모의 해킹 보고서

분석자: 지윤배

Contents  
   
  
 1. 개요

1.1 모의해킹 정의   
 1.2 수행 일정 및 인원   
 1.3 수행 대상 및 장소  
 1.4 수행 단계

1.5 수행 시나리오

1.6 점검 항목

1.7 점검 도구

2. 결과 요약

2.1 영향성 평가

2.2 취약점 요약

2.3 총평

3. 취약점 상세 설명 (나중에)

3.1 환경 분석

3.2 취약점 발견 및 분석 서술

4. 대응 방안 (나중에)

4.1 환경 분석

4.2 취약점 대응 방안 제시

1 페이지

**개요**

**1.1 모의 해킹 정의**

**본 모의해킹 진단은 도메인을 통한 정보수집(DNS), 말테고를 이용한 정보수집**

**(ipeofur, www, dns, ns, isp, 국가/도시, 전화번호, 이메일,사람…).GHBD를 이용한 정보수집 서비스의 관련된 모든 정보 자산에 대해 취약점을 도출/분석 하여 대책을 수립하기 위함 입니다. 헤커와 동일한 환경과 조건, Hacking skill 을 가지고 모의적인 침투에 의해 이루어지며, 발견된 취약점에 대해서는 사전적인 예방을 통한 효과를 발생시키는데 목적이잇습니다.**

**1.2 수행일정/수행인원**

**본 모의해킹은 2019 년 8월 23일에 진행이되며, 총 1명이 투입됩니다.**

2 페이지

**1.3 수행 대상 및 장소**

본 모의해킹은 아래의 대상들을 전달받앗다. 해당 대상에 대해 점검이 이루어 집니다.

* **도메인을 통한 정보수집(DNS) :**

**nslookup, dig, host, dnsenum, dnsmap…**

* **말테고를 이용한 정보수집 : 도메인을 통해 정보수집 단계별**

**(ip대역, www, dns, ns, isp, 국가/도시, 전화번호, 이메일, 사람,….)**

* **포트 스캔 : nmap(TCP Half Open 스캔)**

**< ---- >**

**VMware 내부(타겟 : CENTOS, win2008)**

3 페이지

**1.4 수행 단계**

1. 정보수집

(Information Gathering): 대상에 대한 서버/네트워크/서비스에 대한 불필요한 서비스 접근 가능성, 외부에서 파악할 수 잇는 정보들을 수집하는 단계

1. 취약점 수집

(Vulnerablilty Assesment): 네트워크에 적합한 centos gnome system-monitor, wireshark를 이용하여 발생하는 취약점에 대한 정보를 수집하는 단계

1. 침투단계

(Gaining Access): 취약점 수집단계를 통해 획득한 정보를 기반으로 수동점검(Manual)을 통해 내부시스템을 확인하는단계

1. 상세 분석

(Maintaining Access): 취약점이 도출되엇을 경우에 공격에 의해서 보안 위협이 시스템 및 비즈니스 측면에서 어느정도의 영향을 줄수 잇는지 분석하는 단계

1. 보고서 작성

(Report): 취약점이 도출되엇을 경우에 공격에 의해서 보안 위협이 시스템 및 비즈니스 측면에서 어느정도의 영향을 줄수 잇는지 분석하는 단계

4 페이지

**1.5 수행 시나리오**

Kali-Linux 를 이용해 도메인을 통한 정보수집(DNS)을 진행하고,

Kali-Linux 를 이용해 말테고를 이용한 정보수집을 단계별로 진행해보고,

Nmap 을 통해 포트스캔을 진행할 것이다.

