

Week 27_

구글해킹으로 계정 정보 알아내기

Refactoring Study

2022.06.01 Kwon Moonjeong

inurl:/wp-content/uploads/ ext:txt "username" AND "password" | "pwd" | "pw"

- Wordpress : 콘텐츠 관리 시스템(Content Management System)의 한 종류
- Wordpress의 계정 정보를 찾는 구글 검색문으로, 계정 탈취 및 로그인에 성공할 경우 Wordpress로 제작된 홈페이지의 모든 정보에 접근 및 수정하는 권한을 가질 수 있음

← → ↻ charterslawfirm.com/wp-content/uploads/2015/04/Sawchuck-apr25.txt
업 Union SQL Injectio... 상물관제 접근해보... T Dig(DNS 조회) 메모용 ASCII to a String KISA 후이즈검색 w... [Network] HTTP 해... OpenSSL 취약:

what is the username and password for http://www.sawchuckwealth.com/wp-login.php?redirect_to=/clientt/private-client-section-home-page/

wp-login details

username: admin
pwd: 73osrx\$V7

Ftp login details

host: ftp.ord1-1.websitesettings.com
username: terrysaw98xx
pwd: ef6&SGcU!

← → ↻ 주의 요함 | ostademusic.com/wp-content/uploads/2014/09/pass.txt
업 Union SQL Injectio... 상물관제 접근해보... T Dig(DNS 조회) 메모용 ASC

host
http://www.ostademusic.com:2082

Username: ostademu
Password: 4x9p0A3oPm

webmail: http://www.ostademusic.com:2095
info@ostademusic.com
http://www.ostademusic.com:2095/cpsess795403767/horde/login.php
.....
Aweber

Your login name is : arvin37
Your password is : NSF6Gkzms

wordpress user:

username: manager
password: 9c3tWYTAP!VQ
G0DG0DG0037payline

wordpress administrator:

username: u@arsh.omic84
password: G0DG003737

email:

login url: webmail.ostademusic.com or ostademusic.com:2095

username: info@ostademusic.com
password: R2IK(WJciiC#

UA-363803958-1

inurl:password site:shodan.io

- Shodan : 라우터, 스위치, FTP, 특정 웹 서버(Apache, IIS 등)에 대한 정보를 수집하여 결과를 보여주는 서비스를 제공하는 웹사이트 취약점 진단용으로 외부사이트에 의한 시스템 운영정보 노출 여부 확인 가능
- Shodan으로 사용자 이름이 **admin**, 비밀번호가 **1234**인 서버를 찾을 수 있음

Shodan search results for the query `name:admin password:1234`.

TOTAL RESULTS
3,633

TOP COUNTRIES

Country	Count
Taiwan	2,496
Thailand	290
United States	228
Spain	74
Italy	53
More...	

TOP PORTS

Port	Count
8080	2,806
80	335
9000	62
88	54

401 Unauthorized

HTTP/1.0 401 Unauthorized
Date: Thu, 19 May 2022 07:41:23 GMT
Server: Bob/0.94.14rc21
Accept-Ranges: bytes
Connection: Keep-Alive
Keep-Alive: timeout=10, max=1000
WWW-Authenticate: Basic realm= "Default Name=admin Password=1234"
Content-Type: text/html

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

Login Form:

로그인
http://150.116.142.221:8080/
이 사이트의 연결은 제공자가 아닙니다.
사용자이름:
비밀번호:
로그인 취소

inurl:password site:shodan.io

- Shodan으로 계정 정보 입력 없이 접근 가능한 FTP 서버도 찾을 수 있음

The screenshot displays the Shodan search interface. The search bar contains the query `230 Any password will work port: 21`. The results page shows 1,598 total results. A map highlights the top countries, with the United States being prominent. A detailed view of a result for IP `198.91.94.102` is shown, including a screenshot of a terminal window connecting to the FTP server.

