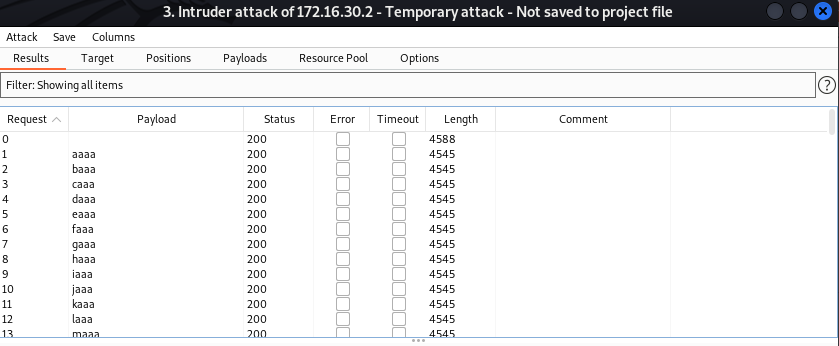
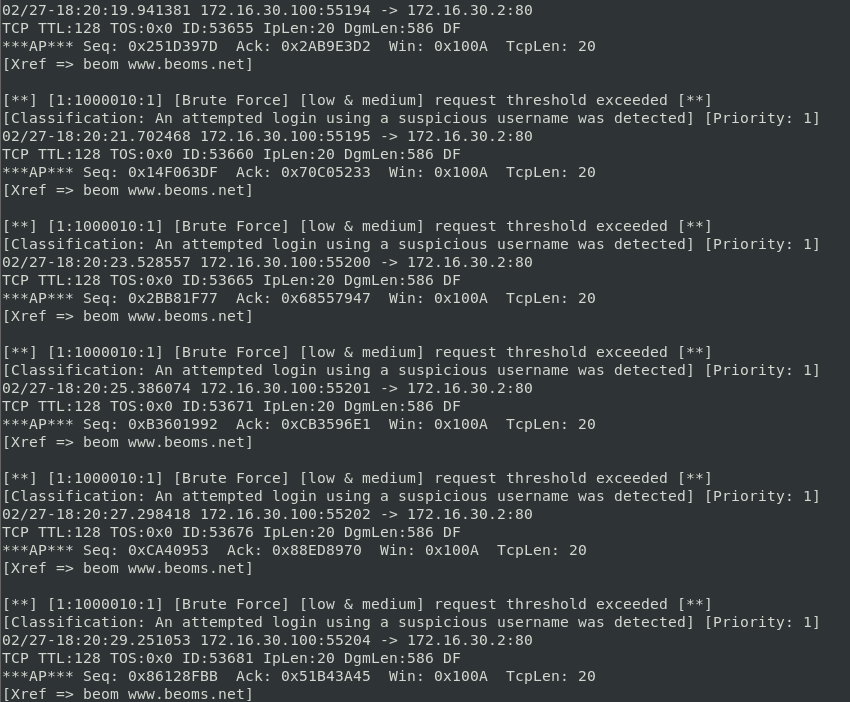
**각 취약점의 low 와 medium 단계의 공격을 Kali 에서 각각 시도하고 이를 탐지하는 세가지 방법을 각각 캡쳐해서 취약점의 단계별 (low medium) 로 정리한다**

