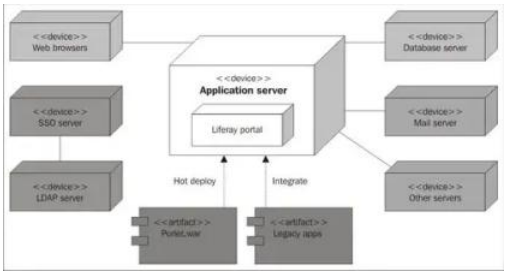
TPDanh Follow
Nov 15, 2020 · 3 min read · Listen

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 Vulnerabilitiess

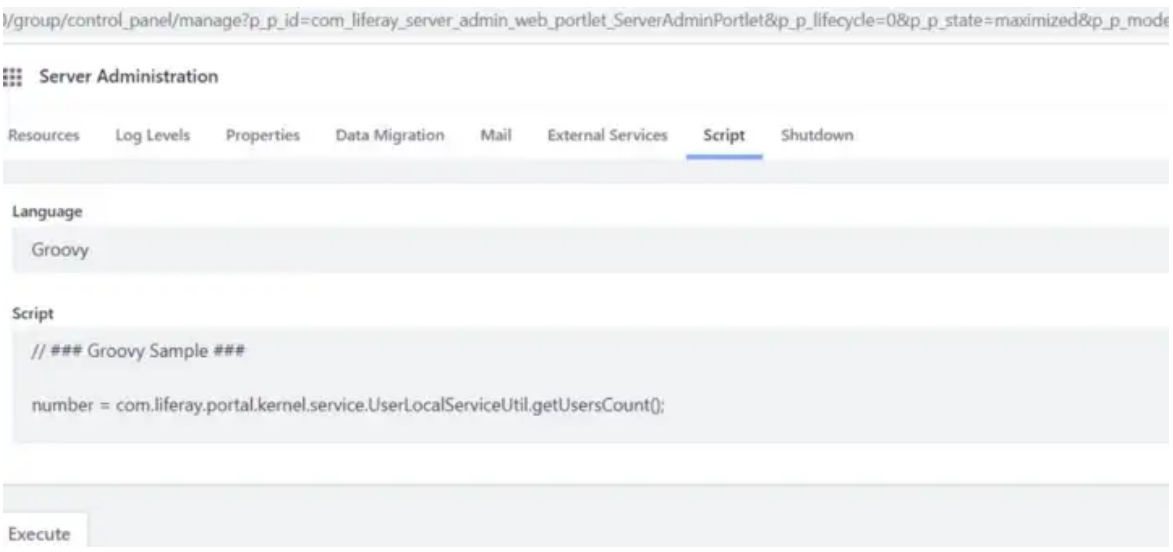
When try to exploit the target (Liferay Portal Server), I found that I can access with admin privilage with default account **test@liferay.com/test**(critical bug). With admin privilage, I can do many thing but my purpose is Remote Code Execution (RCE) the target. That's why I found 2 way to execute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

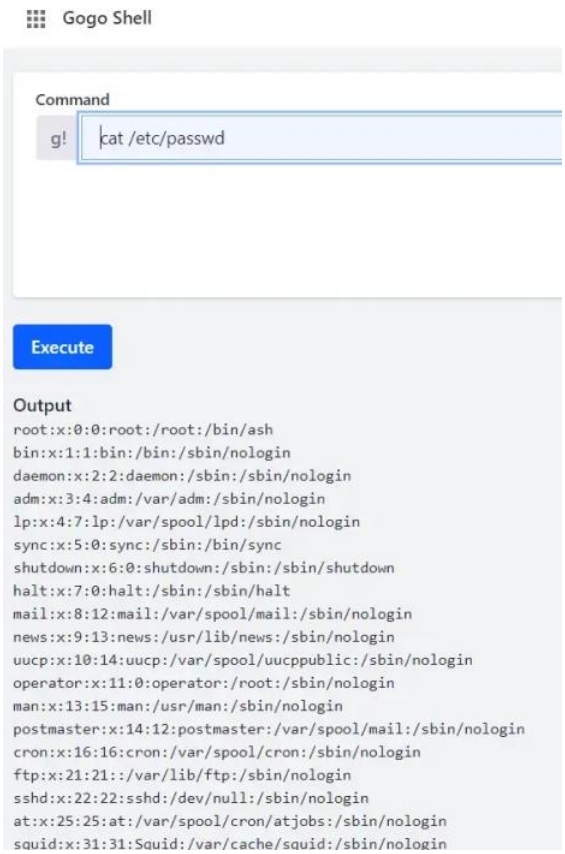
The script get the command, execute it on the server and get standard output, standard error then print to browser.

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*

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.



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 suppoting me to find out these vulneratbilities.

Liferay Rce Exploit