[주식회사 닦다] 방어보고서

실전 웹서버 해킹과 대응 2조

조

2022. 06. 22

< 목 차 >

I. 개요

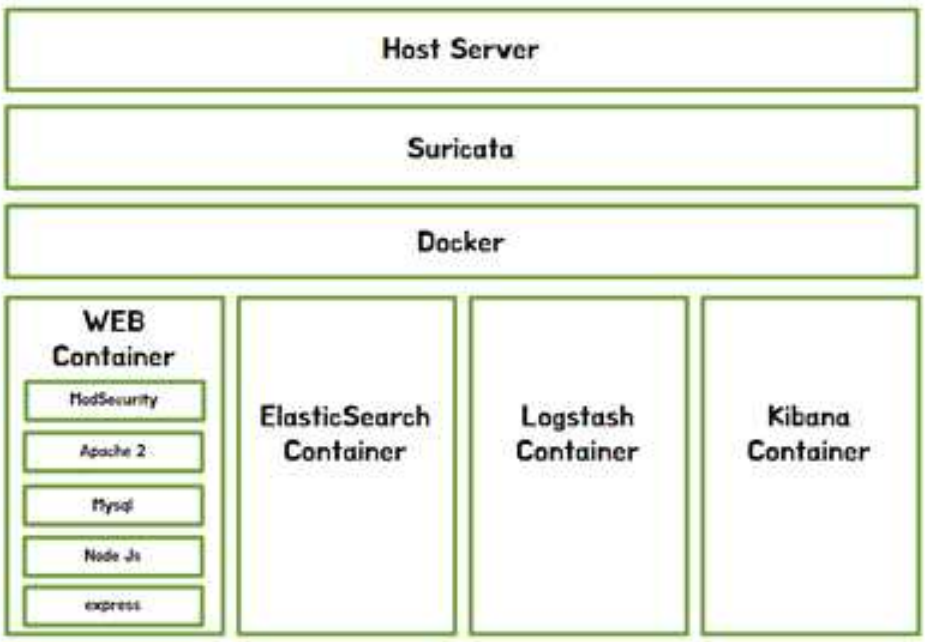
1. 방어•관제 개요

❍ 목 적

– 주식회사 닦다에서 운영 중인 웹 서비스에 클라우드를 이용하여 관제 시스템을 구성하였음. 서비스 안전성을 점검하기 위하여 웹 취약점 진단을 진행함. 해당 과정에서 정상적으로 시스템이 작동하는지와 로그 수집 및 비정상적 행위 탐지가 가능한지 확인함에 목적이 있음.

❍ 시스템 개요

– 상단에 1)HOST Server를 구성하고 밑에 2)침입 탐지와 방지를 위해 오픈소스 IDPS인 Suricata를 구축하였음. 서비스 안정성을 위해 3)Docker Container를 이용하여 웹 서비스와 관제 시스템을 분리 구축하였음. 4-1)Web Container에는 ModSecurity와 Apache, Mysql, Node js, express와 웹 서비스에 동작하는 서비스를 구축함. 관제 시스템은 4-2)ElasticSearch, LogStash, Kibana Container로 분리시켜 연동함. 이렇게 Container를 이용하여 분리함으로서 서비스 장애 발생 시 가용성을 보장받을 수 있음 동시에 Devops가 가능한 효과가 있음.