**(1 snort alert, 2 elasticsearch 로그 3 wireshark capture 파일)**

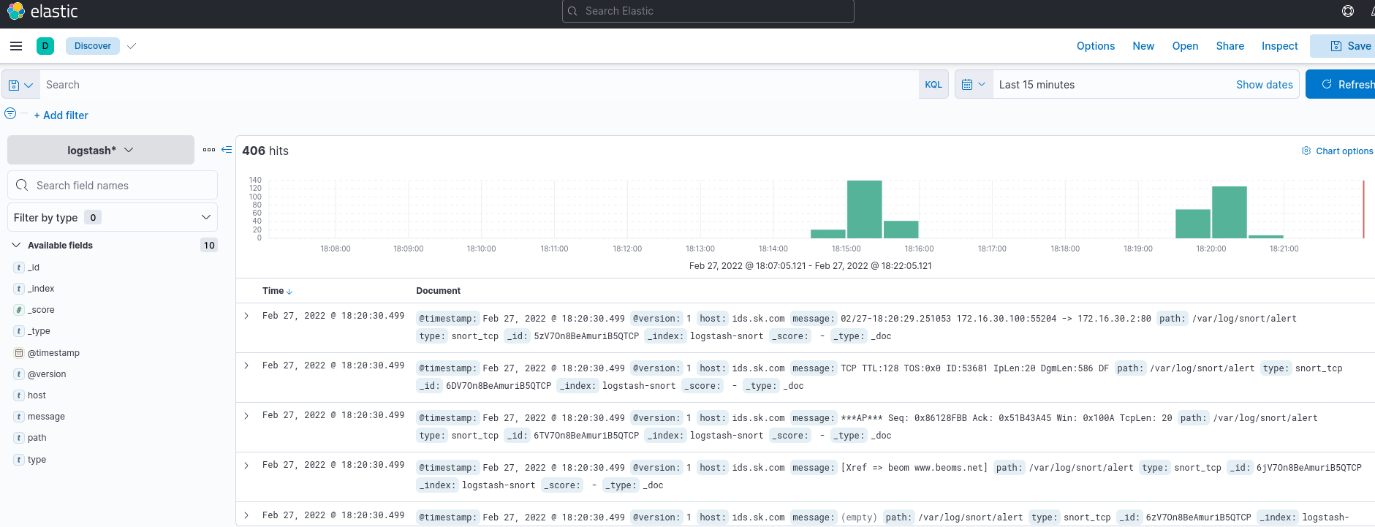
**Brute Force**



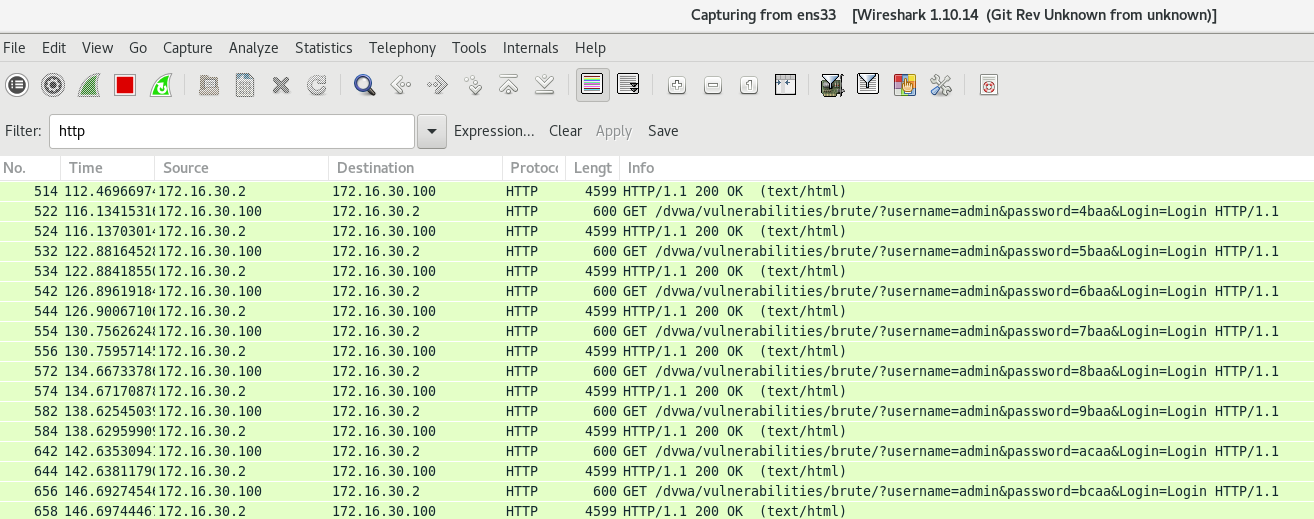
Kali에서 Brute Force 공격 시도

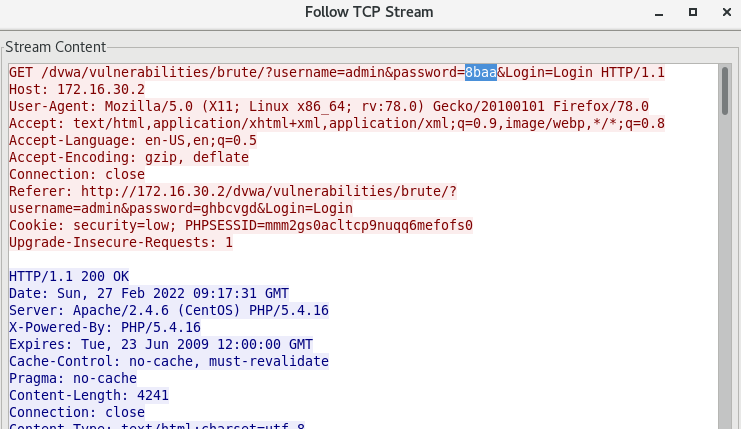


Snort alert



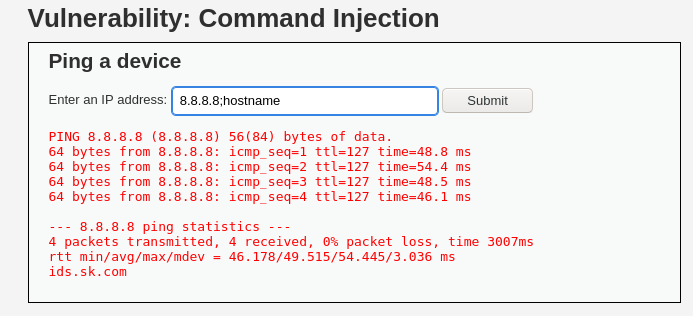
Elasticsearch log



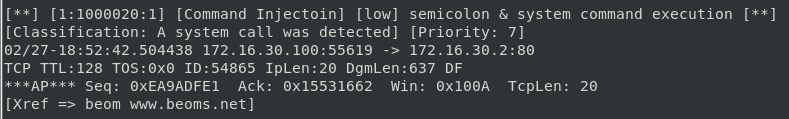


Wireshark capture

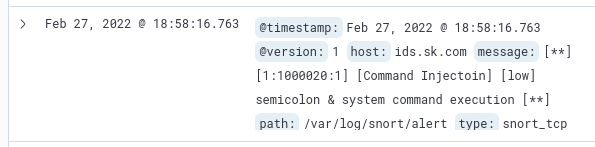
**Command Injection Low**

****

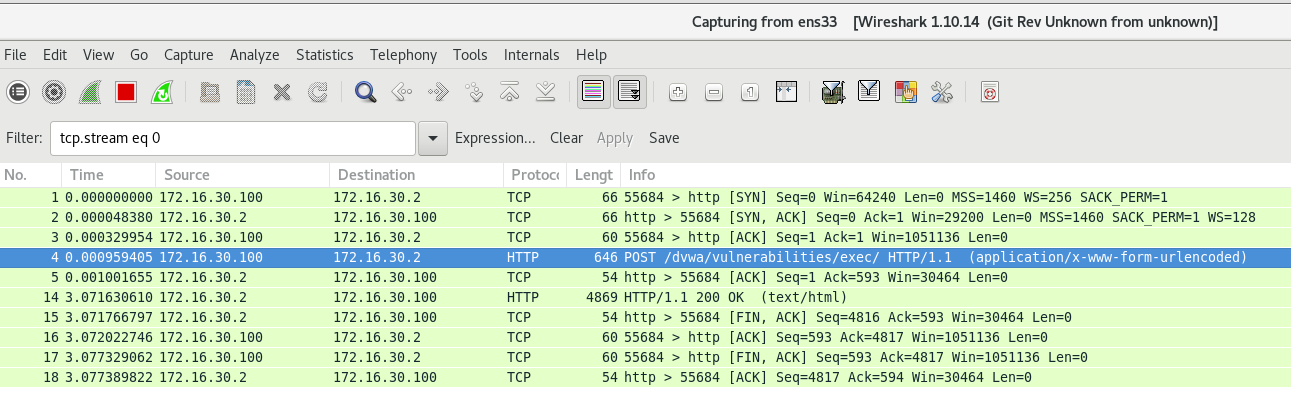
Kali에서 공격 시도



Snort alert

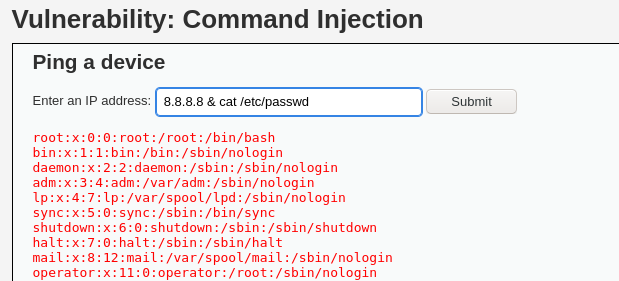


Elasticsearch log

