|  |  |
| --- | --- |
| NAME: VAISHNAVI PARULEKAR | ROLL ID: 22203A0048 |
| COURSE:CO (COMPUTER ENGINNERING) | Task Assignment: Task Assignment: Identifying Vulnerable Sites Using Google Dorks |
| COMPANY: SECURER CYBER FUTURE | COLLEGE: VIDYALANKAR POLYTECHNIC |

REPORT

**Task Assignment: Identifying Vulnerable Sites Using Google Dorks**

**A list of the 5 identified vulnerable websites.:**

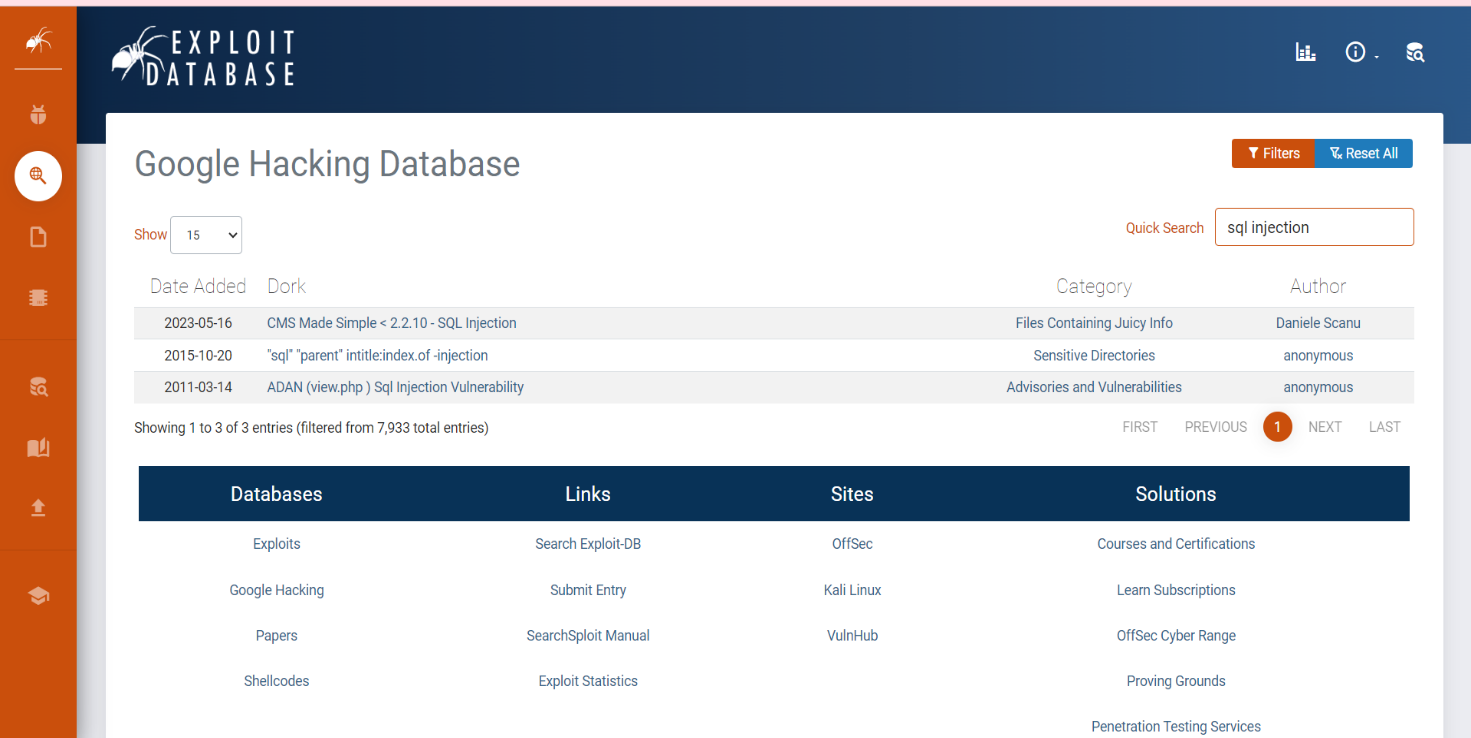
* SQL injection
* Files containing password of Gmail
* Admin login page
* Network or Vulnerability data
* Vulnerable servers

**The specific Google Dorks used to find these vulnerabilities.:**

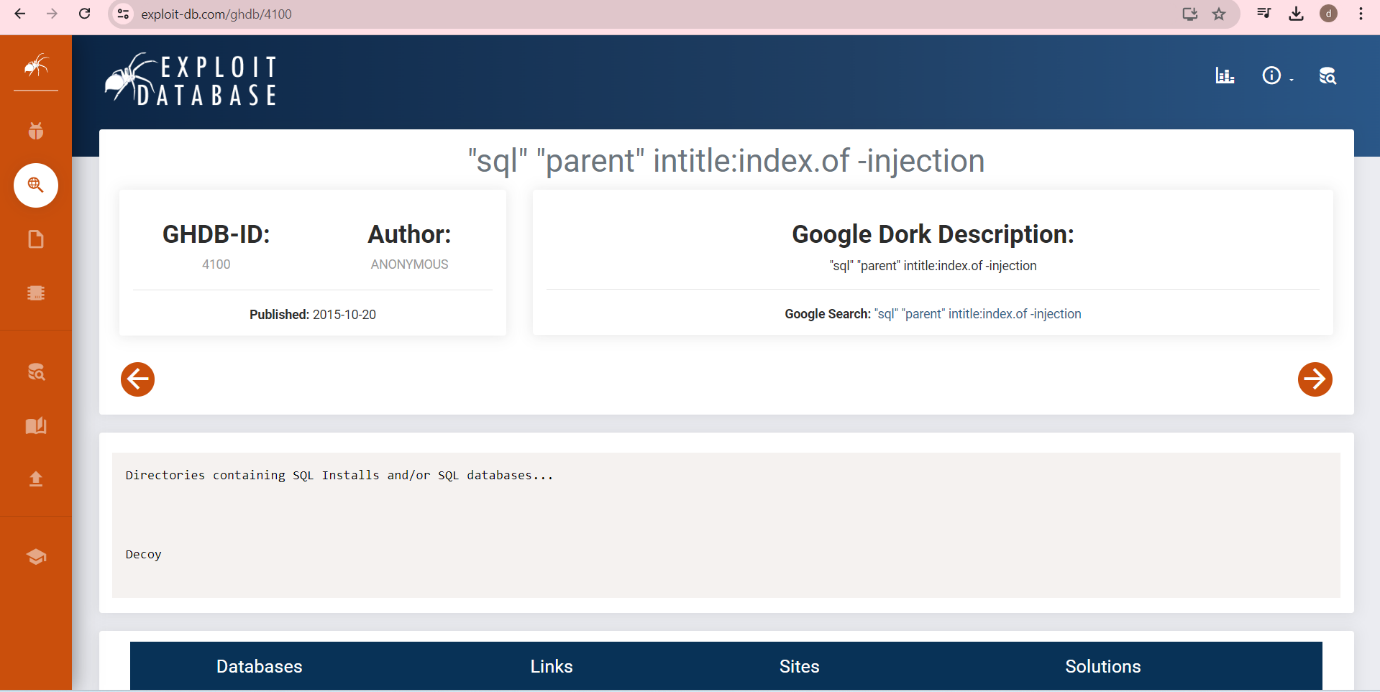
* SQL injection: - intitle: index. of
* Files containing password of Gmail: - site:
* Admin login page: - inurl:
* Network or Vulnerability data: - intext:
* Vulnerable servers: filetype

