Practical 11 Google Dorking for Penetration Testers

What is Google Dork?

-> It is basically a search string the uses advanced search query to find information that are not easily available on the websites. It is also regarded as illegal google hacking activity which hackers often uses for purposes such as cyber ~~terros~~ terrorism and cyber theft.

* Special google search operators.

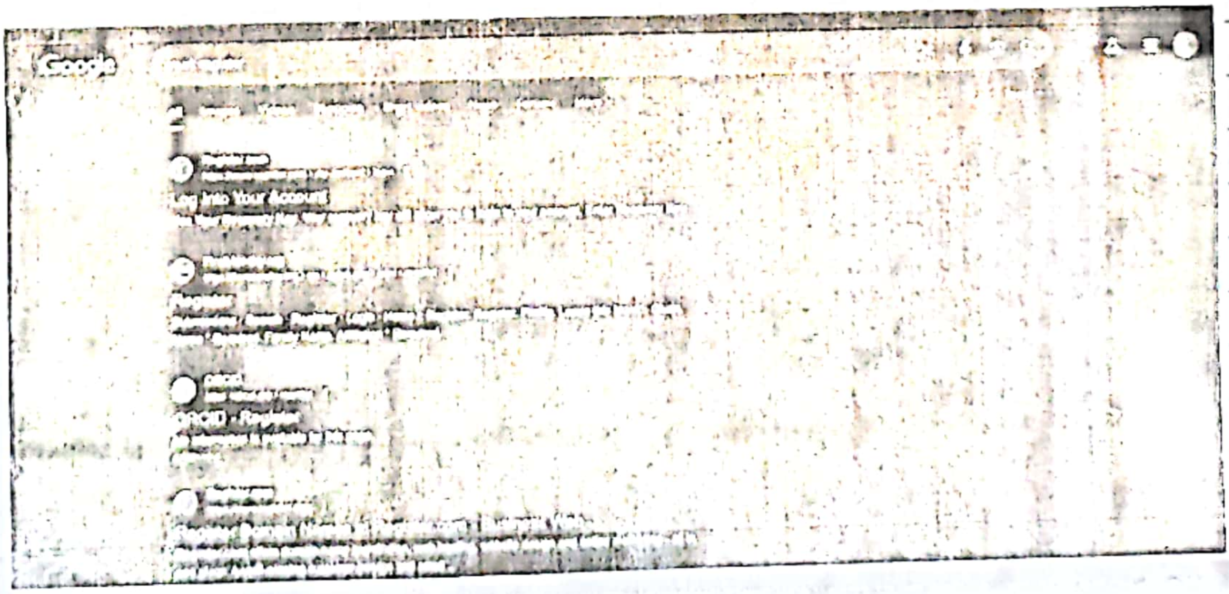
-> Before starting with google dorks, you need to have basic understanding of few special google search operators and also how it functions.

* intitle

This will ask google to show pages that have the term in their html title.

1. inurl:

Searches for specified term in the URL.
For example : inurl:register



Log Into Your Account

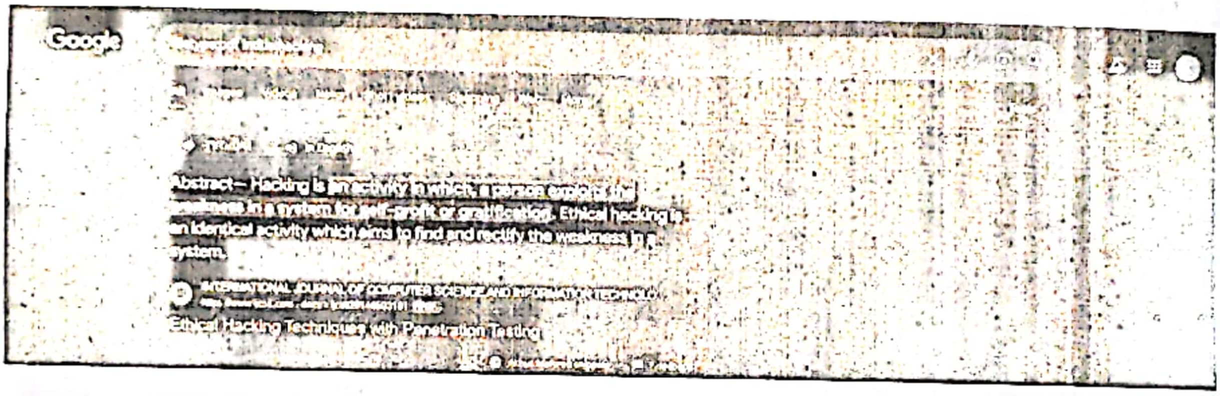
Register

ORCID - Register

2. Filetype:

Searched for certain file type.

Example : filetype:pdf will search for all the pdf file in the websites.



Google

Abstract— Hacking is an activity in which, a person exploits the weakness in a system for self-profit or gratification. Ethical hacking is an identical activity which aims to find and rectify the weakness in a system.

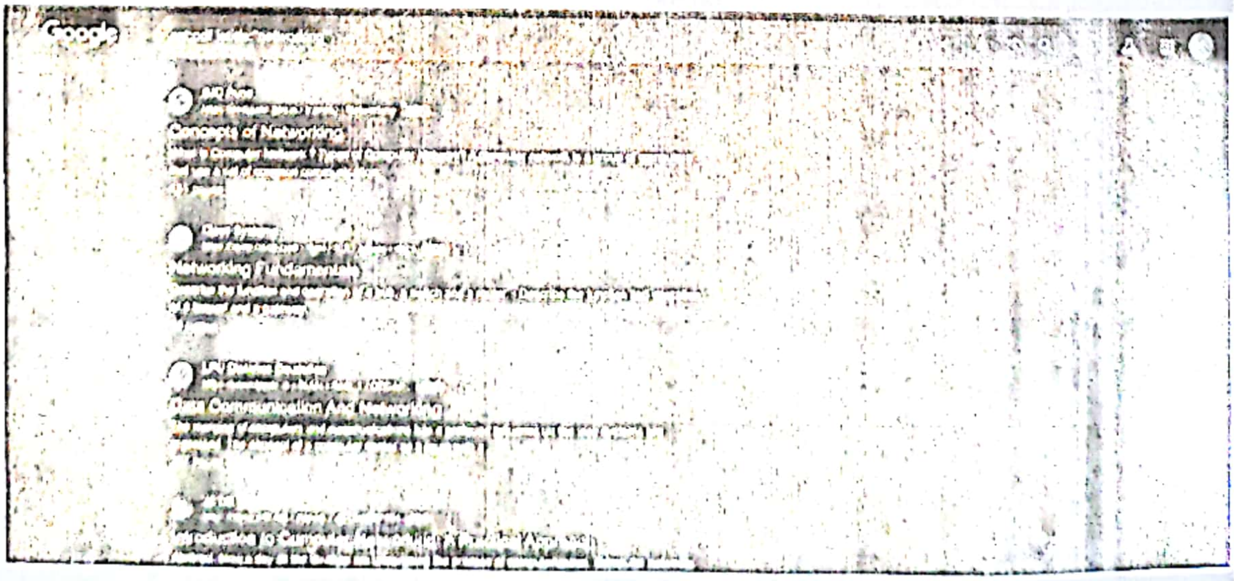
INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND INFORMATION TECHNOLO

Ethical Hacking Techniques with Penetration Testing

3. ext:

It works similar to filetype

Example: ext:pdf finds ~~d~~pdf extension file.