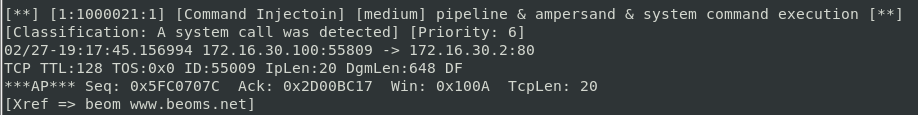


Wireshark Capture

**Command Injection Medium**



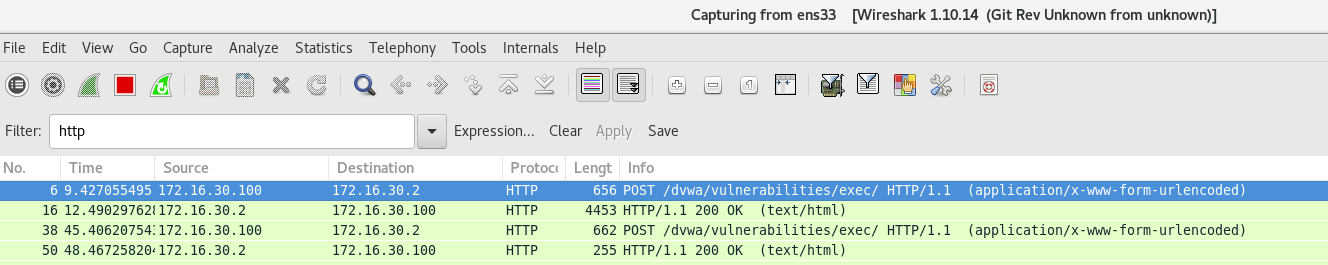
Kali에서 공격 시도



Snort alert

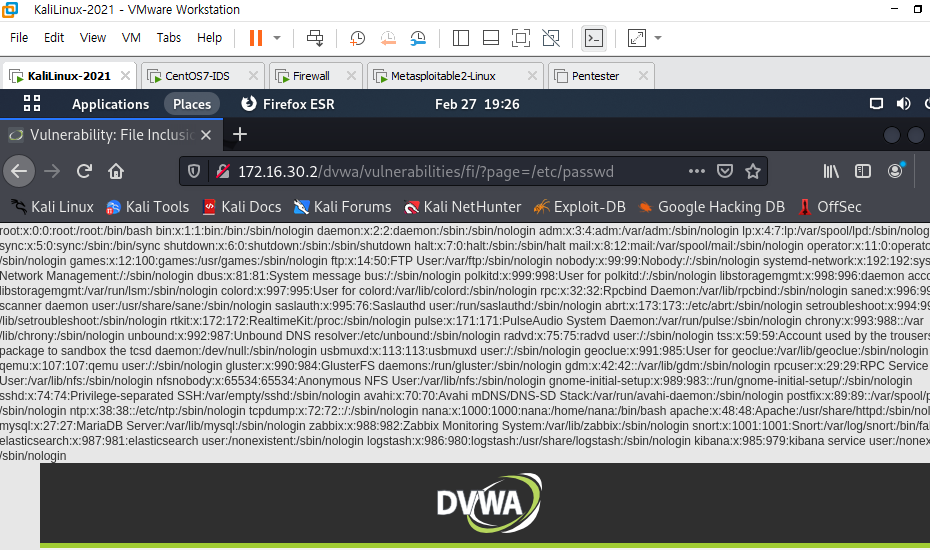


Elasticsearch log

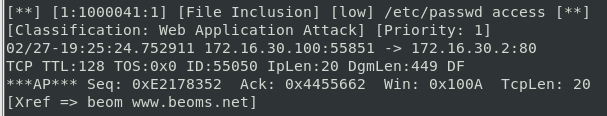


Wireshark Capture

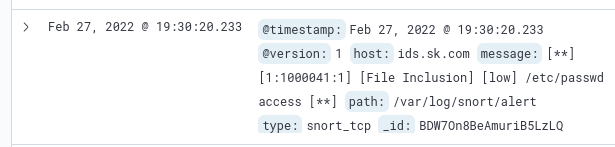
**File Inclusion Low**



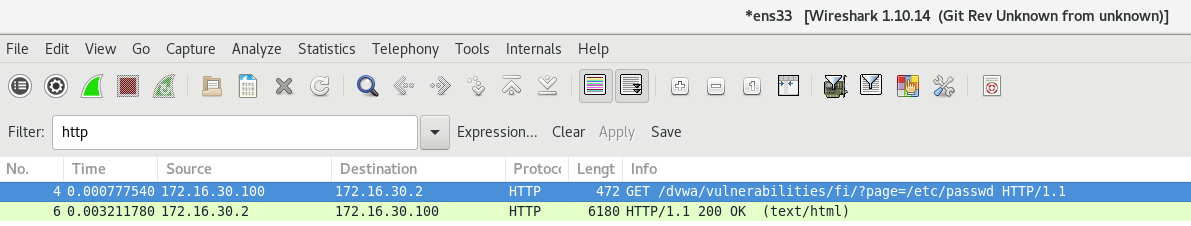
Kali에서 공격 시도



Snort alert

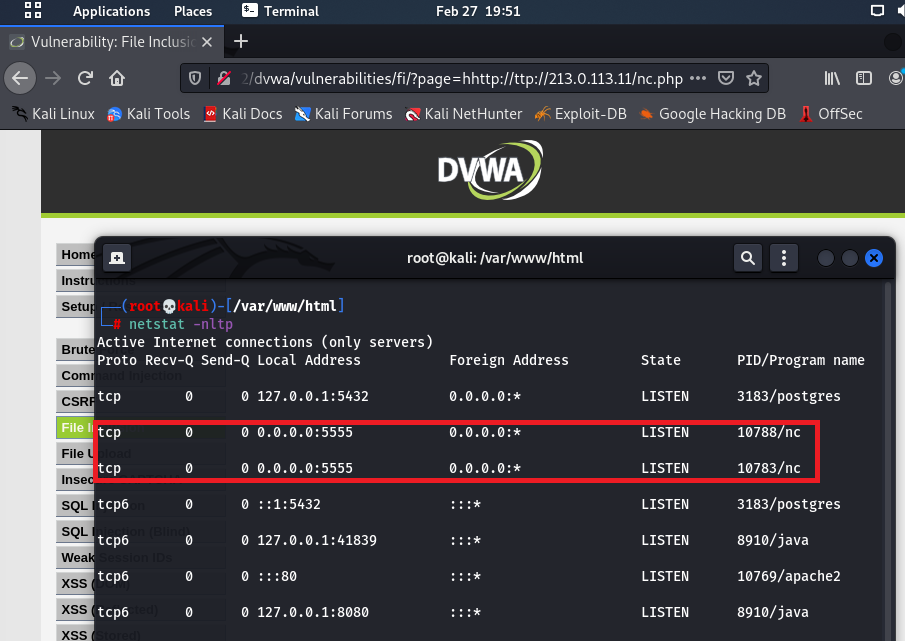


Elasticsearch log

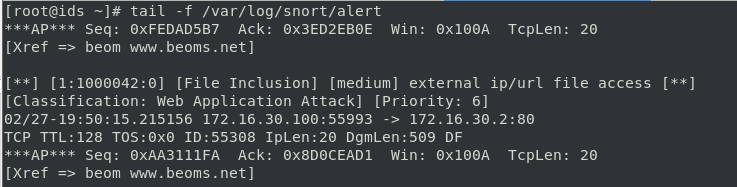


Wireshark Capture

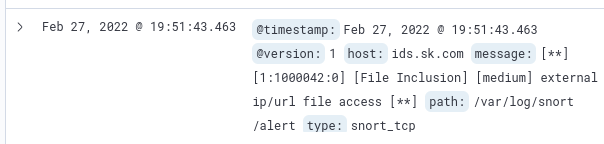
