The Scrutiny on Critical Infrastructure Owners Referencing Privacy Violating Towards With the Open-Source Intelligence Threat Evaluation Framework

Dr. Jigneshkumar A.Chauhan
AMPICS College, Ganpat University, Kherva
Email: jigneshkumar.chauhan@ganpatuniversity.ac.in
Achyuttam Vyas
Research Scholar, Ganpat University, Kherva
Email : achyuttamvyas@gmail.com
Dr. Satyen M.Parikh
AMPICS College, Ganpat University, Kherva
Email: satyen.parikh@ganpatuniversity.ac.in

ABSTRACT

OSINT stands for Open-Source Intelligence Technique. OSINT includes all non-authorized and all openly available sources of information, this information we can access either online or offline, in the airwaves and on paper. In cyber security world, OSINT plays an important role. It is the initial part of hacking which is also known as reconnaissance– information gathering. The more information we can gather about our victim, the easy it will be for us to get into the organizations network and exploit the vulnerabilities present in the organization. As world is getting attracted and addicted to digitalization the more and more users and organizations privacy and data is at risk. Attackers are getting smarter day by day with their skills and techniques they always try to be creative with their new fond of attacks. In same way the Critical Infrastructure Sector has now been a target for attackers as these can lead to many disastrous things example: - Stuxnet and Black energy. In this paper we are going to target Pharmacy Sector using PV OSINT Framework to identify all the issues / vulnerabilities which can help organizations to mitigate the vulnerabilities so that they are saved from future cyber-attacks.

Keywords - **Industrial Control Systems (ICS), Information Gathering, Open-Source Intelligence (OSINT), Privacy Violation, Reconnaissance.**

I. INTRODUCTION

India has recently been a target of lot of cyber-attacks [1], as India is growing rapidly and quickly adopting digitalization. This further arises the question, “Are we that much secure?” Infrastructure Control Systems are now under target more than ever. Due to most recent ransomware attack on a hospital the services were halted including loss of lives. [2]. Open-Source Intelligence Techniques is a process of gathering information from all over the internet. Hackers use the gathered information about the organization or any individual in a malicious way to harm or to bring their reputation down, for organizations which may also impact their business and loss of clients. State/Nation Sponsored hackers use Open-Source Intelligence Technique to get some valuable information / data about their enemy countries example getting some military data, blueprints, government employees list etc. Whereas Cops / Police use it to catch criminals or Cyber criminals

1.1 Types of OSINT

1.1.1 Active OSINT

Active OSINT communicates with the target. Provides well- aimed and updated information. There are more chances of getting caught while performing active OSINT. Attackers need to trick target into clicking on some link via social engineering attacks such as phishing email, spear phishing, vishing, smishing, and whaling to gather some more information. [3]

1.1.2 Passive OSINT

Passive OSINT never communicates with target. It relays on third-party information. Passive scanning like google dorks, social media accounts such as Facebook, Twitter, LinkedIn etc. Passive OSINT tries to gather public or technical records to show patterns.[3] In passive OSINT attackers also try to get access to some critical PII data or passwords or any other important file uploaded on the website openly and asks for no authorization to the user who is accessing it. Getting geolocations about the devices and servers or other connected devices is also a part of passive OSINT.

1.2 Understanding OSINT life cycle

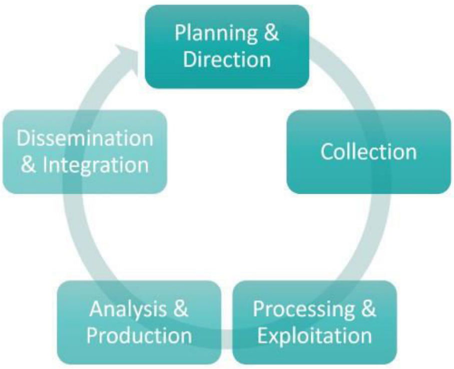


Fig. 1. - Open-source intelligence life cycle [4]

Planning and Direction: - Prior to start with our collection of information, analysts should have proper understanding about what information do they need and how to find out that information?

Collection: - After the first phase, we can begin with our collection of OSINT. OSINT resources may include anything i.e., any tools, websites, news articles, blogs, social media posts about our target.