Google

Concepts of Networking

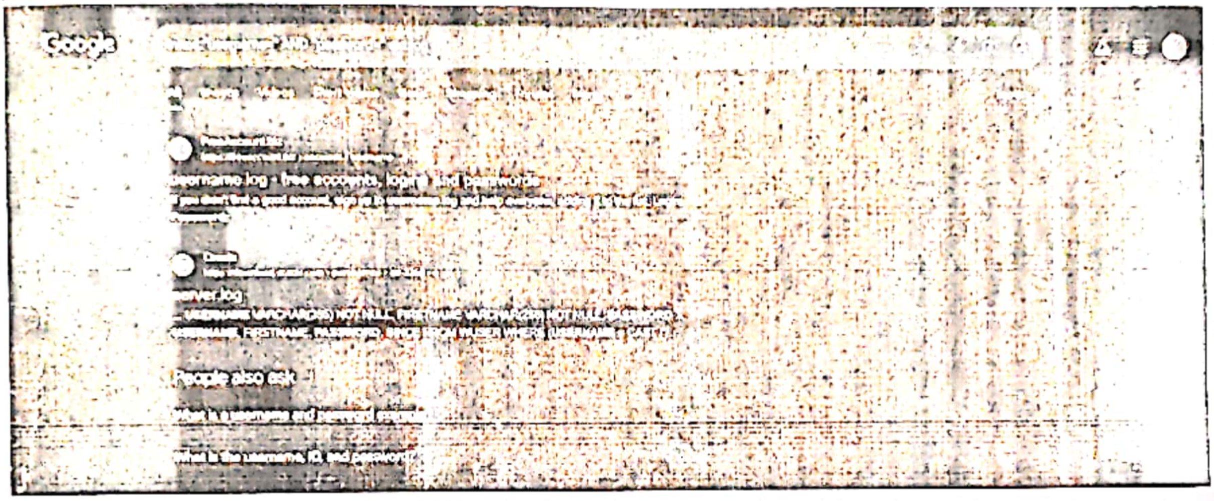
Networking Fundamentals

Data Communication And Networking

Introduction to Computer

4. intext :

This will search content of the page. This works somewhat like plain google search.



username.log - free accounts, logins and passwords

server.log

... USERNAME VARCHAR(255) NOT NULL, FIRSTNAME VARCHAR(255) NOT NULL, PASSWORD ... USERNAME, FIRSTNAME, PASSWORD, SINCE FROM WUSER WHERE (USERNAME = CAST(...

People also ask

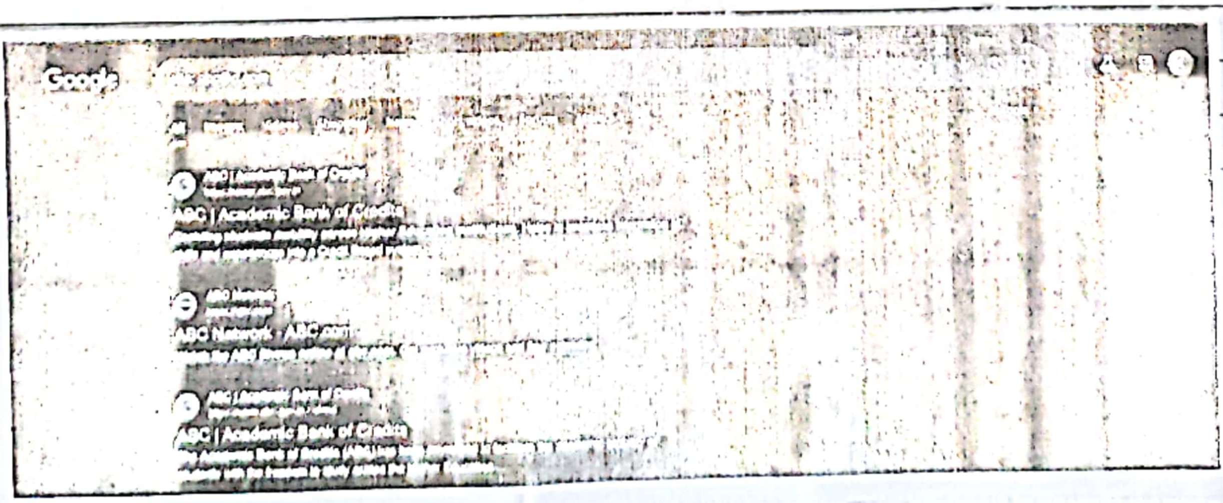
What is a username and password example?