**1.6 점검항목/점검도구**

DNS : nslookup , dig, host, dnsenum, dnsmap

Maltego : ip대역, www, dns, ns, isp, 국가/도시, 전화번호, 이메일, 사람

Kali-Linux 를 통한 nmap (TCP Half-open 스캔),

VMware,.. 등등 사용

5 페이지

Nmap 을 활용한 포트 스캔

TCP Half-Open 스캔

1) 포트가 활성화된 경우

공격자 타겟

Syn ->

<- Syn, Ack

Rst ->

2) 포트가 비활성화된 경우

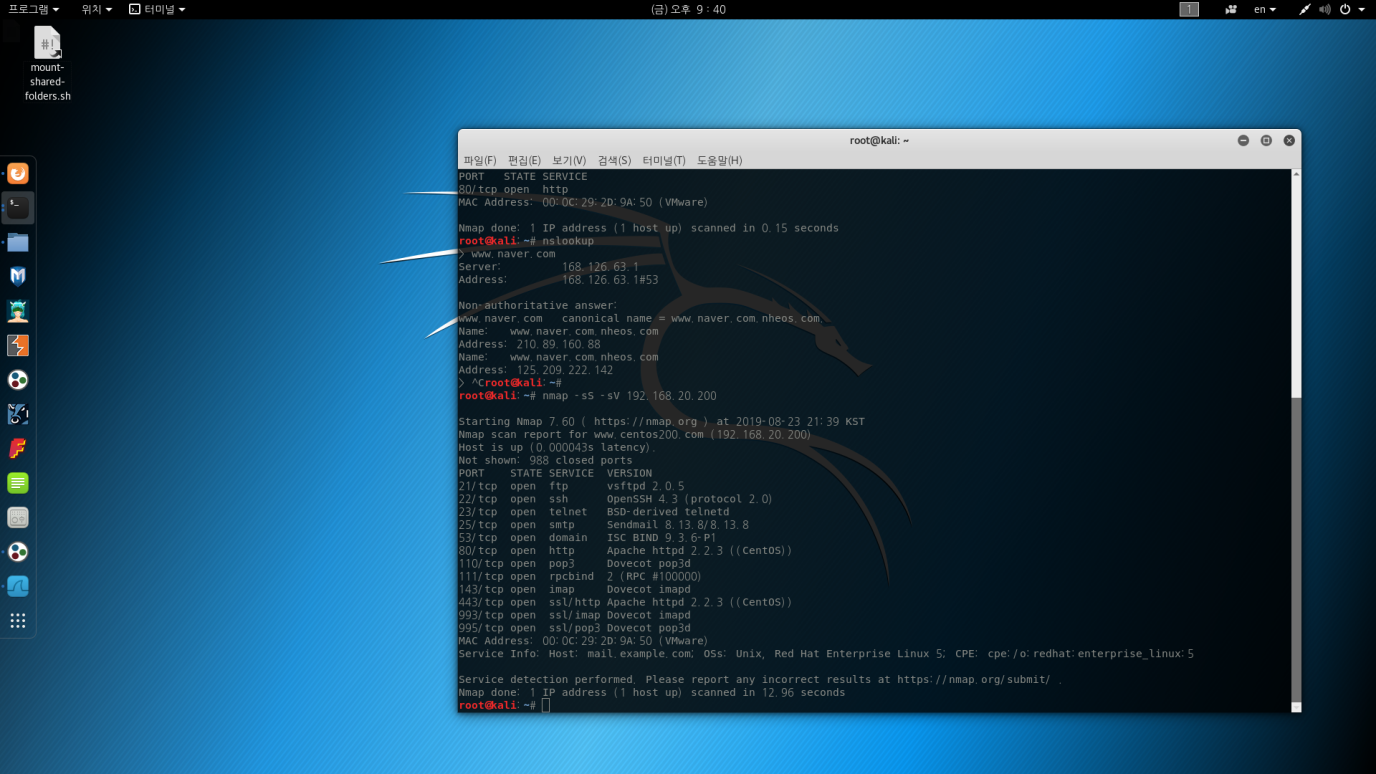
공격자 타겟

Syn ->

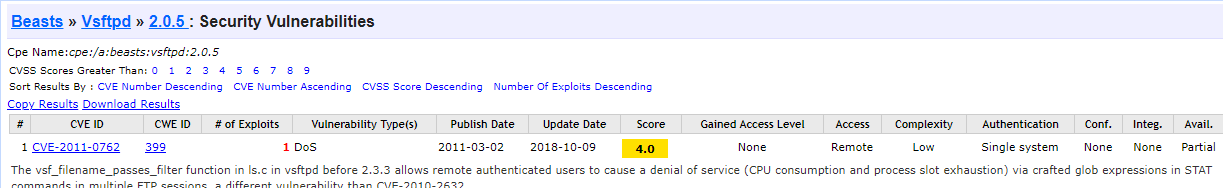
<- RST, Ack

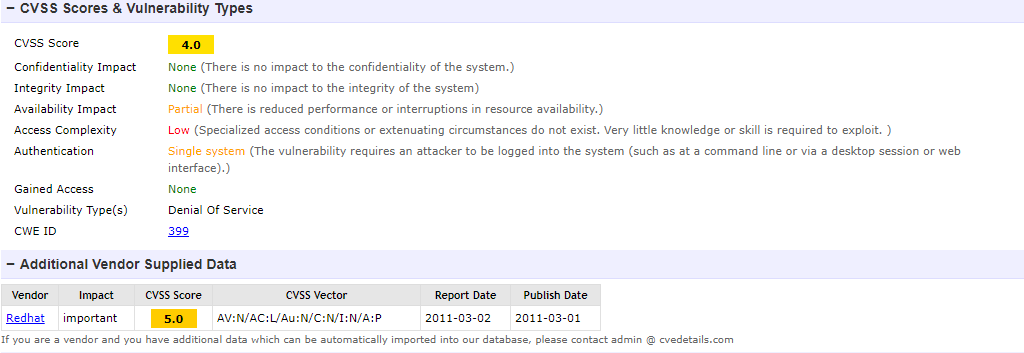
6 페이지

Nmap 을 통한 서비스 버전(여러가지)



