

Module:- SECURITY CONCEPT
(Reconnaissance)
Name:- Prithviraj Nikam

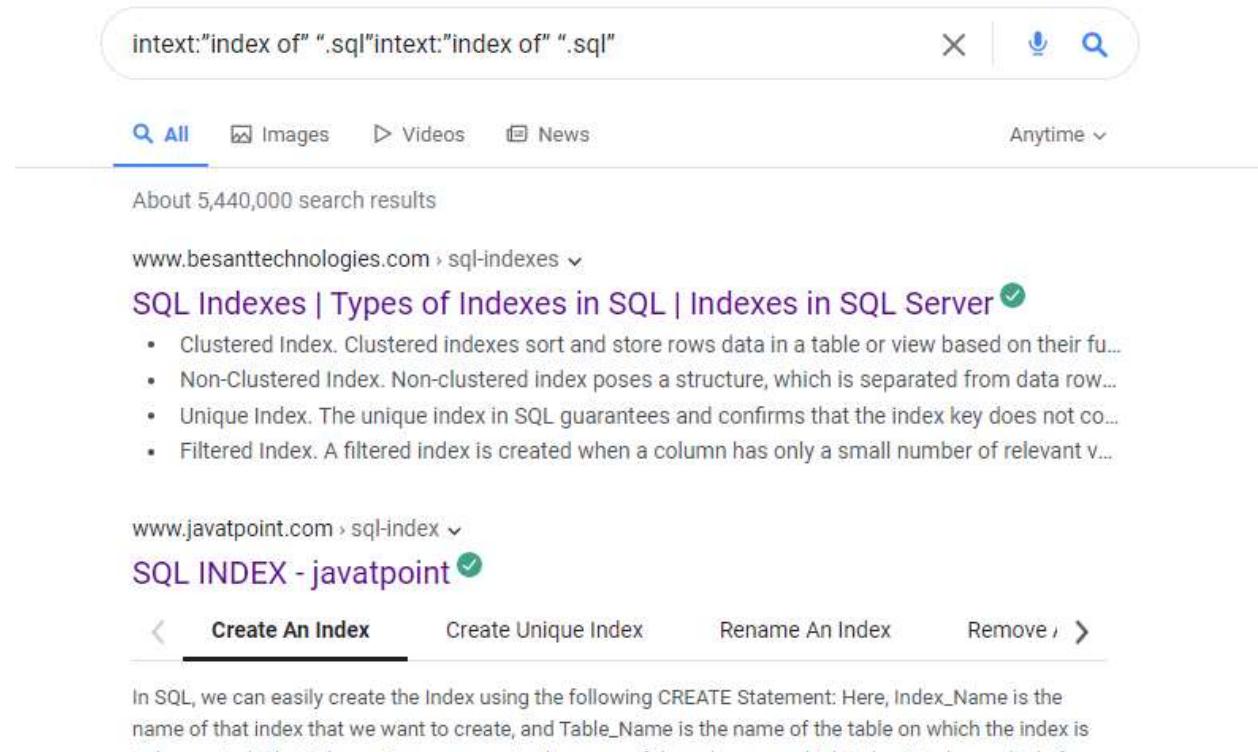
Lab Assignments:

Reconnaissance: This is the first phase where the Hacker tries to collect information about the target. It may include Identifying the Target, finding out the target's IP Address Range, Network, DNS records, etc. Let's assume that an attacker is about to hack a websites' contacts.

1. Execute following Google Dorks and write their short descriptions.

→intext:"index of" ".sql"

It is show the SQL content of web all data



intext:"index of" ".sql" intext:"index of" ".sql"

All Images Videos News Anytime

About 5,440,000 search results

[www.besanttechnologies.com › sql-indexes](http://www.besanttechnologies.com/sql-indexes)

SQL Indexes | Types of Indexes in SQL | Indexes in SQL Server ✓

- Clustered Index. Clustered indexes sort and store rows data in a table or view based on their fu...
- Non-Clustered Index. Non-clustered index poses a structure, which is separated from data row...
- Unique Index. The unique index in SQL guarantees and confirms that the index key does not co...
- Filtered Index. A filtered index is created when a column has only a small number of relevant v...