**Detailed descriptions of the vulnerabilities found on each site.**

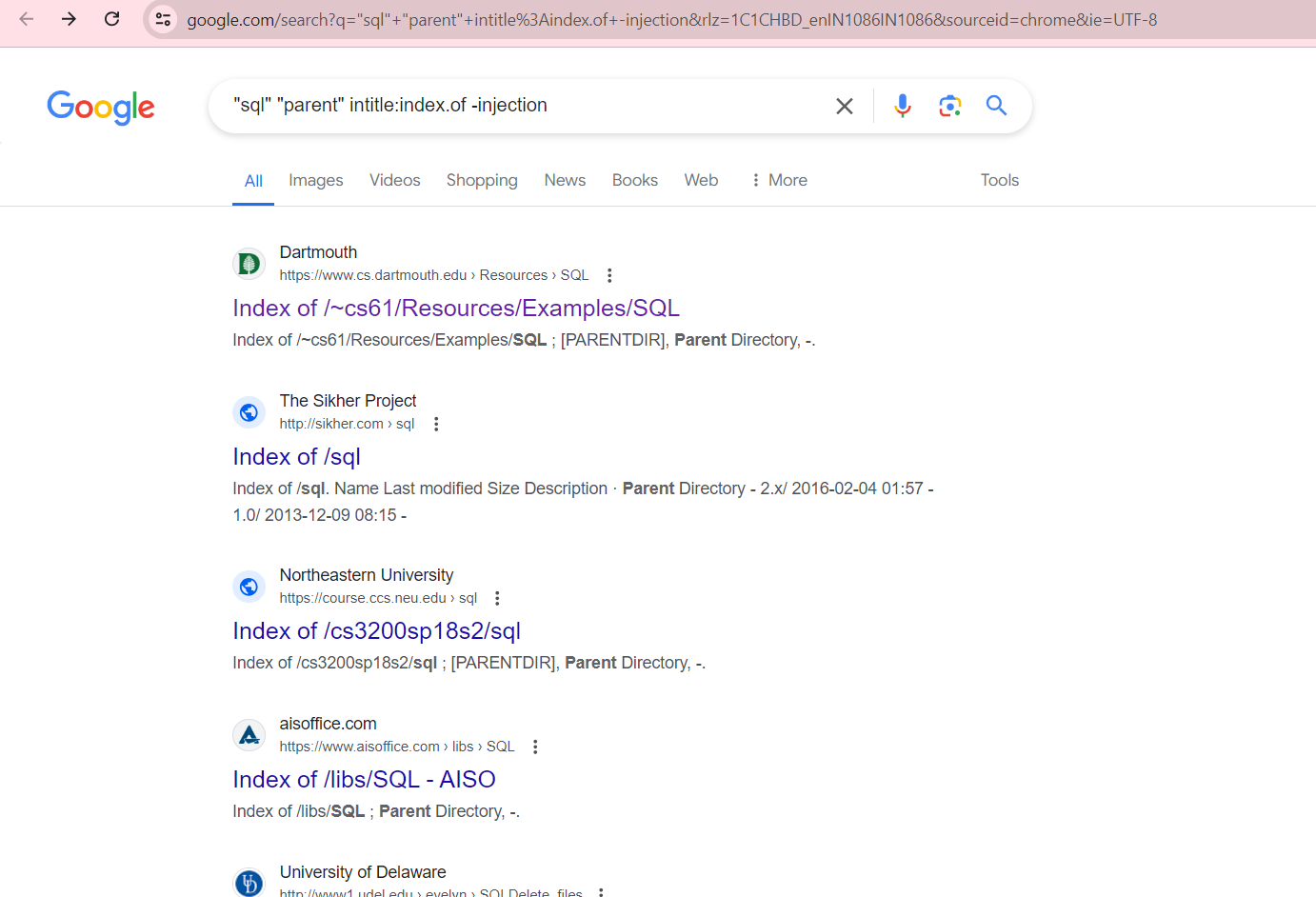
* SQL injection



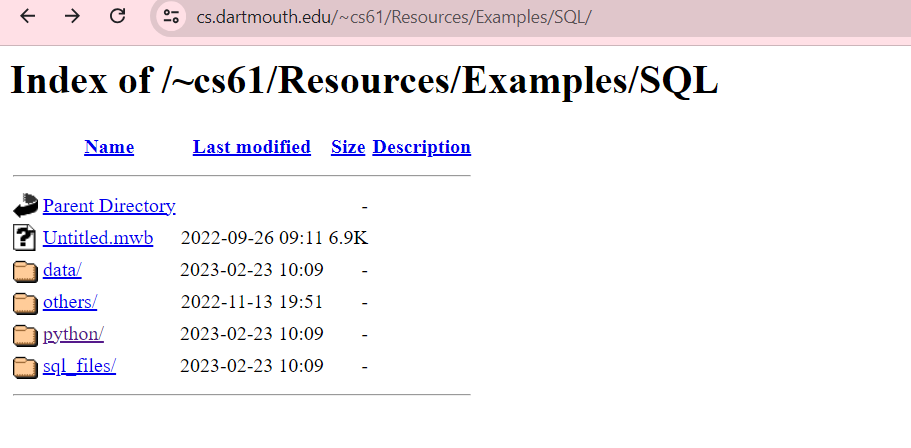
Here I searched for sql injection



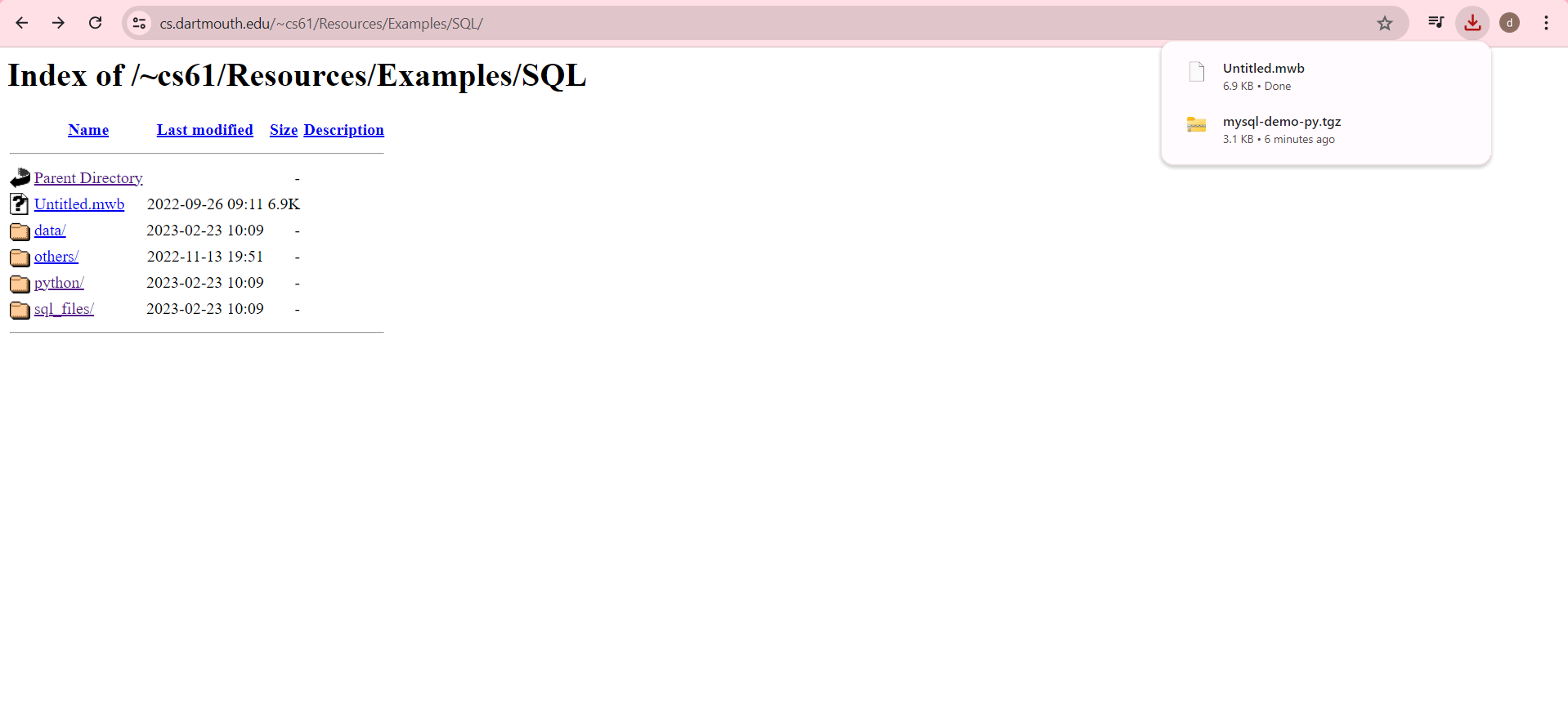
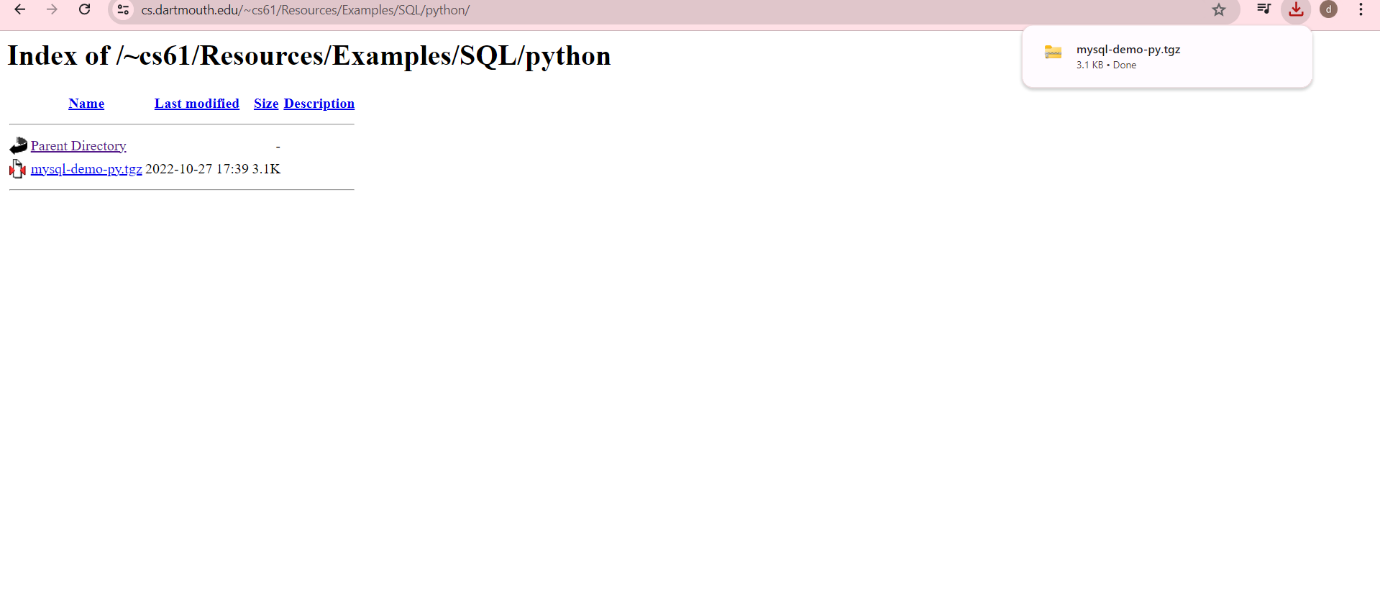
After clicking on the link, it tells us it’s the directory containing SQL install and SQL database. It is a sensitive directory. If this directory listing reveals SQL backups or scripts, it could potentially expose database schemas, queries, or even sensitive data that could be leveraged in other attacks.