Search Query: `230 Any password will work port: 21`

Total Results: 1,598

TOP COUNTRIES: United States, Chicago

198.91.94.102 2022-05-19T07:08:11.659011

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

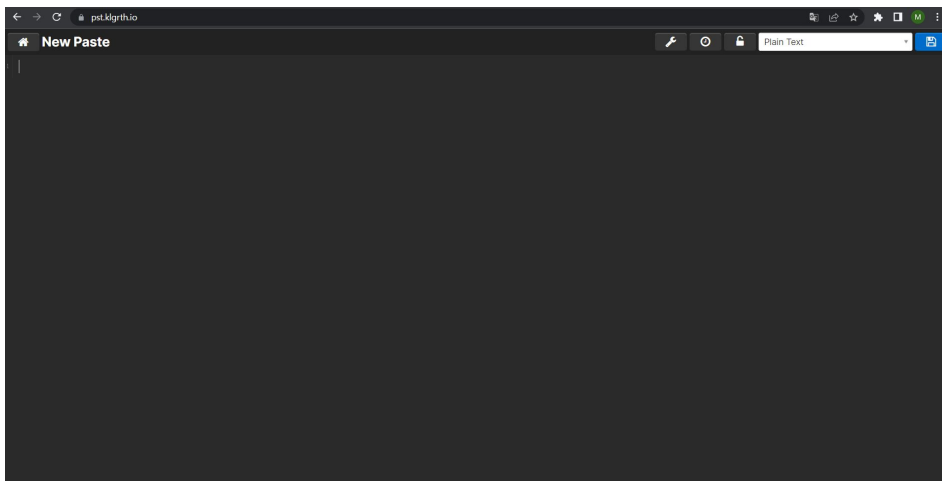
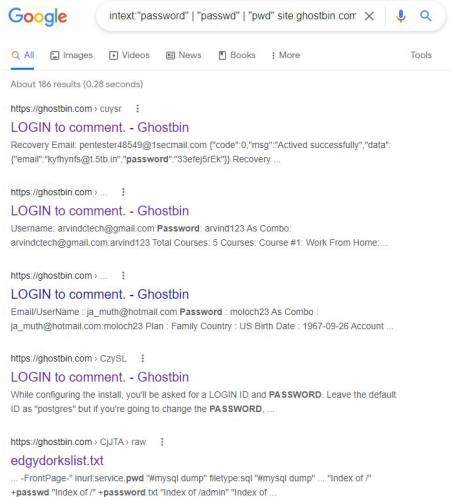
Terminal Output:

```
Microsoft Windows [Version 10.0.17763.316]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users#\0300053>ftp 198.91.94.102
198.91.94.102에 연결되었습니다.
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 3 of 50 allowed.
220-Local time is now 03:18. Server port: 21.
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
504 Unknown command
사용자(198.91.94.102:(none)):
```

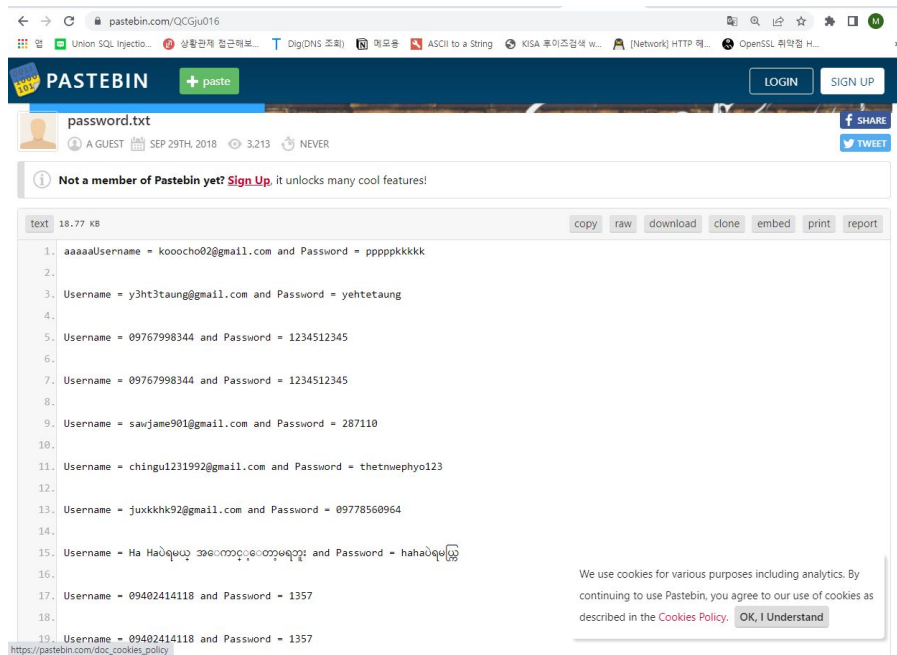
intext:"password" | "passwd" | "pwd" site:ghostbin.com