**File Inclusion Medium**



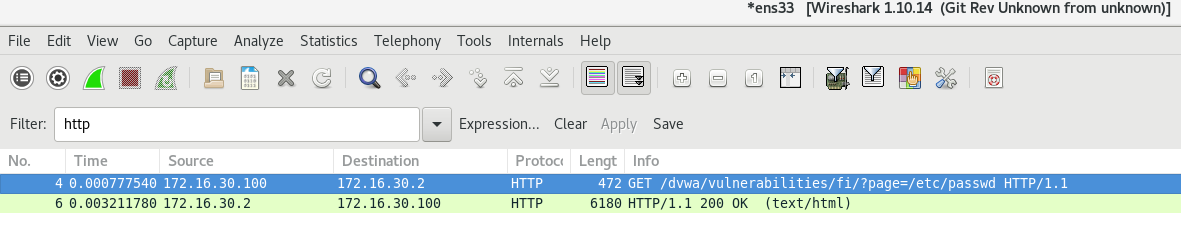
Kali에서 공격



Snort alert

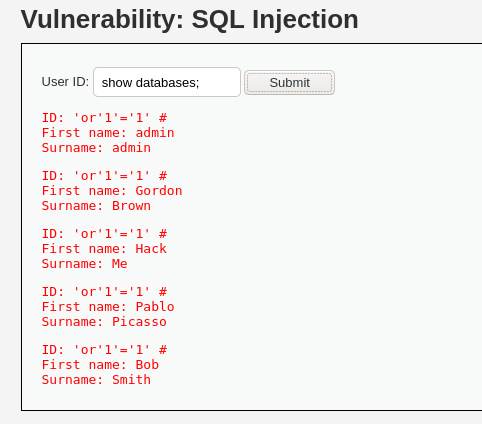


Elasticsearch log

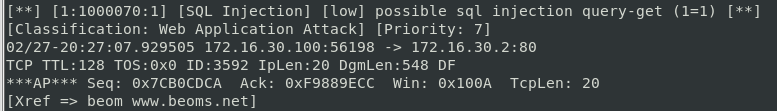


Wireshark Capture

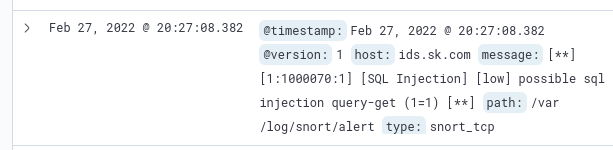
**SQL Injection Low**



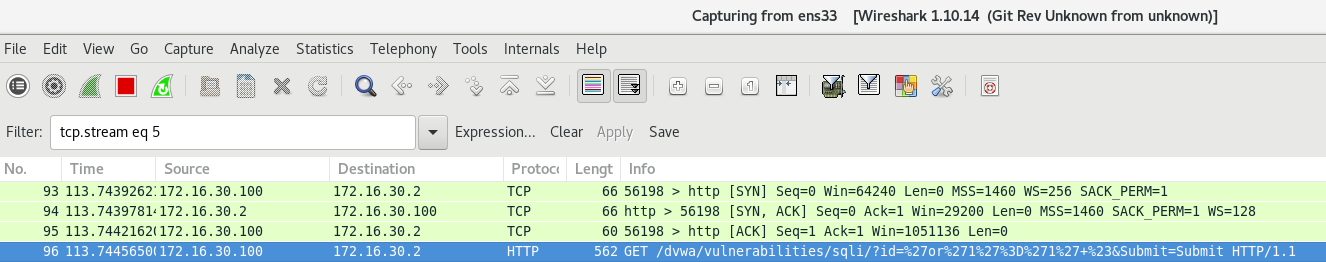
Kali에서 공격



Snort alert

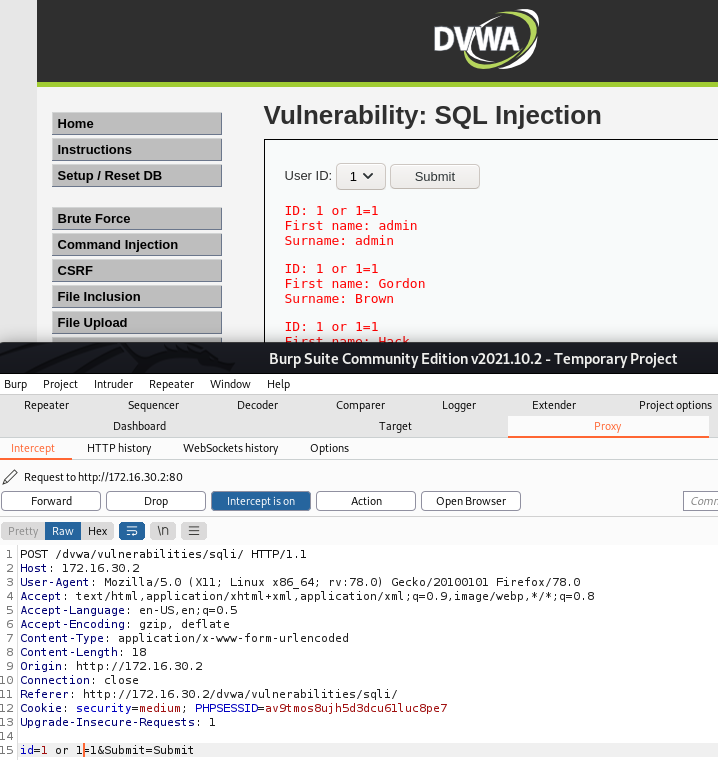


Elasticsearch log

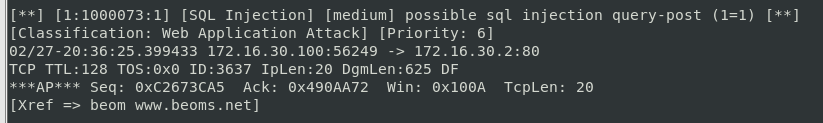


Wireshark capture

**SQL Injection Medium**



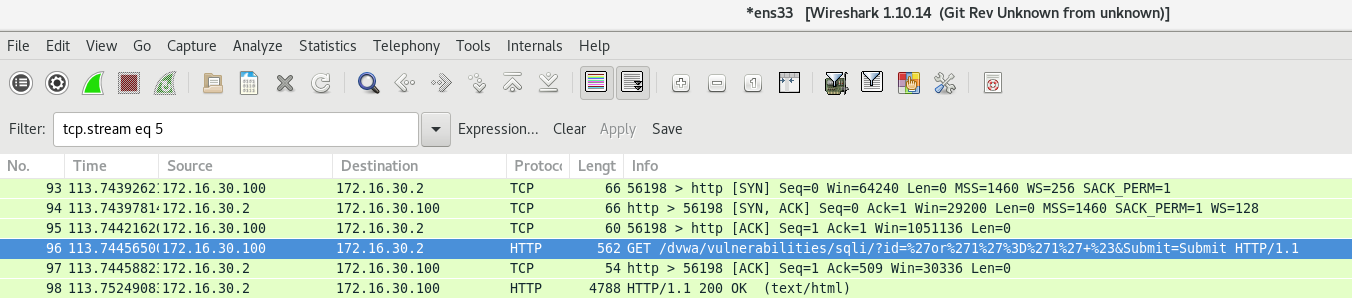
Kali에서 공격



Snort alert

