

[Open in app](#)[Get started](#)

GrimTheRipper

[Follow](#)

May 27 · 2 min read · [Listen](#)



Save



# [CVE-2022-32061] Snipe-IT Version v6.0.2 — Malicious File Upload

## Description

# An Issue is discovered in Snipe-IT Version v6.0.2.

# This exploit allows you to upload malicious files on server.

# We found malicious file upload when we upload file at the People menu.

## Payload Attack



1





Normal text file	length: 6,310 lines: 112	Ln: 10 Col: 10 Pos: 800	Unix (LF)	ANSI	INS
------------------	--------------------------	-------------------------	-----------	------	-----


First, we login to the target application with admin privileges.



Open in app

Get started

<h1>test</h1>

 Username

sa

 Password

.....

☐ Remember Me

Login

[I forgot my password](#)

Then select People Menu and select User.





Open in app

Get started

Assets

Licenses

Accessories

Consumables

Components

Predefined Kits

**People**

Import

Settings

Reports

Requestable

Current Users

Export Show Deleted Users Create New

Bulk Checkin & Delete Go Search

Showing 1 to 5 of 5 rows

<input type="checkbox"/>	Name	Title	Email	Phone	Username
<input type="checkbox"/>	AgentMeoww Eiei	Meowwx2	mooslice003@gmail.com		agentmeoww
<input type="checkbox"/>	Jane Smith		you@example.com		admin
<input type="checkbox"/>	sa				sa
<input type="checkbox"/>	tester<h1>hello</h1> sosecure<h1>hello</h1>	<h1>hello</h1>	tester.sc@gmail.com	123	tester
<input type="checkbox"/>	user lowPriv		user@gmail.com		user

Showing 1 to 5 of 5 rows

after that click Upload.

Snipe-IT Asset Management

Dashboard

Assets

Licenses

Accessories

Consumables

Components

Predefined Kits

**People**

Import

Settings

Reports

Requestable

View User sa

Info Assets Licenses Accessories Consumables File Uploads History Managed Locations

Upload Actions

Name sa

Username sa

Groups --

Last Login 2022-05-27 09:25 AM

Created at 2022-05-27 09:22 AM

Remote No

Login Enabled Yes

LDAP No

2FA Active No

2FA Device Enrolled No

superadmin

Edit User

Clone User

Print All Assigned

Delete

Checkin & Delete User



Open in app

Get started

Select File...

infected.pdf (6.16 KB)

✓ Allowed filetypes are png, gif, jpg, jpeg, doc, docx, pdf, xls, xlsx, txt, lic, xml, zip, rtf and rar. Max upload size allowed is 2M.

Notes (Optional)

Cancel

Upload

then select File Uploads Tab it will show malicious files

View User sa

✓ Success: File(s) successfully uploaded.

Info Assets Licenses Accessories Consumables **File Uploads 1** History Managed Locations

Upload Actions

Search

Showing 1 to 1 of 1 rows

File Type	Image	File	File Size	Notes	Download	Created at	Actions
		user-6-hSPmV26O-infected.pdf	6.16 KB			2022-05-27 09:28:58	

Showing 1 to 1 of 1 rows

if someone try to download and open it the payload will be excuted.





Open in app

Get started

We found the XSS!

**Author**

Grim The Ripper Team by SOSECURE Thailand

[About](#) [Help](#) [Terms](#) [Privacy](#)

Get the Medium app