- Ghostbin은 2013년에 시작된 붙여넣기 서비스를 제공하는 웹사이트로, 평문 텍스트를 업로드 및 저장한 다음, 링크를 다른 사람들과 공유할 수 있음
- Ghostbin에 계정 정보를 복사/붙여넣기 한 경우, 구글 캐쉬로 저장되어 구글 검색으로 확인 가능.
→ 크리덴셜 스터핑 공격에 이용 가능



site:pastebin.com intext:pass.txt

- Pastebin은 평문 텍스트 정보만을 저장하고, 이에 대한 서비스를 제공하는 호스팅 서비스임
- 따라서 Pastebin에 계정 정보를 복사/붙여넣기 한 경우, 계정 정보가 평문으로 저장되어 구글 검색으로 확인 가능. → 크리덴셜 스테핑에 이용 가능



allintext:"*.*@gmail.com" OR "password" OR "username" filetype:xlsx

- 지메일 계정이 저장된 엑셀 파일을 발견하는 구글 검색문으로, gmail을 활용하여 생성된 계정을 찾을 수 있음.

CN-JNTU08 BATCh.xlsx [C:\Users\Wo030053\Downloads\W] - Excel				
파일(F) 편집(E) 보기(V) 도움말(H)				
D26				
A	B	C	D	E
1	username	password	firstname	lastname email
2	10081D0003	D6DA62M1	srujan	10081D0003 creativesrujan@gmail.com
3	10081D0004	ZD28WN89	Amarnathreddy	10081D0004 ammupersonalmail@gmail.com
4	10081D0005	83CSX37T	Satya Prasad	10081D0005 asprasad02@gmail.com
5	10081D0009	K3HEC346	Revanth	10081D0009 revanth4now@gmail.com
6	10081D0011	8KP8JJ13	Krishna Chaitanya	10081D0011 k.krishnachaitanya86@gmail.com
7	10081D0012	W0562XNA	kiran kumar	10081D0012 kiran.msit@gmail.com
8	10081D0014	71VVF53	chalasani L N Chowdary	10081D0014 chalasanil.chowdary2002@gmail.com
9	10081D0017	392E2QHU	Phanindra	10081D0017 phani.pala@gmail.com
10	10081D0018	7SW6V43I	chandra babu	10081D0018 creativechandra@gmail.com
11	10081D0019	YEM3110M	K.RaghavendraChari	10081D0019 raghavendrachari08@gmail.com
12	10081D0020	90Z58IPS	Raghavendra S	10081D0020 1Raghavendra1@Gmail.com
13	10081D0023	L740C5XN	Suman	10081D0023 marthasuman@gmail.com
14	10081D0024	86DD7Y8N	krishna kanth	10081D0024 kewldude.kris@gmail.com
15	10081D0026	3W69YI2Y	uday	10081D0026 uday.mothukuri@gmail.com
16				
17				
18				
19	The usernames and passwords are for Wiki			

allintext:"*.*@gmail.com" OR "password" OR "username" filetype:xlsx

- 본 검색문으로 Gmail 계정은 아니지만, MS Teams 로그인 계정을 발견함. 초기화된 비밀번호를 변경하지 않았다면 이 엑셀 파일의 계정으로 로그인 가능.

