PRESENTATION OF DATA EXHALATION USING JIRA TOOL

A REPORT

Submitted by

Sai Vardhan Reddy

[RA2111030010186]

Under the Guidance of

Dr. D. Deepika

Assistant Professor, Department of Networking and Communications

In partial satisfaction of the requirements for the degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE ENGINEERING

with specialization in CYBER SECURITY

SCHOOL OF COMPUTING

COLLEGE OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR – 603203

MAY 2024

COLLEGE OF ENGINEERING & TECHNOLOGY
SRM INSTITUTE OF SCIENCE & TECHNOLOGY
S.R.M. NAGAR, KATTANKULATHUR – 603203

BONAFIDE CERTIFICATE

Certified that this project report **"PRESENTATION OF DATA EXHALATION USING JIRA TOOL"**is the bonafide work of **"SAI VARDHAN REDDY"**of III Year/VI Sem B. Tech (CSE) who carried out the mini project work under my supervision for the course 18CSE386T PENETRATION TESTING AND VULNERABILITY ASSESSMENT in SRM Institute of Science and Technology during the academic year 2023-2024(Even sem).

SIGNATURE
Dr. D. Deepika
Assistant Professor
Networking and Communications

SIGNATURE
Dr. Annapurani Panaiyappan K
Professor and Head
Networking and Communications

CASE STUDY ON "**PRESENTATION OF DATA EXHALATION USING JIRA TOOL**"

EVEN Semester (2023-2024)

Course Code & Course Name: 18CSE386T – Penetration Testing and Vulnerability Assessment

Year & Semester : III/VI

Report Title : The Presentation od data exhalation using jira tool

Course Faculty : Dr. D. Deepika

Student Name : Sai Vardhan Reddy[RA2111030010186]

Evaluation:

S. No	Parameter	Marks
1	**Problem Investigation & Methodology Used**	
2	**Tool used for investigation**	
3	**Demo of investigation**	
4	**Uploaded in GitHub**	
5	**Viva**	
6	**Report**	
	Total	

Date:

Staff Name:

Signature:

TABLE OF CONTENTS

INTRODUCTION

Data collection sale was started on 4th December 2023 containing more than 200 million Twitter profiles. The breached data was released as a 59 GB RAR archive. The vulnerable API was compromised by the scrapers using earlier data collections. •Twitter users should be aware of targeted phishing scam campaigns.

On 4th December 2023, on the hacking forum, a threat actor sold a data collection containing more than 200 million Twitter profiles for hacker forums eight credits, which were worth almost $2.These profiles included both private phone numbers and email addresses, usernames, screen names, following counts, account creation dates as well as public data.On numerous online hacker forums and marketplaces dedicated to cybercrime, threat actors have been selling and disseminating large data collections of scraped Twitter user profiles since 22nd July 2022.

The breached data have been released as a 59 GB RAR archive including six text files.Specific customer information may or may not be in this data collection, depending on whether or not the email address was revealed in prior data breaches.In addition, this disclosure raises serious privacy concerns, particularly for anonymous Twitter users.

It might be feasible to identify anonymous Twitter users using this leak and reveal their true identities, which can put at risk many dissidents, journalists, activists, and similar users around the world.These data collections were produced in 2021 by exploiting a vulnerability in the Twitter API that let users enter

email addresses and phone numbers to check whether they were linked to a Twitter ID.In this data breach, threat actors merged available public data with private email addresses and phone numbers to develop profiles of Twitter users by using another Twitter API to scrape the public Twitter data for the IDs.

Reuters could not independently verify if the data on the forum was authentic and came from Twitter. Screenshots of the hacker forum, where the data appeared on Wednesday, have circulated online.Troy Hunt, creator of the breach notification site Have I Been Pwned, viewed the leaked data and said on Twitter that it seemed “pretty much what it’s been described as”.