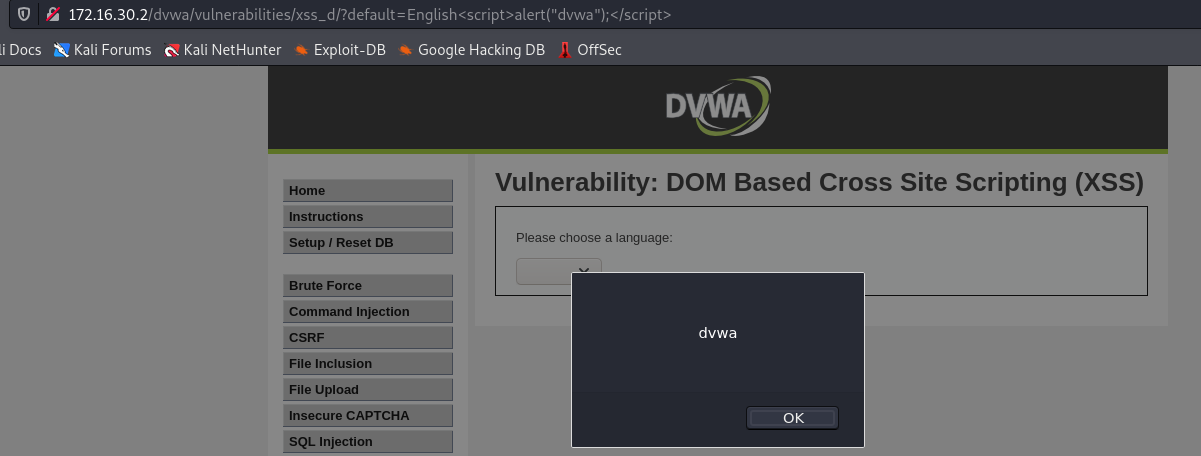


Elasticsearch log

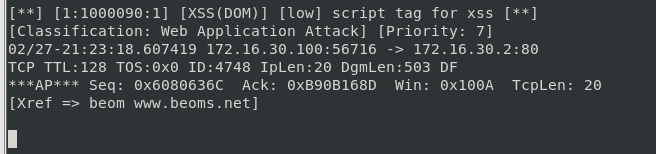


Wireshark capture

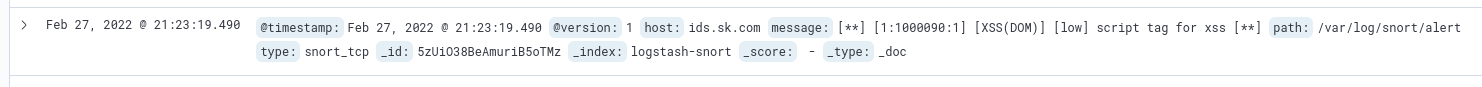
**DOM XSS Low**



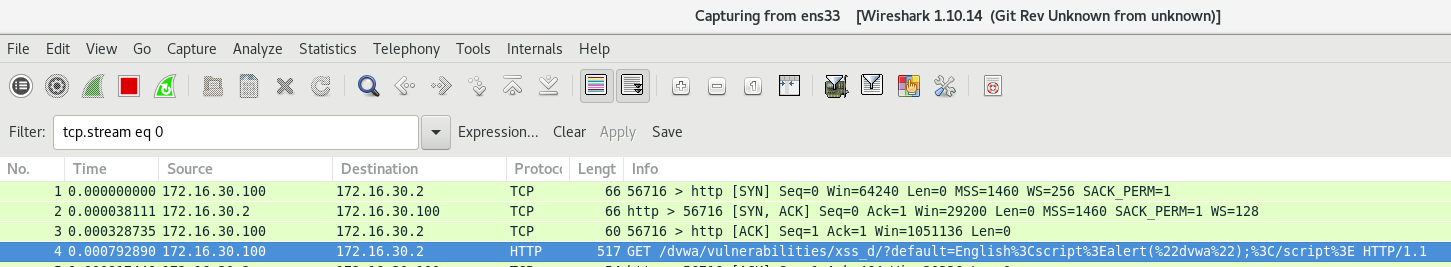
Kali에서 공격



Snort alert

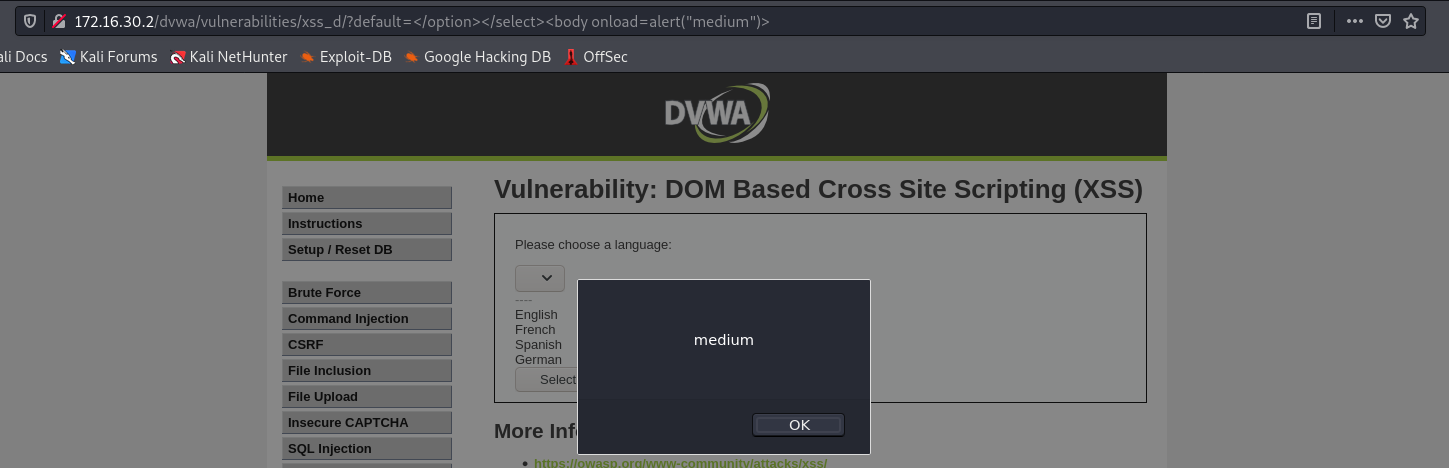


Elasticsearch log

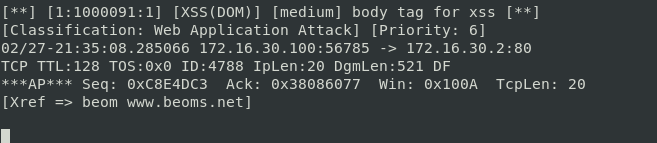


Wireshark capture

**DOM XSS medium**



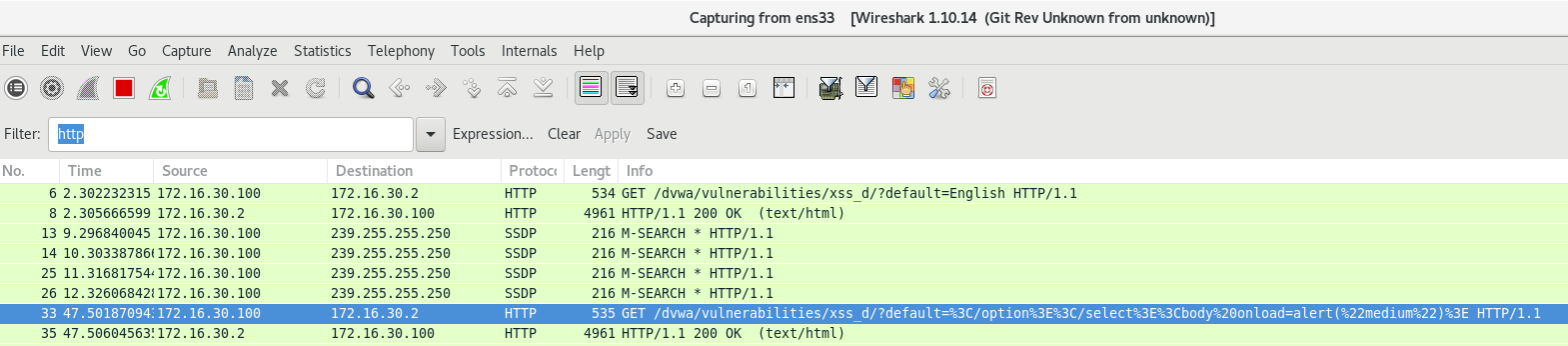
Kali에서 공격



Snort alert

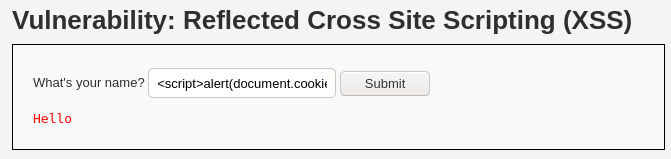


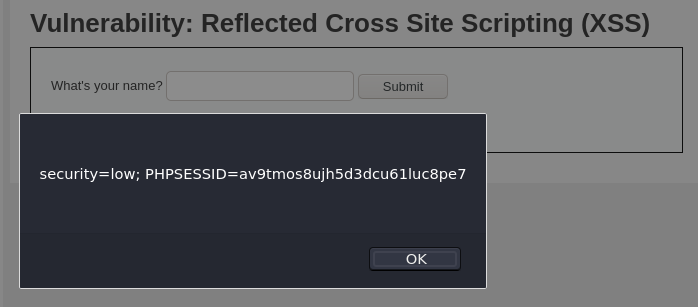
Elasticsearch log



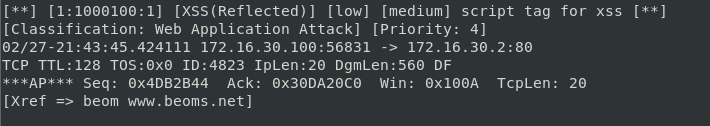