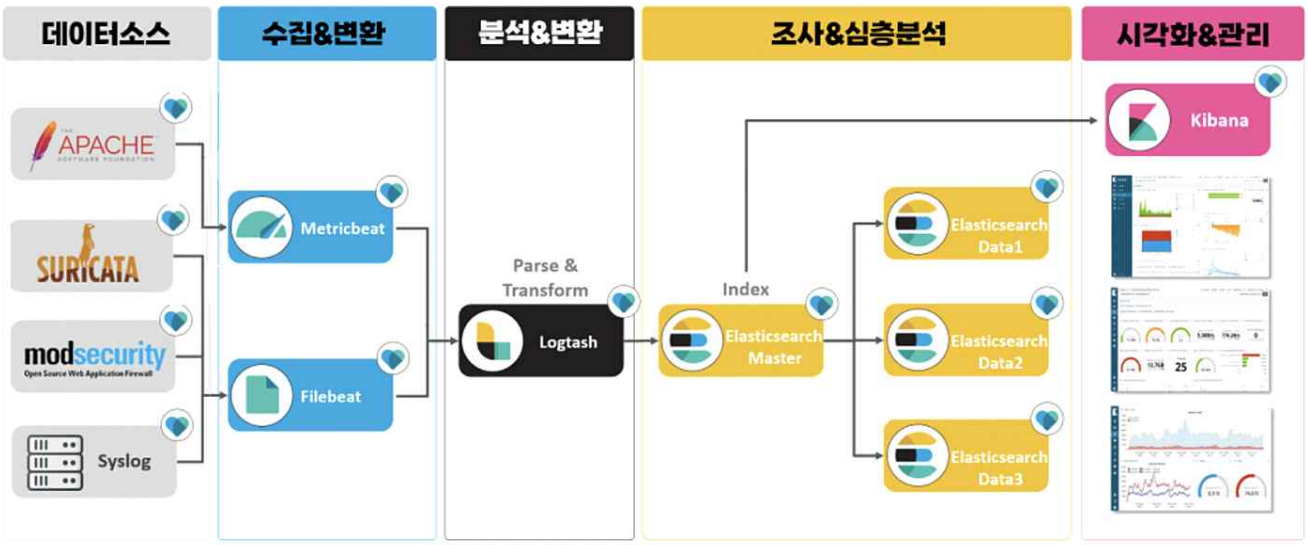
2. 서비스 구축 환경

대상	설명	환경
Apache 2	Web Application Server	Version: 2.4.46 Built: 2022-04-12T19:46:16
Mysql	Web Database	Version: 8.0.25
Nodejs	Web Framework	NPM Version: 6.2.0 Cookie-paser Version: 1.4.6 Doteny Version: 16.0.0 Ejs Version: 3.1.6 Nodemailer Version 6.7.3
express	Web Framework	Version: 4.17.3 express-fileupload Version: 1.3.1 express-session Version: 1.17.2

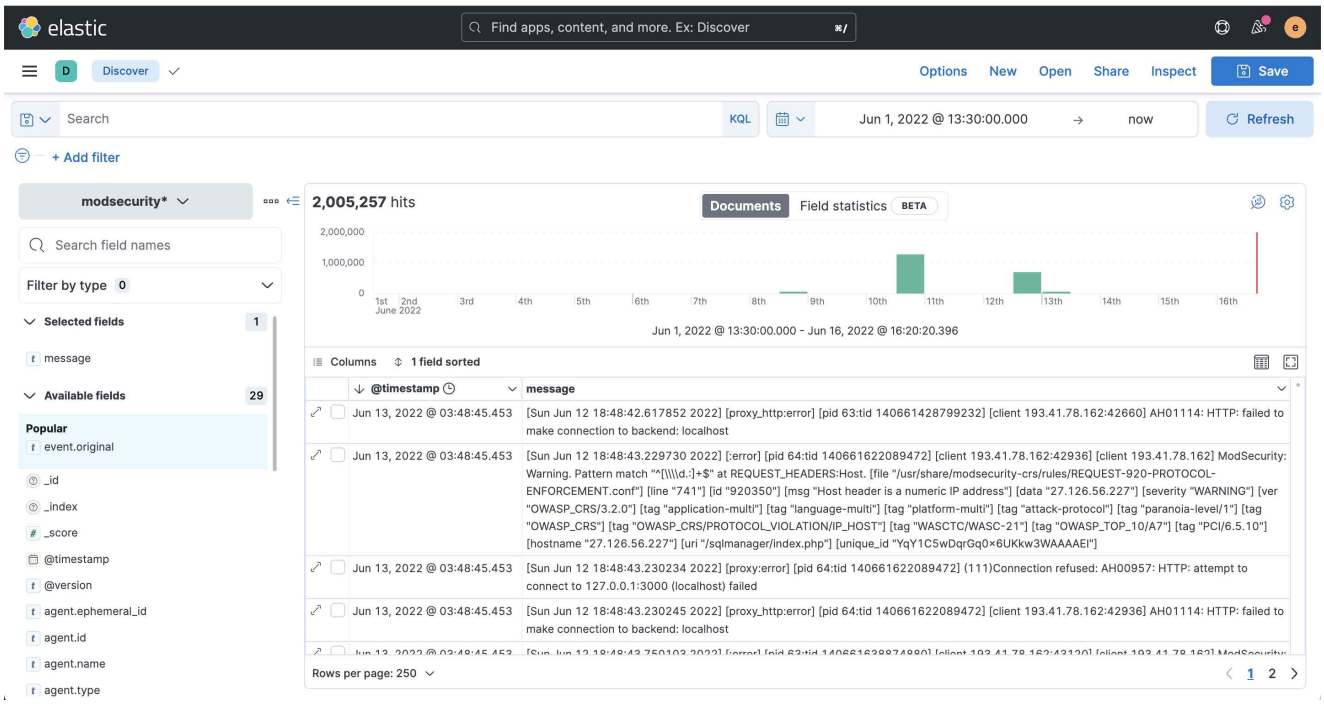
대상	설명	환경
Host Server	호스트 서버	Ubuntu 18.04.1 LTS
Docker	가상화 컨테이너	Version: 20.10.1 Built: Fri Apr 9 22:44:13 2021 OS/Arch: linux/amd64 Experimental: false
Elasticsearch	로그 수집 검색 엔진	Version: 7.10.2 Jvm memory Assignment: 2Gb Port (Inbound:Outbound) - 9200:9200 - 9300:9300
Logstash	로그 수집 및 파싱 엔진	Version: 7.10.2 Jvm memory Assignment: 1Gb Port (Inbound:Outbound) - 5044:5044 - 5000:5000 - 9600:9600
Kibana	로그 분석 및 시각화 플랫폼	Version: 7.10.2 Max payload (M/b): 50 Port (Inbound:Outbound) - 8080:5601
Suricata	네트워크 방화벽	Version: 7.5.0 Ruleset: Emerging threat snort rules Mode: IDS
Modsecurity	웹 방화벽	Version: 3.0.6 Ruleset: OWASP ModSecurity Core Rule Set (CRS) Mode: IDS