What is the username, ID, and password?

5. site :

This limits the search to a specific site only.

Ex :- site : abc@d.com will limit search to only abc@d.com



ABC | Academic Bank of Credits

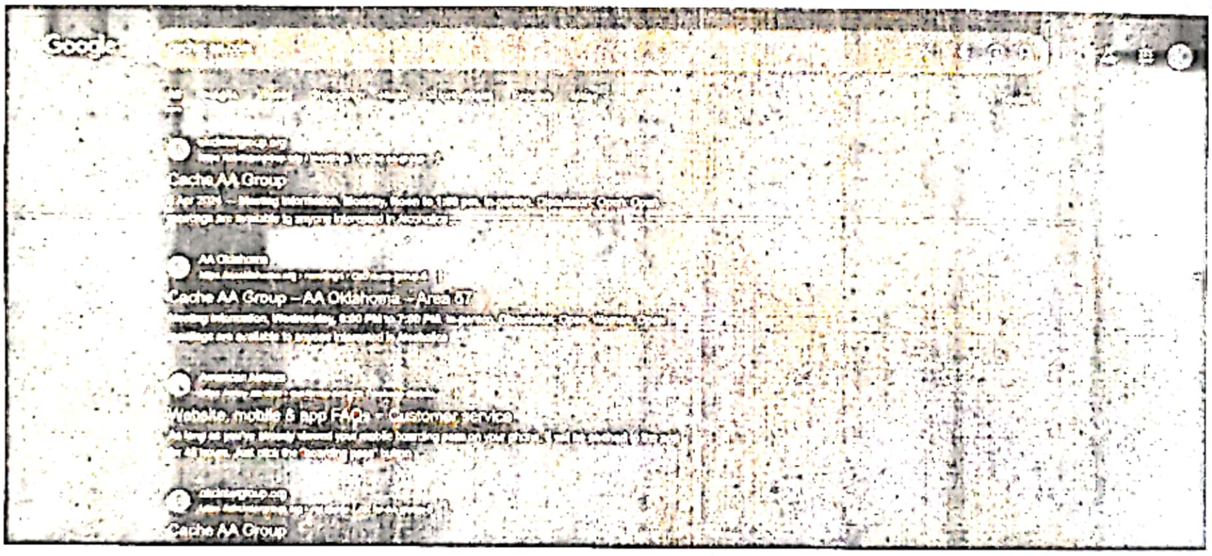
ABC Network - ABC.com

ABC | Academic Bank of Credits

6. Cache :

This will show you cached version of any website.

Ex :- cache:aa.com



[illegible]

Cache AA Group

[illegible] Apr 2024 — Meeting Information, Monday, Noon to 1:00 pm, In-person, Discussion, Open. Open meetings are available to anyone interested in Alcoholics ...

AA Oklahoma

[illegible]

Cache AA Group – AA Oklahoma – Area 57

Meeting Information, Wednesday, 6:30 PM to 7:30 PM, In-person, Discussion, Open, Women, Open meetings are available to anyone interested in Alcoholics

American Airlines

[illegible]

Website, mobile & app FAQs − Customer service

As long as you've already viewed your mobile boarding pass on your phone, it will be cached in the app for 48 hours. Just click the boarding pass button.