[www.javatpoint.com › sql-index](http://www.javatpoint.com/sql-index)

SQL INDEX - javatpoint ✓

Create An Index Create Unique Index Rename An Index Remove >

In SQL, we can easily create the Index using the following CREATE Statement: Here, Index_Name is the name of that index that we want to create, and Table_Name is the name of the table on which the index is to be created. The Column_Namerepresents the name of the column on which index is to be applied. If we want to create an index on the combinatio...

[See full list on javatpoint.com](#)

----->intitle:"index of" inurl:superadmin

The screenshot shows a search results page from a web browser. The search query is "intitle:"index of" inurl:superadmin". The results are filtered by "All" and show approximately 119 results in 0.20 seconds. The first result is a directory listing for "https://connect.corover.mobi" under "superadmin". It includes a table with columns for Name, Last modified, and Size, showing files like "addadmin.blade.php" and "addcity.blade.php". The second result is for "https://www.020765.com" under "superadmin", showing an index of files. The third result is for "https://noemata.net" under "superadmin", also showing an index of files.

intitle:"index of" inurl:superadmin

All Images Videos News Books More Tools

About 119 results (0.20 seconds)

<https://connect.corover.mobi> > resources > superadmin

Index of /resources/views/superadmin - CoRover Connect Portal

Name	Last modified	Size
Parent Directory	-	-
addadmin.blade.php	2017-09-11 16:21	4.4K
addcity.blade.php	2017-09-15 11:59	4.2K

[View 23 more rows](#)

<https://www.020765.com> > superadmin

Index of /superadmin

Index of /superadmin. Index of /superadmin. Parent Directory · Superadmin.zip · Superadmin/

<https://noemata.net> > superadmin

Index of /superadmin.etsy - Noemata

Index of /superadmin.etsy. Icon Name Last modified Size Description. [DIR] floppy_files/ 2020-03-20 11:42 - [DIR] fav_files/ 2020-03-20 11:41 - [DIR] ...

—>**intitle:"WAMP SERVER Homepage"**

It is show the how many wamp server are running and its content

intitle:"WAMPSERVER Homepage"



All Images Videos News Anytime

About 368,000 search results

111.68.96.148

WAMPSERVER Homepage - 1|1|1

03/07/2012 · Your Projects. portal; These are your folders in c:/wamp64/www To use them as an http link, you must declare them as VirtualHost

stackoverflow.com › questions › 14727331

wamp - wampserver homepage only visible from localhost ...

Recently I used WAMP server to set up a server environment in a Windows machine. Everything works great, but I have a little problem: everyone can access the wampserver homepage, therefor...

www.inovev.net

Not secure | http://111.68.96.148

Paraphrasing Tool | PDF | CloudFile | Use-cases — YETI 1... | Welcome to YETI's... | Yeti - Your everyday...

WampServer

Server Configuration

Apache Version: 2.4.41 - [Documentation](#)

Server Software: Apache/2.4.41 (Win64) PHP/7.3.12 - Port defined for Apache: 80

PHP Version: 7.3.12 - [Documentation](#)

Loaded Extensions:

• apache2handler	• bcmath
• Core	• ctype
• exif	• fileinfo
• gmp	• hash
• json	• ldap
• mysqli	• openssl
• pdo_sqlite	• Phar
• SimpleXML	• soap
• standard	• tokenizer
• xmlreader	• xmlrpc
• zip	• zlib

MariaDB Version: 10.4.10 - Port defined for MariaDB: 3306 - Default DBMS - [Documentation](#)

MySQL Version: 8.0.18 - Port defined for MySQL: 3308 - [Documentation](#)

→ intitle:"IIS Windows Server"

It show the result about web server(IIS) in windows Server

https://in.search.yahoo.com/search;_ylt=Awr1Qfrs26pjzV0ffAi7HAx;_ylc=X1MDMjExNDcyMzAwMwRfcgMy
Paraphrasing Tool |... PDF https://home.mcafe... CloudFile Use-cases — YETI 1... Welcome to YETI's... H9 Yeti - Your everyday

intitle:"IIS Windows Server"

