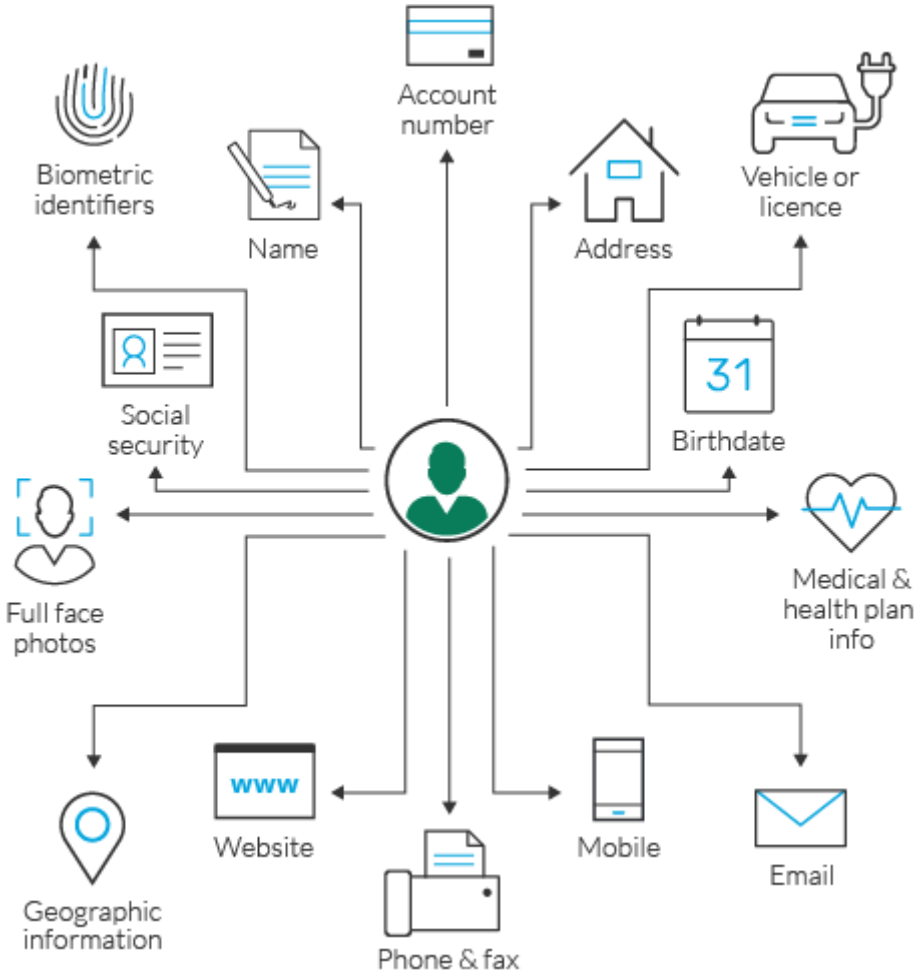
INFORMATION DISCLOSURE VULNERABILITY

WHAT IS INFORMATION DISCLOSURE VULNERABILITY?

When a website is unable to protect the sensitive information is known as Information Disclosure or Sensitive Data Exposure. The data can be personal information, financial information such as username, date-of-birth, credit card details or net banking details respectively. Also, it can be business related any sensitive data or may be technical information of website such as source code of the website.