There were no clues to the identity or location of the hacker or hackers behind the breach. It may have taken place as early as 2021, which was before Elon Musk took over ownership of the company last year.Claims about the size and scope of the breach initially varied with early accounts in December saying 400m email addresses and phone numbers were stolen.

SCOPE

If the data of more than 200 million Twitter users were leaked, it would represent a significant data breach with potentially far-reaching consequences. Here are some potential aspects to consider regarding the scope and implications of such a breach:

1. Personal Information Exposure: The leaked data could include various personal information about Twitter users, such as usernames, email addresses, phone numbers, birthdates, and potentially even passwords or password hashes. This information could be exploited by cybercriminals for identity theft, phishing attacks, account takeover, or other malicious activities.

2. Priracy Concerns: The exposure of personal information raises significant privacy concerns for affected Twitter users. Many individuals use Twitter to share thoughts, opinions, and personal experiences, and a breach of their data could result in their private information being exposed to the public or used for nefarious purposes without their consent.

3. Reputation Damage: A data breach of this magnitude could damage Twitter's reputation as a trusted platform for communication and social networking. Users may lose trust in Twitter's ability to protect their data, leading to decreased user engagement, loss of advertising revenue, and potential legal repercussions.

4. Regulatory Compliance: Depending on the jurisdiction and the nature of the leaked data, Twitter could face regulatory investigations and potential fines for non-compliance with data protection laws and regulations, such as the General Data

Protection Regulation (GDPR) in the European Union or the California Consumer Privacy Act (CCPA) in the United States.

5. Security Implications: The data breach may indicate weaknesses or vulnerabilities in Twitter's security infrastructure and practices. Twitter would need to conduct a thorough investigation to determine the cause of the breach, remediate any security flaws, and implement additional security measures to prevent future incidents.

6. Impact on Trust and Confidence: The breach could erode trust and confidence not only in Twitter but also in other social media platforms and online services that handle user data. Users may become more cautious about sharing personal information online and may demand greater transparency and accountability from companies regarding data protection practices.

7. Legal and Financial Consequences: Twitter could face lawsuits from affected users, shareholders, or regulatory authorities seeking damages for the breach.

OBJECTIVE

1. Monetary Gain: The primary objective for leaking the data could be financial profit. The perpetrators may intend to sell the stolen user data on the dark web or to other cybercriminals, who could then use it for various malicious purposes, such as identity theft, fraud, or phishing scams.

2. Espionage or Intelligence Gathering: State-sponsored actors or intelligence agencies may seek to gather intelligence or monitor the activities of specific individuals or groups by accessing their Twitter accounts and associated personal information. This could be part of broader espionage efforts or surveillance activities.

3. Political Motivations: Hacktivist groups or individuals with political agendas may leak Twitter user data as a form of protest, activism, or to expose perceived injustices or wrongdoing. The leaked data could be used to embarrass individuals or organizations, disrupt online communications, or influence public opinion.

4. Revenge or Retaliation: In some cases, data breaches may be motivated by personal vendettas or grievances against specific individuals, organizations, or entities. Perpetrators may leak sensitive user data as a form of revenge or retaliation for perceived slights or injustices.

5. Cyber Warfare or Sabotage: Nation-states or malicious actors with geopolitical motives may conduct cyberattacks aimed at destabilizing or disrupting social media platforms like Twitter. Leaking user data could be part of a broader strategy to

undermine public trust, sow discord, or inflict economic harm on targeted countries or organizations.

6. Demonstration of Skill or Notoriety: Some hackers may leak large amounts of user data simply to demonstrate their hacking skills, gain notoriety within the hacking community, or to challenge the security measures of high-profile organizations like Twitter. These types of breaches are often driven by ego or a desire for recognition.

7. Insider Threats or Malicious Insider Actions: In some cases, data breaches may be the result of insider threats or malicious actions by employees or contractors with access to sensitive systems or data. These individuals may leak user data for personal gain, retaliation, or to facilitate external attacks.