Process and Exploitation: - At this stage the investigator will try to figure out the required and important information from the collected information. The collected information can be processed further based upon use-cases.

Analysis and Production: - Once the primary preparation of data collection is completed, we can then deep dive into analysis of the information. This is very important step in OSINT life cycle.

Dissemination and Integration: - The closing step in the OSINT cycle leads to deliver the collected and analyzed intelligence to the proper organizations. Analysts then hear back an answer, which instruct them whether the OSINT cycle should begin again.

II. ANALYSIS

In this paper we have focused on both passive and active reconnaissance.

Passive Reconnaissance: - At this point we embarked with HTML source code review to identify clear text passwords, api's, network paths.

Further we moved our investigation over available job postings on job portals such as LinkedIn, here we tried to gather information about the required positions in the firm, their job description and tools used by the organization.

Sub domains are always in a target by the attackers. Organizations usually miss securing sub domains and keep it open for the access. Attackers take benefit of these mis configurations and get access to critical data or services which could later lead to data breach and may impact confidentiality, integrity and availability.

Active Reconnaissance: - At this phase, we tried to scan and explore open ports and services, operating systems used, kernel versions by some OSINT tools.

III. PV-OSINT FRAMEWORK

Open-Source Intelligence is very ancient and important existing technique used by cyber criminals to target organizations or their victim. The effectiveness of this technique can lead in finding, sorting, extracting information without any exploitation.[5] The below-mentioned framework is the referenced framework used by us to consider OSINT on Critical Infrastructure Organizations. The framework indicates that at very first step any analyst should try to identify all the publicly facing devices, social media presence, third party hosted information (tools used and its information, architecture, version of tools, client list etc.)

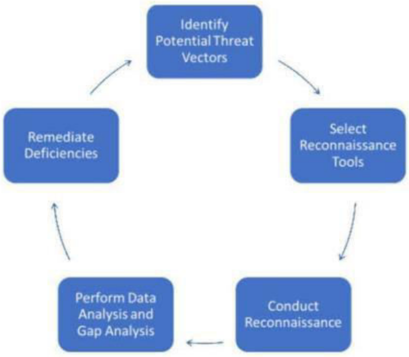

Identify Potential Threat Vectors
Select Reconnaissance Tools
Conduct Reconnaissance
Perform Data Analysis and Gap Analysis
Remediate Deficiencies

Fig. 2. Privacy violation osint framework [6]

Proper analysis and information gathering will lead our investigation to success. At next step we can get our arsenal ready and try to gather as much as information.

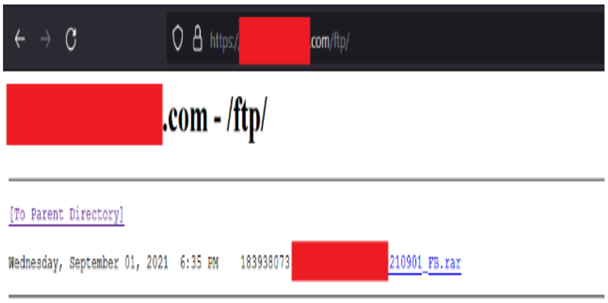
At third stage we can conduct reconnaissance from all over the internet such as emails, data breaches, client's data breaches, known vulnerabilities, open ports, misconfigurations and improper access to some directories. Once the information gathering step is finished, the firm should move into the Perform Data and Gap Analysis phase. In this step, the firm should record all identified vulnerabilities, grade them in sequence of priority, discover the gap in their cybersecurity risk management record, and in the end try to identify the root of the privacy violation. The severity of the vulnerabilities will be dependent upon CVSS score and organizations architecture. At last, we can mitigate the vulnerabilities by identifying the root cause of the confidential and critical data available on the internet which also leads to privacy violation. Organizations should keep a close track on this and close the report once all the vulnerabilities are mitigated.

IV. Key Findings

While gathering information using OSINT tools, we found many valuable information on pharma organizations.