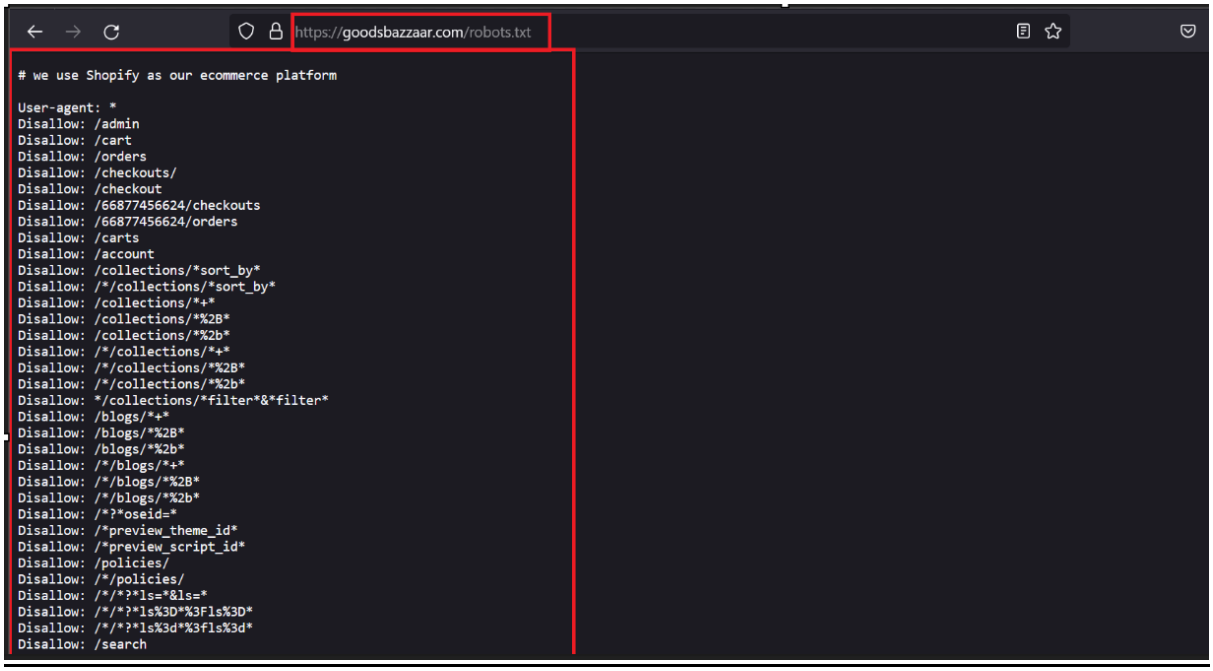
Sometimes Information disclosure is considered as high severity on its own according to the leak data how sensitive it is.



SCREENSHOT: PII DISCLOSURE

EXAMPLES OF INFORMATION DISCLOSURE

1. Disclose the name of hidden directories and the structure and their contents via **robots.txt** file or directory listing.