change-pasword-request.xlsx [C:\Users\Wo00053\Downloads\W] - 한컴오피스 한글 2014 VP 님대

파일(F) 편집(E) 보기(V) 도움말(H)

100%

D79 jahangeemoi323@gmail.com

	A	B	C	D	E	F	G	H
	Select Your Issue	If Password Change request Enter your correct MS Teams ID	Student Id No	Full Name	Enter Roll No	Stream	Year	Reset Password
1	Change Password Request	OWAIS18612@maharashtracollege.org	2449733	SHAIKH OWAIS ALTAF HUSSAIN	161	I.T	F.Y (1st year of degree)	Puv63737
2	Change Password Request	MOHSIN16932@maharashtracollege.org	515488	MOHSIN KHAN	619	C.S	T.Y (3rd year of degree)	Dak39553
3	Change Password Request	Husna16132@Maharashtracollege.com	1779180	Husna Mubin Qureshi	121	Arts	S.Y. (2nd year of degree)	Roc36593
4	Change Password Request	Khan MUBSHRA16697@maharashtracollege.org	1525323	Khan mubshra akram	123	Science	S.Y. (2nd year of degree)	Gat39642
5	Change Password Request	ANABIA18075@maharashtracollege.org	2446336	Parmar anabia md sharukh	32	Arts	F.Y (1st year of degree)	Pud54993
6	Change Password Request	MALIKA16021@maharashtracollege.org	1583745	Chaudhary Malika Shahid Hussain	12	Arts	S.Y. (2nd year of degree)	Sof54539
7	Change Password Request	AFROZJAHAN16168@maharashtracollege.org	422360	MUKERI AFROZ JAHAN ABID ALI	101	Arts	T.Y (3rd year of degree)	Has25697
8	Change Password Request	Huda16197@maharashtracollege.org	1823920	Huda Mahadiwala	7	Arts	T.Y (3rd year of degree)	Quc43775
9	Change Password Request	Yusra16799@maharashtracollege.org	1559744	Yusra Nasir Khan	828	BMS	S.Y. (2nd year of degree)	Wuj05544
10	Change Password Request	AYESHA18241@maharashtracollege.org	2536429	Ayesha mujawar	246	Science	F.Y (1st year of degree)	Tob43720
11	Change Password Request	KHAN19191@maharashtracollege.org	1985254	Arshad khan	1355	Commerce	M.Com-II	Kox98299
12	Change Password Request	Saniya19006	2686895	Saniyaa amjad qureshi	52	Arts	F.Y (1st year of degree)	Mah01714

allintext:"*.*@gmail.com" OR "password" OR "username" filetype:xlsx

- 엑셀에 gmail 계정이 포함되어 있어 검색됐던 것

change-pasword-request.xlsx [C:\Users\Wo0300053\Downloads\W] - 한컴오피스 한셀 2014 VP 뷰어

파일(F) 편집(E) 보기(V) 도움말(H)