All Images Videos News Anytime

About 970,000 search results

www.server-world.info › en › note ›

[Windows Server 2019 : IIS : Windows Authentication - Server World](#) ✓
IIS : Windows Authentication (GUI) On GUI configuration, set like follows. Run [Start] - [Server Manager] and enter [Add roles and features], then check a box [Windows Authentication] and insta...

fwedb.gov.pk › 2022/12/18 › iis-windows-server-2016 ›

[Iis windows server 2016 standard free download - Forest ...](#) ✓
18/12/2022 · How To Install IIS In Windows Server Posted by Jarrod on August 24, Leave a comment (17) Go to comments Here we're going to show you how to install the Internet...

—>intitle:"index of" intext:"Apache/2.2.3"

https://in.search.yahoo.com/search;_ylt=AwrKEsNU3apjgiwelxO/HAx;_ylc=X1MDMjExNDcyMzAwMwRfcgMy
Paraphrasing Tool |... PDF https://home.mcafe... CloudFile Use-cases — YETI 1... Welcome to YETI's... H9 Yeti - Your eve

intitle:"index of" intext:"Apache/2.2.3"

All Images Videos News Anytime

About 987,000 search results

yum.baseurl.org › download › 3 ›

[Index of /download/3.2 - yum](#) ✓
Parent Directory - yum-3.2.0-1.src.rpm 16-May-2007 22:09 290K yum-3.2.0.tar.gz 16-May-2007 22:08 281K yum-3.2.1-1.src.rpm 21-Jun-2007 18:57 311K yum-3.2.1.tar.gz 21 ...

downloads.apache.org › httpd ›

[Index of /httpd - The Apache Software Foundation](#) ✓
Apache Http Server Source Code Distributi... Important Notices Downlo >

---->inurl:"index.php?page=news.php"

It is show the news related result(Web page Content)

The screenshot shows a search results page from in.search.yahoo.com. The search query is "inurl:index.php?page=news.php". The results page includes a navigation bar with "All", "Images", "Videos", and "News" tabs, and a date filter set to "Anytime". The search count is "About 1,360,000,000 search results". The first result is a link to "www.exploit-db.com" with the title "inurl:index.php?page=news.php - **Advisories and ...**". The second result is a link to "www.msaaircraft.com" with the title "MSA - Aircraft Products, Inc.". Both results have a green checkmark icon.

inurl:index.php?page=news.php

All Images Videos News Anytime

About 1,360,000,000 search results

[www.exploit-db.com](#) › ghdb › 8029 › inurl:"index.php?page=news.php" - **Advisories and ...** ✓
18/08/2022 · The Exploit Database is maintained by Offensive Security, an information security training company that provides various Information Security Certifications as well as high end...

[www.msaaircraft.com](#) › index › MSA - Aircraft Products, Inc. ✓
MSA Aircraft Products was founded in 1986 and is a leading designer, manufacturer and supplier of highly engineered window systems and associated composite components for use in Business Je...

---->inurl:/sym404/root

It is show the content about root file

The screenshot shows a search results page from in.search.yahoo.com. The search query is "inurl:/sym404/root". The results page includes a navigation bar with "All", "Images", "Videos", and "News" tabs, and a date filter set to "Anytime". The search count is "About 53,700 search results". The first result is a link to "ipaddress.com" with the title "Inurl /sym404/root - Learn more about it - ipaddress.com". The second result is a link to "www.exploit-db.com" with the title "inurl:/sym404/root - Files Containing Juicy Info GHDB Google Dork". Both results have a green checkmark icon.

inurl:/sym404/root

All Images Videos News Anytime

About 53,700 search results

[ipaddress.com](#) › analysis › inurl+ › Inurl /sym404/root - Learn more about it - ipaddress.com ✓
Learn more about Inurl /sym404/root from our Websites analysis here on IPAddress.com.
Websites. root.cz Alexa Rank 159,723 Domain WHOIS Registered with REG-INTERNET-CZ on...