Overall, the objective of leaking the data of more than 200 million Twitter users is likely to be driven by a combination of factors, including financial motives, ideological beliefs, geopolitical considerations, personal vendettas, and a desire for notoriety or recognition within the hacking community.

TOOL DESCRIPTION

Tool: JIRA

JIRA is a widely-used project management and issue tracking software developed by Atlassian. It's commonly used by software development teams, IT departments, and various other teams to plan, track, and manage their work.

Feature's Of Jira:

1. Issue Tracking: JIRA allows users to create, track, and prioritize different types of issues or tasks within a project. These issues can include bugs, new feature requests, improvements, and other work items.

2. Customizable Workflows: JIRA offers customizable workflows that allow teams to define the stages and transitions that issues go through during their lifecycle. Workflows can be tailored to match specific project requirements and team processes.

3. Scrum and Kanban Boards: JIRA provides agile project management capabilities through Scrum and Kanban boards. Scrum boards facilitate sprint planning, backlog management, and progress tracking, while Kanban boards visualize work in progress and enable continuous delivery.

4. Dashboards and Reporting: JIRA offers customizable dashboards that allow users to create and share visualizations of project metrics, progress, and status updates. Built-in reports provide insights into team performance, issue trends, and project health.

5. Integration with Development Tools: JIRA integrates seamlessly with various development tools and services, including version control systems (e.g., Git, SVN), continuous integration servers, and build automation tools. This integration enables real-time visibility into code changes, builds, and deployments**.**

6. Extensibility and Add-ons: JIRA's flexibility is enhanced by its extensive marketplace of add-ons and integrations. Users can extend JIRA's functionality with plugins and add-ons for specific use cases, such as test management, time tracking, and customer support.

7. User Permissions and Security: JIRA provides robust user management capabilities, allowing administrators to define user roles, permissions, and access controls at the project and issue level. This helps enforce security policies and ensure data privacy.

Plan, Track and Work Faster

JIRA is a bug-tracking tool mainly used to track, organize, and prioritize the bugs, newly added features, improvements for certain software releases. Projects are subdivided into issues and issues can be of multiple types such as bug, new feature, improvement, and documentation tasks.

When the release date of software comes near, then software developers need to focus on the remaining issues which are to be fixed before the specified date. It also becomes difficult for

the QA to maintain the status of the documentation, i.e., sometimes it becomes hard to keep track of everything.

JIRA is a good choice for handling the above issues. It enables software developers to track issues and improvements. It manages the projects as well as maintain the technical documentation.

The main source of information:

JIRA is the primary source of information for the next software release. On JIRA, the whole team of the software developers can plan for the new features which are to be added and bugs to be fixed in the next release.

It also helps the QA team in writing the technical documentation. Through JIRA, the QA team can check the status of each feature that is newly added by the software developers, and according to that, they can plan how to document for the new version.

Overall, JIRA is a powerful and versatile tool for managing projects, tracking issues, and facilitating collaboration among teams.

TOOL INSTALLATION PROCEDURE

Installing Jira, a popular project management and issue tracking tool developed by Atlassian, involves several steps. Here's a general guide to installing Jira:

1. Check System Requirements: Before beginning the installation process, review the system requirements for the version of Jira you plan to install. Ensure that your server meets these requirements in terms of hardware, operating system, Java version, and other dependencies.

2. Download Jira: Visit the Atlassian website or the official Jira download page to obtain the installation files for the desired version of Jira. You may have the option to download a standalone installer, a WAR (Web Application Archive) file, or a Docker image, depending on your preferences and deployment environment.

3. Choose Deployment Option: Decide on the deployment option that best suits your needs. You can choose to install Jira on-premises, in the cloud using Atlassian's hosted service (Jira Cloud), or in a self-managed environment using Atlassian's Data Center deployment option.

4. Prepare Database: Set up a compatible database for Jira to use. Jira supports various databases, including PostgreSQL, MySQL, Oracle, and Microsoft SQL Server. Follow the instructions provided by Atlassian to create a new database instance and configure it for use with Jira.