3. 관제 시스템 구성도

❍ 구성도



❍ 관제 시스템



II. 탐지 및 로그 분석

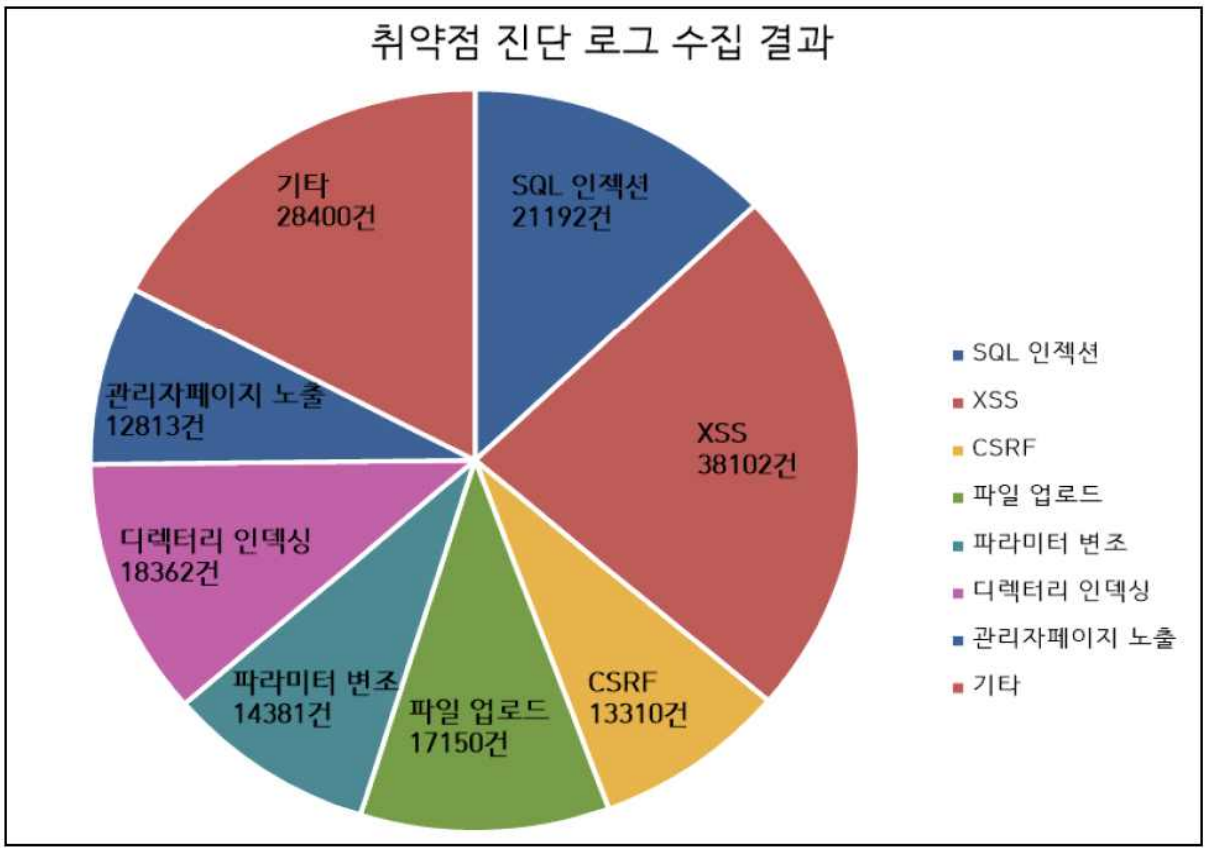
1. 로그 통계

❍ 개요

– 2022년 5월23일 ~ 6월15일 기간동안 진행한 웹 취약점 진단 관제 로그임. 전체 로그는 596,626건이며 비정상 행위로 판단되어 공격 탐지로 판단한 로그는 163,710건임.

– 공격 유형으로 분류 하였을 때 XSS 공격은 38,102건, SQL 인젝션 공격 21,192건, 디렉터리 인덱싱 18,362건, 파일업로드 17,150건, 파라미터 변조 14,381건 외에 파일업로드, CSRF, 관리자 페이지 노출이 있음.

– 공격 탐지 기준의 경우 방화벽에 적용된 룰셋이며, 공격 유형 분류는 룰셋의 이벤트 로그와 삽입된 데이터, 경로 등에 근거함.