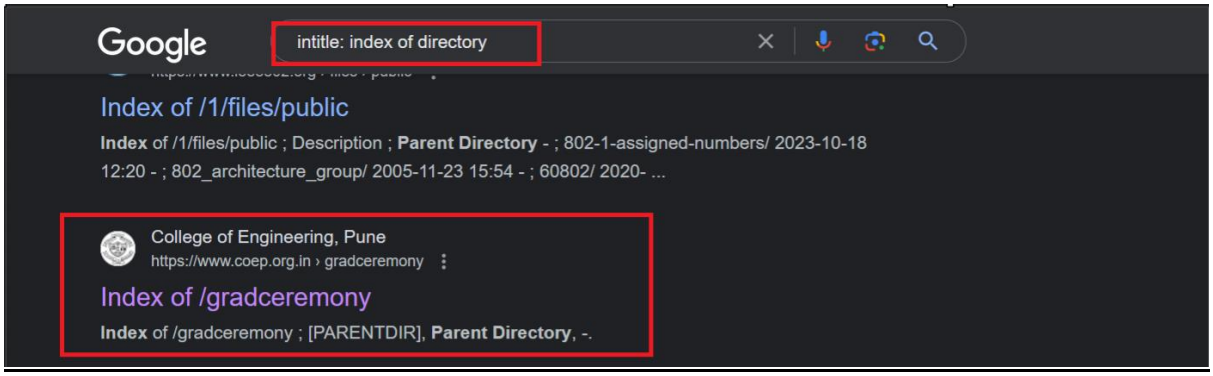


SCREENSHOT: ROBOTS.TXT IN URL

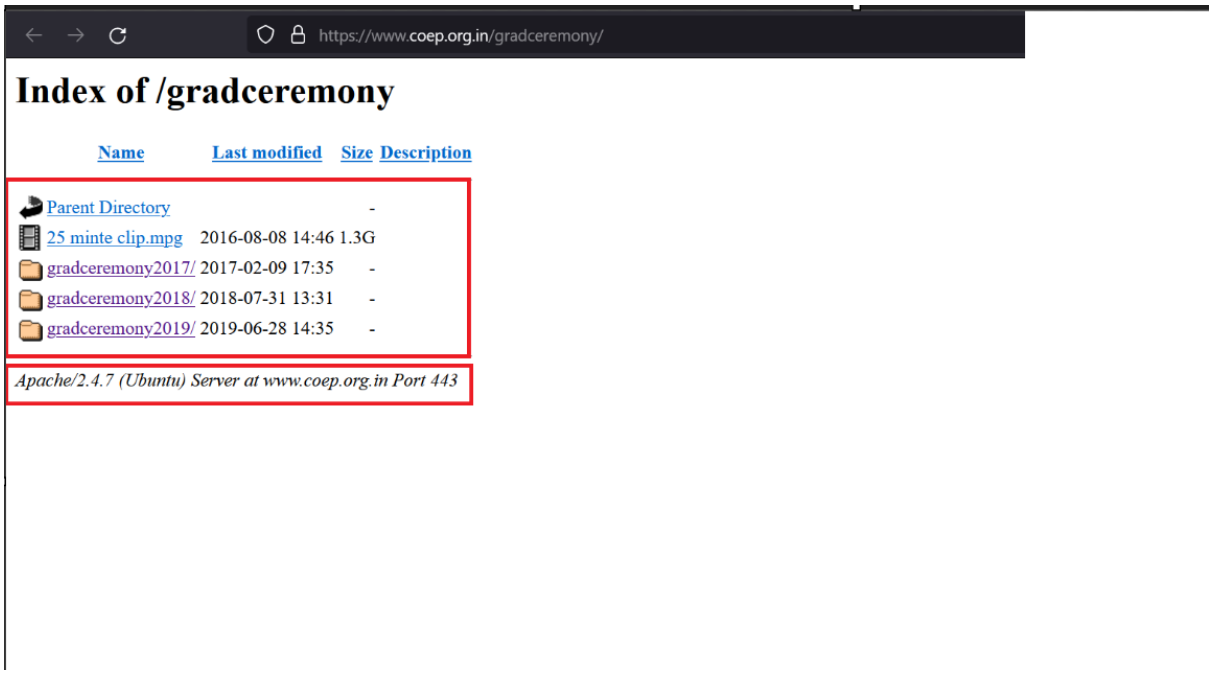
2. Providing access to source code file via temporary backups.
3. Mentioning database table name or column in the error message.
4. Unnecessarily exposing highly sensitive information such as credit card details
5. Hard-coding API keys, database credentials and IP address in the source code.

TYPES OF INFORMATION DISCLOSURE ATTACK

1. **Directory Indexing:** Exploits a function of a website that lists down the file of the directory if the base file is not present.



SCREENSHOT: GOOGLE DORKING (INTITLE: INDEX OF DIRECTORY)



SCREENSHOT: DIRECTORY LISTING

When a user types in a request for a page in the website, the webserver process the request and searches the web documents in the root directories and send the page to the user, if the page cannot be found then the issue arises and web page list all the directories as output in HTML format to the user.

The directory listing disclosed to the user because of software vulnerabilities that are combined with the web page.

The information leak might include some of these files or user information:

- Backup files that use file name extension such as BAK, OLD & ORIG.
- Temporary files that have purged from the server, that might still be available.
- Hidden files.
- Configuration file content that might contain access control data and use file name such as extension CONFIG, CONF or CFG.

Signature Triggered by This Attack:

Signature Name	Description
HTTP_Apache_Macros_dir	Detects an HTTP GET request for `the.dS_store` or `.FBCIndex` files.
HTTP_Tomcat_Nulllist	Checks for a specially crafted URL designed to obtain a list of directories from an Apache Tomcat servlet container.

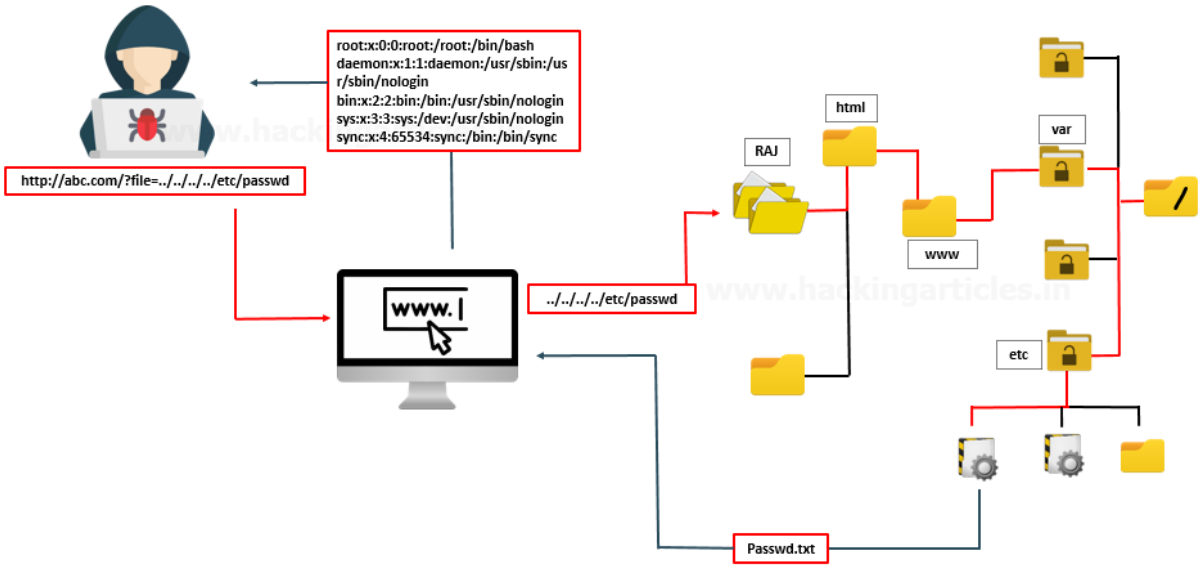
2. **Information Leakage:** Exploits a website that reveals sensitive information i.e., error messages or developer comments.