4.1 Directory Listing

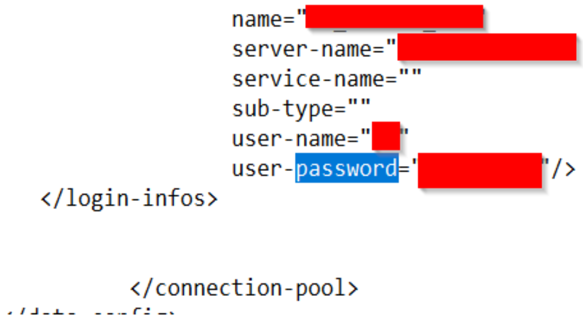
Directory Listing is a misconfiguration which allows attacker to view or download some critical files stored on web server.



```
https://[redacted].com/ftp/

[redacted].com - /ftp/

[To Parent Directory]

Wednesday, September 01, 2021  6:35 PM    183938073 [redacted]210901_FB.rar
```

Fig. 3. - Directory listing and ftp directory accessible

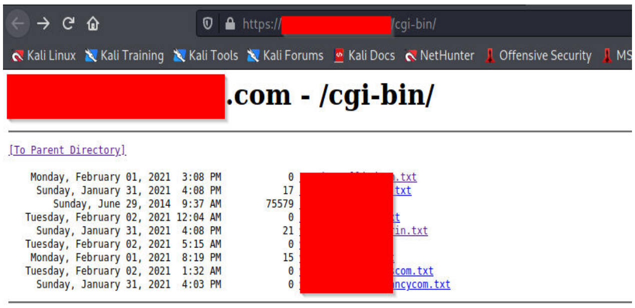
A .rar file was observed in the ftp directory which was openly accessible over the internet. The rar file was further unzipped, which contained a backup file. To analyse the .bak file we converted it into a txt file using strings command. The file was their mysql database backup file which further contained table_name, database_name, queries that were readable for us. Then we searched for words such as password and username.



```
                  name="[redacted]
                  server-name="[redacted]
                  service-name=""
                  sub-type=""
                  user-name="[redacted]"
                  user-password='[redacted]"/>
    </login-infos>


          </connection-pool>
```

Fig. 4. Database name and id password

We found the username and password for the database with database name and IP address.



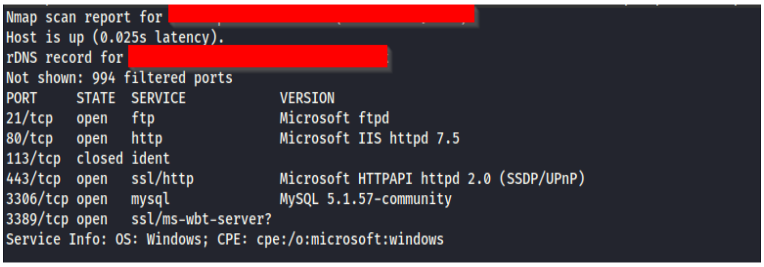
```
https://[redacted]/cgi-bin/

[redacted].com - /cgi-bin/

[To Parent Directory]

  Monday, February 01, 2021  3:08 PM          0 [redacted].txt
   Sunday, January 31, 2021  4:08 PM         17 txt
      Sunday, June 29, 2014  9:37 AM      75579
Tuesday, February 02, 2021 12:04 AM          0 t
   Sunday, January 31, 2021  4:08 PM         21 in.txt
Tuesday, February 02, 2021  5:15 AM          0
  Monday, February 01, 2021  8:19 PM         15
Tuesday, February 02, 2021  1:32 AM          0 com.txt
   Sunday, January 31, 2021  4:03 PM          0 ncycom.txt
```

Fig. 5. - Directory listing and other client information was accessible

Another directory listing was accessible to us /cgi-bin, which contained some critical client information and employee details.

4.2 Open Ports and Version Information

Digging deeper to gather more information about the organizations, we performed port scanning. Port scanning is very reliable and efficient way of reconnaissance, attackers always use this technique to gather information about the servers, open ports and their services as it would be really easy for an attacker to find the known exploits or vulnerabilities from the installed services and could easily try to get into the system.