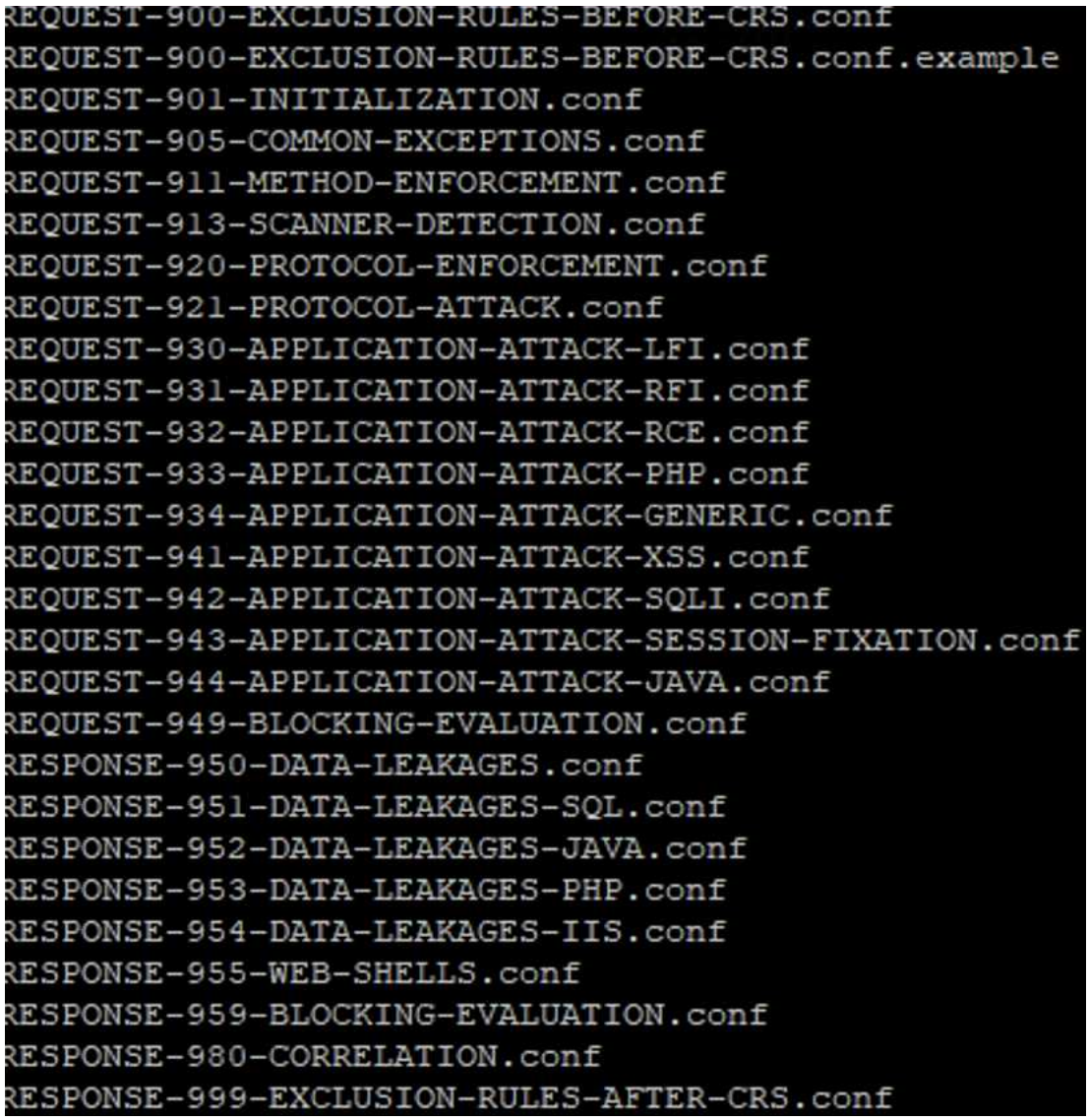


2. 방화벽 규칙 적용

❍ 구성

- 방화벽 규칙은 OWASP ModSecurity Core Rule Set을 적용시킴.
- https://github.com/coreruleset/coreruleset

- 탐지 목록으로 SQL 주입(SQLi), 교차 사이트 스크립팅(XSS), 로컬 파일 포함(LFI), 원격 파일 포함(RFI), PHP 코드 주입 , 자바 코드 주입 HTTPoxy, Shellshock, Unix/Windows Shell 주입, 세션 고정, 스크립팅/스캐너/봇 탐지, 메타데이터/오류 누출 등이 적용됨.



3. 탐지 공격 분석

❍ 공격 유형

1. Cross-Site-Scripting (XSS)

[Sun Jun 12 09:43:57.638504 2022] [:error] [pid 63:tid 140661605304064] [client 211.206.14.216:4954] [client 211.206.14.216] ModSecurity: Warning. Pattern match "(?i)[\\\\s\\"`;\\\\/0-9=\\\\x0B\\\\x09\\\\x0C\\\\x3B\\\\x2C\\\\x28\\\\x3B]+on[a-zA-Z]+[\\\\s\\\\x0B\\\\x09\\\\x0C\\\\x3B\\\\x2C\\\\x28\\\\x3B]*?=" at ARGS:content. [file "/usr/share/modsecurity-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"] [line "123"] [id "941120"] [msg "XSS Filter - Category 2: Event Handler Vector"] [data "Matched Data: \\x22 onclick= found within ARGS:content: \\x22 onclick=alert(1)//<button ' onclick=alert(1)//> */ alert(1)// "] [severity "CRITICAL"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-xss"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "OWASP_CRS/WEB_ATTACK/XSS"] [tag "WASCTC/WASC-8"] [tag "WASCTC/WASC-22"] [tag "OWASP_TOP_10/A3"] [tag "OWASP_AppSensor/IE1"] [tag "CAPEC-242"] [hostname "27.126.56.227"] [uri "/board/update/82"] [unique_id "YqW1XbobYw-09JB34cGwmQAAAAQ"], referer: http://27.126.56.227/board/update/82