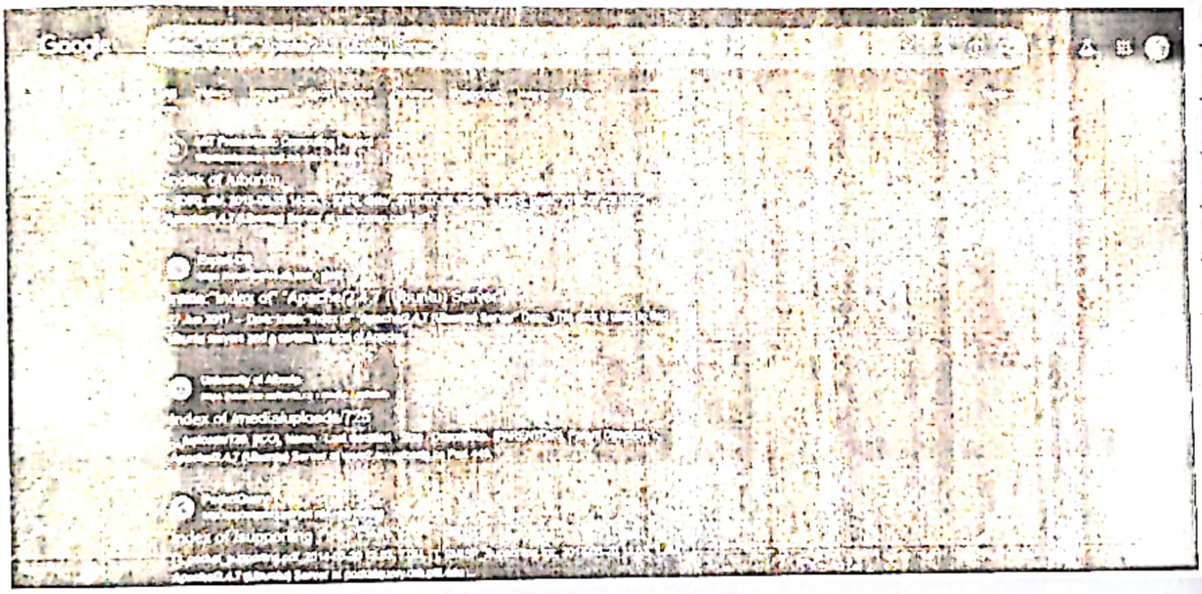
[illegible]

Cache AA Group

* Examples of Google Dorking

1. Finding vulnerable versions of software.

intitle : "index of "Apache/2.4.7 (Ubuntu) Server"



Google

Index of /ubuntu

[illegible]

intitle: "index of" "Apache/2.4.7 (Ubuntu) Server"

[illegible]

Index of /media/uploads/725

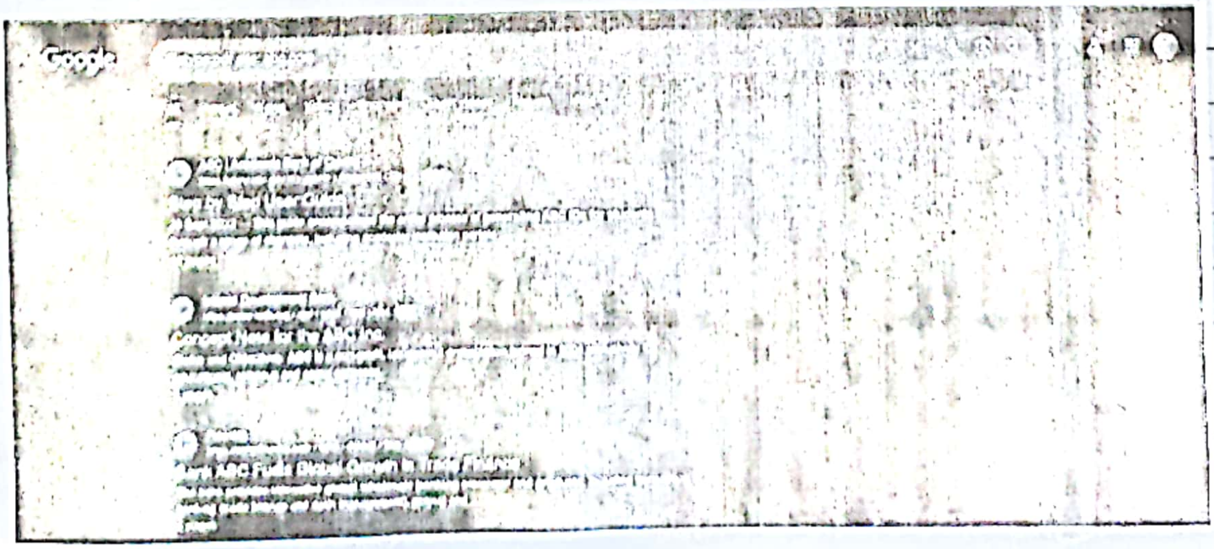
[illegible]