21/ftp VERSION vsftpd 2.0.5

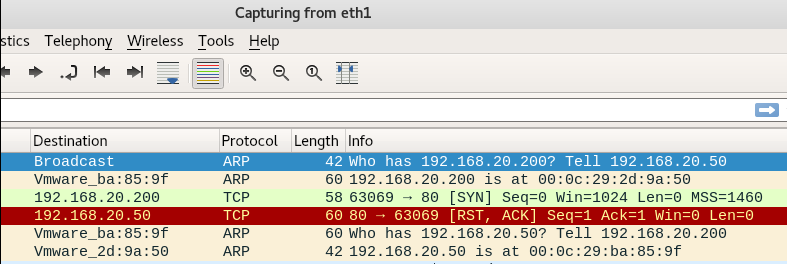




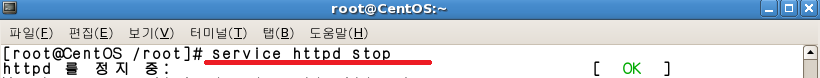
7 페이지

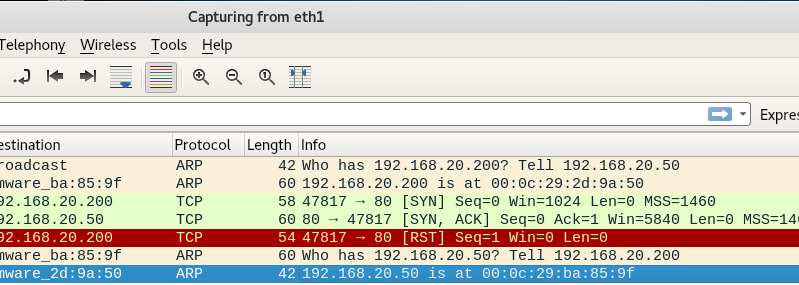
Nmap 을 활용한 포트 스캔