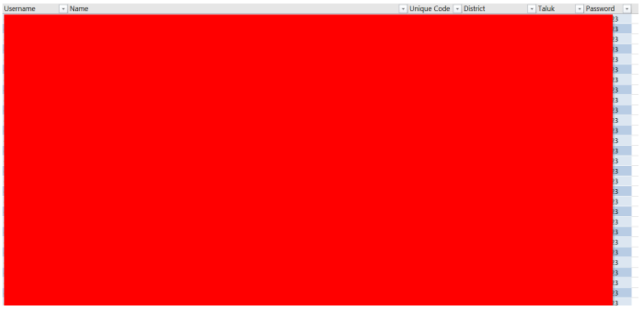
```
Nmap scan report for [redacted]
Host is up (0.025s latency).
rDNS record for [redacted]
Not shown: 994 filtered ports
PORT     STATE  SERVICE             VERSION
21/tcp   open   ftp                 Microsoft ftpd
80/tcp   open   http                Microsoft IIS httpd 7.5
113/tcp  closed ident
443/tcp  open   ssl/http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3306/tcp open   mysql               MySQL 5.1.57-community
3389/tcp open   ssl/ms-wbt-server?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Fig. 6. Open ports and server version found

The above image confirms that port 21- ftp, IIS 7.5 is running on port 80 – http and Mysql database with mysql 5.1.57-community version is running on port 3306.

4.3 Personal Identity Information

We also found some critical client’s information and PII data while using google dorks technique. Google Dorks is an advanced search query which crawls over the internet according to our query and gives us the result according to it.

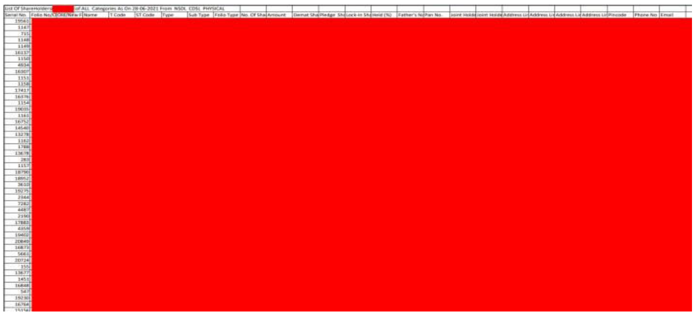


Username	Name	Unique Code	District	Taluk	Password
[redacted]					

Fig. 7. - Customers user id and passwords were visible in plain text

We found the username, customer name and their location with their passwords.

Other crucial PII observed were shareholders information including their email, PAN card number, name, DEMAT amount, pin code, Father’s name etc. Using this information any attacker can plan misuse the users PII for Loan, Forgery etc.



List Of ShareHolders [redacted] of ALL Categories As On 28-06-2021 From NSDL CDSL PHYSICAL

Serial No.	Folio No/CLID/New F	Name	T Code	ST Code	Type	Sub Type	Folio Type	No. Of Sha	Amount	Demat Sha	Pledge Sh	Lock-in Sh	Held (%)	Father's N	Pan No.	Joint Holde	Joint Holde	Address Li	Address Li	Address Li	Address Li	Pincode	Phone No	Email
19561	[redacted]																							
1147																								
715																								
1148																								
1149																								
16137																								
1150																								
4934																								
16307																								
1151																								
1158																								
17417																								
16376																								
1154																								
19035																								
1161																								
16752																								
14546																								
13278																								
1162																								
1788																								
13678																								
283																								
1157																								
18790																								
18852																								
3610																								
19275																								
2344																								
7282																								
4487																								
2190																								
17883																								
4359																								
19402																								
20846																								
16873																								
5661																								
20724																								
155																								
13677																								
1451																								
16848																								
547																								
19230																								
16764																								
15156																								

Fig. 8. - Shareholders details with pan card and personal email address is visible

We also found some users personal email address and phone numbers using some social media searchers over Twitter, LinkedIn, Facebook, Telegram, Instagram and by using Google Dorks.

4.4 Missing Security Headers

Security headers and HSTS configuration were missing which could lead to some possible web attacks according to OWASP. Web attacks such as: -