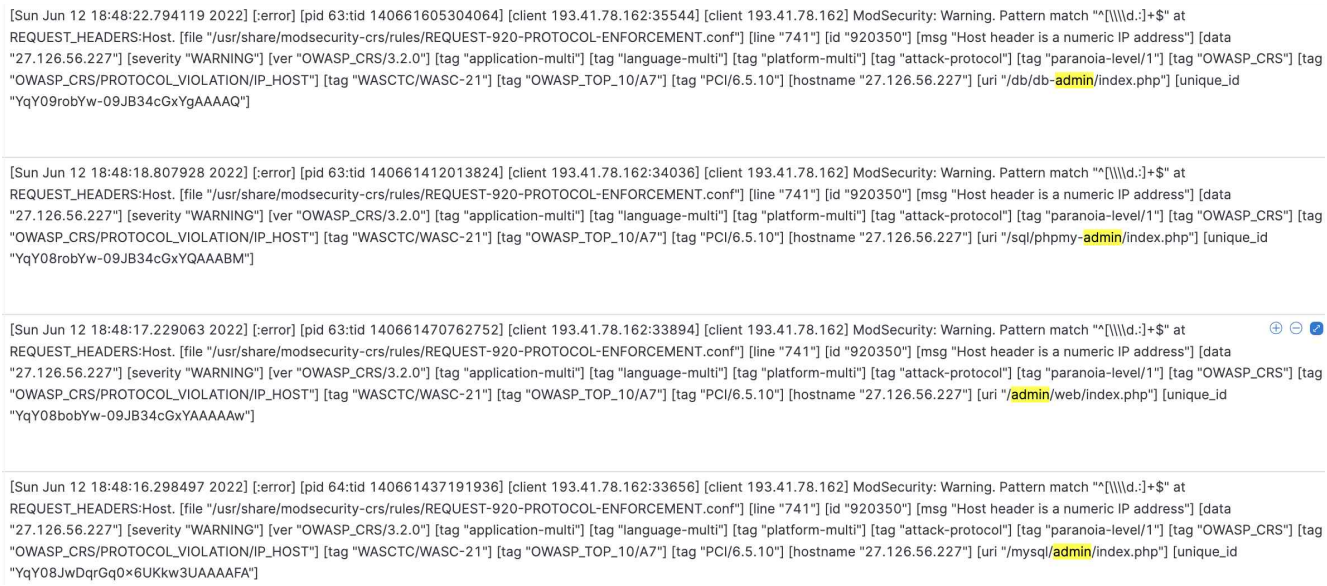
일시: Sun Jun 12 09:43:57.638504 2022
접속IP: 211.206.14.216
룰셋: REQUEST-941-APPLICATION-ATTACK-XSS.conf
이벤트 로그: XSS Filter - Category 2: Event Handler Vector
탐지 데이터: \\x22 onclick=alert(1)//<button ' onclick=alert(1)//>
보안등급: CRITICAL
경로: http://27.126.56.227/board/update/82

2. SQL Injection

[Sun Jun 12 09:13:58.000101 2022] [:error] [pid 63:tid 140660623525632] [client 211.105.196.201:12921] [client 211.105.196.201] ModSecurity: Warning. detected SQLi using libinjection with fingerprint 's&sos' [file "/usr/share/modsecurity-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "68"] [id "942100"] [msg "SQL Injection Attack Detected via libinjection"] [data "Matched Data: s&sos found within ARGS:password: 1'or'1'='1'"] [severity "CRITICAL"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-sqli"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [tag "WASCTC/WASC-19"] [tag "OWASP_TOP_10/A1"] [tag "OWASP_AppSensor/CIE1"] [tag "PCI/6.5.2"] [hostname "27.126.56.227"] [uri "/login"] [unique_id "YqWuVbobYw-09JB34cGs1wAAABg"], referer: http://27.126.56.227/login

일시: Sun Jun 12 09:13:58.000101 2022
접속IP: 211.105.196.201
룰셋: REQUEST-942-APPLICATION-ATTACK-SQLI.conf
이벤트 로그: SQL Injection Attack Detected via libinjection
탐지 데이터: password: 1'or'1'='1
보안등급: CRITICAL
경로: http://27.126.56.227/login

3. 관리자페이지 노출 시도



일시: Sun Jun 12 18:48:22 2022

접속IP: 193.41.78.162

룰셋: REQUEST-920-PROTOCOL-ENFORCEMENT.conf

이벤트 로그: Host header is a numeric IP address

탐지 데이터: Admin Page Direcotry Indexing

보안등급: WARNING

경로: /db/db-admin/index.php, /sql/phpmy-admin/index.php, /admin/web/index.php