TCP Half-Open 스캔

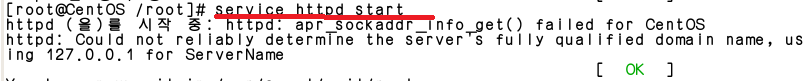


포트가 비활성인 경우





포트가 활성화된 경우

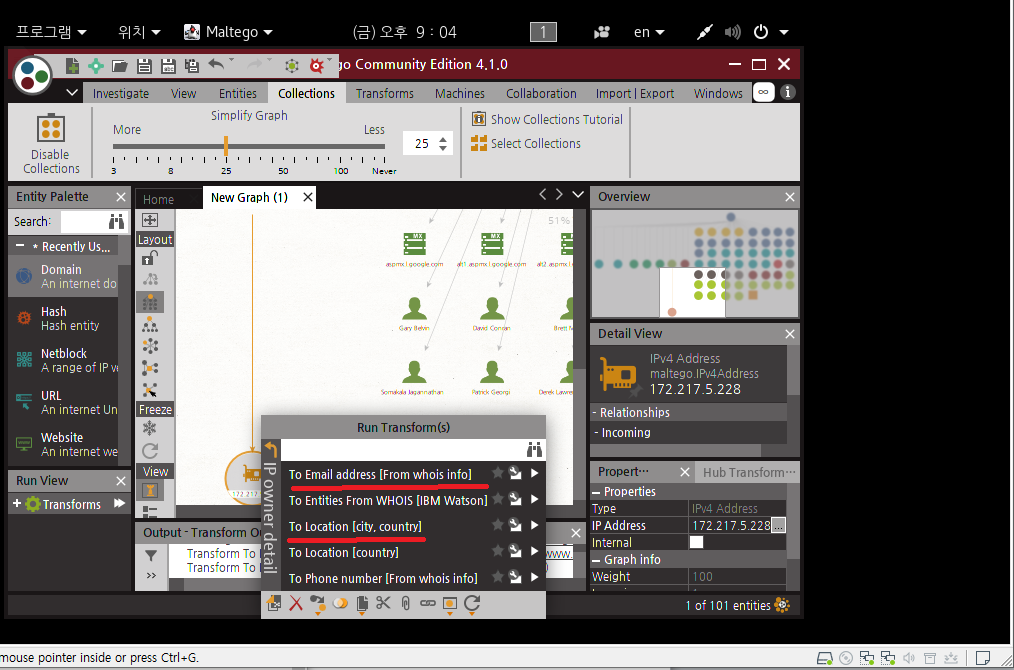


8 페이지

**도메인을 통한 정보수집(DNS) : Nslookup**