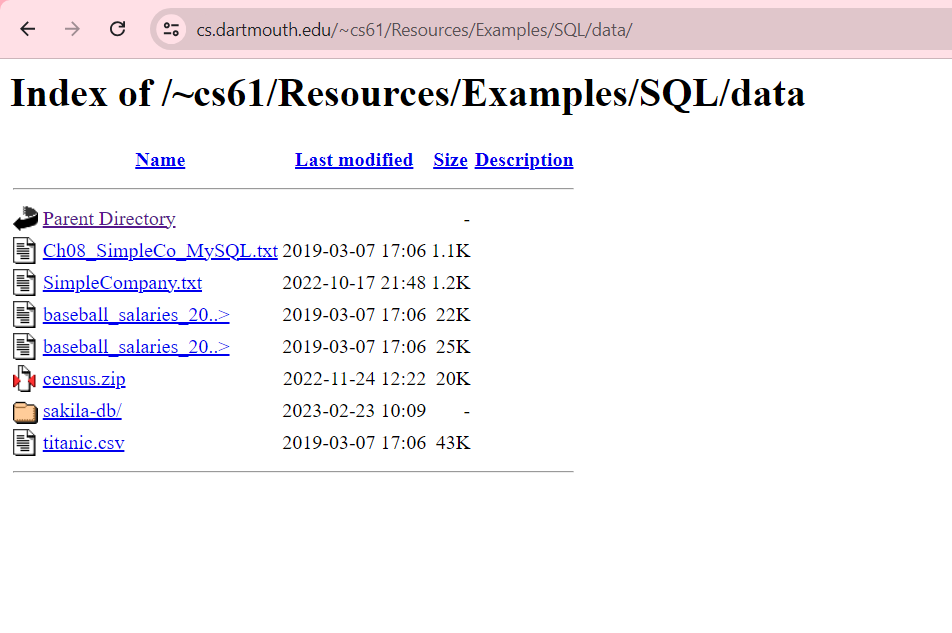


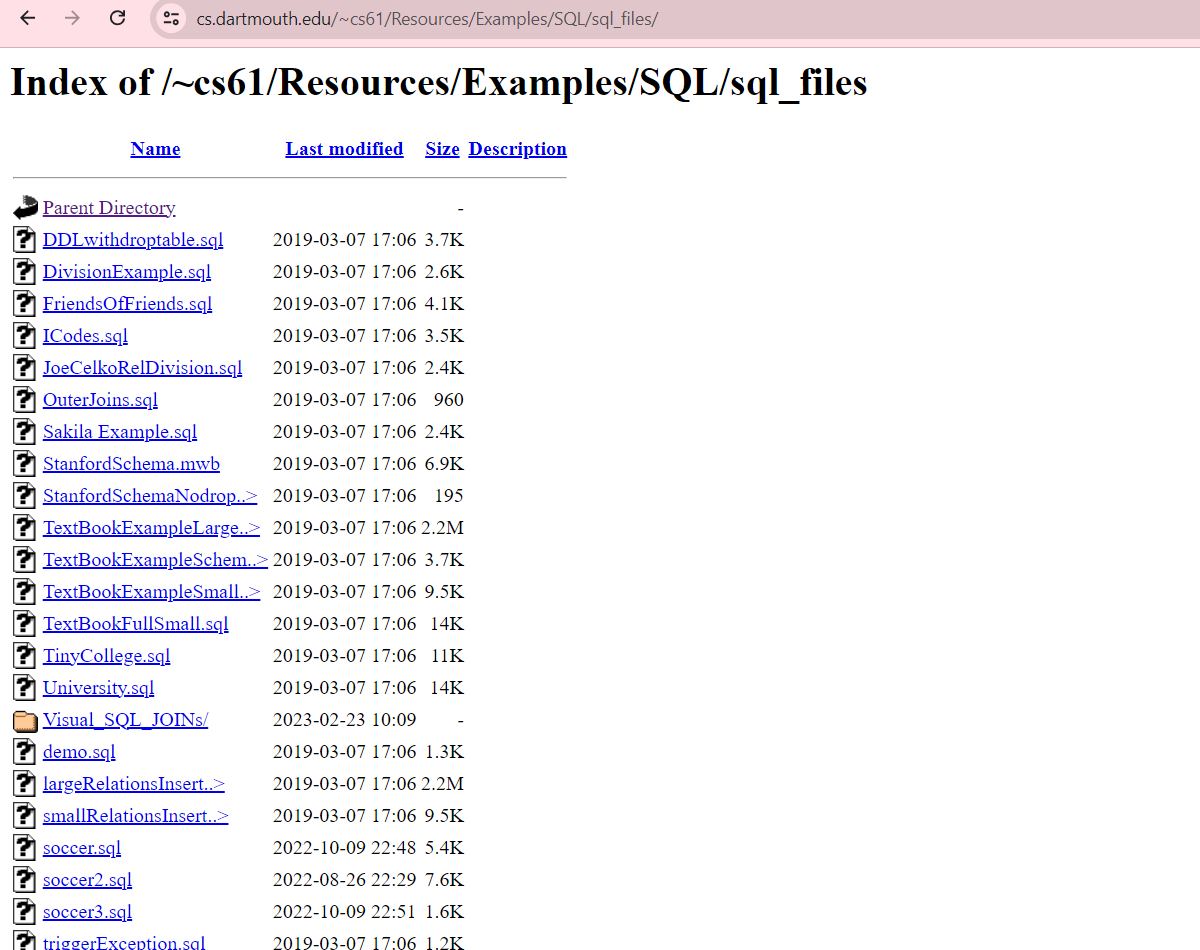
By doing google dock search of the URL containing intitle in it.