5. Install Java Development Kit (JDK): Jira requires Java to run. Install the appropriate version of the Java Development Kit (JDK) on your server if it's not already installed. Ensure that you're using a supported version of Java according to Atlassian's documentation.

6. Run the Installer: If you downloaded a standalone installer for Jira, execute the installer file to begin the installation process. Follow the on-screen prompts to specify installation options, such as installation directory, ports, and database connection settings.

7. Configure Jira: After the installation is complete, access the Jira setup wizard via your web browser. Follow the prompts to configure basic settings for your Jira instance, such as application title, base URL, and administrator account details.

8. Database Configuration: Provide the necessary information to connect Jira to the database you prepared earlier. This typically includes the database type, hostname, port, database name, username, and password.

TOOL IMPLEMENTATION PROCEDURE

1. Download JIRA:

wget <download_url>

2. Make Installer Executable:

chmod a+x <installer_file>

3. Run the Installer:

sudo ./<installer_file>

4. Follow Installation Wizard:

sudo <jira_installation_directory>/bin/start-jira.sh

5. Access JIRA:

http://localhost:8080 or http://<server_ip>:8080

Steps of Ethical Hackin that you have done on your applications using Jira tool

Jira is not a tool specifically designed for hacking or exploiting vulnerabilities in external systems like Twitter. Instead, Jira is primarily a project management and issue tracking tool developed by Atlassian. However, ethical hackers or security professionals may use Jira as part of their toolkit for managing and tracking security-related tasks, such as:

1. Vulnerability Management: Use Jira to track and manage vulnerabilities identified during security assessments or penetration tests. Create issues for each vulnerability, assign them to appropriate team members, and track the progress of remediation efforts.

2. Incident Response: Utilize Jira to facilitate incident response activities in the event of a security incident involving Twitter accounts or other systems. Create incident tickets, document incident details, and coordinate response actions among team members.

3. Security Audits and Assessments: Use Jira to plan, execute, and track security audits and assessments of Twitter account management processes, access controls, authentication mechanisms, and other security-related aspects. Document findings, recommendations, and action items for remediation.

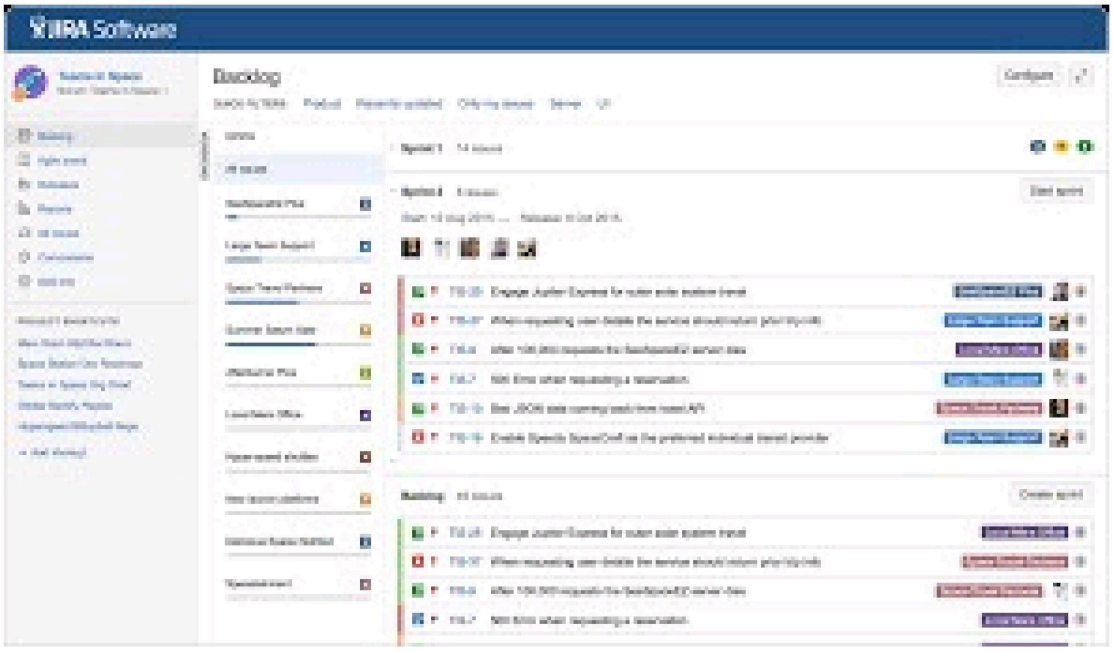
4. Security Policy Enforcement: Use Jira to track compliance with security policies, standards, and regulations related to Twitter account management and data protection. Create tasks for policy reviews, compliance audits, and enforcement actions as needed.