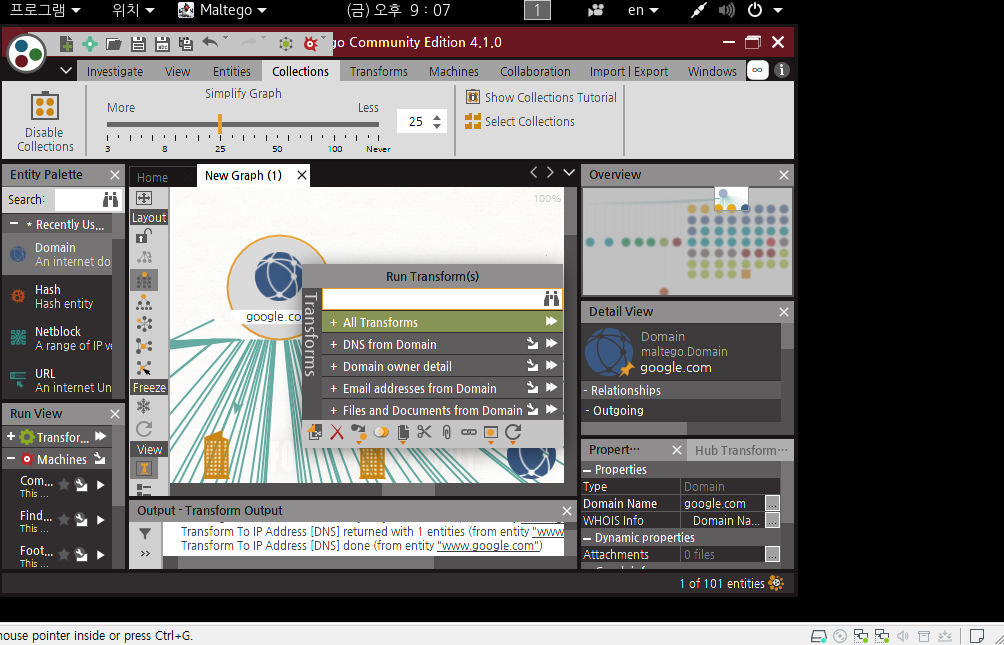
[그림 1-3] 네이버 정보수집 nslookup

**말테고를 이용한 정보수집**

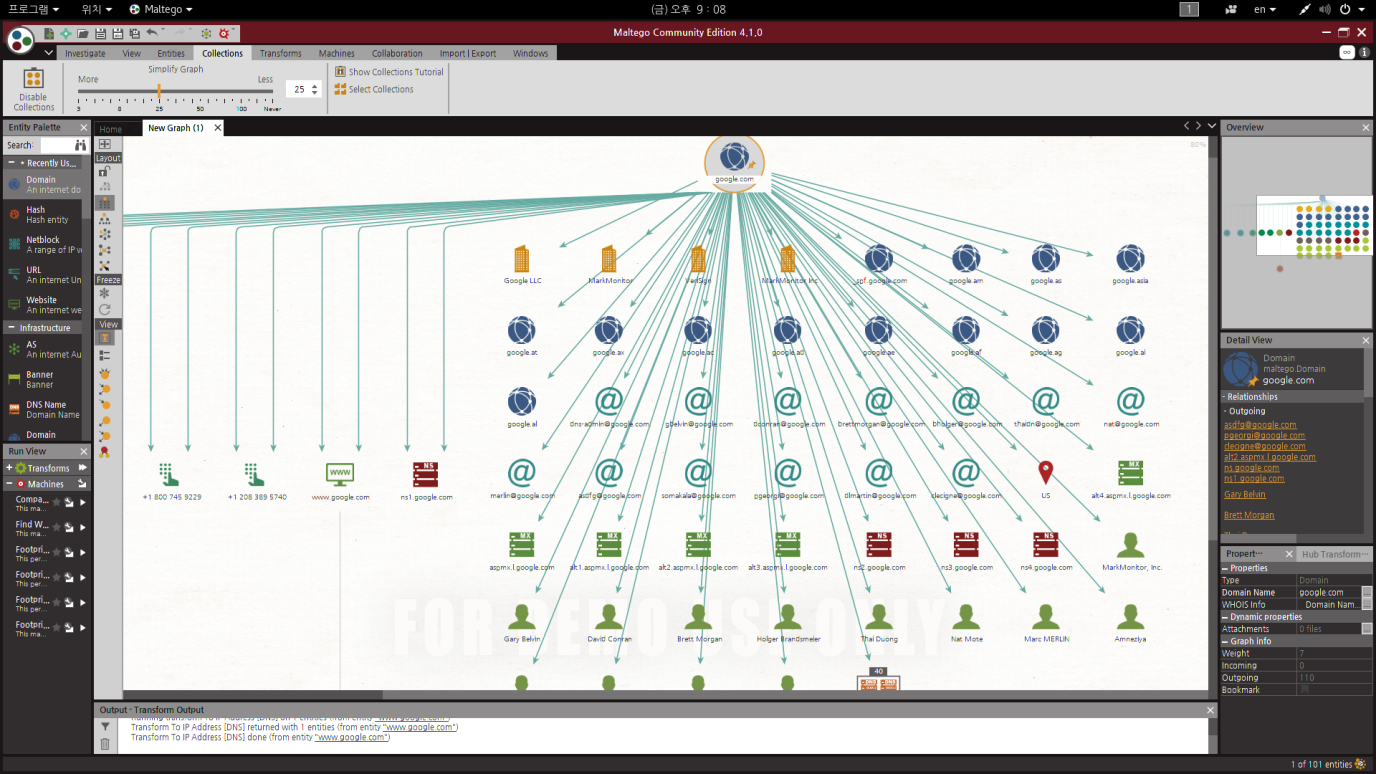
국가/도시

9 페이지

말테고를 이용한 정보수집

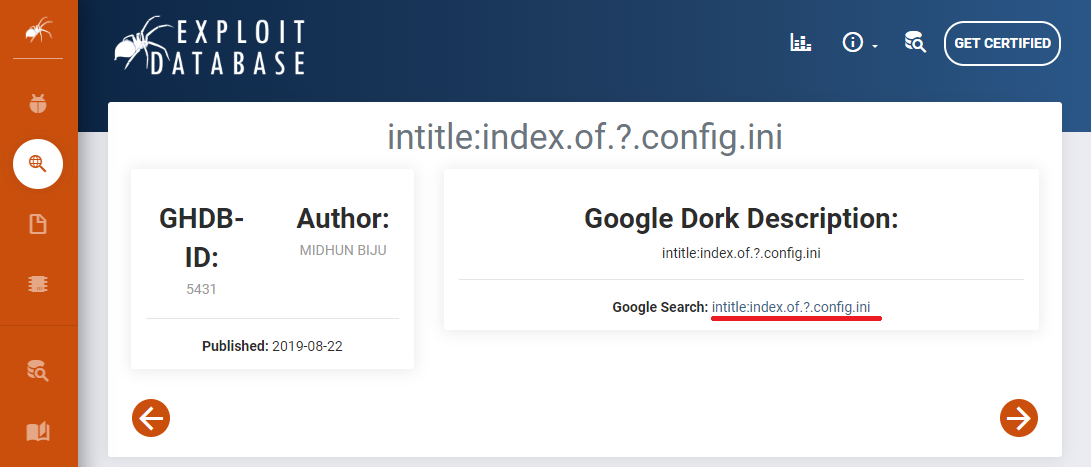


