

Local File Inclusion			Severity: <b>High</b>
CVSS v3.1	7.7	Vector	AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N
Privileges	SAS Developer		
Version	SAS 9.4 for predictive performance management extension		

Local file inclusion (LFI) is a vulnerability which allows an attacker to include files that are locally stored on the server. This kind of vulnerability allows the attacker to obtain access to information which may lead to more severe type of attacks up to a full server compromise.

This is achieved by exploiting a dynamic file inclusion mechanism which is not correctly implemented on the application. This allows the attacker to manipulate the input in order to access files which should not be visible.

The vulnerable resource:

- <https://<application-baseurl>/SASStudio/sasexec/sessions/9f121b79-9148-4b47-bcc6-8afc845847ba/workspace/~~ds~~etc/passwd>

### Follow the steps below to replicate the results

The target application allows for file download. An attacker can manipulate the file path to download in order to include other files present on the target filesystem.

Below, an example of including the `/etc/passwd` file.

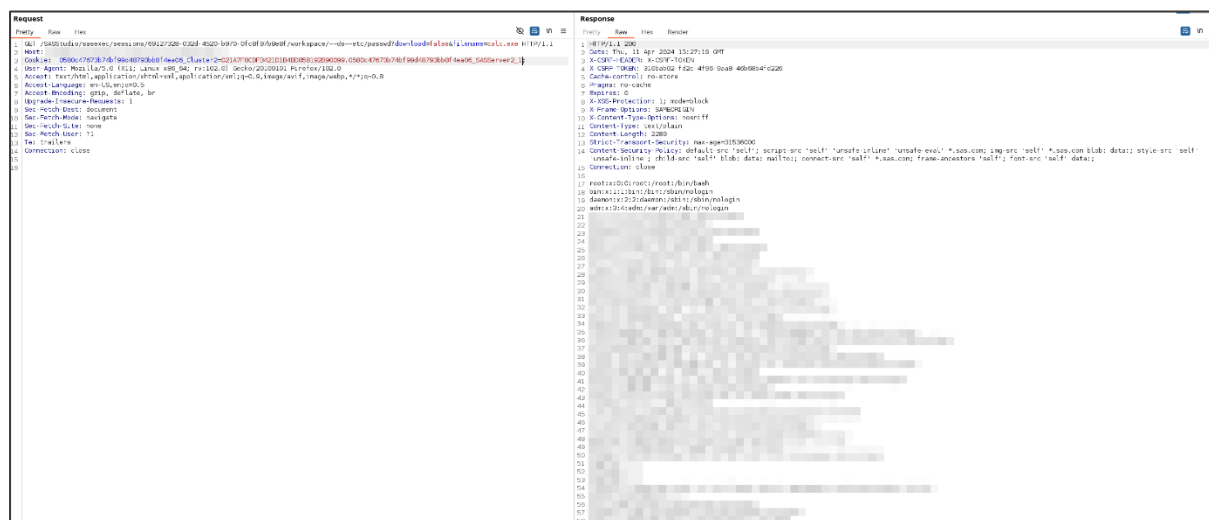


Figure 1: `/etc/passwd` file inclusion.

This vulnerability also allows for directory listing which grants the attacker valuable information to enumerate files which can then be downloaded.