5. Training and Awareness: Use Jira to manage security training and awareness initiatives aimed at educating users about best practices for securing Twitter accounts, identifying phishing attempts, and protecting sensitive information.

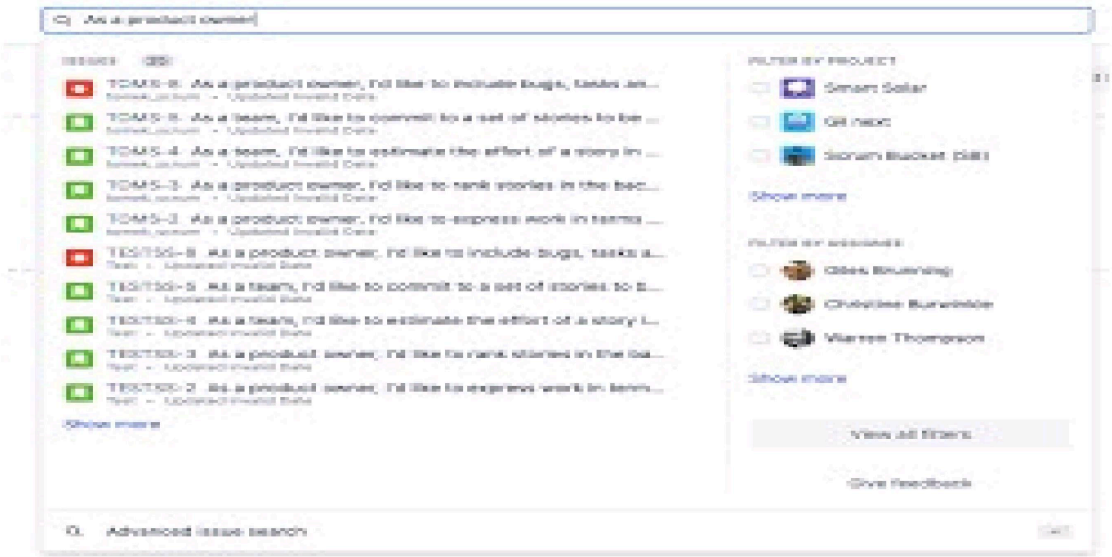
While Jira itself is not a hacking tool, it can be used as part of a comprehensive security program to organize and manage security-related activities, including those related to securing Twitter accounts. However, any ethical hacking activities involving Twitter or other systems should be conducted responsibly, with proper authorization, and in compliance with relevant laws and ethical guidelines. Additionally, it's important to obtain permission from the organization or individuals responsible for the Twitter accounts before conducting any security testing or assessments.