어떤 사이트의 정보를 볼수잇는 여러옵션

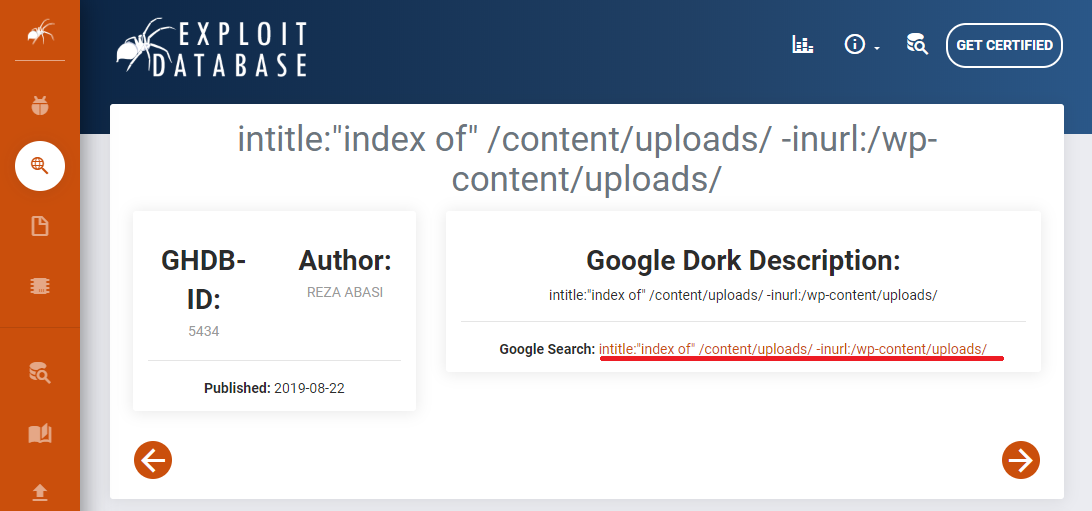


10 페이지

**Exploit-db 를 이용한 GHDB**

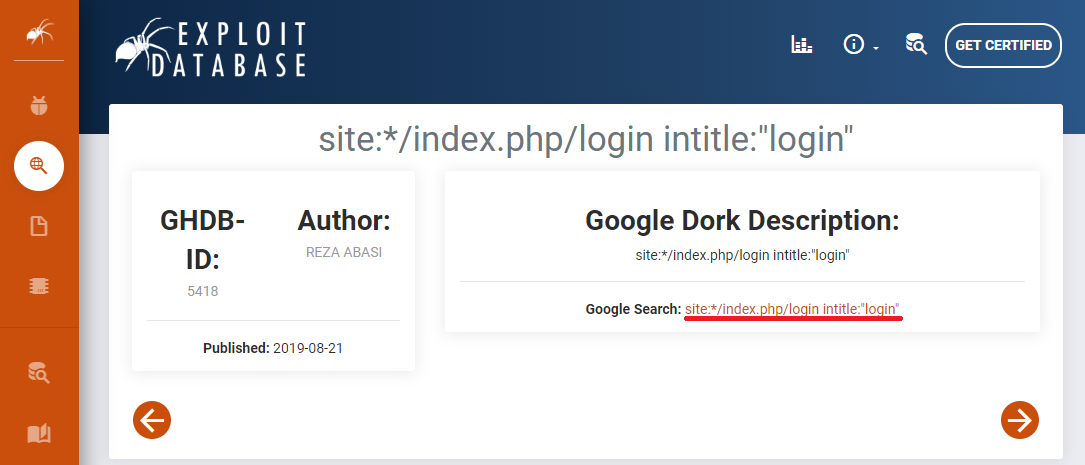


[그림 1-3] Google Search