Wireshark capture

**Reflected XSS Low**





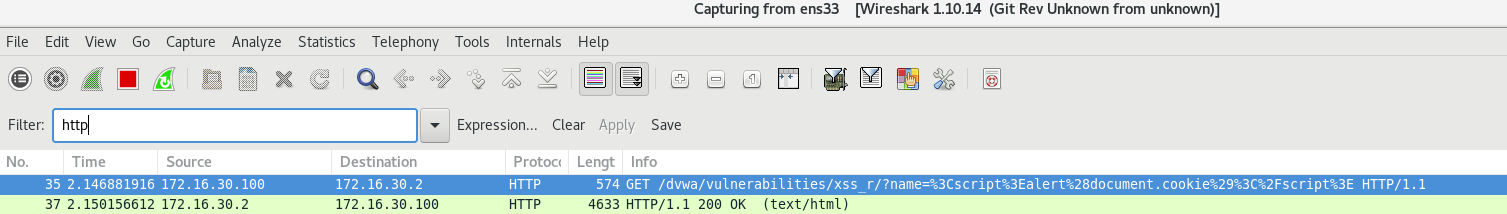
Kali에서 공격



Snort alert

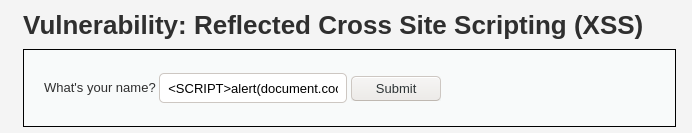


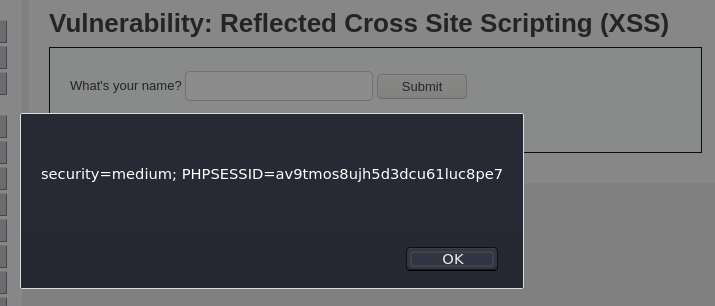
Elaticsearch log



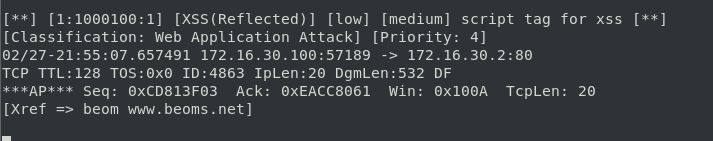
Wireshark capture

**Reflected XSS Medium**

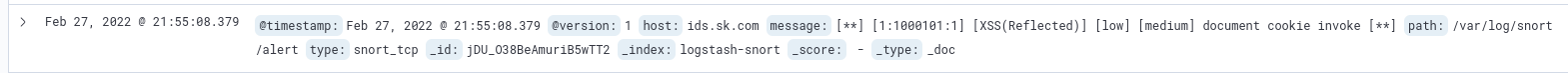




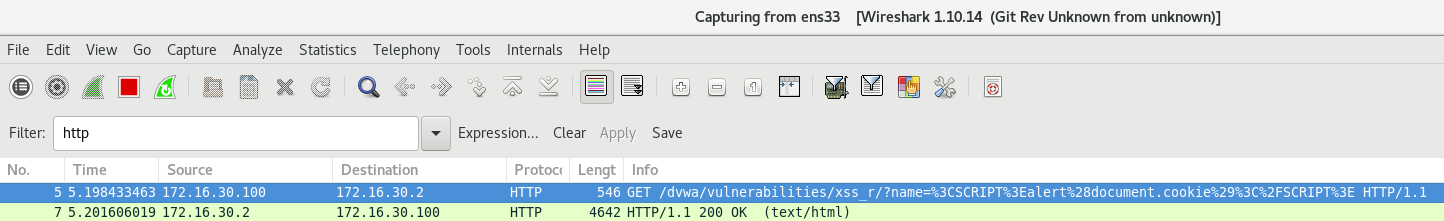
Kali에서 공격



Snort alert

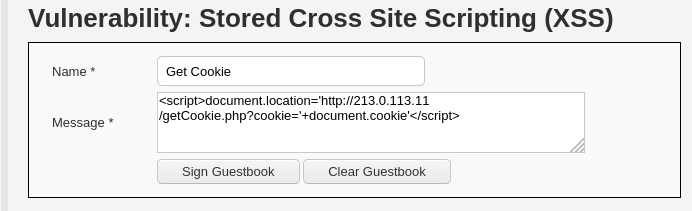


Elasticsearch log

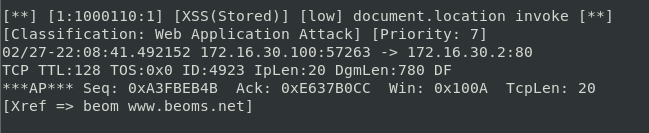


Wireshark capture

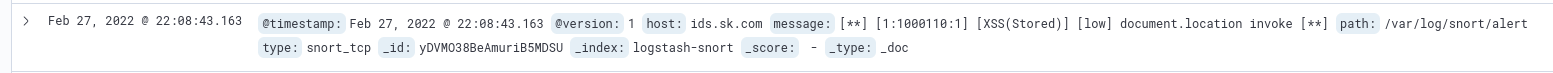