- Cross Site Scripting (XSS),
- Man in the middle attack (MITM),
- Click Jacking,
- Cookie Stealing,
- Session Hijacking,
- Cross Site Request Forgery (CSRF) and
- Server Site Request Forgery (SSRF).

Fig. 10. - Tool names and location

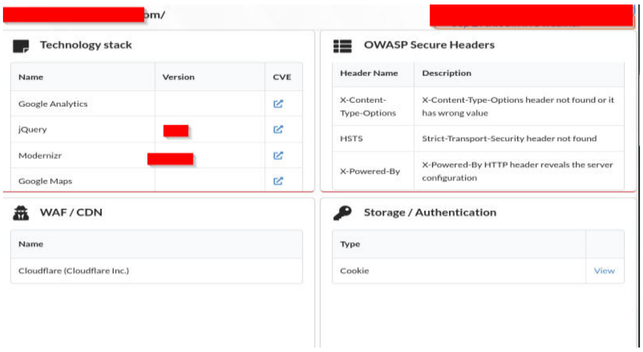
Branch: Visakhapatnam	
FTIR	1
GC-ECD/FPD	1
GC-FID	1
GCMS with Head Space	1
HPLC-FLD with Photochemical reactor	1
ICPMS	1
Ion Chromatograph	1
LCMS	1
Microscope	1
UV-VIS spectrometer	1
UV Inspection Cabinet	1

Branch: Kolkata	
AAS	1
FTIR	1
GC-ECD/FPD	1
GC-FID	1
GCMS with Head space	1
HPLC-FLD with Photochemical ractor	1
Ion Chromatograph	1
LCMS	1
Microscope	1
PCR - RT	1
UV-VIS spectrometer	1
UV Inspection Cabinet	1

Branch: Cochin	
FTIR	1
GC-ECD/FPD	0
GC-FID	1
GCMS with Head Space	1
HPLC-FLD with Photochemical Reactor	1

Branches : Clinical Reference Labs

Branch: Vijayawada	
Advia Centaur CP	1
Beckman Coulter	1
Dimension Xpand Plus	1
D10 Biorad Analyser	1
Celenium Junior	1



[redacted]om/ [redacted]

Technology stack

Name	Version	CVE
Google Analytics		↗
jQuery	[redacted]	↗
Modernizr	[redacted]	↗
Google Maps		↗

OWASP Secure Headers

Header Name	Description
X-Content-Type-Options	X-Content-Type-Options header not found or it has wrong value
HSTS	Strict-Transport-Security header not found
X-Powered-By	X-Powered-By HTTP header reveals the server configuration

WAF / CDN

Name
Cloudflare (Cloudflare Inc.)

Storage / Authentication

Type	
Cookie	View

Fig. 9. - Missing security headers

4.5 Tool names and location

We were also able to get tool names the organizations use and the quantity of the tools and at what branch they are located at.

4.6 RDP (Remote Desktop Protocol)

Port 3389 was open, and it was revealing some system and username information directly on the internet. Any attacker could use this information and run a brute force attack, Dictionary or Rainbow attack. RDP is a user graphical interface used to connect to some other computer via network. Any client with proper credentials can connect to server and get system access allowing him to view files of the server / connected system. [7]

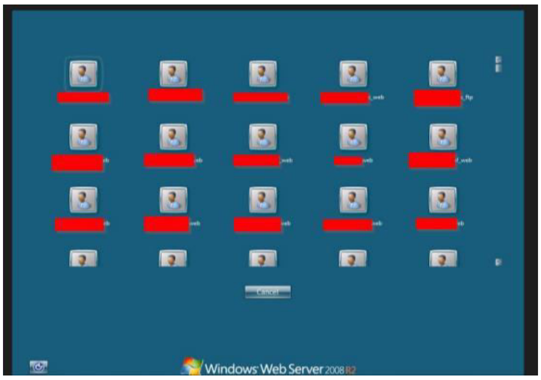
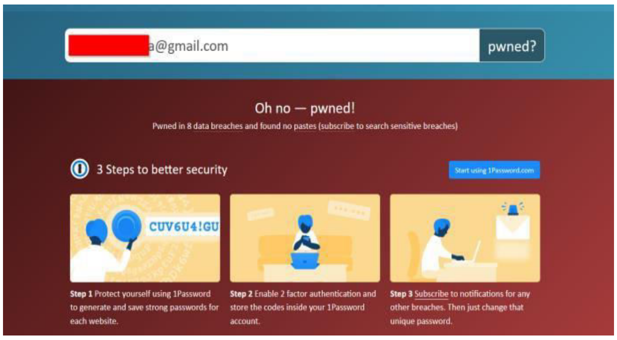

[redacted] [redacted] [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted] [redacted]
Cancel
Windows Web Server 2008 R2

Fig. 11. - RDP access and hostname

4.7 Have I been Pwned?

Using the Personal Identity Information about the users such as their personal email address and phone number, we check on “have I been pwned?”. “Have I been pwned” is large collection of leaked and breached database of multiple organizations. It let us know whether our email address or phone number was leaked in some data breach and guides us how to stay safe from the attackers and share some password tips with us. While investigation some users email address were found in the data breach such as Indiamart, LinkedIn, Ixigo, Zomato, Big Basket, Money Control, Verifications.io, Dominos, MyfitnessPal and some unknown breaches. [8]



[redacted]a@gmail.com pwned?

Oh no — pwned!

Pwned in 8 data breaches and found no pastes (subscribe to search sensitive breaches)

3 Steps to better security

Start using 1Password.com

Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.

Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.

Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

Fig 12 - Have i been pwned information

V. Tools Used – This table contains the list of tools used during the research.

Category	Tools	Purpose
Directory Listing	Dirb [9]	It contains a word list of all the common directories used. It runs a directory search and gvies us the result
	Gobuster [10]	This is the advanced version of dirb