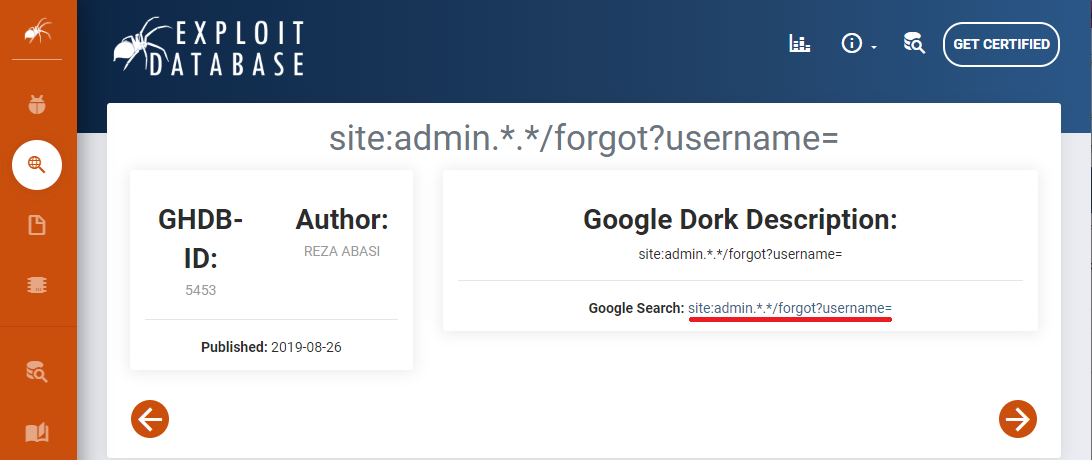


[그림 1-4] Google Search

11 페이지



[그림 1-5] Google Search

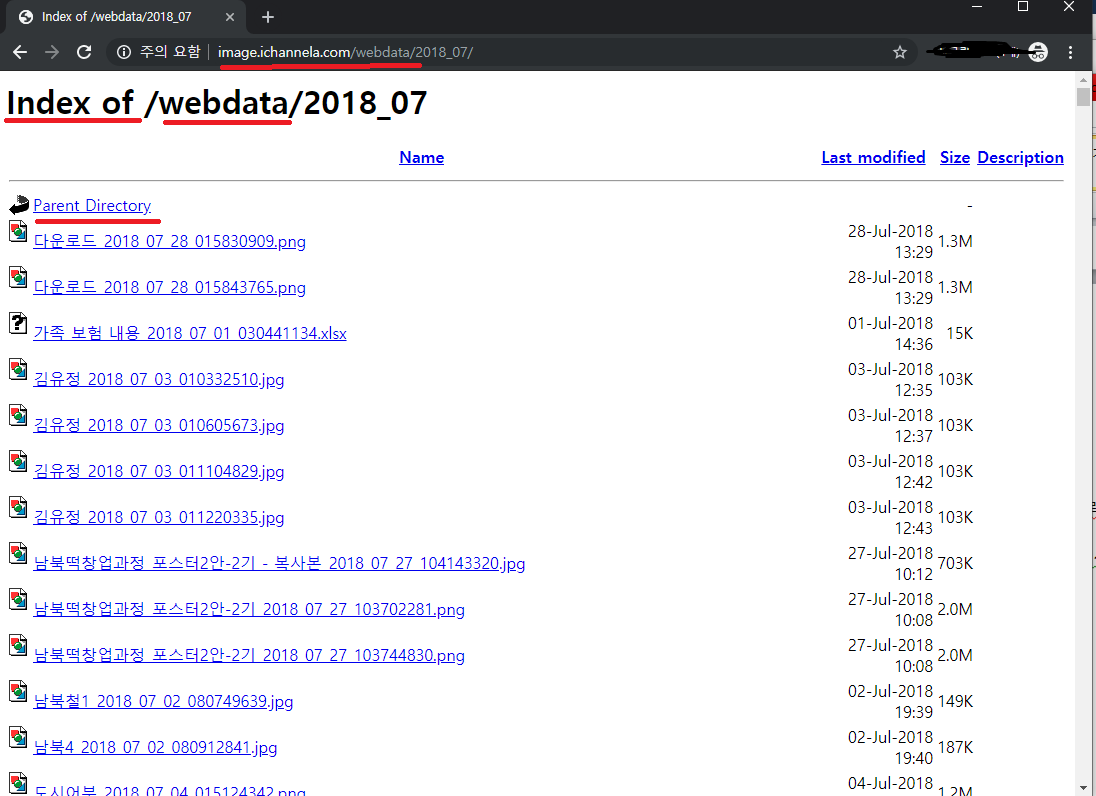


[그림 1-6] Google Search

12 페이지

