
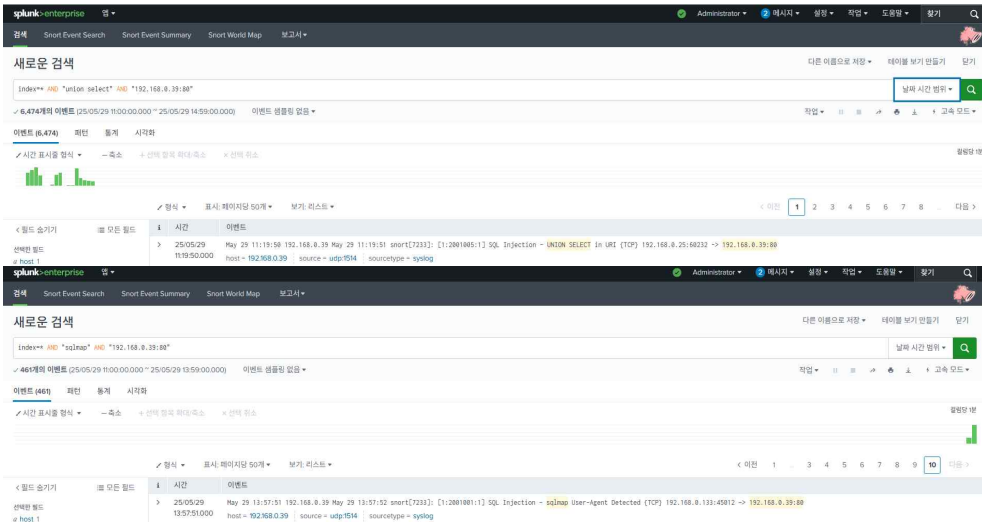


SQL Injection 침해사고 대응보고서

탐지 일시	<table><tr><td>구분</td><td>SQLMap</td><td>Union Select</td></tr><tr><td>일시</td><td>2025. 5.29(금) 13:59</td><td>2025. 5.29(금) 11:19</td></tr></table>	구분	SQLMap	Union Select	일시	2025. 5.29(금) 13:59	2025. 5.29(금) 11:19									
구분	SQLMap	Union Select														
일시	2025. 5.29(금) 13:59	2025. 5.29(금) 11:19														
공격 유형	SQL Injection(SQLMap Tool, Union Select 공격)															
탐지 장비	pfSense(IPS), Splunk <div></div>															
근무자 / 연락처	소속: 보안관제팀 직급: 선임 이름: 이정빈 연락처: 010-1234-5678															
공격자 정보	<table><tr><td>구분</td><td>IP</td><td>Port</td><td>국적</td><td>공격유형</td></tr><tr><td>내용</td><td>192.168.0.133</td><td>3000</td><td>대한민국</td><td>SQLMap</td></tr><tr><td></td><td>192.168.0.41</td><td>80</td><td>대한민국</td><td>Union Select</td></tr></table>	구분	IP	Port	국적	공격유형	내용	192.168.0.133	3000	대한민국	SQLMap		192.168.0.41	80	대한민국	Union Select
구분	IP	Port	국적	공격유형												
내용	192.168.0.133	3000	대한민국	SQLMap												
	192.168.0.41	80	대한민국	Union Select												
목적지 정보	192.168.0.39:80(문치시스템) <div></div>															
RawData	SQLMap RawData GET /rest/products/search?q=test%25%27%20AND%20SUBSTR%28%28SELECT%20COALESCE%28createdAt%2CCHAR%2832%29%29%20FROM%20Wallets%20LIMIT%200%2C1%29%2C27%2C1%29%3ECHAR%2867%29%20AND%20%27Twtw%25%27%3D%27Twtw HTTP/1.1 Cache-Control: no-cache User-Agent: sqlmap/1.9.2#stable (https://sqlmap.org)															