**Stored XSS Low**



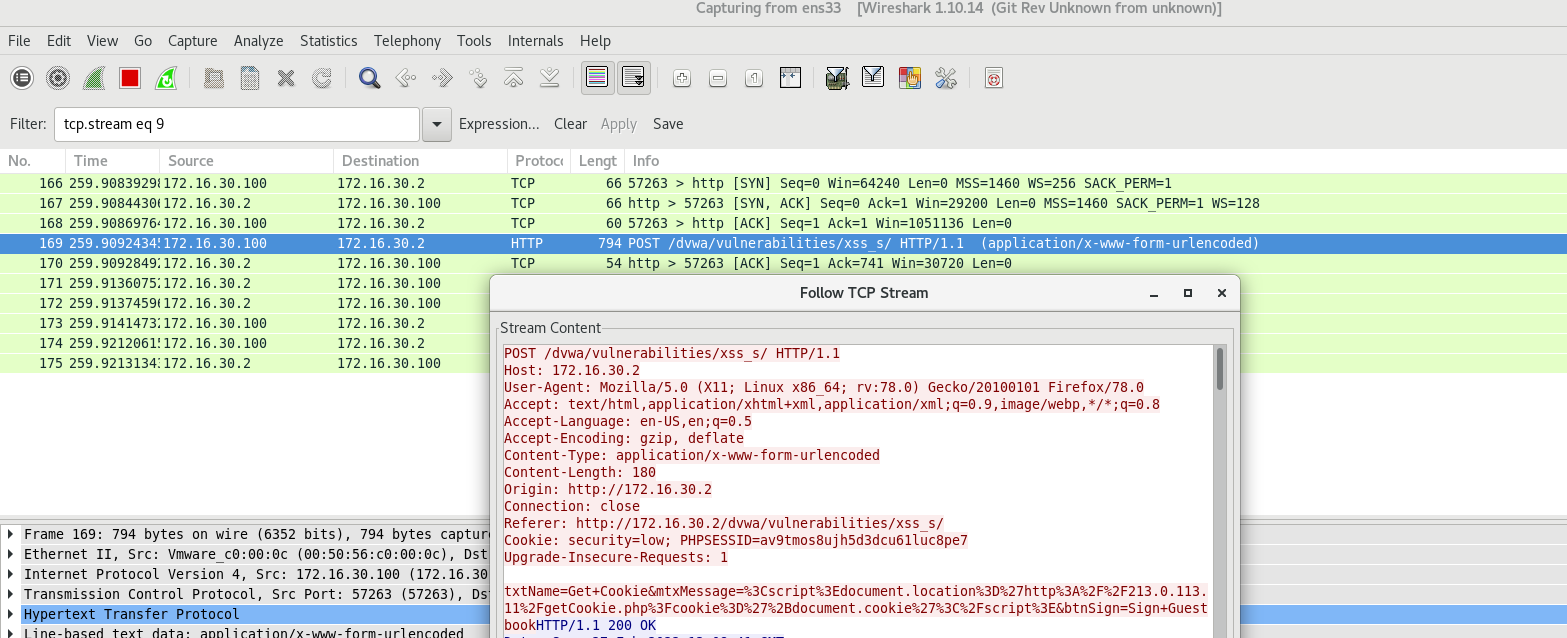
Kali에서 공격



Snort alert

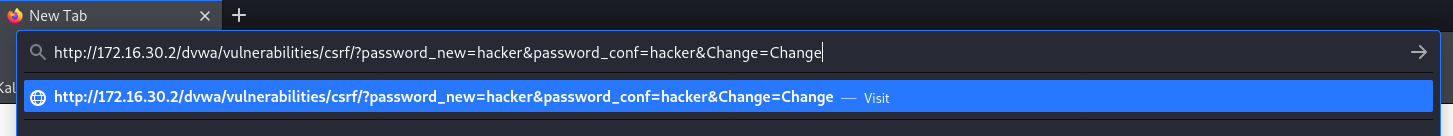


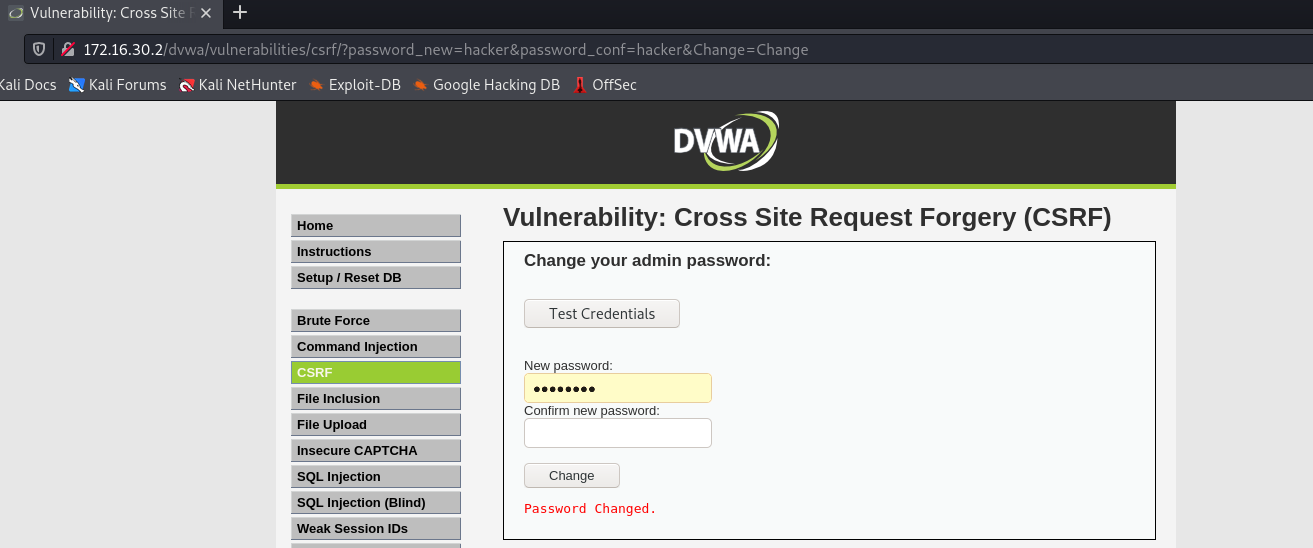
Elasticsearch log



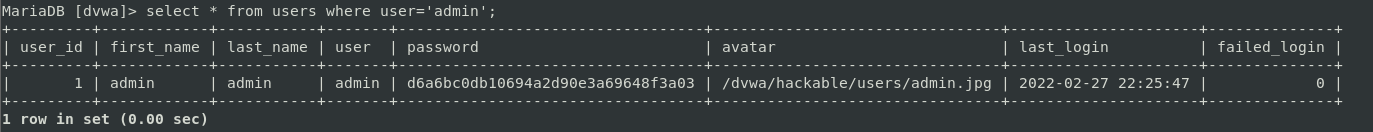
Wireshark capture

**CSRF Low**

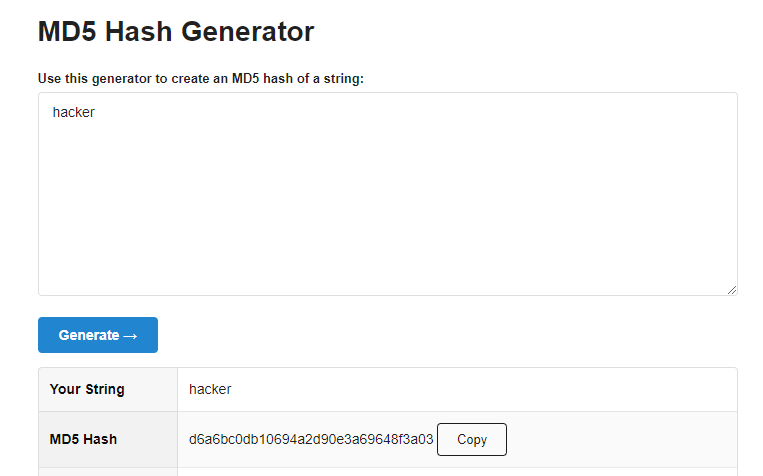




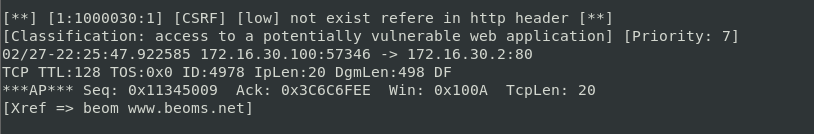
Kali에서 공격



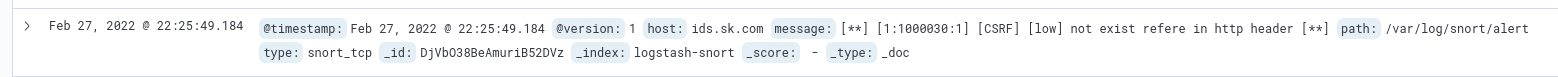
CentOS에서 DB 확인



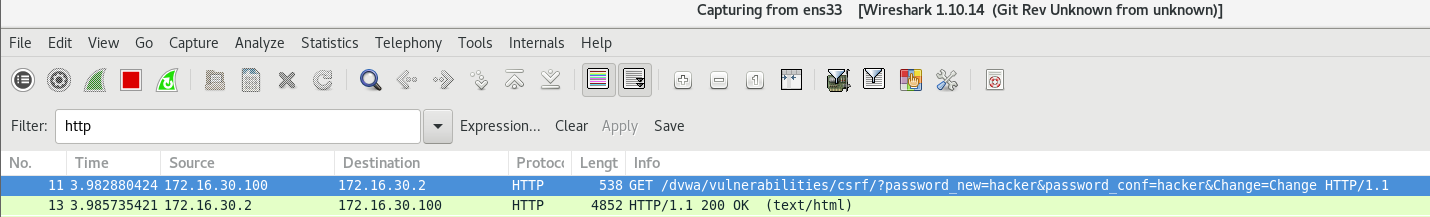
hacker와 해시 값이 일치하는 것을 확인함



Snort alert

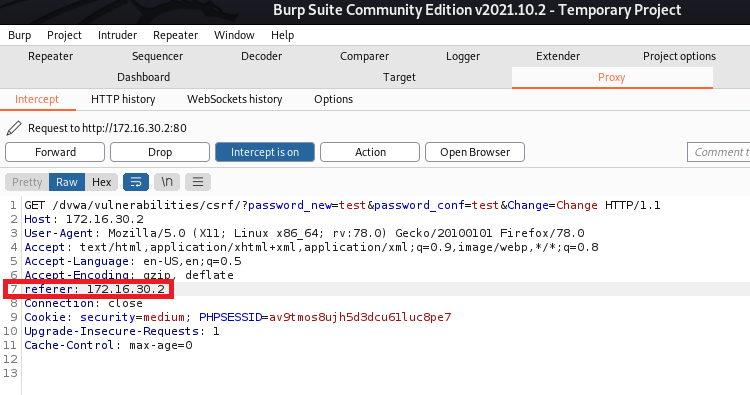


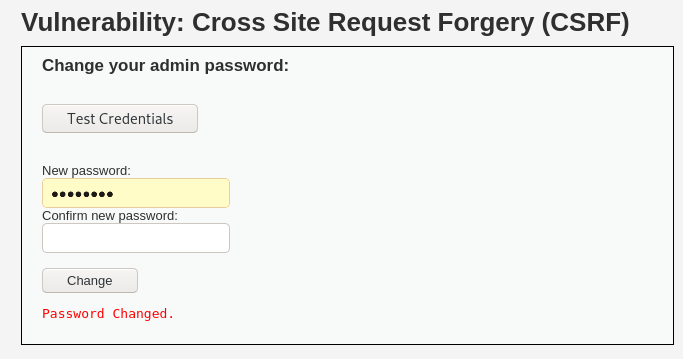