Index of /supporting

[illegible]

2. Finding publicly exposed documents:

filetype : pdf site : abc.com

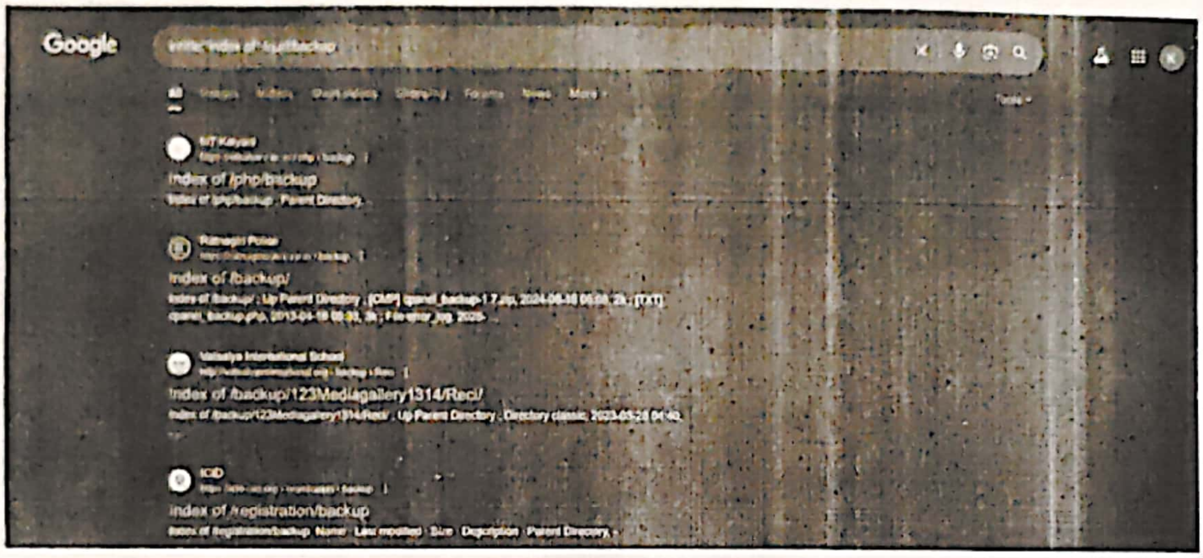


Google

[illegible]

3. Finding exposed directories:

intitle: "index of" inurl: backup



Google

intitle:"index of" inurl:backup

IIIT Kalyani

index of /php/backup

Index of /php/backup . Parent Directory.

Ratnagiri Police

index of /backup/

Index of /backup/ . Up Parent Directory . [CMP] cpanel_backup-1.7.zip, 2024-06-10 06:08, 2k . [TXT] cpanel_backup.php, 2013-04-19 08:03, 3k ; File error_log, 2025- ...

Vatsalya International School

Index of /backup/123Mediagallery1314/Reci/

Index of /backup/123Mediagallery1314/Reci/ . Up Parent Directory . Directory classic, 2023-03-28 04:40.