[www.exploit-db.com](#) › ghdb › 8028 › inurl:/sym404/root - Files Containing Juicy Info GHDB Google Dork ✓

The screenshot shows a web browser window with multiple tabs open. The active tab is for IPAddress.com, displaying information about the URL 'inurl:/sym404/root'. The page includes a header with the site's logo and name, followed by a main content area with sections for 'Websites' and 'ROOT.CZ'. Under 'ROOT.CZ', it shows Alexa Rank (159,723), Domain WHOIS details (registered on Oct 27, 1998, updated on Feb 12, 2019, expires on Oct 29, 2023), and IP addresses (IPv4: 91.213.160.188, IPv6: 2001:67c:68::76).

Inurl /sym404/root

Learn more about "**Inurl /sym404/root**" from our Websites analysis here on IPAddress.com

Websites

ROOT.CZ

Alexa Rank
159,723

Domain WHOIS
Registered with REG-INTERNET-CZ on October 27, 1998
WHOIS updated on February 12, 2019
Domain expires on October 29, 2023

IPv4 Address
91.213.160.188 • cz Czechia (CZ)

IPv6 Address
2001:67c:68::76 • Vienna Vienna 1040, AT Austria (AT)

--->inurl:viewer/live/index.html

It is show the content or result of all index.html file that file is live and viveable

Assignment | Shodan Search Engine | inurl:viewer/live/index.html - Yahoo | +

← → C ⌂ https://in.search.yahoo.com/search;_ylt=AwrPpHLh3qpjI9Ue2Jy7HAx;_ylc=X1MDMjExNDcyMzAwMwRf

Paraphrasing Tool | PDF https://home.mcafee... CloudFile Use-cases — YETI 1... Welcome to YETI's... H9 Yeti - Your ever

inurl:viewer/live/index.html

All Images Videos News Anytime

About 20,300,000 search results

www.exploit-db.com › ghdb › 8019

[inurl:viewer/live/index.html - Various Online Devices GHDB ...](#) ✓
17/08/2022 · The Exploit Database is maintained by Offensive Security, an information security training company that provides various Information Security Certifications as well as high end...

219.111.32.218 › viewer › live

[VB Viewer - 219.111.32.218](#) ⓘ
Your web browser is not supported. ... User Name:

forums.anandtech.com › threads › inurl-view-index

[inurl:/view/index.shtml | AnandTech Forums: Technology ...](#) ✓
10/09/2007 · I've seen things like this before, pretty damn cool. I was watching traffic in Japan last time I messed around with this stuff.

Assignment | Shodan Search Engine | inurl:viewer/live/index.html - Yahoo | inurl:view/index.shtml | AnandTech | +

← → × ⌂ https://forums.anandtech.com/threads/inurl-view-index.shtml.84586/

Paraphrasing Tool | PDF https://home.mcafee... CloudFile Use-cases — YETI 1... Welcome to YETI's... H9 Yeti - Your everyday... Harpoon: an OSINT...

≡ ANANDTECH Search...

Featured Home Forums

Trending

Search forums:

What's new

inurl:/view/index.shtml

BrokenVisage · Sep 10, 2007

Forums > Social > OT Discussion Club

 BrokenVisage Lifer 	Sep 10, 2007 Copy and paste "inurl:/view/index.shtml" into Google (with or without the quotes) and it brings up a w Happy snooping. 😊
 Jan 29, 2005	24,769
 10	81

--->intitle:Index of “/venv”

It shows the result or content Virtual environment

The screenshot shows a search results page from in.search.yahoo.com. The search query is "intitle:Index of "/venv"". The results are filtered by "All". There are about 4,070 search results. The top result is a link to "Virtual environnement – MIC-SEC-2022 documentation" with a green checkmark. Below it is a link to "GitHub - jonassorgenfrei/LUMACH-SphinxDemo: Based on: Sphinx..." with a green checkmark. The third result is a link to "Index - GROMACS 2023-rc1 documentation" with a green checkmark.