After clicking on the link

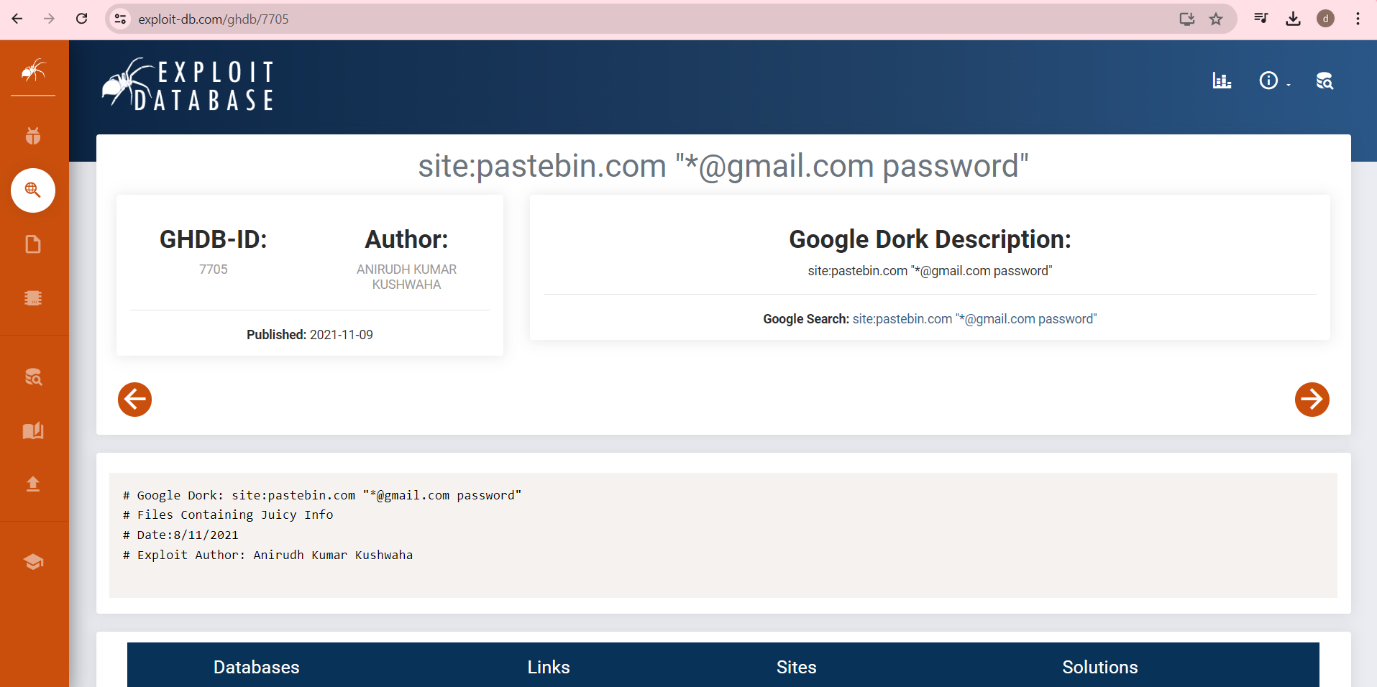
After clicking on it, it gets download



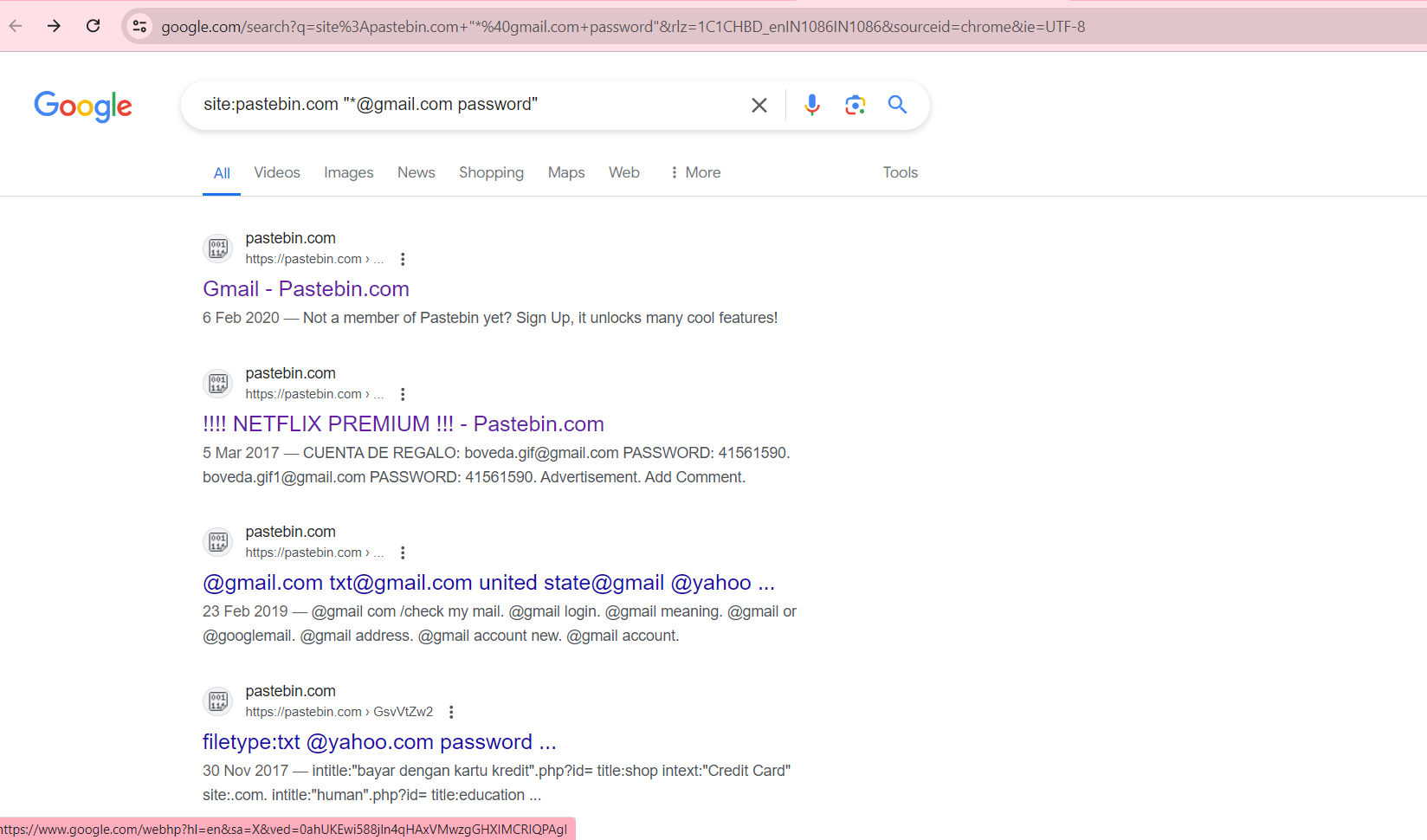


After clicking on sql files I got various link with date, time and size as it is a sensitive directory