IMPLEMENTATION

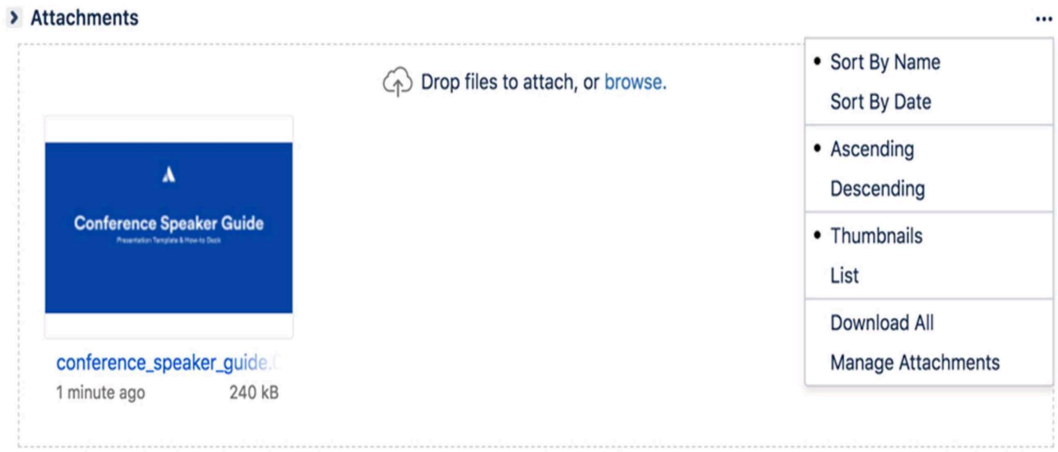
Screenshots:



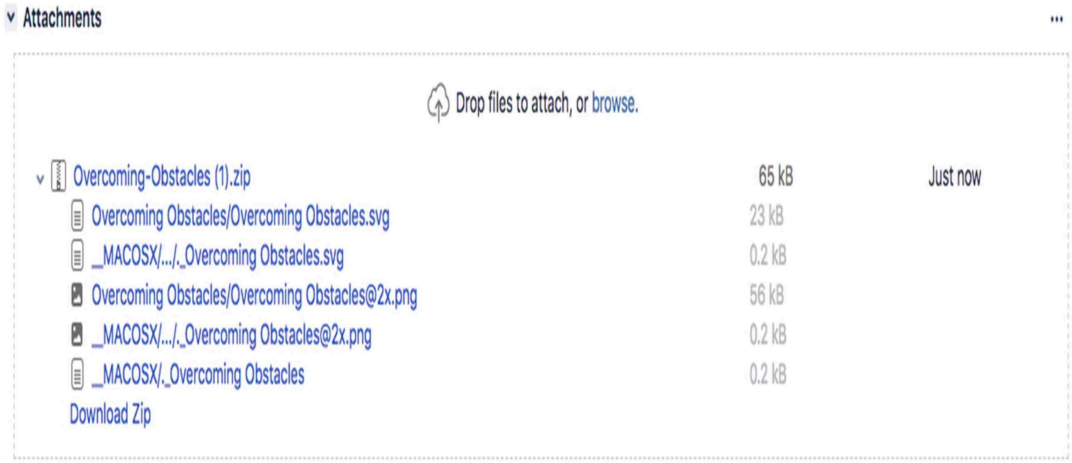
Plan, Track, Work



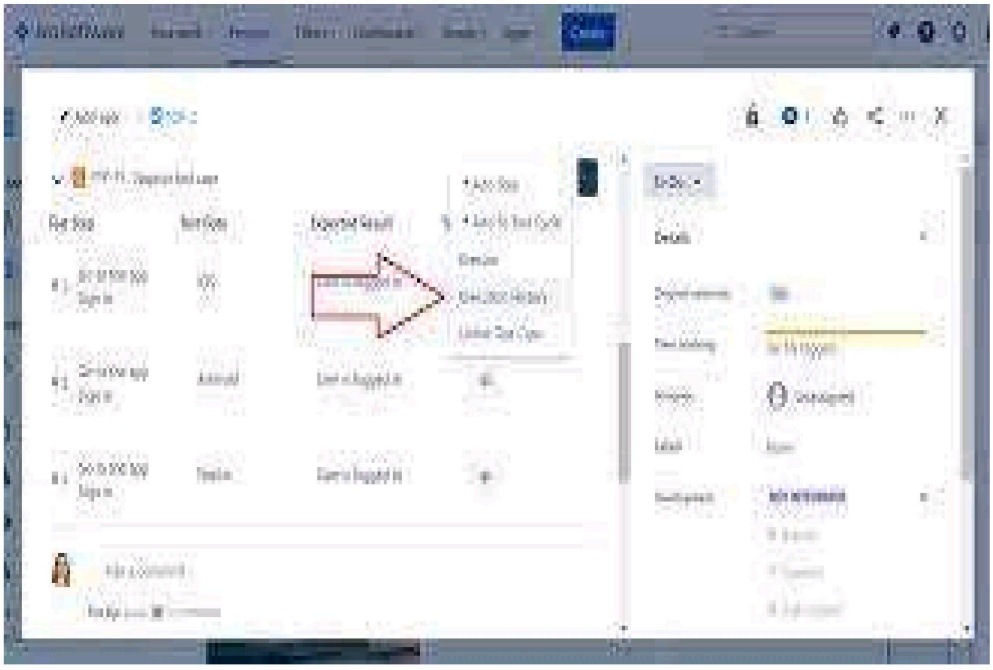
Service Management Cloud



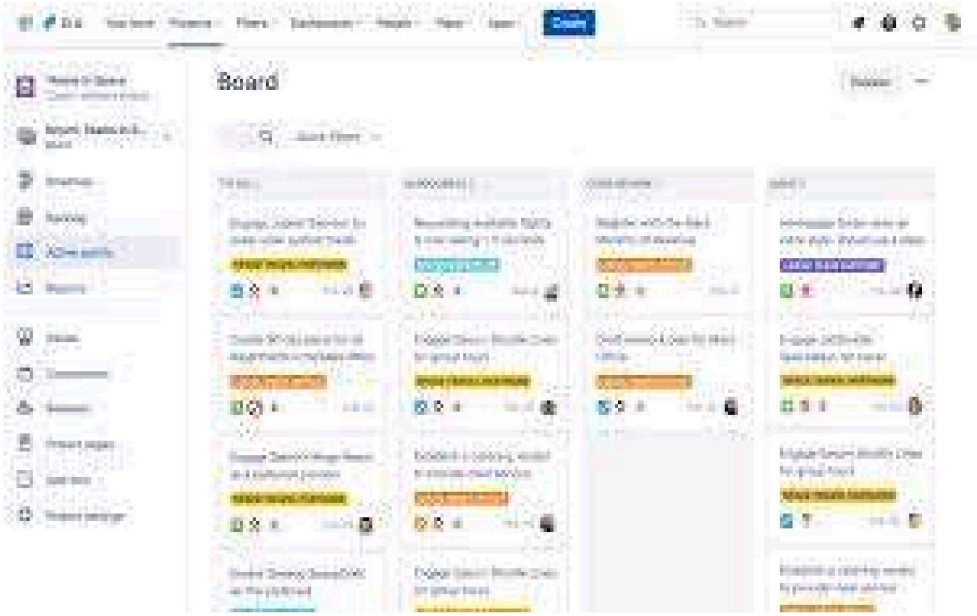
Manage the attachments



Access zip file contents



Test Cases



Integrate Jira Cloud

CONCLUSION

Twitter has refuted claims that the 200 million user emails and passwords leaked earlier this month were obtained through an exploit of its security systems. The social media giant said it had conducted a “comprehensive investigation” following reports that a dataset containing the account details of its users had been posted online, but failed to find any evidence of a vulnerability in its systems being the source of the leak.The personal details found in the 200-million-email dataset, it wrote “were found to be the same as those exposed in August 2022” and “could not be correlated with the previously reported incident or any data originating from an exploitation of Twitter systems.”

References

https://www.fox5dc.com/news/nearly-300-million-email-addresses-leaked-in-recent-twitter-data-hack

https://www.forbesindia.com/article/crypto-made-easy/multiple-indian-twitter-accounts-hacked-nft-content-posted/75265/1

https://www.atlassian.com/software/jira