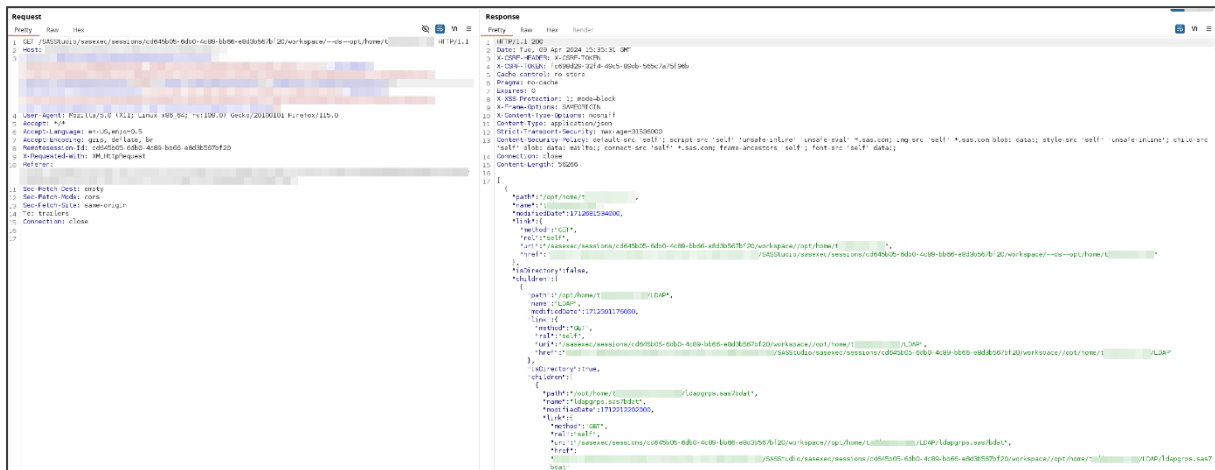


Figure 2: Directory listing for /opt/home/<user>.

By combining the directory listing with the local file inclusion, it is possible to easily download the entire directories with their content.

In this example, a python script has been developed in order to download the content of the /opt/home/<user> directory.

\$sys.config.lev.web.appserverlogs.dir)	1 item Folder	Thu 11 Apr 2024 10:59:08 AM CEST
SASWebReportStudio4.4.log	10.8 kB Application log	Thu 11 Apr 2024 10:59:08 AM CEST
ApacheDirectoryStudio	4 items Folder	Thu 11 Apr 2024 10:52:55 AM CEST
Cert_...	3 items Folder	Thu 11 Apr 2024 10:59:11 AM CEST
intermediate.crt	2.1 kB X.509 Certificate	Thu 11 Apr 2024 10:59:10 AM CEST
root.crt	1.4 kB X.509 Certificate	Thu 11 Apr 2024 10:59:10 AM CEST
server.crt	2.5 kB X.509 Certificate	Thu 11 Apr 2024 10:59:11 AM CEST
LDAP-SYNC	0 items Folder	Thu 11 Apr 2024 10:52:55 AM CEST
SAS	1 item Folder	Thu 11 Apr 2024 10:52:46 AM CEST
SAS_...	0 items Folder	Thu 11 Apr 2024 10:59:03 AM CEST
...	3 items Folder	Thu 11 Apr 2024 10:59:02 AM CEST
profbak.sas7bcat	20.5 kB Unknown	Thu 11 Apr 2024 10:59:03 AM CEST
profile.sas7bcat	20.5 kB Unknown	Thu 11 Apr 2024 10:59:02 AM CEST
registry.sas7bitm	32.8 kB Unknown	Thu 11 Apr 2024 10:59:01 AM CEST
ApacheDirectoryStudio-2.0.0.v20210717-M17-linux.gtk.x86_64.tar.gz_133.63MB.sh	993 bytes Shell script	Thu 11 Apr 2024 10:52:55 AM CEST
jduck.jpg	13.5 kB JPEG image	Thu 11 Apr 2024 10:59:16 AM CEST
jconn4.jar_2.02MB.sh	883 bytes Shell script	Thu 11 Apr 2024 10:58:59 AM CEST
...	980.2 kB RPM package	Thu 11 Apr 2024 10:59:15 AM CEST
plan.xml	468.8 kB XML document	Thu 11 Apr 2024 10:59:00 AM CEST
report_depotcheck.txt	1.2 kB Plain text document	Thu 11 Apr 2024 10:59:07 AM CEST
Rules-Maintainer-Group.ldif	250 bytes LDIF address book	Thu 11 Apr 2024 10:59:06 AM CEST
T_...ldif	951 bytes LDIF address book	Thu 11 Apr 2024 10:59:09 AM CEST
Vigilanesi.ldif	1.0 kB LDIF address book	Thu 11 Apr 2024 10:59:12 AM CEST

Figure 3: Downloaded content for the directory /opt/home/<user>.

## REMEDIATION:

In order to prevent Local File Inclusion, it is advisable to:

- If you need dynamic path concatenation, ensure you only accept required characters such as "a-Z0-9" and do not allow ".." or "/" or "%00" (null byte) or any other similar unexpected characters.
- Allow inclusion only from a directory and directories below it. This ensures that any potential attack cannot perform a directory traversal attack.
- Ensure the user cannot supply all parts of the path – surround it with your path code.

For further information, please refer to:

- [https://owasp.org/www-community/attacks/Path\\_Traversal](https://owasp.org/www-community/attacks/Path_Traversal)