The screenshot shows the "Virtual environnement" page from sourcesup.renater.fr. The URL is https://sourcesup.renater.fr/www/mic-sec-2022/venv/index.html. The page has a sidebar with navigation links like "MIC-SEC-2022", "Lab-STICC", "Search docs", "CONTENTS:", "Introduction", "Quick start guide", and "Virtual environnement". The main content area has a "Note" section stating "This chapter is not mandatory." It also contains a note about installing tools and a "Prerequisites" section with a note about software requirements.

--->intitle:"WEB SERVICE" "wan" "lan" "alarm"

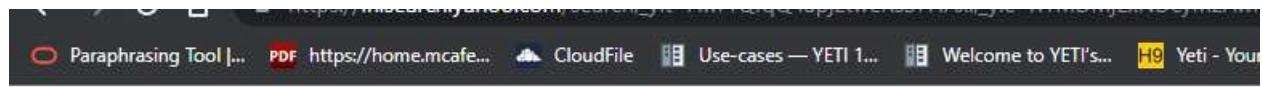
Above content result shows the active web service and wide area network, local area network

The screenshot shows a search results page from a search engine. The search query is "intitle:'WEB SERVICE' 'wan' 'lan' 'alarm'". The results are filtered by "All" and show "About 36 search results".

- 88.247.41.22**
WEB SERVICE ?
PlaybackDisclaimer, Accept Decline, preview; playback; EventSearch; Export; intel; **alarm**
- 202.188.211.194**
WEB SERVICE ?
set; info; exit
- sohometals.com** › xsmzat2p › wan-configuration-huawei
wan configuration huawei - sohometals.com ✓

--->allintitle:"Log on to MACH-ProWeb"

It is show the Login page of Mach-ProWebsite



allintitle:"Log on to MACH-ProWeb"

X |

All Images Videos News Anytime

About 813,000,000 search results

[www.exploit-db.com](#) › [ghdb](#) › 8023

[allintitle:"Log on to MACH-ProWeb" - Pages Containing Login ...](#) ✓

17/08/2022 · Google Dork Description: # Google Dork: allintitle:"Log on to MACH-ProWeb" # Pages Containing Login Portals # Date: 13/08/2022 # Exploit Author: HackerFrenzy.

[holyapostles.net](#) › login

[Log on to MACH-ProWeb](#) ✓

Log on to MACH-ProWeb. Please log on to HOLY APOSTLES. User name: Password: Log on.

A screenshot of a web browser window. The address bar shows "Log on to MACH-ProWeb". The main content area displays the MACH-ProWeb login interface. At the top, there is a logo for "MACH-ProWeb™ BUILDING CONTROLLER / WEB SERVER" and a globe icon. Below that is a login form with fields for "User name:" and "Password:", and a "Log on" button. The background of the page is dark.

---->inurl:"admin/default.aspx"

It is show the url and content of default.aspx (active server page)

The screenshot shows a search interface with the query "inurl:admin/default.aspx" entered. Below the search bar, there are filters for "All", "Images", "Videos", and "News". A date range filter "Anytime" is also present. The search results indicate approximately 94,100,000 results. The first result is a link to "Admin Panel : Login - Ministry of External Affairs ...". The second result is a link to "inurl:admin/default.aspx" from "www.exploit-db.com".

---->filetype:reg [HKEY_USERSDEFAULT]

The screenshot shows a search interface with the query "filetype:reg [HKEY_USERSDEFAULT]" entered. Below the search bar, there are filters for "All", "Images", "Videos", "Shopping", "News", and "More". A "Tools" button is also present. The search results indicate about 91 results. The top result is a link to "shell-random/HKEY_USERS--.DEFAULT--AppEvents.reg at ...". Below it, there is a snippet of the file content: "shell-random/dead/Windows XP/notes/event sounds/before/HKEY_USERS--.DEFAULT--AppEvents.reg · Go to file T · Go to line L · Copy path · Copy permalink". Further down, there is another result for "http://web.mit.edu/fastcart/system/mwsystem" with a snippet of the file content: "... [hkey_local_machine\software\mainsoft\rpc] "BaseNumberOfPings"=dword:00000003 "BasePingInterval"=dword:00000078 [hkey_users] ; Entries for comcat.dll ...".