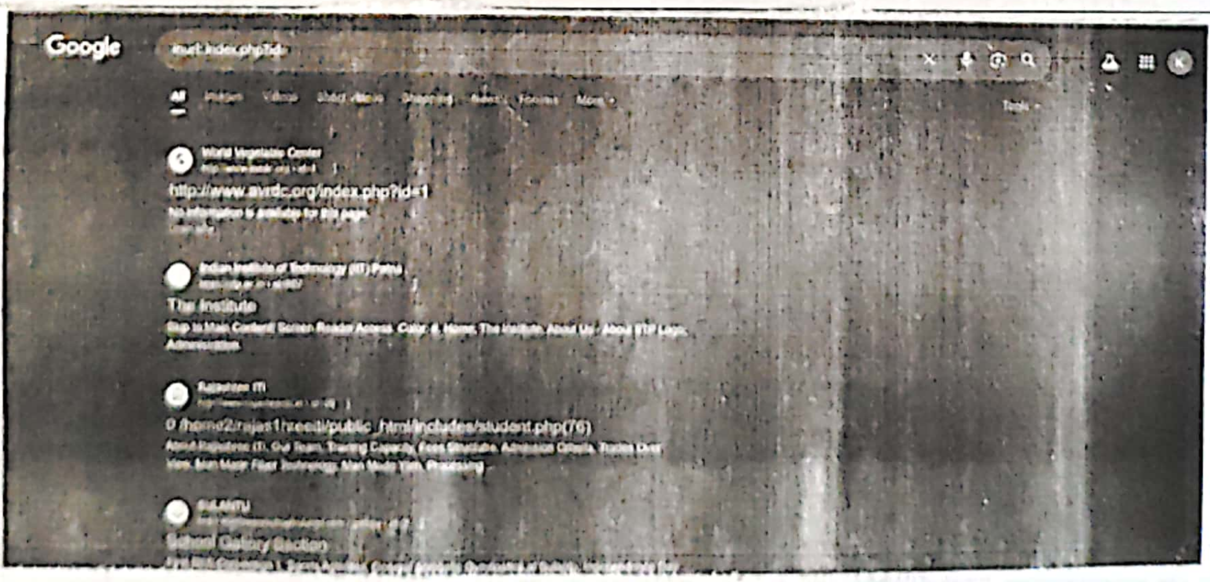
ICID

index of /registration/backup

Index of /registration/backup. Name · Last modified · Size · Description · Parent Directory. ·

4. Finding SQL injection vulnerabilities:

inurl : index.php?id =



Google

inurl:index.php?id=

World Vegetable Center

http://www.avrdc.org/index.php?id=1

No information is available for this page.

Indian Institute of Technology (IIT) Patna

The Institute

Skip to Main Content| Screen Reader Access. Color: . Home; The Institute. About Us · About IITP Logo. Administration.

Rajasthan ITI

0 /home2/rajast1hreeiti/public_html/includes/student.php(76)

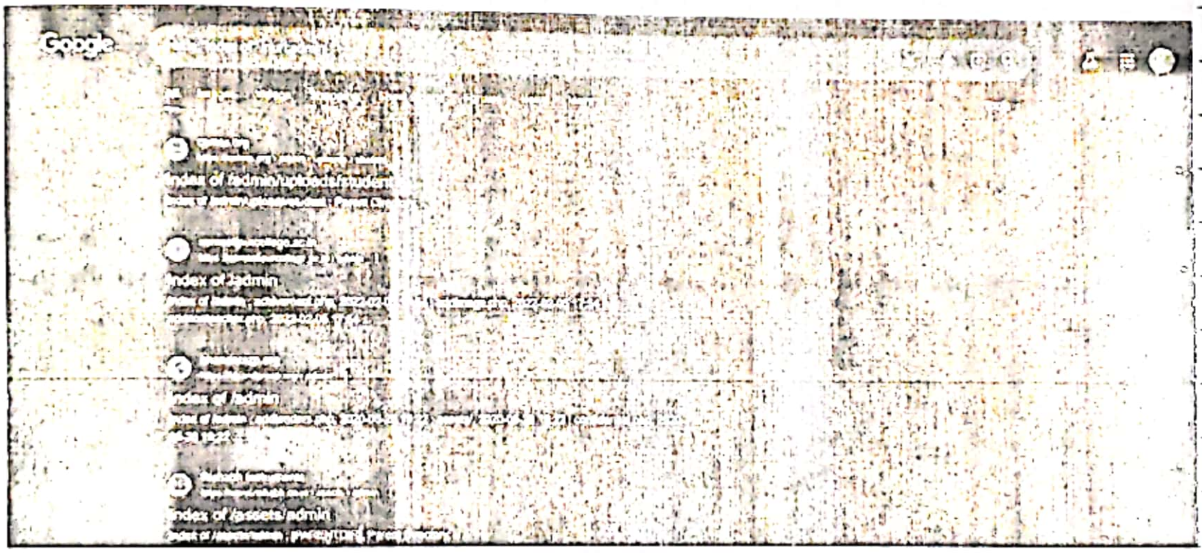
About Rajasthan ITI, Our Team, Training Capacity, Fees Structure, Admission Criteria, Trades Over View, Man Made Fiber Technology, Man Made Yarn, Processing