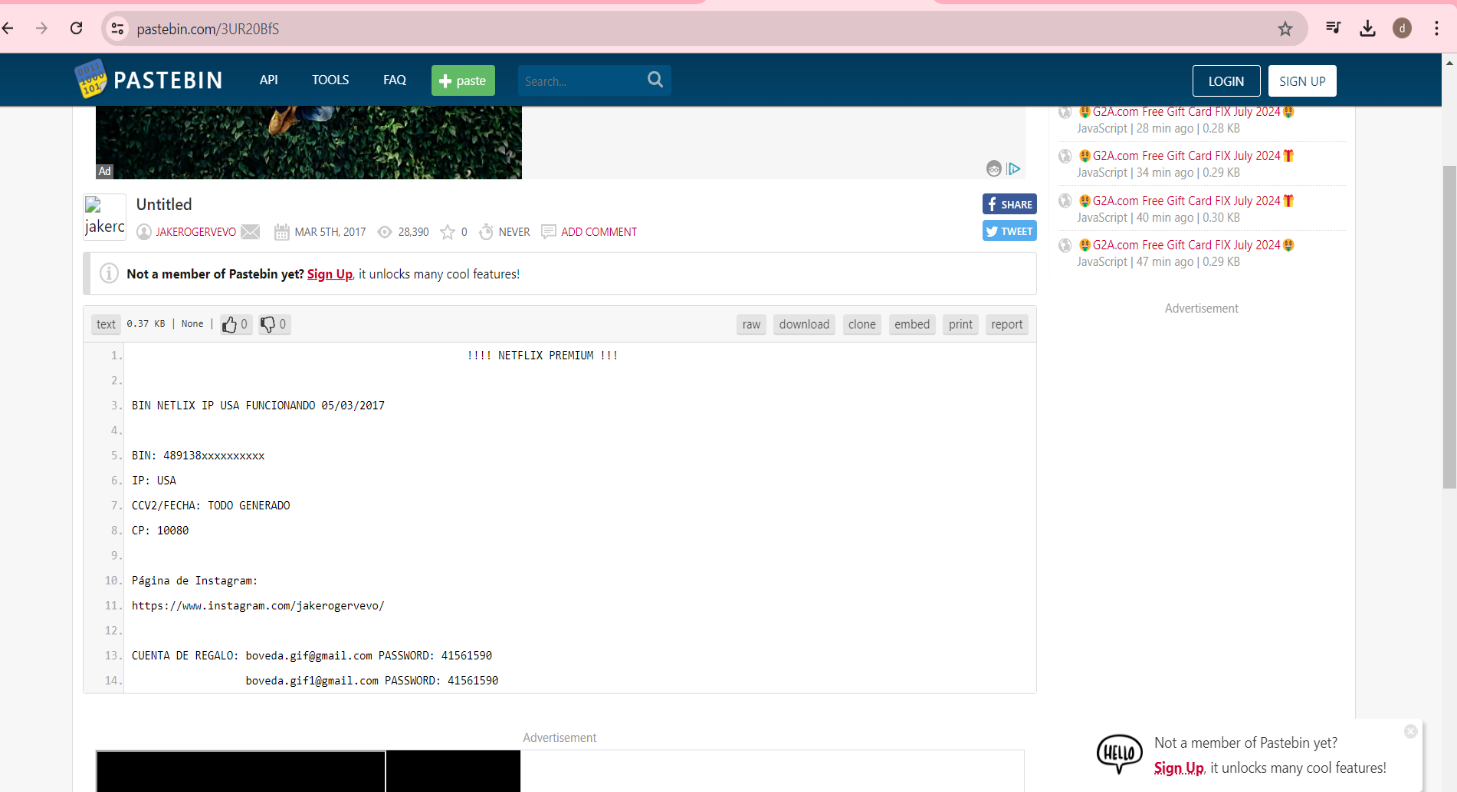
* Files containing password of Gmail



This link contains juicy info

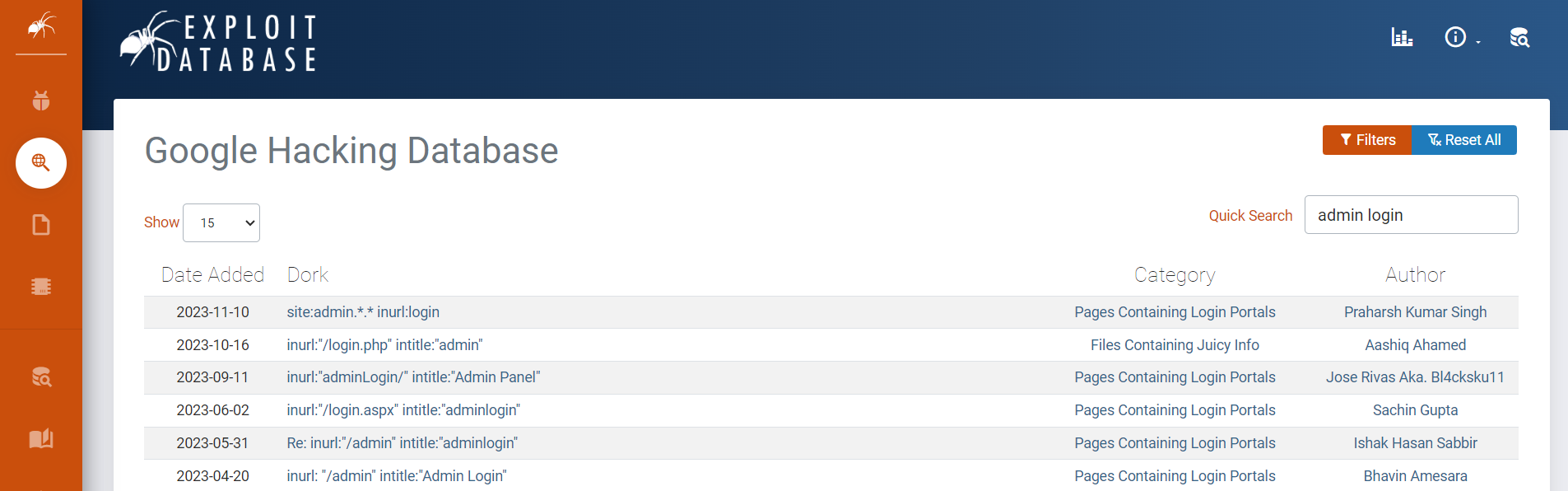


This link contains site: of google dork

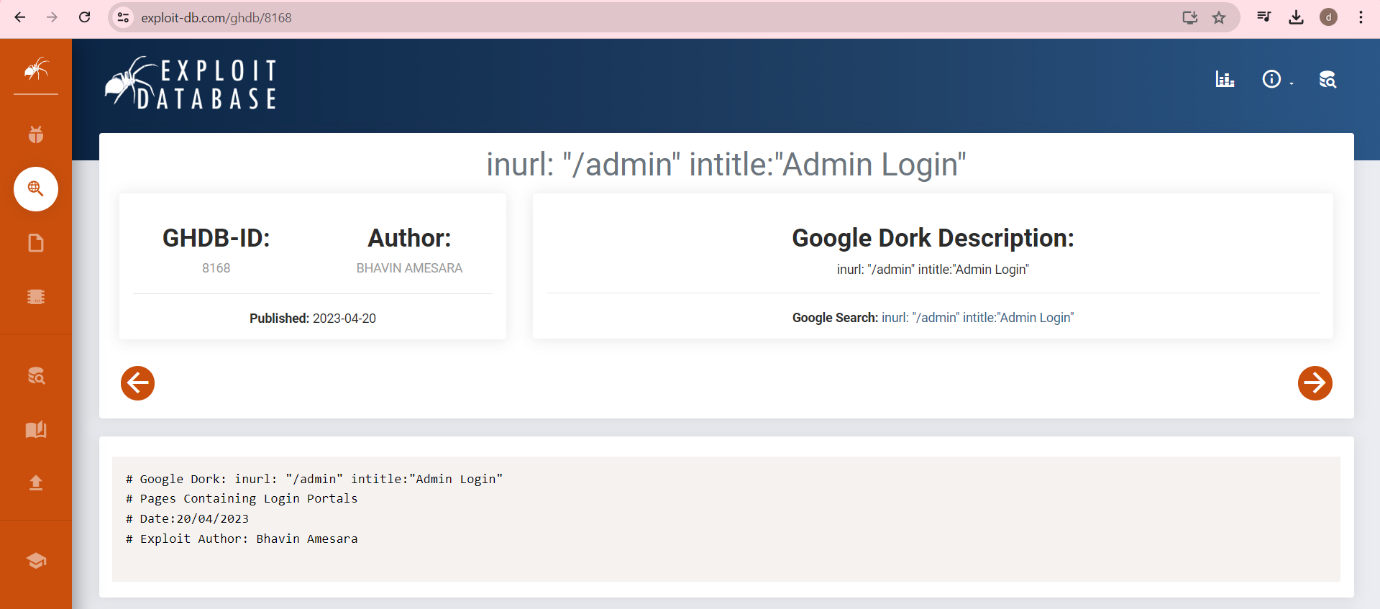


When we open the link of Gmail is shows mail id and password which is vulnerable