---->intitle:"index of"|"access_token.json"

It is show the content of JavaScript Object Notation (JSON) in intitle:

A screenshot of a search results page. The search query is "intitle:index of access_token.json". The results are filtered to "All" types. There are approximately 66,800,000 search results. The top result is from "www.sitepoint.com" titled "Using JSON Web Tokens with Node.js - SitePoint" with a green checkmark. It includes a snippet of code for retrieving tokens. Below it is a result from "stackoverflow.com" titled "javascript - Get index of a key in json - Stack Overflow" with a green checkmark. It includes a snippet of code for finding a key in a JSON object.

A screenshot of the SitePoint website homepage. The header features the SitePoint logo, navigation links for "Blog", "Discord", and "Forums", and a search bar. Below the header, there are category links: Python, Programming, Mobile, WordPress, PHP, Web, Entrepreneur, and HTML. A "JavaScript" link is highlighted in purple.

A screenshot of a SitePoint article. The title is "Using JSON Web Tokens with Node.js" by Lukas White, published on April 25, 2014. The article has two categories: "Node.js" and "Tools & Libraries". Below the article, there is a "Share" button with icons for Facebook, Reddit, Twitter, LinkedIn, and Email.

---->inurl: /wp-includes/uploads

It is shows the web page uploads content

inurl: /wp-includes/uploads



All

Images

Videos

News

Anytime

About 63,100,000 search results

ipaddress.com › analysis › inurl+ ▾

Inurl /wp-Includes/uploads - Learn more about it

Learn more about **Inurl /wp-Includes/uploads** from our Websites analysis here on IPAddress.com. Websites.uploads.mobi Alexa Rank 431,466 Domain WHOIS Registered with NameCheap, Inc. c

www.exploit-db.com › ghdb › 8018 ▾

inurl: /wp-includes/uploads - Files Containing Juicy Info ...



IPAddress.com

The Best IP Address Tools

Inurl /wp-Includes/uploads

Learn more about "**Inurl /wp-Includes/uploads**" from our Websites analysis here on IPAddress.com.

Websites

UPLOADS.MOBI

Alexa Rank

431,466

Domain WHOIS

Registered with NameCheap, Inc. on May 9, 2020

WHOIS updated on May 14, 2022

Domain expires on May 9, 2023

IPv4 Addresses

104.21.0.179 • us United States (US)

172.67.128.43 • us United States (US)

---->intitle:"index of" "release.sh"

It shows the content release file or repo file

A screenshot of a search results page from a search engine. The search query is "intitle:'index of' 'release.sh'". The results show two main entries:

- repo.anaconda.com** › archive ✓
Index of [repo.anaconda.com] ✓
Filename Size Last Modified SHA256.winzip / - <directory> Anaconda3-2022.10-Linux-aarch64.sh:
534.5M: 2022-10-17 16:15:40 ...
- repo.anaconda.com** › miniconda ✓
Index of [repo.anaconda.com] ✓
These Miniconda installers contain the Conda package manager. Once Miniconda is installed, you can use the conda command to install any other packages and create environments, etc.

---->intitle:"index of" "configure.sh"

This content shows the all index of configuration result

A screenshot of a search results page from a search engine. The search query is "intitle:index of 'configure.sh'". The results show two main entries:

- www.rubydoc.info** › gems › tiny_tds ✓
Top Level Namespace – Documentation for tiny_tds (1.0.4)
Libraries » tiny_tds (1.0.4) » Index » Top Level Namespace. Top Level Namespace Defined Under Namespace. Modules: TinyTds Classes: BuildRecipe Constant Summary collapse ICONV_VERSIO...
- github.com** › apache › nuttx ✓
arm64/pinephone: Add driver for LCD Panel (Xingbangda XBD599)
The Driver Code is derived from my Reverse-Engineering of the PinePhone Display Driver, based on the logs captured from the PinePhone p-boot Bootloader: "Rendering PinePhone's Display (DE and...