Elasticsearch log



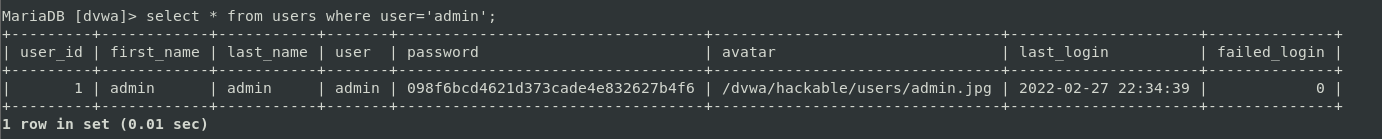
Wireshark capture

**CSRF Medium**

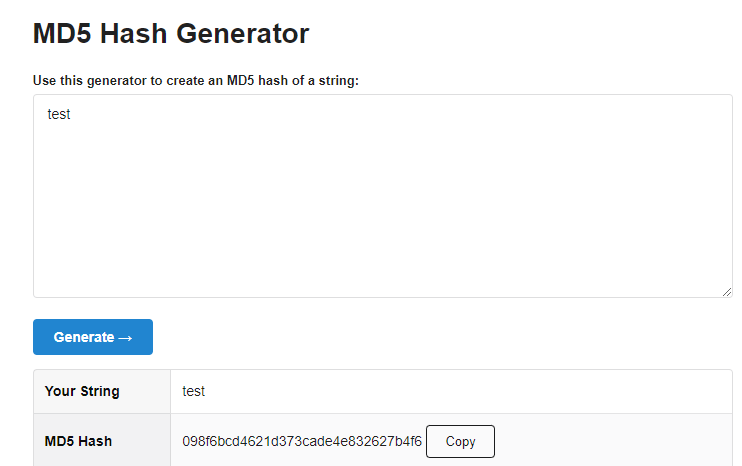




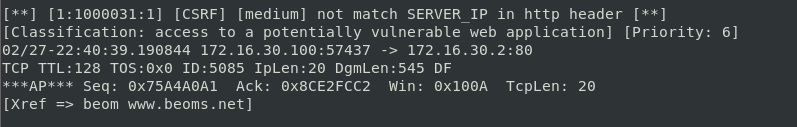
Kali에서 공격



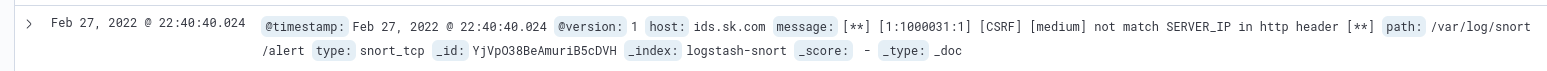
CentOS DB에서 확인



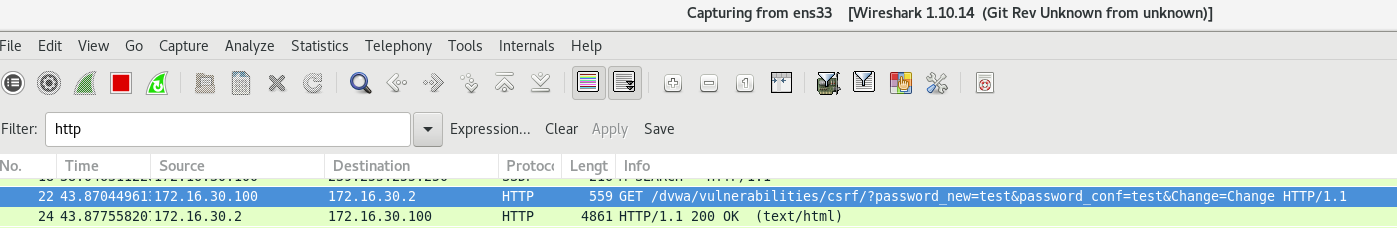
test와 해시 값이 일치하는 것을 확인함



Snort alert

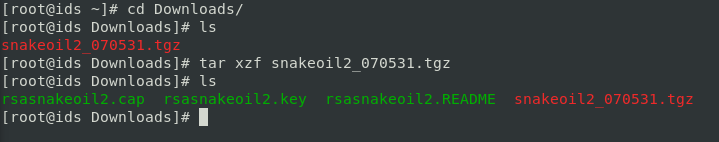


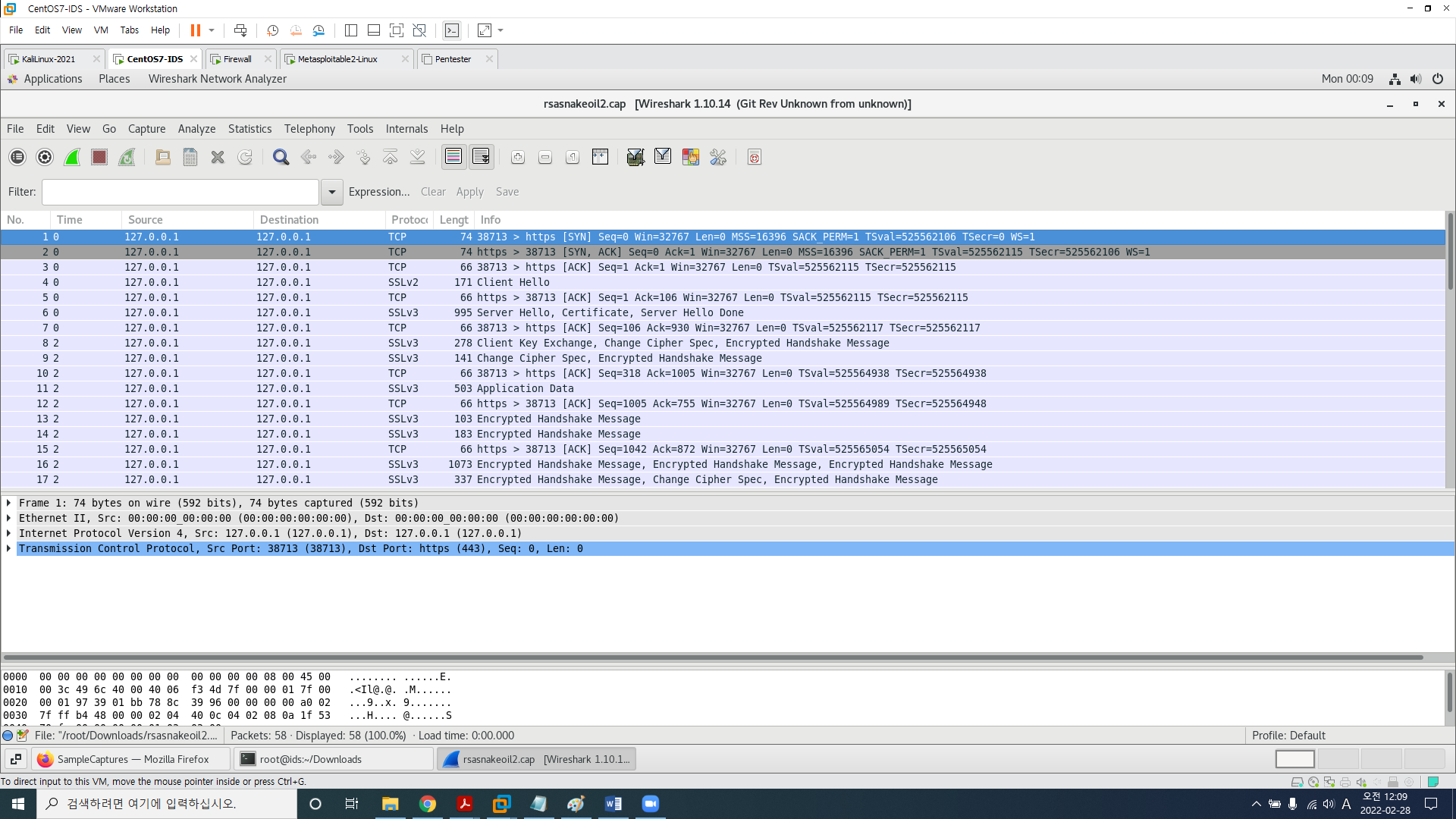
Elasticsearch log



Wireshark capture

CentOS 7 서버에 snakeoil 2 파일을 다운로드하고 wireshark 로 불러온다





snakeoil 2 파일에서 Server 가 보낸 인증서를 추출하고 그 내용을 텍스트 파일로 저장한다