3. **Path Traversal:** This attack forces to access the directories, files and command that are located outside the web document root directory.

   An attacker can exploit a URL in a way that the website executes or discloses contents of files on the web server. Even though most websites restrict user access to the web document root or CGI root directory, an attacker can gain access to these directories by using special character sequences.

The ../ sequence is a common sequence that is used by an attacker to access files or to execute commands on the file system. Even though most web servers prevent this technique from escaping the web document root, you should check for the following alternate encodings of this sequence that might be used to bypass security filters:

- Valid and non-valid Unicode-encoding ..%u2216 or ..%c0%af of the forward slash character.
- Back slash characters ..\ on Windows based servers.
- URL encoded characters such as %2e%2e%2f.
- Double URL encoding ..%255c of the back slash character.



SCREENSHOT: PATH TRAVERSAL

When an attack occurs, it often leaves behind recognizable traces or patterns that can be identified through various means such as network packet analysis, system log analysis, or behavioural analysis. Security analysts and researchers study these patterns and develop signatures to detect and mitigate the attack.

When a security system detects network traffic or behaviour matching a known attack signature, it triggers an alert or takes action to block or mitigate the attack. Therefore, when someone mentions "signatures triggered by this attack," they are referring to the specific indicators or patterns of malicious activity that have been identified and programmed into security systems to detect and respond to that particular attack.

4. **Predictable Resource Location:** Uncovers hidden website content and functions.

TECHNIQUES TO FIND INFORMATION DISCLOSURE VULNERABILITES

1. **Manual Code Review:** It is a process to identify any instance where the sensitive information has been hardcoded or improperly handled such as API Keys, Passwords, etc.

2. **Automated Code Scanning:** This technique automates the process to analyse the code using tools such as Checkmarx or Fortify to identify potential vulnerabilities and information disclosure.

3. **Fuzz Testing:** This technique is use to generate invalid, unexpected or random data as input to application so it may reveal with any sensitive information disclosure vulnerability.

4. **Web Application Scanner:** We can use OWASP ZAP, Nessus, and Burp Suite application to scan the website in order to get the information disclosure vulnerability.

5. **Manual Testing:** We can interact with website using different techniques and roles where web application shows unexpected behaviour which helps to analyse the information which leaks sensitive information.

6. **Error Handling Analysis:** Analyse error message and responses triggered by web application which may leak sensitive information such as stack traces, file paths and database schemas.

7. **HTTP Header Analysis:** Analyse the HTTP Header responses which may accidentally reveals any sensitive information such as software server version or debug information.

8. **Directory Listing:** You can check If directory is enabled on web server, as this can potentially expose sensitive information files or directory containing confidential information.

9. **API Testing:** Test API thoroughly to ensure that API is not leaking any data because of improper authentication, sufficient access control or in any error message.

10. **Data Leakage Detection Tools:** Basically this tools are very helpful in organization to detect any data leakage due to poor network security and software misconfiguration which helps to prevent leakage of data.

TOOLS USE TO DISCLOSE INFORMATION FOR A WEBSITE

1. **Shodan.io:** It is nothing but a search engine for internet connected devices, which exposes the data on the internet and that might be disclosing any information.

   https://www.shodan.io/

2. **Burp Suite:** It is a popular website scanning tool that uses by security professional to test websites, which disclose sensitive information in the website.

3. **Git-cola:** It is very powerful open source graphical interface tool which is widely used for distributed version control system. Git-cola allows users to create, clone, open, and manage Git repositories through an easy-to-use interface.

4. **SQLMAP:** SQLMap is a popular open-source tool for detecting and exploiting SQL injection vulnerabilities in web applications. Since SQL injection vulnerabilities can lead to information disclosure, SQLMap can be used to identify such vulnerabilities and their impact.

5. **Google Dorking:** It is not a tool. However, a technique uses for advance search about the target system which exposes sensitive information and hidden links.

REFERENCE

https://www.ibm.com/docs/en/snips/4.6.0?topic=categories-information-disclosure-attacks

https://portswigger.net/web-security/information-disclosure#what-is-information-disclosure

https://cyberw1ng.medium.com/basics-of-information-disclosure-vulnerability-in-web-app-penetration-testing-2023-fce8786b227b