

일반 사용자 -> 관리자 -> 내부망으로 이어지는 권한 확장 시나리오를 통해, 잘못 설계된 인증·세션 권한 관리가 서비스 운영,고객 데이터에 미치는 영향을 보여줌으로써 권한 상승과 접근 제어의 중요성을 확인한다.

3.4 피해 시나리오로 리스크 인식 제고

쿠폰 악용으로 인한 수익 손실, 관리자 권한 탈취, 좌석 업그레이드까지 이어지는 연쇄적 비즈니스 피해를 단계별로 확인함으로써, 작은 보안안 취약점이 실제 비즈니스에 미치는 재무적·평판적 영향을 단계적으로 이해하게 된다.

4. 교육·훈련 효과

4.1 최신 IT 환경 및 취약점 반영

- **Spring4Shell(CVE-2022-22965)**, **JWT 알고리즘 혼동(Alg Confusion)**, **Race Condition** 등 최근 발생했던 주요 웹 취약점을 포함하여, 실습자가 **최신 공격 기법과 보안 트렌드**를 직접 경험할 수 있다.
- 단일 취약점 실습이 아닌 **다단계 체이닝 공격 흐름**(회원가입 → 쿠폰 중복 적용 → JWT 변조 → RCE → DB 리버스 셸 → 내부망 터널링 → Flag 획득)을 제공하여, 현실적인 공격 시나리오를 훈련할 수 있다.

4.2 내부망 침투 훈련 역량 강화

- 단순 웹 해킹을 넘어 **내부망 자원(DB 서버, 관리자 서버)에 대한 침투 과정**을 포함한다.
- **chisel 리버스 터널링**과 같은 실제 공격자가 사용하는 기법을 경험함으로써, 실습자는 **내부망 보호의 중요성**과 **방화벽·망분리 정책의 필요성**을 체감할 수 있다.
- 이는 단순 웹 취약점 대응에서 한 단계 확장된 **종합적인 사이버 공격·방어 사고 훈련**으로 이어진다.

4.3 MITRE ATT&CK 기반 보안 사고 대응 훈련

- 시나리오 전체가 **MITRE ATT&CK 매트릭스**에 맞춰 9단계로 매핑되어 있어, 실습자는 각 공격 행위가 어떤 전술·기법(Tactic/Technique)에 해당하는지 학습할 수 있다.
- 이를 통해 **공격자 시각**뿐만 아니라 **방어자 시각**에서 로그 분석, 이상 행위 탐지, 대응 포인트를 명확히 인식할 수 있다.
- 교육 후에는 참가자가 ATT&CK 프레임워크를 활용하여 **자사 시스템의 위협 모델링**을 수행할 수 있는 능력을 기를 수 있다.

4.4 실전 중심의 종합 보안 감각 배양

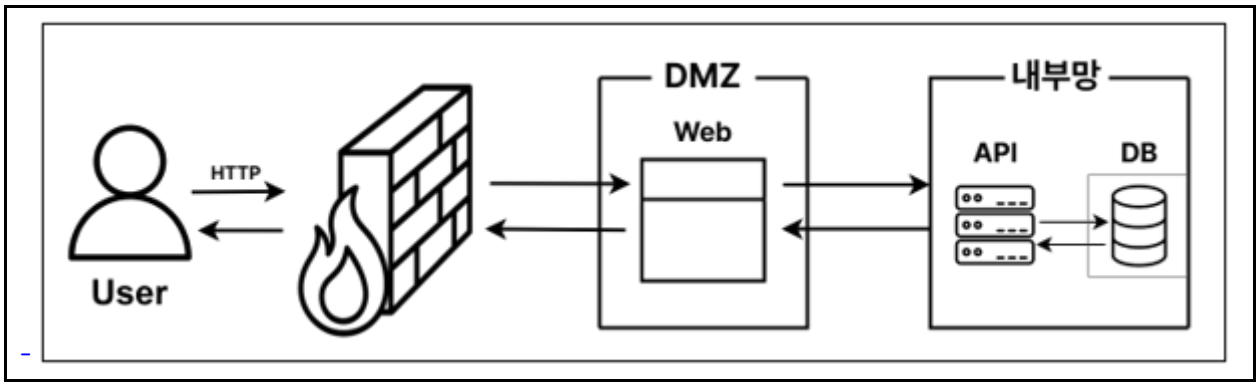
- **비즈니스 로직 취약점**(항공권 예매, 쿠폰 중복 적용)부터 **프레임워크 취약점**(Spring4Shell), **시스템 보안 취약점**(DB 권한 남용, 터널링)까지 다층적으로 다룸.
- 실습자는 공격자 관점에서 "작은 허점이 연쇄적으로 어떤 심각한 결과(좌석 업그레이드, 데이터 변조, Flag 탈취)로 이어지는지" 경험하게 되어, **리스크 분석 및 보안 사고 대응 사고력**을 키울 수 있다.