Port scanning	Nmap [11]	This is used to find out

		the open ports, services running and version of the services running, Operating system information and its version.
Unrar files	Winrar [12]	It extracts / unzips the zipped and rar files
To convert .bak file to text file	Strings [13]	It is used to convert our .bak file to text file so we could view the data available inside it
Check headers and requests	Pentest tool kit [14] [15]	This is an alternative to burpsuite. It is a plugin which allows us to check request and response from the website and also allows us to check its security headers.
Reconnaissance	Have I been pawned? [8]	Checks if users email address or phone number were found in any of the data breaches.
	OSINT Framework [16]	Huge collection of OSINT tools
	Maltego [17]	Used for information gathering, usernames, sub domains, dns information
	Google Dorks [18] [19] [20]	It crawls over the internet according to our searched queries and gives us the result
	Shodan [21]	Used to find geo locations of servers, port scanning and open RDP connections
	TheHarvester [22]	Used to get username and email address of the employees and other relevant information
	Censys [23]	Used to find geo locations of servers, port scanning and open RDP connections

VI. POSSIBLE ATTACK ANALYSIS FROM KEY FINDINGS

From our key findings we hypothesize the possible attacks on the organizations by the attackers.

Man-in-the-middle attack is possible as website operates HTTP and not HTTPS. It should use Hypertext Transfer Protocol Secure (HTTPS). The firm is likely to be vulnerable to MITM attacks as the attacker could sniff user credentials or other critical information via wireless nodes or while data is in transit.

Data Breach is possible as we have all the information of the database with its username and passwords. Possibly connection to the database from the .bak file could lead to data breach for the enterprise.

Phishing attacks and Spear-Phishing were possible as we have personal email id's of the employees. Adversary could send a phishing email to the employees and try to gain some more valuable information about the firm or employee that could help him to plan his attack accordingly.

- Smishing and Vishing attacks are also possible as we have the phone numbers or the users and their residential address.
- Brute Force attack is possible as there is no strong password policy for the organization. Any attacker could run a word list and try to brute force to get into the system and gain access of the system.
- SSL stripping is possible because HSTS was not enabled.

HSTS is HTTP strict transport security which forces websites to work on https instead to http. If HSTS is not enabled any attacker could use SSL Strip technique and force websites to work on HTTP. [24]

- DDOS attack is possible because it is vulnerable to IIS

7.5 (CVE-2010-1899) via a crafted request, related to asp.dll, aka "IIS Repeated Parameter Request Denial of Service Vulnerability." [25]

- Buffer overflow in Microsoft Internet Information Services (IIS) 7.5, when FastCGI is enabled, allows remote attackers to exploit arbitrary code via crafted headers in a request, aka "Request Header Buffer Overflow Vulnerability." CVE-2010-2730 [26]
- Cross Site Scripting attack is possible because in security headers "**Content-Security-Policy: default-src 'self**" and "**X-XSS-Protection: 1; mode=block"** is missing. Attacker could use XSS attack to steal cookies which could lead to session hijacking attack or defamation of the website which could lead to trust and reputational loss. [27] [28]
- Click Jacking attack is possible because **X-frame options** value with sameorigin is not set. Clickjacking or Click Hijacking usually occurs when a user clicks on a web page element which is disguised as another element. [29]