	<p>Referer: http://192.168.0.39:3000/rest/products/search Host: 192.168.0.39:3000 Accept: */* Accept-Encoding: gzip,deflate Connection: close HTTP/1.1 200 OK Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN Feature-Policy: payment 'self' X-Recruiting: /#/jobs Content-Type: application/json; charset=utf-8 Content-Length: 30 ETag: W/"1e-JkPcl+pGj7BBTxOuZTVVIm91zaY" Vary: Accept-Encoding Date: Thu, 29 May 2025 02:21:04 GMT Connection: close</p> <p>{"status":"success","data":[]}</p> <p>Union Select RawData</p> <p>GET /rest/products/search?q= %27))%20union%20select%20id,email,password,4,5,6,7,8,9%20from%20users-- HTTP/1.1 Host: 192.168.0.39:3000 Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36 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 Accept-Encoding: gzip, deflate Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 Cookie: language=en: PHPSESSID=fa17404001c2b0abc7830218466d6396 If-None-Match: W/"1219-rO7d1Av5Kp/7uXwmF+3QGsWOOQU"</p>
대응 방법	<ul style="list-style-type: none">- 탐지된 공격자IP[192.168.0.133(sqlmap), 192.168.0.41(union select)]를 pfSense 방화벽을 통해 차단 조치함- Snort 룰을 확인하여 탐지 룰이 정상적으로 작동하는지 검토

	<ul style="list-style-type: none"> - 공격 시점에 유출된 정보 또는 이상 행위가 없는지 내부 확인 진행 - 웹 애플리케이션 검색 기능의 입력값에 대한 필터링 정책 적용 또는 보완중임 - 사건 내용을 내부 보안팀에 공유하고, 필요 시 CERT와 연계 대응을 검토함
확인 및 조치 사항	<p>공격에 대한 이기종 보안장비 로그 확인 및 캡처 후 보안관제센터에 회신(이메일)</p> <p>공격 확인 후 침해사고로 판단 시 해당 시스템은 즉시 네트워크와 절체 및 침해분석 인력이 현장에 도착 시까지 타 인원 접근 금지</p> <p>공격에 대한 문의사항은 보안관제센터 유선 (02-0000-0000) 또는 이메일로 연락</p>

시스템 관리자 조치 결과

- 공격자 IP [192.168.0.133 (sqlmap), 192.168.0.41 (union select)]에 대해 pfSense 방화벽에 차단 정책을 등록함
- Snort 탐지 로그(alert.log)를 통해 SQL Injection 공격을 식별하고, 탐지를 위한 커스텀 룰을 적용함
- 공격 시점 로그 분석 결과, 일부 테이블 구조 및 데이터가 외부로 출력된 정황이 확인됨
- 본 실습 환경에서는 DB 계정 권한 조정이 제한되어 있으나, 실제 운영 환경에서는 유사한 공격 발생 시 계정 비밀번호 변경 및 최소 권한 적용 등의 즉각적인 대응이 필요함.
- 아래는 pfSense 방화벽에서 차단 정책이 실제로 적용되고 기록된 로그

1. pfSense 방화벽 로그를 통해 **차단된 IP(192.168.0.133, 192.168.0.41)**로부터 반복적인 접속 시도가 있었으며, 해당 트래픽이 정상적으로 차단되었음을 확인(Reject 적용)

Firewall / Rules / WAN

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Floating WAN LAN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/0 B	IPv4 TCP	192.168.0.41	*	*	*	*	none	Rejected IP manually	
<input type="checkbox"/>	0/0 B	IPv4 TCP	192.168.0.133	*	*	*	*	none	Rejected IP manually	

2. 차단 룰이 실효성 있게 작동함을 로그로 입증할 수 있었음(Reject 방식)

Last 500 Firewall Log Entries. (Maximum 500)

Action	Time	Interface	Rule	Source	Destination	Protocol
	Jun 2 11:23:45	WAN	Rejected IP manually (1748829297)	192.168.0.133:47650	192.168.10.100:80	TCP:S