4.5 정보보호 인재 양성과 기업 연계 효과

- 시나리오를 통해 훈련된 참가자는 단순 취약점 분석 능력이 아니라 **체이닝 기반 공격 설계·탐지·대응 능력**을 갖추게 된다.
- 이는 기업이 요구하는 **실전 침투테스트 및 보안관제 능력**과 직접 연결되며, 대회 목적 중 하나인 **전문성과 역량을 갖춘 신규 인재 발굴**에 기여한다.
- 또한 사이버레인지 기반 교육 콘텐츠로 확장할 경우, **글로벌 수준의 모의훈련 환경**으로 발전시킬 수 있다.

결과적으로 해당 시나리오를 통해 실습자는 단순한 웹해킹 실습을 넘어, **Spring4Shell, JWT 알고리즘 혼동, Race Condition** 등 최신 취약점을 활용함으로써 **Real World 보안 위협에 대한 이해도**를 높일 수 있다. 또한, 내부망 침투와 권한 상승 과정을 단계적으로 체험하면서 **외부 → DMZ → 내부망**으로 이어지는 침투 경로를 실질적으로 경험하게 되고, 이를 통해 **망분리 환경의 중요성**과 **권한 관리 취약점의 심각성**을 체감할 수 있다. 아울러 시나리오 전 과정이 **MITRE ATT&CK 프레임워크**에 기반해 설계되어 있어, 실습자는 공격자의 행위를 체계적으로 분류하고 방어자의 관점에서 **탐지·대응 포인트를 식별**하는 역량을 함께 기를 수 있다. 따라서 본 시나리오는 최신 위협 반영, 내부망 침투 및 권한 상승 훈련, 공격·방어 양측면 사고 확장을 동시에 달성하는 효과적인 정보보호 교육·훈련 콘텐츠로 기능할 수 있다.

시나리오 네트워크 구성도



[그림1] 내부망 침투 시나리오 네트워크 구상도

단계 번호		1단계
단계 명		**일반 회원 가입**
주요 목표		- 합법적인 신규 계정을 생성하여 초기 접근 권한을 획득 - 실습용 자산(포인트, 쿠폰)을 확보해 이후 공격 발판을 마련
유형	공격	- 정찰(회원가입 경로 탐색) - 전달(입력 데이터 제출을 통한 계정 생성)
주요 활동		- 메인 → **회원가입** 이동, 필수 필드 유효성 검증 흐름 확인(클라이언트/서버) - 가입 직후 **세션 쿠키**·JWT 발급 여부 확인(DevTools → Application → Cookies / LocalStorage) - **마이페이지**에서 지급 자산 표시 로직, 잔액/쿠폰의 UI·API 일치 여부 점검 - (교육 포인트) 신규 계정 생성 시 **권한 기본값**(ROLE_USER 등)과 **비활성 플래그** 존재 여부 확인 **교육 효과** • 정상적인 사용자 행위를 가장한 공격자 초기 진입 방식을 이해 • "합법적인 계정"이 공격 시도에 어떻게 악용될 수 있는지 학습 • 계정 생성·세션 관리의 중요성(초기 권한 설계, 최소 권한 부여) 인식
주요 사용 도구 및 기술		- 웹 브라우저 (Chrome/Firefox) - Burp Suite (패킷 확인, 응답 검증)

예상 결과물 및 상태		- **산출물**: 신규 계정 정보(ID, PW, 세션 쿠키), 초기 자산(포인트·쿠폰) - **환경 변화**: DB users 테이블에 새로운 레코드 생성, 사용자 세션 발급 및 자산 초기화
단계 번호		**2단계**
단계 명		**Race Condition을 이용한 이코노미 좌석 예매**
주요 목표		- 쿠폰 적용 로직의 Race Condition을 악용해 정상적으로는 불가능한 예약 결제를 성사 - 제한된 자산으로 이코노미 좌석 예약 확보
유형	**공격**	- 취약점 악용(쿠폰 API 중복 적용) - 설치(예약 데이터 생성)
주요 활동		- 마이페이지에서 보유 자산 확인 (포인트·쿠폰) - 항공편 검색 후 이코노미 좌석 예약 시도 - 결제 API에서 targetPriceType 값을 조작하여 쿠폰을 유류할증료에도 중복 적용 - Postman/Burp로 중복 요청 전송 → 정상 결제 금액이 포인트만으로 충당되도록 유도 - 예약 API(/api/reservations/create) 호출 후 예약 확정 **교육 효과** • **Race Condition** 및 **비즈니스 로직 취약점**의 위험성 학습 • 프론트엔드·백엔드 불일치로 발생하는 **로직 기반 공격** 이해 • 보안 검증이 UI 단계에만 머무르면 발생하는 허점을 체감