VII. CONCLUSION

Cyber-attacks are always going to grow in India. Private sector as well as Government must stay alert and prepared for cyber-attacks. India is a leading and developing country in the world, hence, it has many enemies to target it. Also, the more world will accept digitalization and the more companies get dependent on automation / artificial intelligence the more cyber-attacks are possible. Attackers always come up with some new and creative type of attack, which makes users victim. Organizations much give awareness trainings to employees and must run phishing campaign into their firm. Organizations should also give training for employees about things to post and not to post on social media. India also needs a strong privacy policy which every organization should follow to mitigate and make it difficult for attackers to target into their organizations. Attacks on Infrastructure Control System / SCADA could lead to explosives, bio war or terrorism.

REFERENCES

1. Cyber-attacks on India - https://www.csoonline.com/article/3541148/the-biggest- data-breaches-in-india.html
2. Baby died due to ransomware attack - https://www.nbcnews.com/news/baby-died-due-ransomware-attack-hospital-suit-claims-rcna2465
3. Types of OSINT https://www.varonis.com/blog/what- is-osint
4. OSINT life cycle https://ntrepidcorp.com/case-studies/breaking-down-the-osint-cycle/
5. Kanta, Aikaterini; Coisel, Iwen; Scanlon, Mark, Smarter Password Guessing Techniques Leveraging Contextual Information and OSINT, *Enrico Fermi 2749, 21027 Ispra (VA), Italy*
6. Cartagena, A., Rimmer, G., van Dalsen, T., Watkins, L., Robinson, W. H., & Rubin, A. Privacy Violating Opensource Intelligence Threat Evaluation Framework: A Security Assessment Framework for Critical Infrastructure Owners. *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*
7. Understanding RDP - https://www.cloudflare.com/en- in/learning/access-management/what-is-the-remote- desktop-protocol/
8. Have I been Pwned - https://haveibeenpwned.com/
9. Dirb Tool - https://www.kali.org/tools/dirb/
10. Gobuster - https://github.com/OJ/gobuster
11. Nmap - https://nmap.org/
12. WinRAR - https://www.win-rar.com/start.html?&L=0
13. Strings - https://www.howtogeek.com/427805/how-to- use-the-strings-command-on-linux/
14. Penetration tool kit - https://addons.mozilla.org/en-US/firefox/addon/penetration-testing-kit/

15. Penetration tool kit https://github.com/DenisPodgurskii/pentestkit
16. Accessed OSINT Framework on October 2021 https://osintframework.com/
17. Accessed Maltego on October 2021 - https://www.maltego.com/
18. How to use Google Dorks - https://www.exploit-db.com/google-hacking-database
19. How to use Google Dorks -https://www.exploit-db.com/google-hacking-database
20. How to use Google Dorks - https://securitytrails.com/blog/google-hacking- techniques
21. Accessed Shodan on October 2021- https://www.shodan.io
22. Accessed the Harvester on October 2021 - https://github.com/laramies/theHarvester
23. Accessed censys on October 2021 https://censys.io/
24. Understanding HTTP Strict Transport Security - https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
25. Accessed cve details on October 2021 https://www.cvedetails.com/cve/CVE-2010-1899/
26. Accessed cve details on October 2021 https://www.cvedetails.com/cve/CVE-2010-2730/
27. Understanding security headers - https://www.netsparker.com/blog/web-security/http-security-headers/
28. Understanding security headers https://geekflare.com/http-header-implementation/
29. Understanding click jacking - https://auth0.com/blog/preventing-clickjacking-attacks/