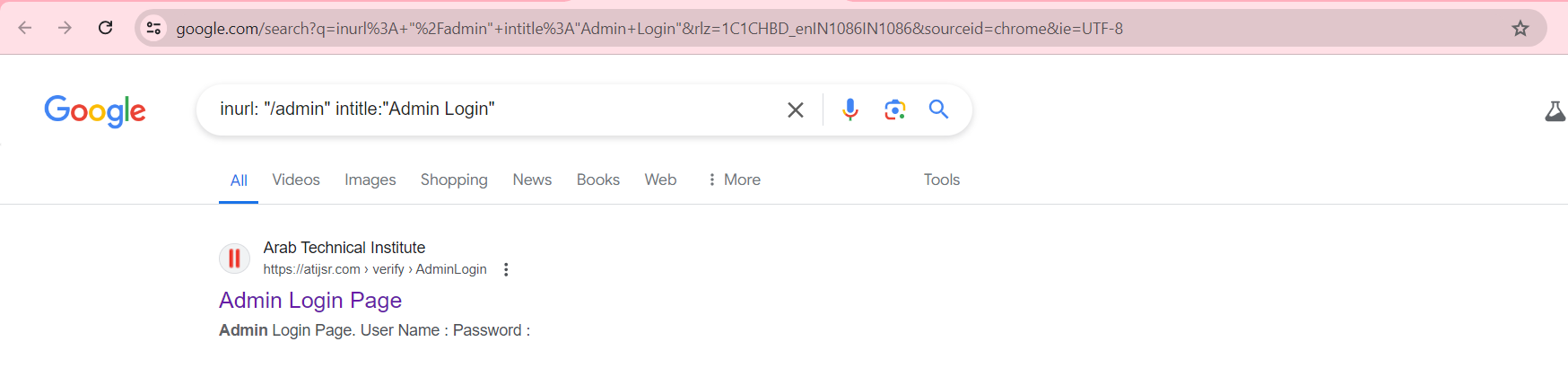
* Admin login page



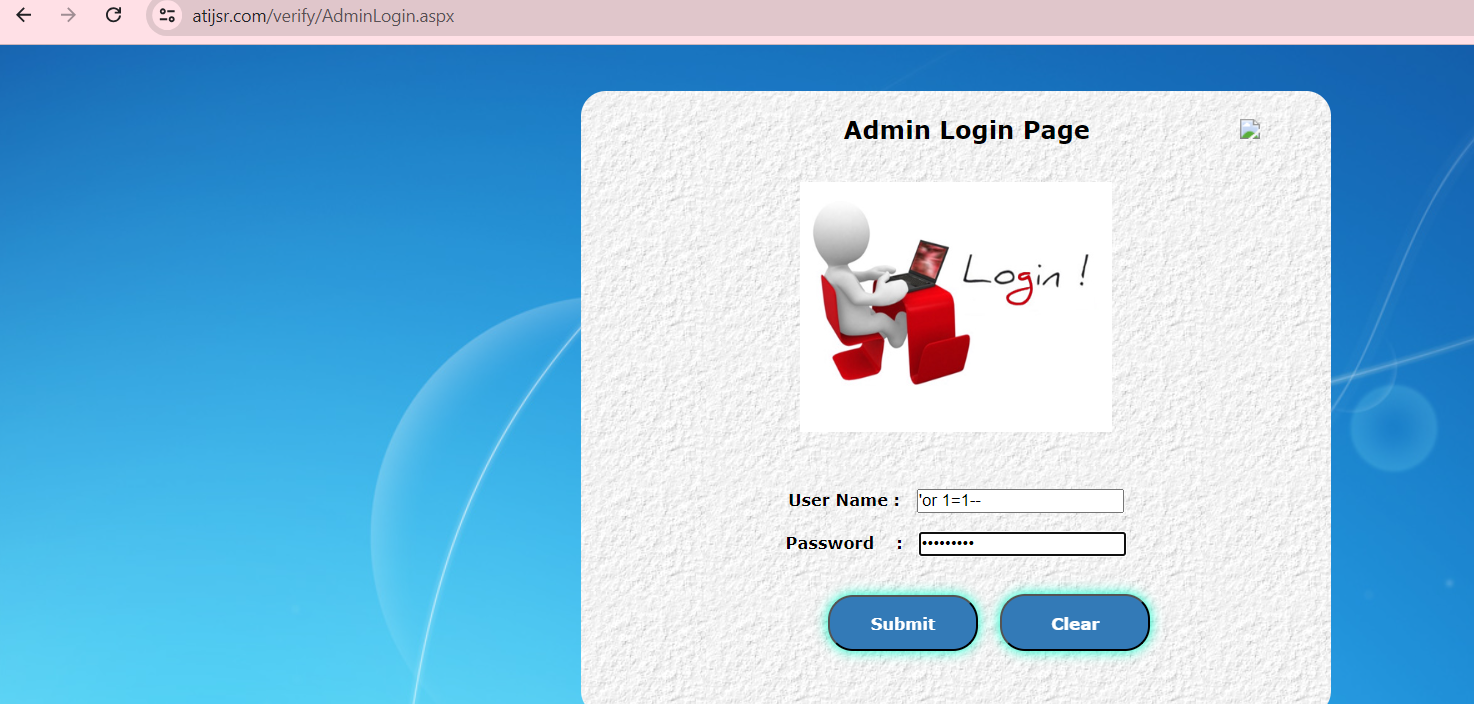
Admin login page



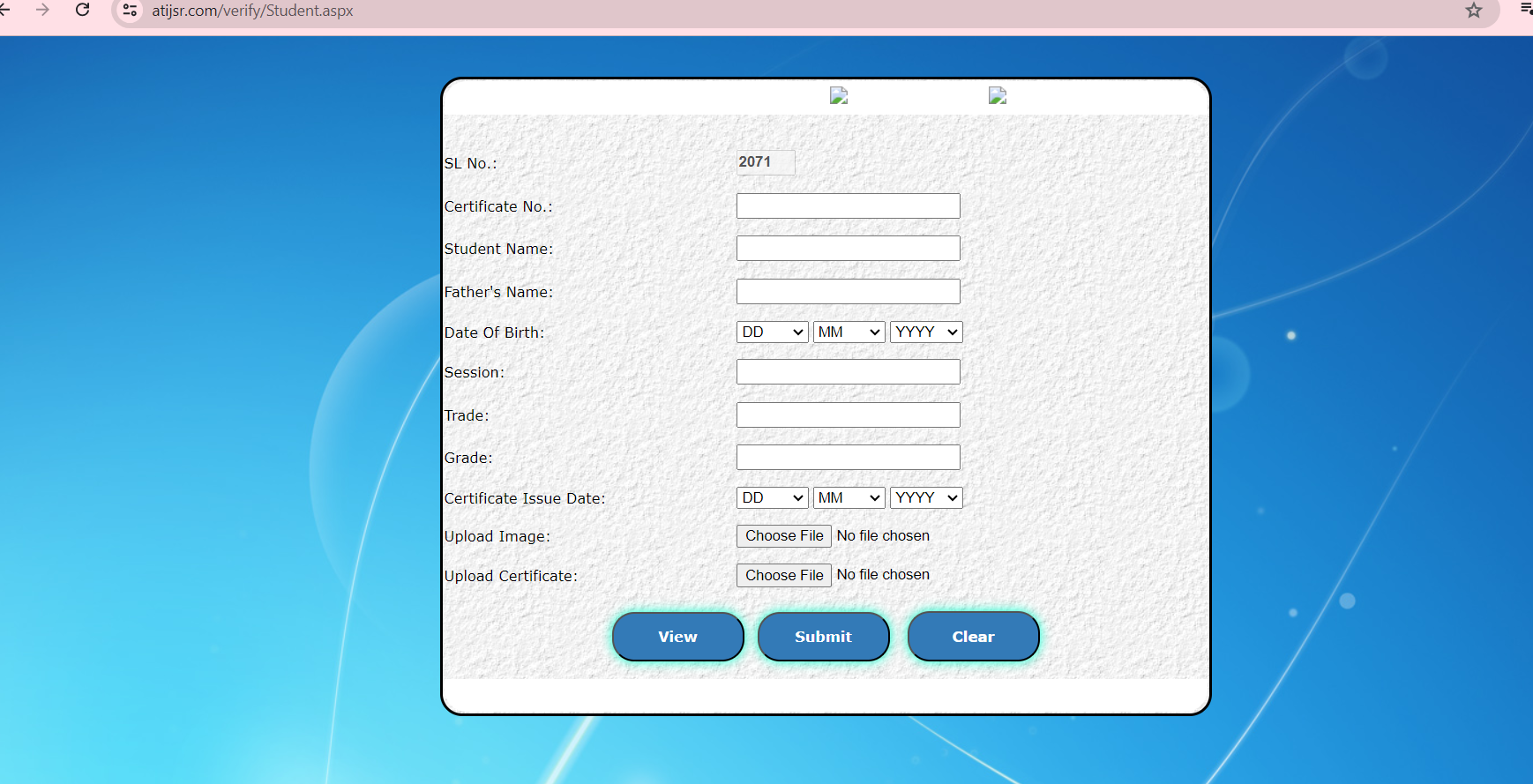
Here is the link where the page contains Login portals which has inurl of google dork