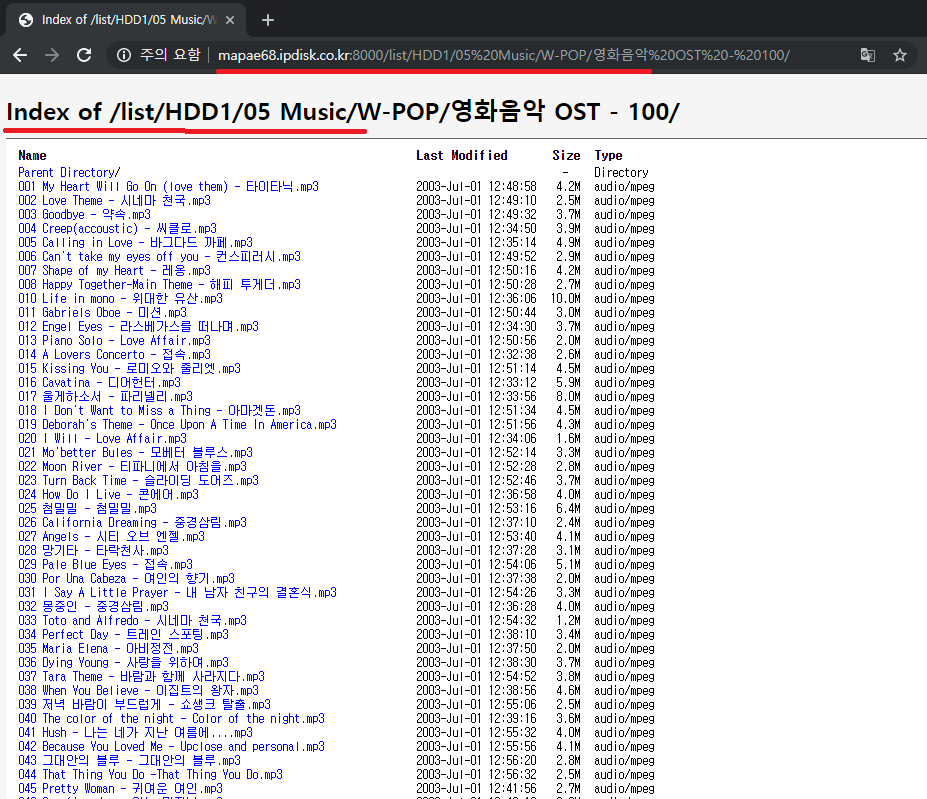
구글 디렉토리 리스팅(취약점)

( 특정 데이터/파일 검색 및 디렉토리 검색 )



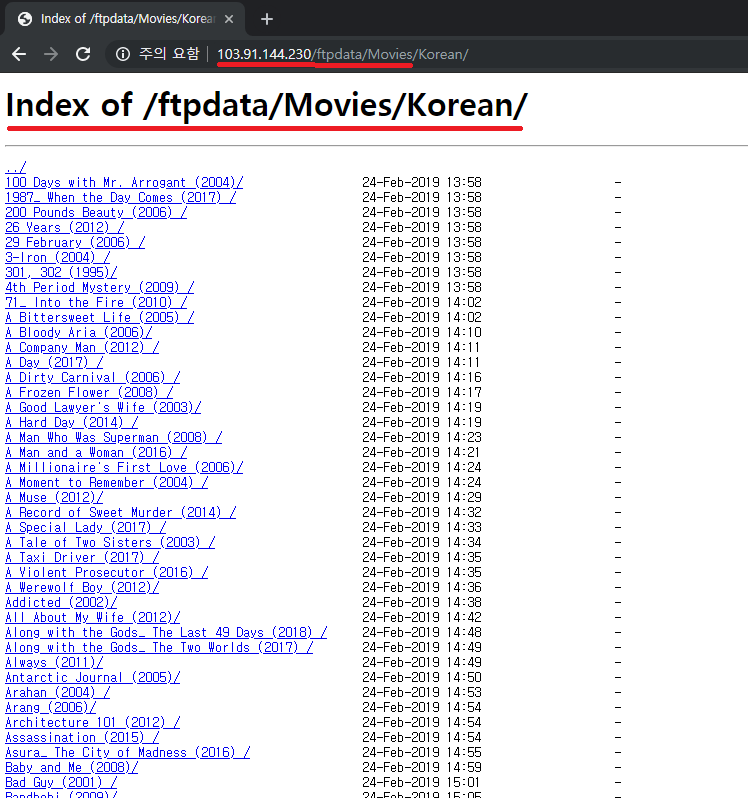
[그림 1-4] GHDB

13 페이지



[그림 1-5] GHDB

14 페이지



[그림 1-6] GHDB

15 페이지