SULANTU

School Gallery Section

5. Finding sites with exposed directories that may contain sensitive files:

intitle: "Index of" inurl: admin



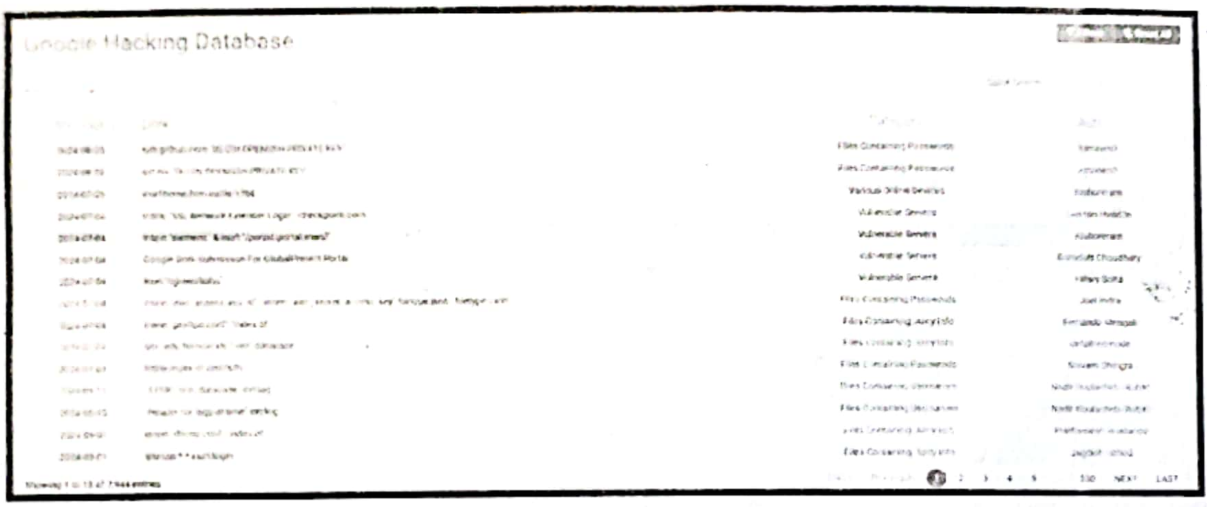
Index of /admin/uploads/studen

Index of /admin

Index of /admin

Index of /assets/admin

The Google Hacking Database (GHDB)



Google Hacking Database

[illegible]	Dork	Category	Author
2024-08-05	[illegible]	Files Containing Passwords	[illegible]
[illegible]	[illegible]	Files Containing Passwords	[illegible]
2024-07-29	[illegible]	Various Online Devices	[illegible]
2024-07-04	intitle:"SSL Network Extender Login" -checkpoint.com	Vulnerable Servers	[illegible]
2024-07-04	[illegible]	Vulnerable Servers	[illegible]
2024-07-04	Google Dork Submission For GlobalProtect Portal	Vulnerable Servers	[illegible] Choudhary
2024-07-04	[illegible]	Vulnerable Servers	[illegible]
[illegible]	[illegible]	Files Containing Passwords	[illegible]
[illegible]	[illegible] "index of"	Files Containing Juicy Info	Fernando [illegible]
[illegible]	[illegible]	Files Containing Juicy Info	[illegible]
[illegible]	[illegible]	Files Containing Passwords	[illegible]
[illegible]	[illegible]	Files Containing [illegible]	[illegible]
[illegible]	[illegible]	Files Containing [illegible]	[illegible]
[illegible]	[illegible]	Files Containing [illegible]	[illegible]
[illegible]	[illegible]	Files Containing Juicy Info	[illegible]

Showing 1 to 15 of 7,944 entries