주요 사용 도구 및 기술	- 웹 브라우저 개발자 도구(F12) - Postman / Burp Suite Repeater
예상 결과물 및 상태	- **산출물:** 예약 완료 내역(reservation_id, seat_class=economy), 결제 영수증 로그 - **환경 변화:** DB reservations 테이블에 이코노미 예약 추가, 서버 로그에 쿠폰 중복 적용 기록 저장
단계 번호	**3단계**
단계 명	**JWT 인증 우회 및 매니저 권한 탈취**
주요 목표	- JWT 토큰 알고리즘 혼동(Alg Confusion) 취약점을 악용해 매니저 권한 계정으로 변조제한된 자산으로 이코노미 좌석 예약 확보 - 관리자 페이지 접근 권한 획득
유형 **공격**	- 취약점 악용(취약점 악용(JWT Alg confusion)) - 권한 상승(매니저 계정 토큰 변조)
주요 활동	- JWT Decoder를 통해 기존 사용자 토큰 구조 확인 (alg=RS256) - /jwks.json 경로에서 공개키 획득 → PEM 포맷 변환 후 HMAC 키로 활용 - alg 필드를 HS256으로 위조 후, sub=wh_manager 삽입하여 새로운 토큰 생성 - 브라우저 쿠키에 위조 토큰 삽입 후 새로고침 → 관리자 권한 획득 **교육 효과** • **JWT 구조와 서명 검증 원리** 이해 • **Alg Confusion** 취약점의 실제 위험성과 권한 상승 메커니즘 학습 • 토큰 기반 인증 체계에서 **알고리즘 고정** 및 **키 관리**의

	필요성 인식
주요 사용 도구 및 기술	- Python PyJWT 라이브러리 - Burp Suite / JWT Decoder
예상 결과물 및 상태	- **산출물:** 변조된 JWT 토큰, 관리자 페이지 접근 세션 - **환경 변화:** 브라우저 UI에 관리자 메뉴 노출, 서버 로그에 비정상 서명 알고리즘 기록
단계 번호	**4단계**
단계 명	**Spring4Shell 취약점 이용**
주요 목표	- Spring4Shell(CVE-2022-22965) 취약점으로 원격 코드 실행(RCE) 달성 - JSP 웹셸 업로드 및 서버 제어권 확보
유형 **공격**	- 취약점 악용(Spring4Shell RCE) - 설치(웹셸 파일 생성)
주요 활동	- 응답 헤더를 통해 Spring Boot 2.6.5 버전 확인 (취약 버전) - 악성 파라미터 전달 → Tomcat 로그 패턴 변조 → JSP 웹셸 작성 - /webapps/ROOT/shell.jsp 생성 확인 후 명령 실행 - POC 파라미터로 **Tomcat AccessLog Pipeline** 속성 변조 - /webapps/ROOT/shell.jsp 생성 확인 → cmd 파라미터로 **OS 명령 실행** **교육 효과** • **프레임워크 취약점(RCE)**의 파급력을 실습 • 최신 공개 CVE(실제 사례)의 공격 과정을 단계별로 체험

	• 패치 미적용·버전 관리 미흡이 어떻게 **치명적 침투 경로**로 이어지는지 학습
주요 사용 도구 및 기술	- Spring4Shell Exploit 코드 (Python) - JSP 웹셸
예상 결과물 및 상태	- **산출물:** JSP 웹셸 파일, 웹셸 접근 URL - **환경 변화:** 서버 루트 디렉토리에 악성 파일 생성, 명령 실행 가능 백도어 확보
단계 번호	**5단계**
단계 명	**DB 서버 접속**
주요 목표	- 웹 서버 환경 변수에서 DB 접속 정보 획득 - 외부 포트(5432) 확인 후 DB 서버 접근
유형 **공격**	- 정찰(DB 포트 스캔) - 취약점 악용(DB 인증 정보 노출 활용)
주요 활동	- - 환경 변수 확인(DB_USER, DB_PASS, DB_HOST) - nmap으로 5432 포트 오픈 확인 - psql 클라이언트로 DB 접속 **교육 효과** • 애플리케이션 환경변수·설정 노출 시 **권한 전이** 가능성을 이해 • 네트워크 포트 스캐닝과 DB 접근을 통한 **서비스 확장 공격** 체험 • **비밀정보 관리(Secrets Management)** 의 중요성 학습