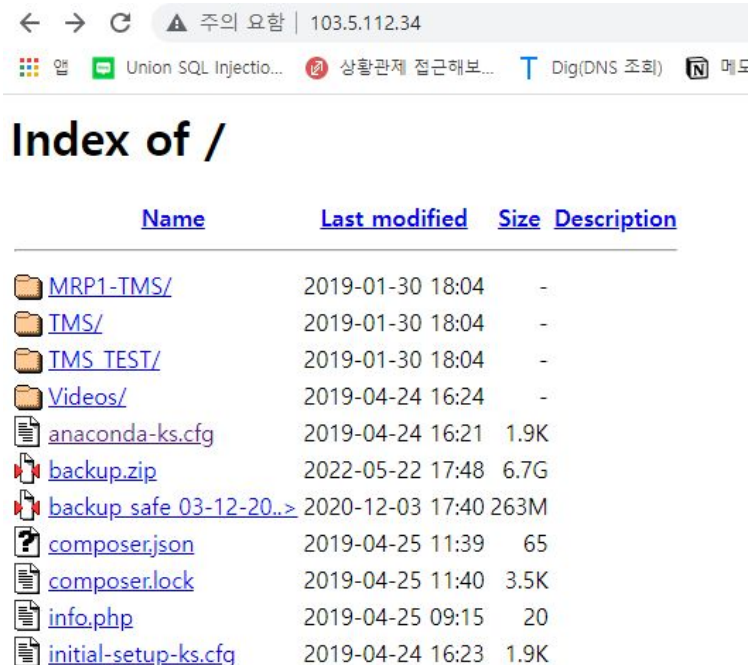
100 %

D79 jahangeermoin323@gmail.com

	A	B	C	D	E	F	G	H
73	Change Password Request	SANYA16704@maharashtracollege.org	1748205	Khan Sanya Firoz	78	Science	S.Y. (2nd year of degree)	Qot50764
74	Change Password Request	RAMZAN16456@maharashtracollege.org	427281	KHAN RAMZAN ANWAR	10	Commerce	T.Y (3rd year of degree)	Soz28028
75	Change Password Request	UMMEKULSUM16026@MAHARASHTRA COLLEGE.ORG	1559226	Ansari umme kulsum mohammed arif.	94	Arts	S.Y. (2nd year of degree)	Suw73489
76	Change Password Request	OSAMA16531@maharashtracollege.org	447547	MUKRI OSAMA DILAWAR	41	Commerce	T.Y (3rd year of degree)	Gog85548
77	Change Password Request	sarahfirdous16058@maharashtracollege.org	1559913	Malik sarah firdous mohammad aziz	27	Arts	S.Y. (2nd year of degree)	Kon84853
78	Change Password Request	MOHDSAHIL18539@maharashtracollege.org	2664737	Mohd Sahil shahabuddin ansari	408	C.S	F.Y (1st year of degree)	Vuz70869
79	Change Password Request	mohinuddin18431@maharashtracollege.org	111	jahangeermoin323@gmail.com	111	Commerce	F.Y (1st year of degree)	Wax15700
80	Change Password Request	GAUSUDDIN16972@maharashtracollege.org	1703689	Shaikh Mohammed gausuddin	260	I.T	S.Y. (2nd year of degree)	Poy83741
81	Change Password Request	SHIFA16643@maharashtracollege.org	1558646	Ansari Shifa Mohammed Arshad	161	Science	S.Y. (2nd year of degree)	Xug22762
82	Change Password Request	HAMZA17133@maharashtracollege.org	1557148	SHAIKH HAMZA MOHD RAFIK YASMIN BANU	249	I.T	S.Y. (2nd year of degree)	Hod37660

intitle:"index of" "anaconda-ks.cfg" | "anaconda-ks-new.cfg"

- Anaconda : 머신러닝이나 데이터 분석 등에 사용하는 여러 가지 라이브러리 패키지가 기본적으로 포함되어있는 파이썬 배포판
- Kickstart는 RedHat Linux 시스템 관리자가 시스템 설치를 자동화하는 데 사용하는 기술으로, anaconda-ks.cfg 파일은 Anaconda를 Redhat Linux에 간편하게 설치할 수 있게 해주는 파일 → anaconda-ks.cfg 파일이 담긴 인덱스에 접근하여 Anaconda의 관리자 비밀번호 (Root Password)를 획득할 수 있음



Name	Last modified	Size	Description
MRP1-TMS/	2019-01-30 18:04	-	
TMS/	2019-01-30 18:04	-	
TMS_TEST/	2019-01-30 18:04	-	
Videos/	2019-04-24 16:24	-	
anaconda-ks.cfg	2019-04-24 16:21	1.9K	
backup.zip	2022-05-22 17:48	6.7G	
backup safe 03-12-20..>	2020-12-03 17:40	263M	
composer.json	2019-04-25 11:39	65	
composer.lock	2019-04-25 11:40	3.5K	
info.php	2019-04-25 09:15	20	
initial-setup-ks.cfg	2019-04-24 16:23	1.9K	