---->intitle:"index of" "setup.sh"
Shows the information about all setup file

intitle:index of "setup.sh"



All

Images

Videos

News

Anytime

About 49,400 search results

github.com › zmkfirmware › zmk ›

[board_index in setup.sh is null · Issue #1580 · zmkfirmware ...](#)

Hi folks, i just tried to flash my nice!nanos for a new corne keyboard using the config setup script and was getting the error: "Wired split not yet supported"; I choose corne in the keybo...

www.dell.com › support › manuals ›

[Dell PowerProtect Cyber Recovery 19.12 Product Guide](#)

The Cyber Recovery product documentation set, available at Dell Online Support, includes: Dell PowerProtect Cyber Recovery Security Configuration Guide. Dell PowerProtect Cyber Recovery on...

---->intitle:"index of" "*db.sh"
It shows the result of all database content

intitle:index of "*db.sh"



All

Images

Videos

News

Anytime

About 3 search results

docs.rhino.metaswitch.com › ocdoc › books ›

[Rhino Production Getting Started Guide](#)

Scattercast endpoints should be determined in advance for all cluster members. Scattercast uses point-to-point UDP mesh layout for cluster membership.

docs.rhino.metaswitch.com › ocdoc › books ›

[Rhino SDK Getting Started Guide](#)

You only need to be aware of the embedded Derby database if you want to remove all state from the SDK (using the init-management-db.sh script). The Rhino SLEE SDK can optionally be...

—>intitle:"index of" "deploy.sh"

Shows the deployed file content

A screenshot of a search results page from a search engine. The search query is "intitle:index of \"deploy.sh\"". The results show approximately 3,780 search results. The top result is from "www.rubydoc.info" and links to "File: README – Documentation for kuby-core (0.3.0)". Below it is a result from "blog.csdn.net" with the title "前端不同场景下的自动化部署方式_领秀5858的博客-CSDN博客". The interface includes standard search controls like All, Images, Videos, News, and a date range selector.

—>intext:"index of" "ipaddress"

It shows the result of ip address of all index file

A screenshot of a search results page from a search engine. The search query is "intext:index of \"ipaddress\"". The results show approximately 69,700,000 search results. The top result is from "www.exploit-db.com" and links to "intext:\"index of\" \"ipaddress\" - Files Containing Juicy Info ...". Below it is a result from "www.ipaddress.com" with the title "What Is My IP Address? Free IP Lookup". The interface includes standard search controls like All, Images, Videos, News, and a date range selector.

---->intitle:"Device(IP CAMERA)" "language" -com|net

The above content shows the result of ip camera,of all domain

intitle:"Device(IP CAMERA)" "language" -com|net

All Images Videos News Anytime

About 205 search results

sourceforge.net › directory
[sourceforge.net](#)
We would like to show you a description here but the site won't allow us.

en.wikipedia.org › wiki › South_Dakota
[South Dakota - Wikipedia](#)
Since 2019, "the language of the Great Sioux Nation, comprised of three dialects, Dakota, Lakota, and Nakota" is the official indigenous language [106] [6]. As of the 2000 census, 1.90% of the

---->allintext:"username" "password"

It shows the username and password related data

allintext:"username" "password"

All Images Videos News Anytime

About 16,100,000 search results

The Fascinating Science of Allintext Username
Password A plaintext username password is a form of
password sharing. It's a way for people to share the
same username and password without granting full
access to them to other users.



download584.weebly.com

elliott.norushcharge.com/allintext-username-password
[Allintext Username Password : Detailed Login Instructions ...](#)

---->site:https://www.cdac.in/ ext:pdf

It show the pdf file type content that extension is .pdf of domain cdac.in

site:https://www.cdac.in/ ext:pdf



All

Images

Videos

News

Anytime ▾

About 8 search results

www.cdac.in › index ▾

Product Information

Centre for Development of Advanced Computing C-DAC Innovation Park, Panchavati, Pashan, Pune - 411 008, Maharashtra (India) Phone: +91-20-25503100

www.cdac.in › index

Corrigendum - Pre-Submission Meeting clarifications

Expression of Interest for Empanelment of Spokes for FutureSkills PRIME Upskilling Programmes on Emerging Technologies Corrigendum - Pre-Submission Meeting clarifications