Search on google and click on admin login page

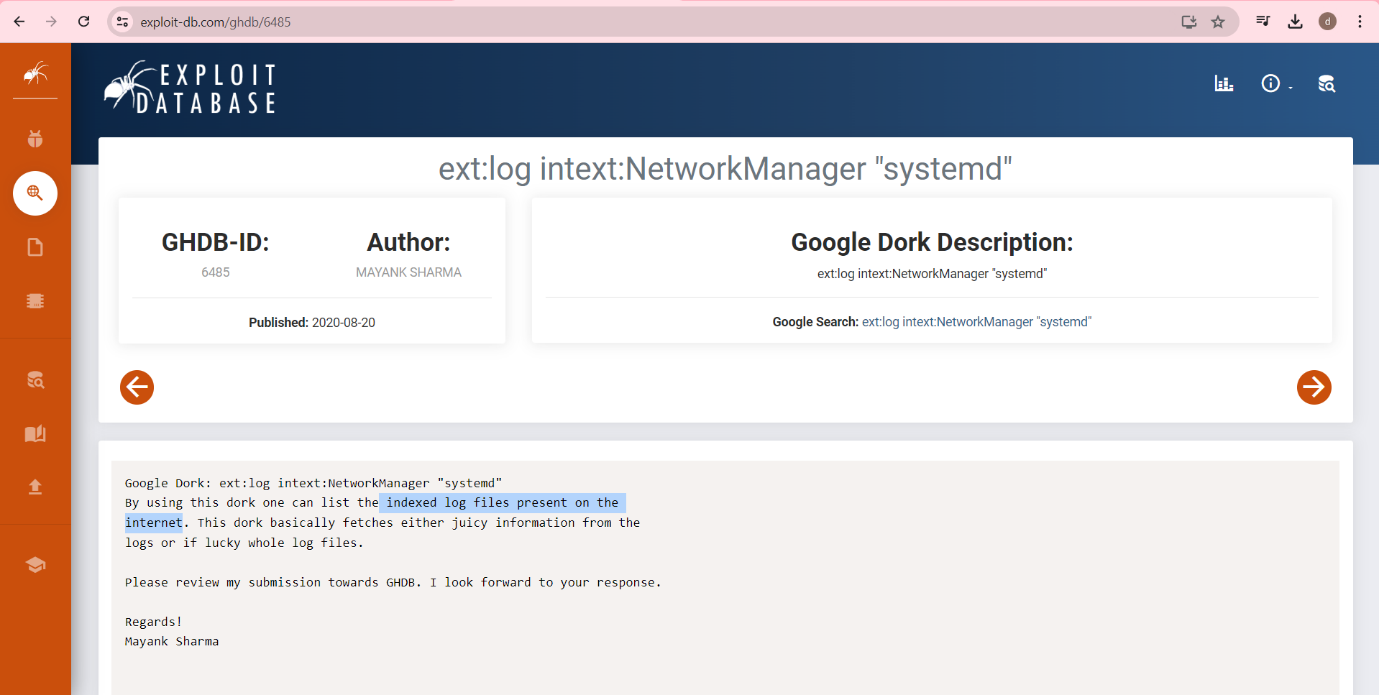


After inserting username and password click on submit

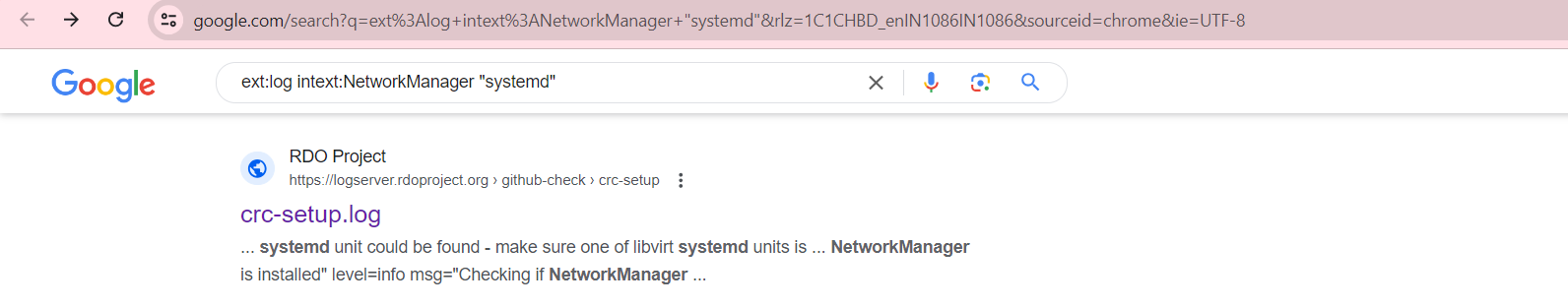


The Login page of admin is getting opened means this site is vulnerable

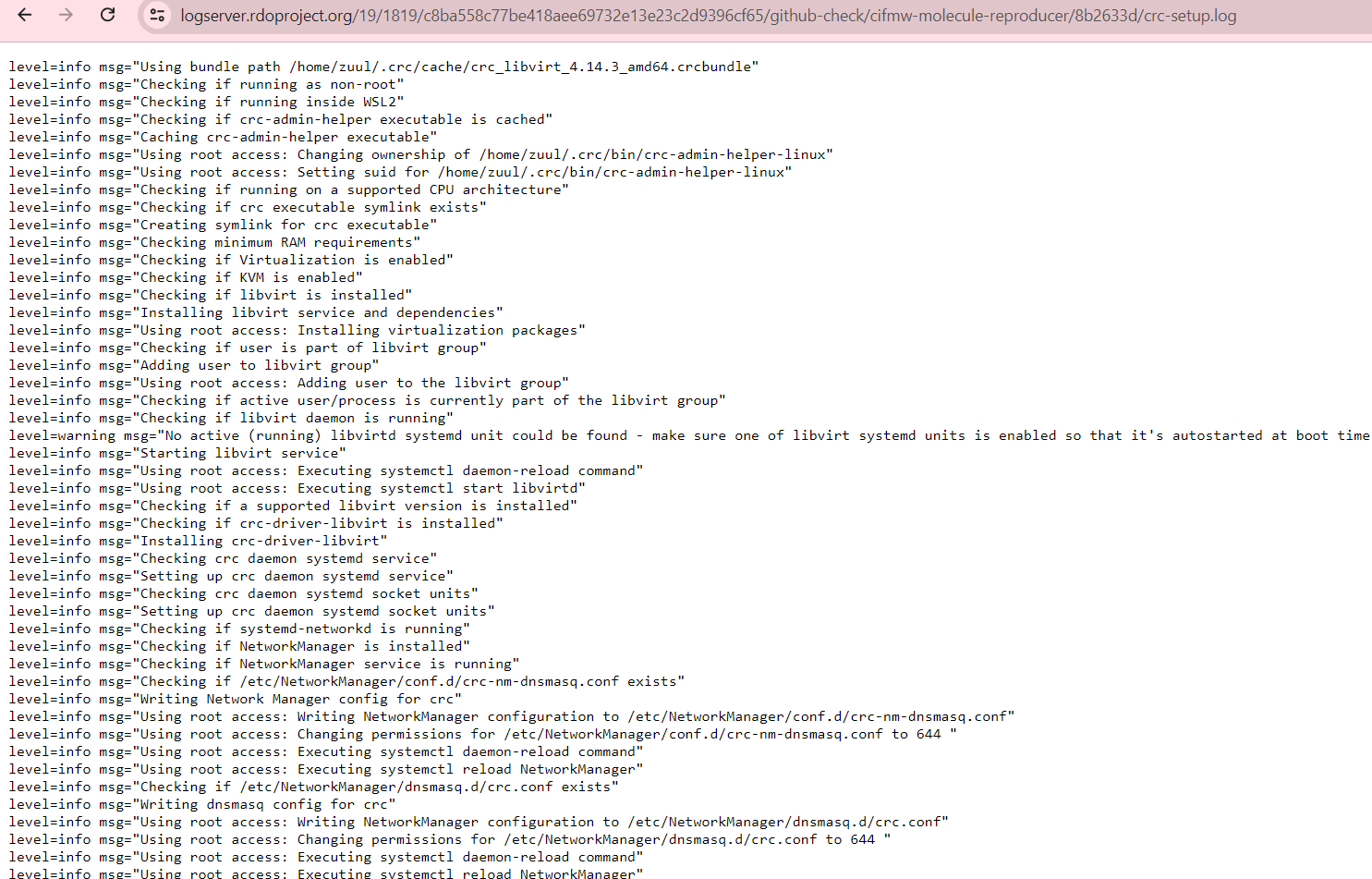
* Network or Vulnerability data



Click on the link for google search

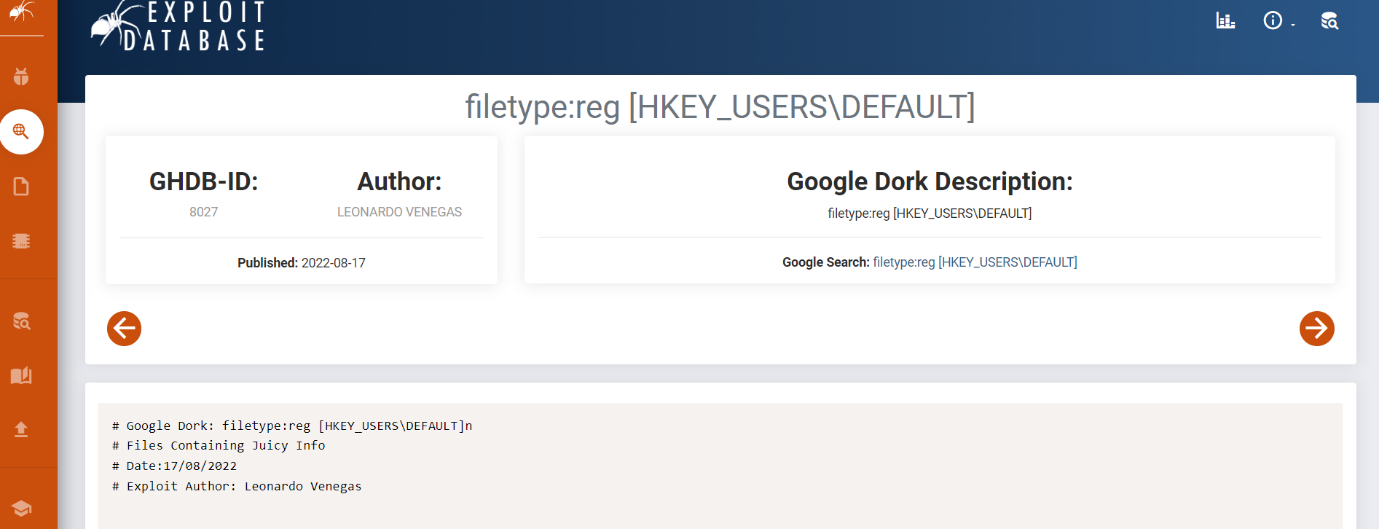


After searching on google it gives me the website

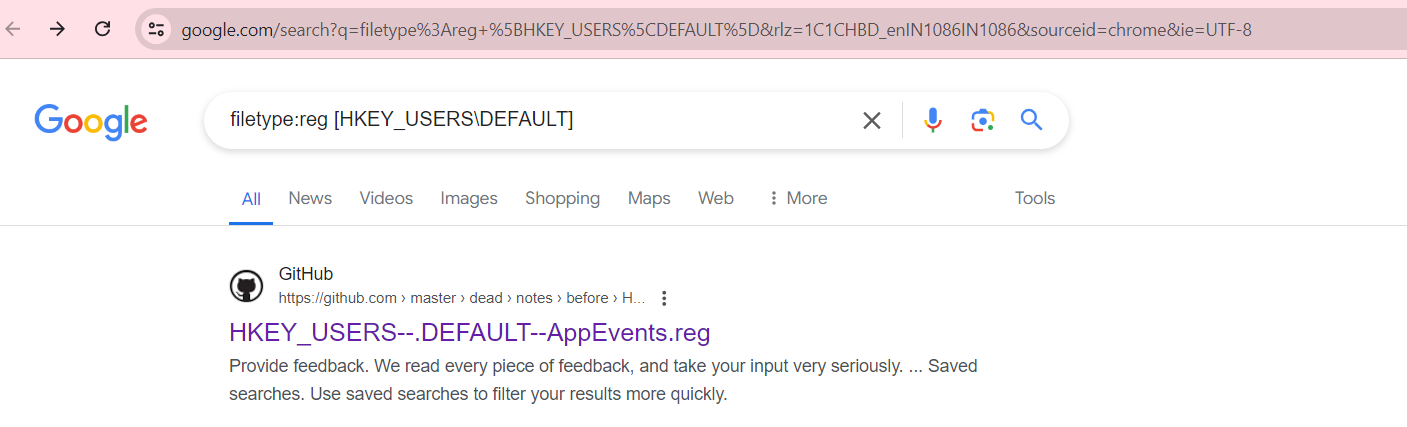


Containing this. This are the log messages provided which are related to the setup or initialization of Code Ready Containers (CRC).