주요 사용 도구 및 기술	- nmap - psql 클라이언트
예상 결과물 및 상태	- **산출물:** DB 세션, 접속 로그 - **환경 변화:** DB 서버 외부 연결 세션 기록, SELECT/INSERT 가능
단계 번호	**6단계**
단계 명	**DB 권한 악용을 통한 리버스 셸 획득**
주요 목표	- PostgreSQL 기능(COPY TO PROGRAM)을 악용하여 DB 서버에서 리버스 셸 획득
유형 **공격**	- 취약점 악용(DB 권한 남용) - 명령 및 제어(Reverse Shell)
주요 활동	- 공격자 PC에서 nc 포트(4444) 대기 - DB 서버에서 COPY TO PROGRAM 구문 실행 → Python one-liner로 reverse shell 생성 - DB → 공격자 연결 세션 확보 **교육 효과** • DB 자체 기능(COPY TO PROGRAM 등)이 어떻게 OS 공격에 활용되는지 경험 • **권한 최소화 원칙(Least Privilege)** 적용 필요성 학습 • 공격자가 DB에서 직접 OS 명령을 실행하는 **피벗 단계**를 체험

주요 사용 도구 및 기술	- Netcat - PostgreSQL COPY TO PROGRAM
예상 결과물 및 상태	- **산출물:** DB 서버 리버스 셸, 실시간 명령 실행 로그 - **환경 변화:** DB 프로세스에서 외부 소켓 연결 생성, OS 명령 실행 권한 탈취
단계 번호	**7단계**
단계 명	**내부망 관리자 서버 접근 (Pivoting)**
주요 목표	- DB 서버에서 내부망 admin-server로의 터널링 확보 - 외부에서는 차단된 내부망을 공격자 브라우저로 접근 가능하게 함
유형 **공격**	- 명령 및 제어(리버스 터널링) - 이동(Pivoting)
주요 활동	- DB 서버에 chisel 다운로드 및 실행 - 공격자 PC의 chisel 서버와 연결 - Firefox + SOCKS5 프록시로 내부망 admin-server 접속 **교육 효과** • **리버스 터널링**과 **프록시 기법**을 통한 내부망 우회 학습 • "외부 차단된 자원도 DB/중간 서버를 거쳐 우회 가능하다"는 현실적 공격 이해 • 망분리·Egress 필터링·네트워크 모니터링의 필요성 학습
주요 사용 도구 및 기술	- chisel (리버스 터널링 도구) - SOCKS5 Proxy

예상 결과물 및 상태	- **산출물:** chisel 실행 로그, 프록시 연결 성공 - **환경 변화:** DB ↔ 공격자 PC 간 터널 구축, 내부망 서비스 접근 가능
단계 번호	**8단계**
단계 명	**관리자 페이지 접근 및 예약 변경**
주요 목표	- 관리자 계정으로 로그인 - 예약 관리 기능 악용 → 좌석 등급 상향(퍼스트 클래스)
유형 **공격**	- 목표 달성(데이터 변조)
주요 활동	- admin/admin 계정으로 로그인 - 예약 관리 메뉴에서 공격자 좌석 업그레이드 - DB 변경 내역 확인 **교육 효과** • 관리자 계정 탈취 후 발생할 수 있는 **데이터 변조 공격** 체험 • **관리자 권한 보호**(2인 승인, 로그 모니터링 등) 필요성 학습 • 실제 비즈니스 데이터(예약 내역)가 변조되는 시나리오를 통해 **사고 영향도 분석 능력** 향상
주요 사용 도구 및 기술	- 웹 브라우저 - Burp Suite
예상 결과물 및 상태	- **산출물:** 관리자 세션, 좌석 업그레이드된 예약 기록 - **환경 변화:** DB reservations 테이블 수정, 관리자 UI 반영, 변경 로그 기록

단계 번호		9단계
단계 명		**Flag 획득**
주요 목표		- 최종 목표인 Flag 값 확보
유형	공격	- 목표 달성(Flag 획득)
주요 활동		- 마이페이지 접속 → 업그레이드된 좌석과 함께 Flag 출력 확인 - 스크린샷 확보 **교육 효과** • 전체 체이닝을 통한 **종합 공격 시나리오 완주 경험** • 공격자가 **최종 목표 달성(Impact)**까지 이어지는 흐름을 직관적으로 이해 • 사고 대응 시 **단일 취약점 차단**만으로는 부족하고, **연쇄적 방어 전략**이 필요하다는 교훈 습득
주요 사용 도구 및 기술		- 웹 브라우저
예상 결과물 및 상태		- **산출물:** Flag 값(FLAG{...}), 스크린샷 - **환경 변화:** UI에 Flag 표시, 훈련 종료 조건 달성