© 2006 The Authors
Journal compilation © 2006 Blackwell Publishing Ltd

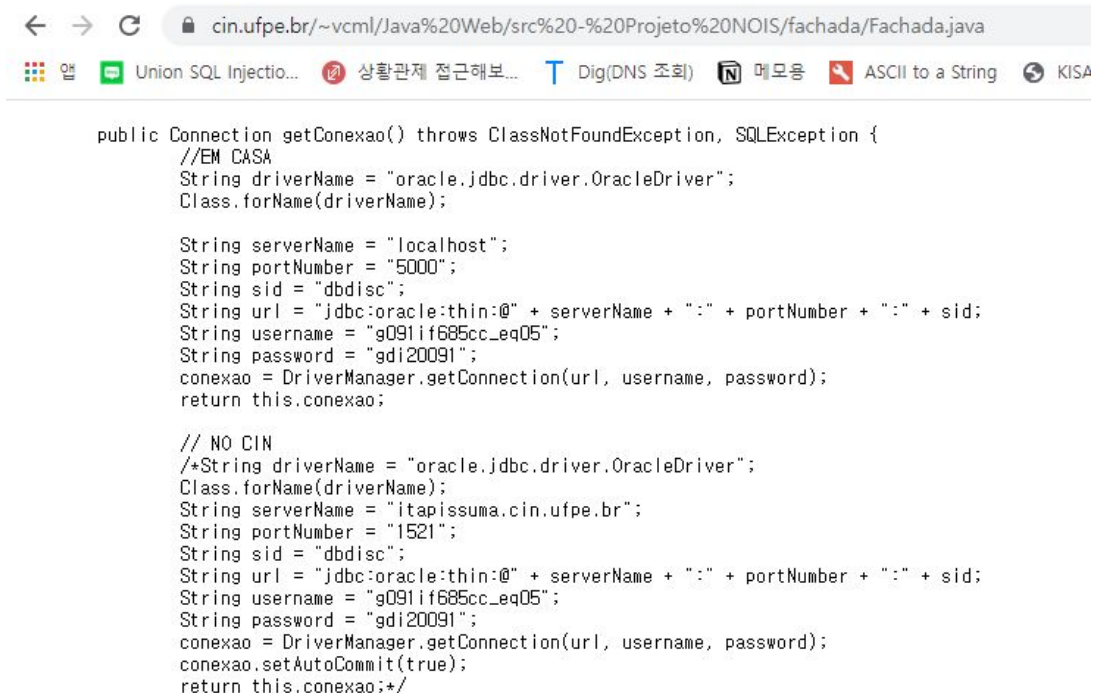
```
#version=DEVEL
# System authorization information
auth --enableshadow --passalgo=sha512
# Use CDROM installation media
cdrom
# Use graphical install
graphical
# Run the Setup Agent on first boot
firstboot --enable
ignoredisk --only-use=sda
# Keyboard layouts
keyboard --vckeymap=in-eng --xlayouts='in (eng)'
# System language
lang en_IN.UTF-8

# Network information
network --bootproto=static --device=enol --gateway=192.168.1.1 --ip=192.168.1.10 --nameserver=4.2.2.2 --netmask=255.255.255.0 --ipv6=auto --activate
network --hostname=localhost.localdomain

# Root password
rootpw --iscrypted $6$kHwZe66dYwlcx/j$.4dQ2B.7mnwiPyruOhIsTEGsBqulB#r#wV7V4aTxNZokMjHv9GygjlbvFM0QVstPB27uGWqaLaYUpfaGZcsjcf/
# System services
services --disabled="chronyd"
# System timezone
timezone Asia/Kolkata --isUtc --nntp
user --groups=wheel --name=muthuramakrishnan --password=$6$WmAr9nfNZJYUnxzs$NfUfQsQnF4XKYNsArSj4S3vin.E4twbHDoFLfgcx/0pubMfQoKlefDrSgLNp1T6gSsdF26JnScIkCXE4oYe/ --iscrypted
--gecos="Muthuramakrishnan"
# X Window System configuration information
xconfig --startxonboot
# System bootloader configuration
bootloader --append=" crashkernel=auto" --location=mbr --boot-drive=sda
autopart --type=lvm
# Partition clearing information
clearpart --all --initlabel --drives=sda
```

intitle:"index of" "anaconda-ks.cfg" | "anaconda-ks-new.cfg"