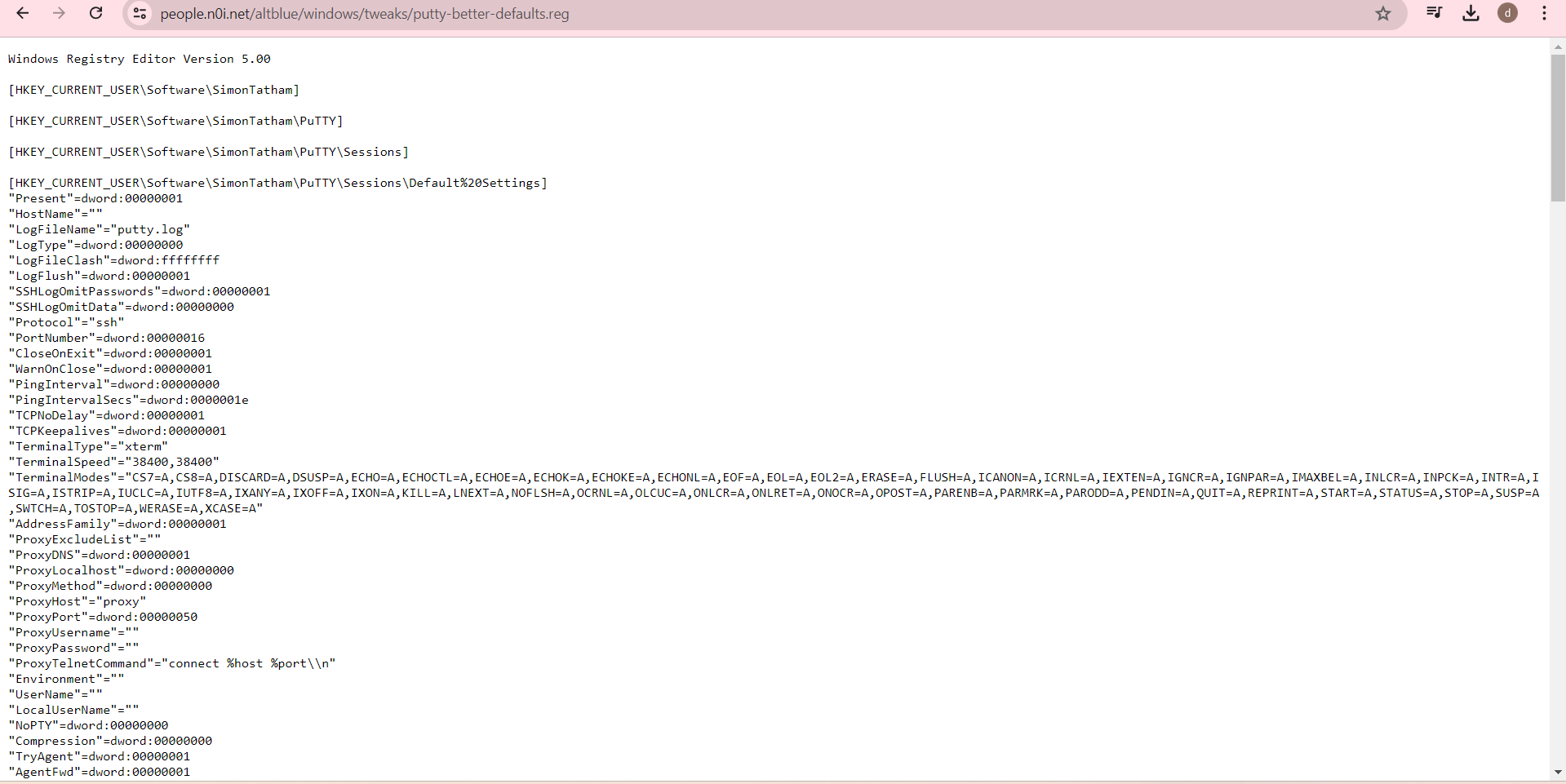
* Vulnerable servers

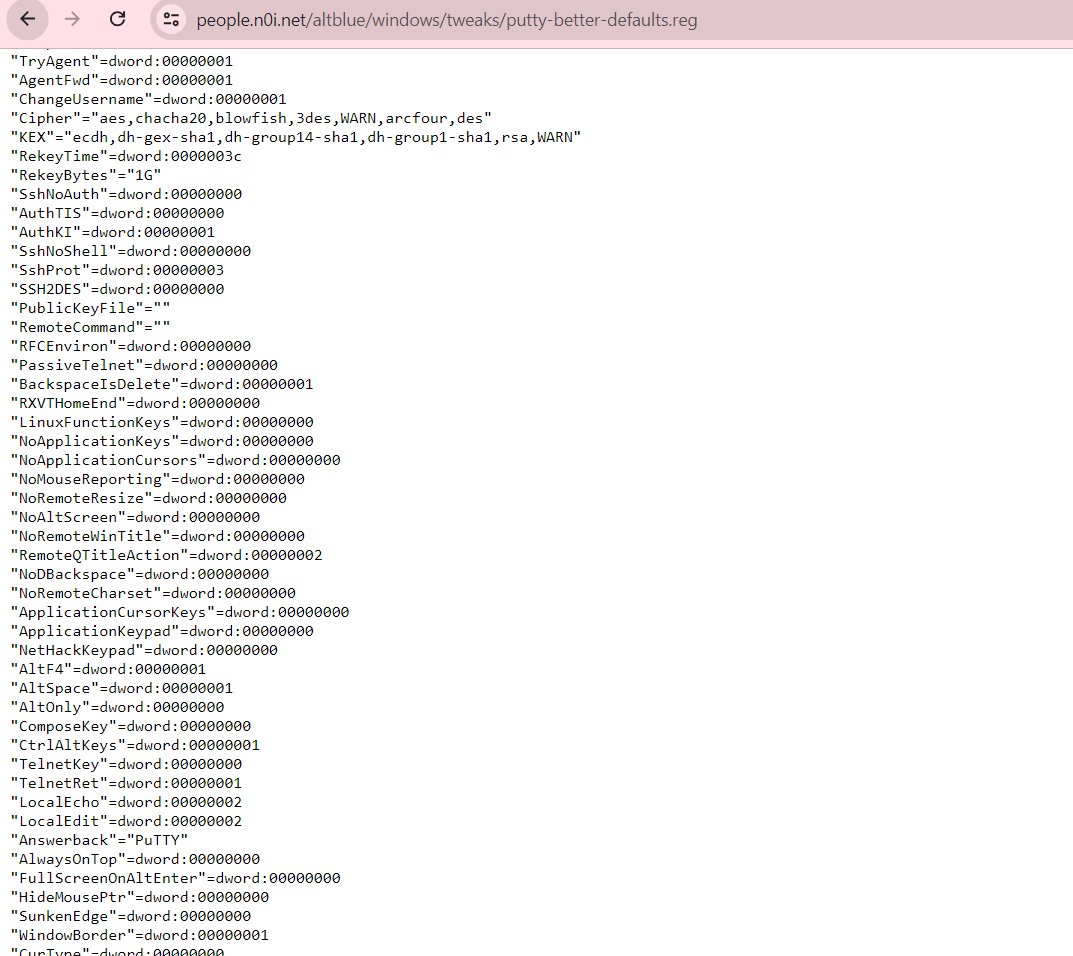


Clink on the link for google search



Open the link





Sensitive data which should not be leaked

**Potential impacts of the identified vulnerabilities.**

**SQL injection**

* Can cause leakage of database of sql or installing the sql which can lead to Financial Fraud, Loss of data, remote code execution and data manipulation

**Password**

* When the password of the user is know it can lead to various problems like reading the sensitive data eg company, government bodies this may lead to financial fraud, reputational damage and Unauthorized transactions can also take place

**Admin login page**

* Attackers gain access to administrative functionalities of the website.
* Downtime, operational inefficiencies, and potential financial losses.
* Compromise of site visitors, blacklisting by search engines, and significant recovery costs.

**Network or Vulnerability data**

* Data theft, system compromise, and potential control over network resources.
* Unauthorized use of services, potential service abuse, and operational disruptions.

**Vulnerable servers**

* Data theft, system compromise, potential control over network resources, and further exploitation of the network.
* Attackers can disrupt server operations by exploiting vulnerabilities or misconfigurations.

**Recommendations for remediation if applicable.**

**SQL injection**

* Ensure that user inputs are treated as parameters, not executable code.
* Validate and sanitize all user inputs to ensure they conform to expected formats and types.
* Avoid exposing detailed database error messages to users. Log errors securely for internal review.

**Password**

* Immediately remove any files containing passwords or sensitive information from public access.
* Conduct regular security audits to identify and remediate exposed files and directories.
* Educate users on the importance of using strong, unique passwords and the dangers of password reuse.

**Admin login page**

* Ensure that the admin login page and all data transmitted are encrypted using HTTPS.
* Regularly conduct security audits to identify and fix vulnerabilities.
* Monitor access logs for unusual activity around admin pages.

**Network or Vulnerability data**

* Implement strict access controls and use network segmentation to limit exposure of sensitive directories and files.
* Regularly audit and remove files containing sensitive information from public access.
* Keep all software, including servers and applications, up to date with the latest security patches.

**Vulnerable Servers**

* Implement strict access controls and use network segmentation to limit exposure of sensitive directories and files.
* Use strong, unique passwords and multi-factor authentication for accessing sensitive information
* Keep all software, including servers and applications, up to date with the latest security patches.