- JDBC : JAVA로 작성된 프로그램을 DB와 연결하여 데이터를 주고 받을 수 있게 하는 프로그래밍 인터페이스
- Oracle DB와 JAVA 프로그램을 연결하는 과정에서 DB에 로그인할 때 사용할 계정을 하드코딩할 수 있음. 해당 소스 코드가 깃랩에 업로드 되어 있을 경우 구글 검색으로 찾을 수 있음.



```
public Connection getConexao() throws ClassNotFoundException, SQLException {  
    //EM CASA  
    String driverName = "oracle.jdbc.driver.OracleDriver";  
    Class.forName(driverName);  
  
    String serverName = "localhost";  
    String portNumber = "5000";  
    String sid = "dbdisc";  
    String url = "jdbc:oracle:thin:@" + serverName + ":" + portNumber + ":" + sid;  
    String username = "g091if685cc_eq05";  
    String password = "gdi20091";  
    conexao = DriverManager.getConnection(url, username, password);  
    return this.conexao;  
  
    // NO CIN  
    /*String driverName = "oracle.jdbc.driver.OracleDriver";  
    Class.forName(driverName);  
    String serverName = "itapissuma.cin.ufpe.br";  
    String portNumber = "1521";  
    String sid = "dbdisc";  
    String url = "jdbc:oracle:thin:@" + serverName + ":" + portNumber + ":" + sid;  
    String username = "g091if685cc_eq05";  
    String password = "gdi20091";  
    conexao = DriverManager.getConnection(url, username, password);  
    conexao.setAutoCommit(true);  
    return this.conexao;*/
```

"/** MySQL database password */" ext:txt | ext:cfg | ext:env | ext:ini

- 웹에 올려진 환경 구성 파일 중 MySQL DB의 관리자 계정 정보가 있는 파일을 찾는 검색 구문
- 워드프레스의 환경 구성 파일이 많이 검색 됨

```
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

/** MySQL settings - You can get this info from your web host */
/** The name of the database for WordPress */
define('DB_NAME', 'devmilkn_wp220');

/** MySQL database username */
define('DB_USER', 'devmilkn_wp220');

/** MySQL database password */
define('DB_PASSWORD', 'k9Sp815l!@');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

```
<?php
define('WP_HOME', 'https://www.soill.org');
define('WP_SITEURL', 'https://www.soill.org');

/**
 * The base configurations of the WordPress.
 *
 * This file has the following configurations: MySQL settings, Table Prefix,
 * Secret Keys, WordPress Language, and ABSPATH. You can find more information
 * by visiting {@link http://codex.wordpress.org/Editing_wp-config.php Editing
 * wp-config.php} Codex page. You can get the MySQL settings from your web host.
 *
 * This file is used by the wp-config.php creation script during the
 * installation. You don't have to use the web site, you can just copy this file
 * to "wp-config.php" and fill in the values.
 *
 * @package WordPress
 */

/** Define Max Memory Limit */
define('WP_MEMORY_LIMIT', '512M');

/** MySQL settings - You can get this info from your web host */
/** The name of the database for WordPress */
//Added by WP-Cache Manager
//Added by WP-Cache Manager

define('DB_NAME', 'jamied6b_soilldb');

/** MySQL database username */
define('DB_USER', 'jamied6b_soillus');

/** MySQL database password */
define('DB_PASSWORD', '1AB5q?t4');

/** MySQL hostname */
define('DB_HOST', 'localhost:3306');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```